



**RESEARCH TOPIC: ANALYSIS OF CYBERCRIME LAWS AND RISING DIGITAL
FRAUD IN INDIA**

***AUTHORS: RIMISSHA UDENIA, DEVALIDHA S., SUDARSHANA PATOWARY,
SUSHANT KAUSHIK, DEBARATI SENGUPTA, VANSHIKA TYAGI, NANDINI
SHARMA, ARUNA TANIKELLA, SHREYA BASENE, SHRUTI MISHRA***

1. Abstract

In the modern era of technological advancement the rapid expansion of digital payments, online banking and social media in India has lead to many new opportunities for both economic and social interaction, but it has also contributed to the growing patterns of problem of digital fraud. This paper examines India 's legal and institutional response to cybercrime, with the particular attention to financial fraud, identity theft phishing, and digital payment scams It analyses the extent to which existing legal framework particularly the Information Technology Act 2000, along with the recent regulatory and institutional measures that are capable of addressing the changing nature of cyber offences.

This paper argues the challenges that is not merely the absence of cyber laws but also their effective implementation, jurisdictional difficulties, lack of public awareness and the rapid evolution of cyber criminal techniques .

By examining these gaps the study seeks to assess whether India 's current approach is sufficiently responsive to emerging forms of digital frauds and identify areas requiring stronger legal and institutional mechanism

Keywords: Cybercrime Law, Digital fraud, Cybersecurity

2. Introduction

India has undergone a dramatic expansion of digital financial infrastructure over the past decade, driven by the Unified Payments Interface, mobile banking and near universal internet access, a shift that has turned digital fraud from a marginal problem into a mass one. Alongside this growth, fraud itself has become more sophisticated, with scammers now using tools such as AI generated voice cloning, deepfake video and cloned



government portals to exploit the same convenience that makes digital payments popular, [producing financial losses that run into thousands of crores every year.](#) India's legal response has centred on the Information Technology Act, 2000, a statute drafted before smartphones, UPI or generative AI existed, and more recent instruments, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, have attempted to modernise this framework without fully resolving it.

Problem Statement

The literature reviewed for this study shows that the persistence of cybercrime and digital fraud in India cannot be explained by legislative gaps alone. Statutory design, enforcement capacity, technological change and socio-economic exposure each shape whether the law functions in practice, yet existing scholarship has largely examined these four dimensions in isolation from one another. This leaves a specific and unanswered problem: no existing study traces a single, well defined category of fraud through all four dimensions at once, from the adequacy of the statute, through the machinery meant to enforce it, to the technological conditions that enable the fraud and the socio-economic groups who bear its cost. UPI and digital payment fraud, the fastest growing and most consequential category identified in the course of this research, is the category through which this study addresses that problem.

Research Question, Objectives and Scope

Research Question: To what extent do India's legal, enforcement and institutional frameworks address the rising scale and sophistication of digital fraud and cybercrime, and what gaps remain in translating legislation into effective protection?

The specific objectives of this study are, first, to assess whether India's governing statutes, principally the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, substantively cover the fraud typologies associated with UPI and digital payments; second, to trace how far a complaint under this framework actually moves from registration through investigation and prosecution to conviction; third, to examine how technological and market design either enable or restrain this category of fraud; and fourth, to consider how the resulting harm is distributed across different groups in society. The scope of the study is deliberately bounded. It is a qualitative, doctrinal and documentary study,



relying entirely on secondary and publicly available material, statutes, official institutional reports and peer reviewed literature, [read through the four regulatory modalities set out in Lawrence Lessig's account of internet regulation](#). It does not involve primary data collection, and its findings are accordingly interpretive rather than statistically generalizable, a limitation that is returned to in the Discussion chapter.

Structure of the Study

The remainder of this study is organised as follows. **Chapter 2 (Thematic literature review)** reviews the existing literature across four themes, legal gaps and policy weakness, enforcement and law implementation, emerging technology and financial fraud, and socio-economic impact, and identifies the research gap this study addresses. **Chapter 3 (Research Methodology)** sets out the research methodology, explaining why a qualitative, doctrinal and documentary design was adopted and how the material analysed in this study was selected and collected. **Chapter 4 (Data Analysis)** presents the data analysis, reading the assembled material against the four analytical dimensions identified in the methodology. **Chapter 5 (Discussion)** discusses what these findings mean when read against the existing literature, and **Chapter 6 (Conclusion)** concludes by answering the research question directly and setting out this study's contribution and its recommendations for future research.



3. Thematic literature review

Methodology Note

This review adopts a doctrinal and analytical approach, evaluating the “extent” posed in the research question against three indicators drawn from the literature and official data: (i) the substantive adequacy of [statutory provisions \(Information Technology Act 2000, Bharatiya Nyaya Sanhita 2023, Digital Personal Data Protection Act 2023\)](#) against evolving fraud typologies; (ii) the investigation-to-conviction pipeline, measured through registered-case growth, chargesheet, and conviction-rate data (NCRB, RBI, NCRP); and (iii) the socio-economic distribution of the resulting harm.

Theoretical Framework

This review is organised around [Lawrence Lessig’s regulatory framework in Code and Other Laws of Cyberspace \(1999\)](#), which identifies four modalities that jointly regulate behaviour in digital environments: law, social norms, the market, and “code” (technological architecture). Themes 1 and 2 correspond to the “law” modality (design and implementation respectively); Theme 3 corresponds to “code” and market forces; and Theme 4 corresponds to social and economic norms. This framework is what justifies treating the four themes as one integrated system rather than four separate literatures, and it is returned to explicitly in the concluding research-gap statement.

Literature Review Overview

India has undergone a dramatic expansion of digital financial infrastructure over the past decade, driven by the Unified Payments Interface (UPI), mobile banking, and near-universal internet access; this scale has made digital fraud a mass phenomenon rather than a marginal one. Alongside this growth, scammers have adopted increasingly sophisticated tools AI-generated voice cloning, deepfake video, and cloned government portals — that exploit the same convenience that makes digital payments popular, producing financial losses that run into thousands of crores annually. India’s legal response has centred on the Information Technology Act, 2000, a statute drafted before smartphones, UPI or generative AI existed, and more recent instruments — the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023 — have attempted to modernise this framework without fully resolving it. This review asks to what extent India’s legal, enforcement and institutional



response addresses the problem, and organises the inquiry into four interlocking themes: the substantive adequacy of the statutes themselves (Theme 1), the operational capacity to enforce them (Theme 2), the role emerging technology plays in both enabling and containing fraud (Theme 3), and the uneven socio-economic burden the resulting harm imposes (Theme 4).

Theme 1: Legal Gaps and Policy Weakness

Theme 1 isolates gaps in the substantive content of India's cybercrime statutes — provisions that are missing, outdated, or too narrow to capture current fraud methods — independent of how well existing law is enforced, a question reserved for Theme 2. This distinction matters: a statute that does not yet recognise a harm cannot be enforced into recognising it, however well-resourced the police force investigating it.

[Kasturi and Ayub Dar \(2024\)](#) and [Santoshkumar and Wamankar \(2025\)](#) illustrate this from two different angles that converge on the same conclusion. Kasturi and Ayub Dar examine the exposure of children and women to online exploitation and argue that existing privacy protections have not kept pace with the platforms through which this exploitation occurs, concluding that India needs updated legislation, stronger privacy safeguards, and greater digital literacy.

[Santoshkumar and Wamankar](#) reach a structurally similar finding through case studies of the Cosmos Bank cyber heist and the Bulli Bai/Sulli Deals incidents, arguing that outdated legal provisions left institutions unable to anticipate either large-scale transactional fraud or coordinated, socially targeted online harassment. Where the two studies diverge is in their prescribed remedy: Kasturi and Ayub Dar look inward, toward privacy-centred statutory reform, while Santoshkumar and Wamankar look outward, toward institutional models drawn from the United States, United Kingdom and Singapore. This divergence is itself instructive — it suggests the substantive gap in Indian law is not a single missing provision but a structural lag spanning both individual-rights protection and systemic financial-crime coverage, one that the IT Act 2000's core architecture, only partially updated by the Bharatiya Nyaya Sanhita 2023 and the Digital Personal Data Protection Act 2023, was not built to anticipate.



Taken together, these two strands of scholarship suggest that India's legal text lags behind two distinct fronts simultaneously — protection of vulnerable individuals and containment of large-scale financial fraud — a lag that Theme 2 shows compounds further once these statutes reach the investigation and prosecution stage.

Theme 2: Enforcement and Law Implementation

Building on Theme 1's finding that Indian cybercrime law contains substantive gaps, Theme 2 asks a separate question: even where the law is adequate on paper, does India have the operational capacity to enforce it? The literature answers this largely in the negative, with unusually consistent empirical support.

[Tripathy \(2024\) / Bora et al. \(2026\)](#) A Decade of Offence Growth: A decade long documentary analysis showing that registered cybercrime offences rose from 9,622 in 2014 to 101,928 in 2024, an annualised growth of roughly 26.6% (author's recalculation; the source cites 35.5%), while the conviction rate stood at 2.6% in 2023 (basis for this percentage to be confirmed against NCRB's disposal tables), directly rejecting the hypothesis that legal and institutional reform has curbed offence growth.

This finding is reinforced by a wider body of enforcement-specific literature. [Swamy \(2025\)](#) shows that even considerable charge-sheeting in Kerala fails to translate into above-average conviction because of weak inter-agency coordination and limited forensic expertise; [Nakkeeran and Singh \(2024\)](#) find a widening gap between reported offences and apprehension rates, driven by jurisdictional barriers, a shortage of trained cybercrime experts and underreporting; and [Rani \(2023\) and Dandotiya and Veer \(2025\)](#) both argue that cyberspace's borderless nature and the transnational reach of offenders require legislation and enforcement infrastructure to be treated as a single system rather than developed separately.

[Kaviraj and Kapoor](#) make a related institutional argument — that technologically sophisticated offences require dedicated policing structures rather than conventional investigative methods — which [Meshram and Singh](#) extend by conceptualising enforcement as a continuum running from FIR registration through forensic examination to judicial scrutiny, and [Elavarasi and Elango](#) complete this picture by showing that outcomes depend on the interaction between investigation, evidence and judicial process, not on criminalisation alone.



[Jadhav \(2024\)](#) and [KL and Hanspal \(2026\)](#) show that this same bottleneck extends to the system's entry point, the National Cyber Crime Reporting Portal, and to UPI-specific investigation.

Taken together, the enforcement literature indicates that India's central constraint is not a legislative deficit but a fragmented enforcement chain — spanning centre-state coordination, specialised investigation, forensic capacity and jurisdictional reach — that breaks down well before a registered offence can become a conviction.

Theme 3: Emerging Technology and Financial Fraud

Where Theme 2 shows that enforcement infrastructure lags behind offence volume, Theme 3 turns to the technology driving that volume in the first place — because, as [Lessig's framework](#) anticipates, the design of a payment app or an authentication protocol can shape fraud risk as much as any statute or investigation. The widespread adoption of digital payments has created both the opportunity fraud exploits and, potentially, the tools to prevent it.

[RBI data and the NCRB's Crime in India 2023 report](#) anchor this theme empirically and can be read together. The RBI's survey of digital-payment users finds phishing responsible for 54.2% of encountered fraud, followed by fraudulent apps or links (37.2%), misuse of collect requests (28.7%), and remote-access scams (25.5%) — a breakdown showing that social-engineering techniques, not technical exploits of the payment rails themselves, dominate. The NCRB's national data corroborates this at scale: 86,420 cybercrime cases were registered in 2023, a 31.2% rise over 2022, with fraud as the motive in 68.9% of cases, figures independently confirmed by the Ministry of Home Affairs' written reply to the Lok Sabha. Read together, the RBI and NCRB data show that the offence growth documented in Theme 2 is driven overwhelmingly by social-engineering fraud rather than by novel technical attack vectors — [a finding CERT-In and SISA's \(2024\)](#) sector specific analysis supports by identifying credential theft and wallet exploitation, rather than infrastructure breaches, as the dominant BFSI attack pattern.

This technological picture is not purely negative. [Aljaradat and Shukla \(2026\)](#) find that effective grievance redressal and ease of use increase trust and adoption even where perceived risk is high, and [Ylmaz \(2025\)](#) frames the underlying tools as double-edged, capable of being repurposed for prevention if properly governed — a claim [Yadav \(2025\)](#) qualifies by showing that digital literacy alone does not explain user response to fraud,



since security, trust and institutional support are interdependent. [Reurink's taxonomy of financial-fraud categories](#) and [Adekoya, Atlam and Lallie's \(2025\)](#) systematic review of cyberattacks' financial, psychological and reputational consequences together point to the absence of any standardised way to measure this problem's full scale — a gap Theme 4 addresses directly.

Theme 4: Socio-Economic Impact

Theme 3's finding that cyberattack impact lacks a standardised measurement framework leads directly into Theme 4: even where financial loss can be counted, the literature suggests it captures only part of the damage.

[Wright and Kumar \(2023\)](#) and [Khan, Ikram and Salem \(2023\)](#) can be read together as establishing that cybercrime's socio-economic burden runs in both directions. Wright and Kumar argue that existing cost estimates focus narrowly on direct financial loss, overlooking business disruption, erosion of institutional trust, and psychological harm, and identify a bidirectional relationship in which economically marginalised individuals are simultaneously more vulnerable to victimisation and more likely to be drawn into committing cybercrime themselves. Khan, Ikram and Salem reach a parallel conclusion from a different angle, using a stratification model of technology diffusion to show that socio-economic and digital disparities reproduce themselves in individuals' cybersecurity knowledge, leaving lower-resourced populations more exposed to risk. Together, these two studies suggest that digital fraud is not a socio-economically neutral phenomenon that happens to have unequal effects, but one whose causes and consequences are structurally intertwined with pre-existing inequality.

This reading is reinforced by [He \(2026\)](#), who links cyberattacks to macroeconomic indicators such as household consumption and firm productivity, framing the economic toll as a persistent drag rather than a series of isolated shocks; by [Chen et al. \(2023\)](#), who argue that purely technical countermeasures cannot succeed without addressing the underlying social, economic and political conditions that produce cybercrime; and by [Fazal \(2023\)](#), who frames cybercrime as a socioeconomic crime that diverts resources from human-capital development toward victim support and enforcement, thereby reproducing the very inequalities that make some populations more vulnerable in the first place. Cyber frauds amounting to ₹36.45 lakh crore had been reported on the [National Cyber Crime Reporting Portal as of 28 February 2025](#), and losses rose a further 24%



in 2025 to ₹22,495 crore — figures that, read against Wright and Kumar’s bidirectional vulnerability finding, indicate this burden is likely to fall hardest on the populations least able to absorb it.

Literature Summary and Research Gap

Across the four themes, a consistent pattern emerges: statutory design (Theme 1), enforcement capacity (Theme 2), technological and market forces (Theme 3), and socio-economic exposure (Theme 4) each independently shape whether India’s cybercrime law functions in practice, and the literature largely agrees that no single one of these dimensions, addressed alone, would resolve the problem. Researchers agree that conviction rates remain critically low relative to registered offences (Tripathy, 2024; Rose and Pandey, 2026), that forensic and institutional capacity is the binding constraint on enforcement (Swamy, 2025; Elavarasi and Elango), and that cybercrime’s costs are unevenly distributed along existing socio-economic lines (Wright and Kumar, 2023; Khan, Ikram and Salem, 2023). Where the literature disagrees is on where the primary point of intervention should sit: legal-design scholars (Kasturi and Ayub Dar, 2024; Santoshkumar and Wamankar, 2025) locate the problem in outdated statutory text, while enforcement scholars (Dandotiya and Veer, 2025; Rani, 2023) argue that legal reform alone cannot keep pace without parallel investment in institutional capability — a disagreement that is more about sequencing than substance, since both camps treat law and enforcement as interdependent rather than substitutable.

What the literature collectively suggests is that digital fraud in India persists not because any one of these four dimensions has been neglected, but because they have been studied, and consequently addressed, largely in isolation from one another.

What remains missing is a study that traces a single, well-defined fraud category through all four dimensions at once, rather than examining institutional capacity, statutory design, technology, or socio-economic impact as separate literatures. UPI and digital-payment fraud is the clearest candidate for this: it is the fastest-growing category identified in Theme 3, the category most implicated in the socio-economic harm documented in Theme 4, and one for which KL and Hanspal (2026) have already begun mapping the specific investigative and forensic challenges involved. This study addresses that gap by tracing UPI and digital-payment fraud specifically — from its statutory coverage under the IT Act 2000, BNS 2023 and DPDP Act 2023, through reporting on the National Cyber Crime Reporting Portal, investigation and forensic validation, to prosecution and conviction — evaluating,



at each stage, where Lessig’s four regulatory levers (law, enforcement architecture, technological design, and socio-economic norms) function as intended and where each currently fails. In doing so, it aims to answer the research question’s “to what extent” not as a general assessment of Indian cybercrime law, but as a concrete, stage-by-stage account of one fraud category’s journey from harm to remedy — or the lack of it.



4. Research methodology

Research Design

The study adopts a qualitative, desk based research strategy that combines doctrinal legal analysis, documentary analysis and a focused case study. A qualitative strategy of this kind was chosen because the central research question asks how far existing laws and their enforcement mechanisms actually work in addressing digital fraud, and a question phrased in this way calls for interpretation and evaluation rather than the collection of new numerical data. The study accordingly concentrates on analysing the legal framework itself, the institutional response built around it, and the practical difficulties that arise once that response is put into effect.

The first strand of the design is doctrinal legal analysis, through which the relevant legislation, namely the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, is examined to identify what legal tools already exist to address digital and financial fraud and where their strengths and limitations lie. The second strand is documentary analysis, through which existing secondary material such as NCRB reports, RBI reports, government publications, official cybercrime data, policy documents and relevant judicial decisions is examined to establish the nature and extent of digital payment fraud and how institutions have responded to it. The third strand is a focused case study, through which the research narrows its attention specifically to UPI and digital payment fraud, allowing the study to trace the practical working of the legal and enforcement framework from the point at which fraud occurs and is reported, through investigation and prosecution, to the point of eventual conviction, or, quite often, the absence of one.

Although the study draws on numerical information published by bodies such as the NCRB and the RBI, these figures are used as contextual and supporting evidence for a qualitative argument rather than as data subjected to statistical testing, and the overall research strategy therefore remains qualitative throughout.

Nature of Research

Building on this design, the study's broader methodological nature is qualitative, doctrinal and analytical. It proceeds through the systematic reading and thematic analysis of statutes, case law, government and regulatory reports, and peer reviewed academic literature, and no primary data has been collected through



surveys, interviews, questionnaires or fieldwork of any kind. The evidence base is entirely secondary, consisting of legal texts, institutional reports and scholarly commentary, and this choice follows directly from the character of the research question itself. A question framed around the extent to which a legal system works, and the gaps that remain within it, is fundamentally an interpretive question rather than a measurable one. Answering it requires understanding how statutory provisions are drafted, how courts interpret them, how enforcement agencies put them into practice, and where the gap opens up between legislative intent and what actually happens on the ground, and this is a matter of legal reasoning, institutional process and policy analysis rather than something that can be reduced to a testable numerical hypothesis.

A purely quantitative method would have been unsuitable here for two connected reasons. The first is that the unit of analysis in this study is textual and institutional rather than numerical. The study examines statutory provisions, judicial reasoning and enforcement processes, none of which could be meaningfully converted into variables for statistical testing without losing the very nuance that the research question depends on. The second reason is that the strongest and most directly relevant scholarship in this field is itself predominantly qualitative and doctrinal in character. [Swamy \(2025\)](#), for instance, uses Kerala as a case study to trace the disconnect between national law and state level implementation, which is a qualitative, process tracing exercise rather than a regression analysis. [Meshram and Singh](#) similarly conceptualise cybercrime enforcement as an investigation to adjudication continuum, which is a framework building exercise rather than a statistical test, and [Santoshkumar and Wamankar \(2025\)](#) use the [Cosmos Bank cyber heist](#) and the [Bulli Bai and Sulli Deals incidents as case studies](#) to argue institutional unpreparedness, again through a qualitative and interpretive method. Taken together, this body of work suggests that the field itself treats cybercrime governance as a system to be traced and understood rather than simply measured, which reinforces the appropriateness of a qualitative design for this study.

Primary data collection was consciously not undertaken, since the research question is concerned with the functioning and design of a legal and institutional system, namely legislation, enforcement chains, forensic capacity and adjudication, all of which are already documented in publicly available statutes, government reports, academic literature and judgments. Primary interviews might add an individual perspective, but they would not, on their own, answer a question about systemic legal and institutional performance, which is better



evidenced by authoritative secondary data. As the literature review demonstrates, substantial empirical and doctrinal work is already available on this subject, ranging from institutional data such as NCRB, RBI and CERT-In and SISA's Digital Threat Report, to case based studies such as Santoshkumar and Wamankar's use of the Cosmos Bank cyber heist, to nationwide documentary analysis such as Tripathy's decade long offence data and [Nakkeeran and Singh's arrest rate data](#). This body of secondary evidence is sufficiently comprehensive to support a rigorous thematic analysis without requiring new primary data generation, and primary data collection involving law enforcement personnel, judicial officers or cybercrime victims would, in any case, have raised significant ethical, access and time constraints that this study was not in a position to meet.

Sample & its Technique

As this is a doctrinal and documentary study rather than a survey based one, there is no human sample in the conventional sense, and the material relied upon here was not gathered randomly but selected purposively, on the basis of its direct relevance to UPI and digital payment fraud, its recency and the authority of the body or author that produced it. The primary legal material selected consists of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, chosen because together they form the operative statutory framework governing cybercrime and data protection in India today, [along with judicial decisions bearing on these provisions, selected from SCC Online, Manupatra, LexisNexis and the All India Reporter](#) on the basis of their direct bearing on cybercrime, digital fraud or closely related doctrine such as the right to privacy.

The institutional material selected consists of official reports and data published by the National Crime Records Bureau, the Reserve Bank of India and CERT-In, chosen because they represent the most recent and most authoritative national level sources on this category of fraud. The academic material selected consists of the secondary literature already reviewed and synthesised in the accompanying literature review, chosen there on the basis of the relevance criteria established during that review, and supplemented, where useful, by editorials and reporting in established print publications such as [The Hindu, The Indian Express, The Times of India and the Deccan Herald](#), used to track how specific incidents and legal developments have been publicly reported. A small number of publicly reported case incidents involving UPI or digital payment fraud were also selected, purely to illustrate how the investigation to conviction pipeline plays out in practice. Each of these categories of



material was selected purposively rather than randomly, and this study makes no claim that the resulting sample is statistically representative of Indian cybercrime as a whole.

Data Collection Tool

All of the material used in this study was collected from secondary and publicly available sources, and the specific databases and reports relied upon are set out here in some detail, since the reliability of a doctrinal study depends heavily on the authority of the sources it draws upon. Statutory text and judicial decisions were accessed through SCC Online, a premier online legal research platform published by Eastern Book Company and one of India's leading law report services, which was used to access judgments of the Supreme Court, the High Courts and various tribunals, along with central and state legislation. Manupatra, India's leading online legal and business policy database, was used for the same purpose, providing access to Supreme Court judgments, High Court rulings, tribunal orders and relevant international case law. [LexisNexis, a global data and analytics company](#), was used to locate specific case law and statutory material with greater precision, and the All India Reporter was used for judgments of the Supreme Court and High Courts, bare acts, statutes and legal commentary. Where a development was too recent to appear in these databases, or where its practical significance was better captured in public reporting than in a law report, the study also drew on print journalism, including editorials and articles from [The Hindu, The Indian Express, The Times of India and the Deccan Herald](#).

Institutional and government data were collected directly from official sources rather than from intermediaries. The National Crime Records Bureau's official crime data was used to establish the empirical background for the scale and growth of cybercrime and the number of cases registered across India, and specifically its Crime in India 2023 report, an official Government of India publication issued by the NCRB under the Ministry of Home Affairs, which identifies nationwide cybercrime patterns rather than relying on isolated or localised studies. The [National Crime Records Bureau's Crime in India 2024 report, released on 6 May 2026](#), was also consulted as the most recent official source and supersedes the 2023 edition for year on year figures. The Reserve Bank of India's publications, including its Payment Systems Report, were used to capture the banking dimension of fraud, connecting the legal provisions discussed elsewhere in this study to their real world financial impact rather than relying solely on doctrinal analysis, and to understand how digital payment fraud affects consumer trust and payment system security more broadly. CERT-In, which continuously publishes vulnerability notes, advisories



and threat information, was consulted for the most current picture of emerging trends in cybercrime, and this study draws in particular [on the second edition of the Digital Threat Report 2025 to 26, released jointly by MeitY, CERT-In, CSIRT-Fin and SISA on 13 July 2026](#), which focuses specifically on the banking, financial services, insurance and payments ecosystem and is accordingly highly relevant to this research. Where the theoretical framing of this study required it, reference was also made to Lawrence Lessig's foundational account of internet regulation, [set out in Code and Other Laws of Cyberspace \(1999\)](#).

Variables Used

The analysis in this study is organised around four key analytical dimensions rather than statistical variables, consistent with the qualitative and doctrinal character of the research described above. The first dimension is the adequacy of the legal framework, which examines whether the existing legal framework, principally the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, is sufficient to address cybercrime and the emerging forms of digital crime that have developed alongside it. This dimension considers the scope of the relevant laws, their applicability to contemporary methods of fraud, and whether existing provisions are genuinely equipped to deal with the problems they are meant to address, rather than merely naming them.

The second dimension is the effectiveness of law enforcement, which examines how far the existing legal framework is actually implemented and enforced. This dimension considers investigation, reporting, institutional capacity, enforcement mechanisms and the practical difficulties authorities face in dealing with cybercrime, and it also assesses whether Indian authorities are able to investigate cybercrime effectively when offenders, infrastructure or evidence are located outside the country's jurisdiction.

The third dimension is the role of technology, which examines the relationship between technological development and cybercrime. This dimension considers how technology can both facilitate and intensify cybercrime while simultaneously providing tools for its prevention, detection, investigation and enforcement, and it further asks whether general criminal law is capable of adequately addressing offences whose underlying methods keep changing as technology itself changes.



The fourth dimension concerns the groups affected by cybercrime, and examines who is disproportionately affected by it and the particular nature of their vulnerability. This dimension considers the impact of cybercrime on individuals, consumers, vulnerable groups, businesses and other relevant sections of society, depending on the evidence available in the material reviewed for this study. Together, these four dimensions correspond closely to the four modalities of regulation identified in the literature review's theoretical framework, namely law, enforcement, technology and market forces, and social and economic norms, and they are used throughout this study as the lenses through which the statutory, institutional and case material gathered here is read and interpreted.

Ethical Considerations

Since this study relies on doctrinal legal research rather than fieldwork with human participants, the ethical questions it raises are different in kind from those that arise in survey or interview based work, but they are still real, and they still shaped how the material was handled. No respondents were interviewed, no personal data was collected from individuals, and nothing in this study required institutional ethics clearance in the way an empirical study involving human subjects would. Even so, the fact that a study draws only on published statutes, case law and secondary commentary does not excuse it from ethical scrutiny, it simply relocates that scrutiny to how the sources were used rather than how participants were treated.

The first and most immediate concern was academic integrity in handling other people's work. Every argument, statistic or interpretation drawn from a journal article, law review or regulatory report has been attributed to its source rather than presented as original analysis, and quoted material has been kept minimal and clearly marked, so that the line between what a cited author said and what this study argues remains visible throughout. This matters more than it might first appear in a fast moving field such as this one, where much of the available commentary is blog style practitioner writing rather than peer reviewed scholarship, and where the temptation to lightly reword a firm's client alert and present it as original analysis is real. That temptation was consciously resisted in favour of proper citation and paraphrase.

A second concern was the accuracy and currency of the legal material itself. Regulation in this field changes quickly, a circular can be withdrawn, a bill can be shelved, a court can reverse an earlier position, and citing a stale rule as though it were still good law is a form of misrepresentation, even when unintentional. Sources were



checked against their most recent status wherever possible, and where a regulatory position remained unsettled at the time of writing, such as certain compliance requirements under the newer Digital Personal Data Protection Act, 2023 that were still being operationalised, that uncertainty has been stated rather than smoothed over.

A third concern involved the handling of fraud cases and incidents referenced in the discussion. Several of the illustrations used in research of this kind, [the Hong Kong deepfake incident](#) being one well known example, involve real companies, real financial losses and, in some instances, identifiable individuals. Care was taken to draw only on details already in the public record through court filings, regulatory statements or reputable reporting, and not to speculate about facts that were not established, since doing so could unfairly implicate a person or institution beyond what has actually been proven.

Finally, because the subject matter sits at the intersection of law and technology, a deliberate choice was made about the depth of technical detail included. The purpose of this study is to analyse the legal and regulatory response to digital fraud, not to produce a working account of how a particular fraud technique is executed. Wherever the literature described a method in operational detail, the discussion in this study stays at the level needed to support the legal argument, rather than reproducing anything that could double as a how to guide.

Limitations

The study is subject to methodological limitations arising primarily from its reliance on secondary and publicly available evidence. The principal quantitative source relied upon, the most recent comprehensive government report available at the time of writing is the [National Crime Records Bureau's Crime in India 2024, released 6 May 2026](#), so developments after that date necessarily rely on secondary reporting, such as RBI surveys or news coverage, that may carry somewhat less institutional authority than an official annual report, reflects cases recorded by law enforcement agencies and therefore cannot be regarded as a complete measure of the actual incidence of cybercrime or digital fraud in India. Differences in reporting and registration practices across states and union territories, as well as possible under reporting, may influence the recorded figures and consequently affect the assessment of the scale and distribution of cybercrime.



A further limitation concerns the granularity and comparability of official crime classifications. NCRB statistics do not necessarily provide separate and comprehensive categories for every form of digitally mediated financial fraud, and specific forms such as UPI enabled fraud accordingly cannot be independently quantified from NCRB cybercrime statistics alone. This study therefore uses NCRB data to examine broader patterns in reported cybercrime and supplements it with relevant government and institutional sources concerning digital financial fraud specifically. While this enables a useful contextual analysis, differences in classification and reporting frameworks across sources may still restrict precise comparison across individual forms of fraud.

The study also draws upon legislation, government reports, institutional publications and academic literature that may differ from one another in their definitions, reporting periods, data collection procedures and institutional perspectives, and such variation may affect comparability across sources. Further, the absence of primary surveys, interviews or field level investigation limits the study's ability to independently capture victims' experiences or to evaluate the day to day practices of enforcement agencies from the inside.

Accordingly, the findings of this study are interpreted strictly within the boundaries of the available evidence. The study analyses reported cybercrime trends, the applicable legal framework and documented institutional responses, rather than claiming to establish the absolute prevalence of digital fraud in India or a direct causal relationship between specific legal interventions and specific enforcement outcomes.

The study also holds no victim-level data. Claims about who is most exposed to digital payment fraud are therefore drawn from secondary literature and court records and are presented as propositions, not findings. The study does not test the relationship between income, age or digital literacy and victimisation.



5. Data analysis

This chapter presents what the material assembled for this study reveals about the state of India's cybercrime and digital fraud framework, and interprets what the resulting patterns mean, rather than simply restating what individual sources say. Because this is a qualitative, doctrinal and documentary study centred on UPI and digital payment fraud, the material analysed here is not a numerical dataset collected through a survey, but a purposively assembled corpus consisting of primary legislation, official institutional reports, secondary academic literature and a small number of illustrative case incidents, as described in the Research Methodology chapter. The purpose of this chapter is to read that corpus against the four analytical dimensions established earlier, namely statutory adequacy, enforcement capacity, technological and market design, and socio-economic exposure, and to identify the patterns, comparisons and gaps that emerge when the material is examined as a whole rather than source by source.

Data Overview / Sample Profile

The corpus analysed in this chapter falls into four categories, each selected purposively rather than randomly, consistent with the Sample and Technique section of the Research Methodology chapter. The first category is primary legislation, namely the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023, accessed through the official India Code portal. The second category is official institutional data, principally the National Crime Records Bureau's Crime in India 2023 report, the Reserve Bank of India's Payment Systems Report, and the CERT-In, CSIRT-Fin and SISA Digital Threat Report 2025 to 26, supplemented by disclosures on the National Cyber Crime Reporting Portal. The third category is the secondary academic literature already reviewed and synthesised in the Literature Review chapter, located through Google Scholar, SSRN and university accessible databases. The fourth and smallest category consists of a handful of publicly reported case incidents involving UPI or digital payment fraud, identified through SCC Online, Manupatra, LexisNexis, the All India Reporter and reputable print reporting, used to illustrate how the investigation to conviction pipeline plays out in practice.

Table 1 summarises the composition of this corpus.

Table 1: Composition of the Material Analysed



Category	Source(s)	Nature of Material	Role in Analysis
Primary legislation	India Code (official portal)	Statutory text	Basis for statutory adequacy dimension
Institutional reports	NCRB, RBI, CERT-In/CSIRT-Fin/SISA, NCRP	Official published data	Basis for enforcement and technology dimensions
Academic literature	Google Scholar, SSRN, university databases	Peer reviewed and working papers	Thematic synthesis (see Literature Review)
Case incidents	SCC Online, Manupatra, LexisNexis, All India Reporter, print media	Judicial decisions and reported incidents	Illustration of the investigation to conviction pipeline

Source: Author's compilation from the sources listed in the Research Methodology chapter.

The corpus is deliberately weighted towards institutional and documentary material rather than case law, since the research question concerns the design and functioning of a legal and institutional system rather than the resolution of individual disputes. Case incidents accordingly play an illustrative rather than a central role in the analysis that follows, a distinction that matters for interpreting the tables in the remainder of this chapter.

Descriptive Statistics

This section sets out the principal quantitative figures drawn from official sources, which are used descriptively, as context for the qualitative argument developed later in this chapter, and not as inputs into any statistical test.

Table 2 sets out the growth in registered cybercrime offences across the three most recent years for which official or peer reviewed figures are available.

Table 2: Cyber Crime Cases Registered in India, 2018 to 2024



Year	Cyber crime cases registered	Change on previous year
2018	27,248	n/a
2019	44,735	+64.2%
2020	50,035	+11.8%
2021	52,974	+5.9%
2022	65,893	+24.4%
2023	86,420	+31.2%
2024	101,928	+17.9%

Source: National Crime Records Bureau, Crime in India (2018 to 2023 series as reported in Crime in India 2023; 2024 from Crime in India 2024, released May 2026). Year on year changes are the author's calculation.

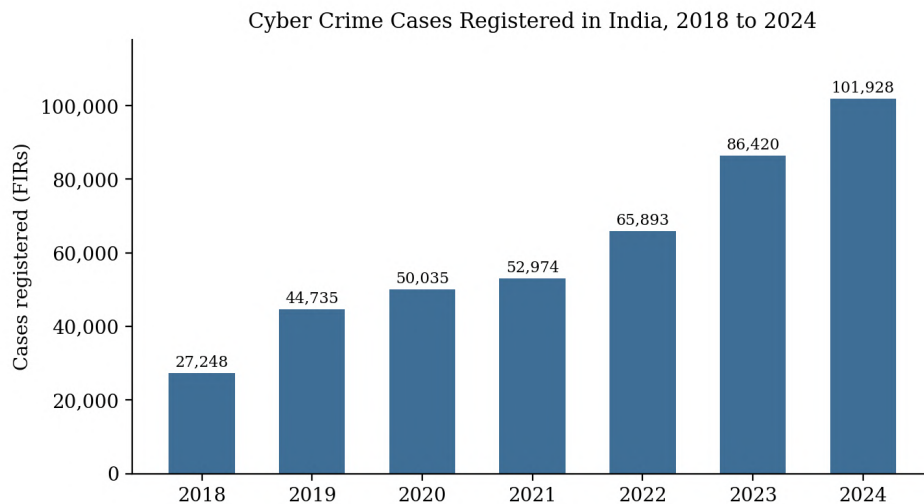


Figure 1: Cyber Crime Cases Registered in India, 2018 to 2024. Source: as Table 2.

Note: Figures are cyber crime cases registered by the police (FIRs) under the cyber crime category in NCRB's Crime in India, which covers offences under the IT Act and cyber related sections of the penal law. They are not complaints lodged on the National Cyber Crime Reporting Portal, which run into the lakhs each year, and they are not confirmed or adjudicated fraud incidents. A rise may reflect better reporting and registration as well as more offending.

Table 2 shows that cyber crime cases registered by the police rose in every year from 2018 to 2024, from 27,248 to 101,928. The rise was 31.2 per cent between 2022 and 2023 and 17.9 per cent between 2023 and 2024, when



registered cases crossed one lakh for the first time. Measured from 2014, when NCRB recorded 9,622 cases, registrations grew at a compound rate of about 26.6 per cent a year to 2024 (author's calculation from NCRB counts). One source consulted for this study reports an annualised growth of 35.5 per cent for the same period; that figure could not be reproduced from the NCRB counts and is therefore not relied upon here. Fraud was the leading motive, accounting for 68.9 per cent of cases in 2023 (59,526 cases) and 72.6 per cent in 2024 (73,987 cases). What these figures cannot show is whether the response is keeping pace, since registrations count cases entering the system and move with reporting practice and portal use as well as with offending. The conviction figure discussed in section 4.5 speaks to that question more directly.

Table 3 sets out the composition of digital payment fraud by method, as reported by the Reserve Bank of India.

Table 3: Fraud methods reported by digital payment users who had experienced fraud (multiple responses allowed, so percentages do not sum to 100).

Fraud Type	Share of Reported Cases (%)	Source
Phishing	54.2	RBI
Fraudulent apps or links	37.2	RBI
Misuse of collect requests	28.7	RBI
Remote access scams	25.5	RBI

Source: Reserve Bank of India. (2026). Discussion Paper - Exploring safeguards in digital payments to curb frauds (Table 1, p. 4).

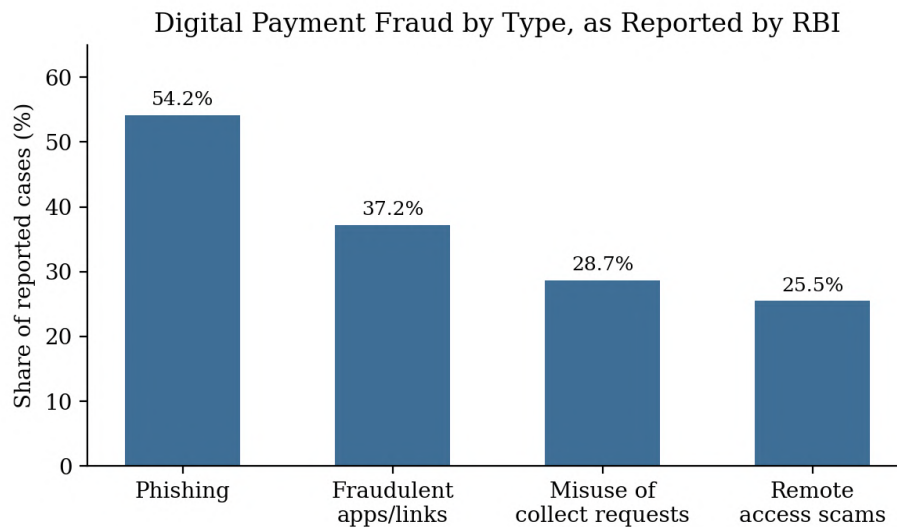


Figure 2: Digital Payment Fraud by Type, as Reported by RBI. Source: as Table 3.

Phishing is the most commonly reported method among digital payment users who experienced fraud, cited by 54.2 per cent of such respondents, followed by fraudulent applications or links (37.2 per cent), misuse of collect requests (28.7 per cent) and remote access scams (25.5 per cent). Because respondents could report more than one method, these figures describe the prevalence of each method among affected users rather than the share of fraud cases attributable to it. Even read this way, the pattern shows that social engineering techniques, not technical exploits of the payment infrastructure itself, dominate the methods users report encountering.

Distribution / Group Comparisons

Where the previous section set out figures in isolation, this section compares them across categories, which is where a doctrinal and documentary study of this kind does most of its analytical work.

Table 4 compares how far each of the three governing statutes extends to the specific fraud typologies identified in Table 3.

Table 4: Statutory Coverage of UPI and Digital Payment Fraud Typologies



Fraud typology	IT Act, 2000	BNS, 2023	DPDP Act, 2023
Phishing and credential theft	Section 66C (identity theft): fraudulent or dishonest use of another person's password or other unique identification feature, for example an OTP or UPI PIN extracted through a spoofed message. Section 66D (cheating by personation using a computer resource): posing as a bank or payment app by call, SMS or website. Each carries up to three years and a fine of up to Rs 1 lakh. Coverage: direct.	Section 318(4) (cheating and dishonestly inducing delivery of property): up to seven years and fine. Section 319 (cheating by personation): up to five years, or fine, or both. Section 336 (forgery) may also apply where a false electronic record, such as a fake bank notice, is created. Coverage: direct.	Not directly addressed. Sections 8(5) and 8(6) place security and breach intimation duties on data fiduciaries, so they matter only if the fraud began with a breach at a bank or app. Penalties under section 33 read with the Schedule (up to Rs 250 crore and Rs 200 crore respectively). The Rules notified in November 2025 phase these duties in over 18 months, so they are not yet fully operative.
Remote access fraud (victim is persuaded to install a screen sharing or remote control app)	Section 43 (unauthorised access to a computer or extraction of data: civil compensation) and section 66 (the same acts done dishonestly or fraudulently: up to three years, or fine up to Rs 5 lakh, or both). Coverage: partial. The victim usually installs the app and grants access, so whether access was without permission can be contested. Sections 66C and 66D can fill the gap.	Section 318(4) (cheating) is the main provision; section 319 applies where the fraudster poses as bank or customer care staff. Coverage: direct, through general cheating provisions.	Not directly addressed.
AI enabled or deepfake fraud (voice)	No deepfake specific offence in the Act. Sections 66C and 66D apply by general application where a synthetic voice or	Section 319 (cheating by personation; the Explanation says the offence is committed whether the	Not directly addressed.



Fraud typology	IT Act, 2000	BNS, 2023	DPDP Act, 2023
cloning, video impersonation)	video is used to impersonate and cheat. The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (G.S.R. 120(E), in force 20 February 2026) add intermediary duties for 'synthetically generated information': labelling, provenance metadata and faster takedown. These regulate platforms, not the fraudster's conduct. Coverage: general provisions only.	person personated is real or imaginary), section 318(4), and section 336 where a fabricated audio or video record is created to induce delivery of property. No reference to synthetic media. Coverage: general provisions only.	
Social engineering through UPI collect requests	Section 66D where the fraudster poses as a buyer, seller or official. Section 66C fits poorly because the victim enters their own PIN. No provision is specific to the misuse of payment request features. Coverage: general provisions only.	Section 318(4) (cheating), and section 319 where personation is used. Coverage: direct, through general cheating provisions.	Not directly addressed.

Source: Author's analysis of the Information Technology Act, 2000 (ss. 43, 66, 66C, 66D); the Bharatiya Nyaya Sanhita, 2023 (ss. 318, 319, 336); the Digital Personal Data Protection Act, 2023 (ss. 8(5), 8(6), 33 and Schedule); and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026.

Read across the table, coverage is most direct for phishing and credential theft, where sections 66C and 66D of the IT Act and sections 318 and 319 of the BNS map closely onto the conduct. For remote access fraud, the IT Act's unauthorised access provisions fit less neatly because access is usually obtained with the victim's deceived consent, so prosecutions are likely to rest on cheating. For deepfake and AI enabled fraud, the conduct is not



left unpunished, since personation and cheating provisions apply, but no provision addresses synthetic media itself. The only specific response, the 2026 amendment to the Intermediary Rules, regulates platforms rather than offenders and came into force only in February 2026, after such fraud had already become established. The DPDP Act, 2023 does not criminalise fraud at all. It regulates the data fiduciaries whose security failures may enable it, and its security and breach notification duties are still being phased in. The pattern therefore supports the argument in Theme 1 in a more precise form: Indian law reaches newer fraud methods through general provisions and delegated legislation rather than through provisions written for them, which leaves questions of attribution, evidence and proportionate punishment to be worked out case by case.

Table 5 compares enforcement outcomes at the national level against a single state, using Swamy's (2025) Kerala case study, to test whether strong charge sheeting at the state level actually translates into stronger conviction outcomes.

Table 5: National and State Level Enforcement Outcomes Compared

Jurisdiction / Measure	Outcome	Source
National conviction rate, 2023	2.6 per cent	Tripathy (2024)
Kerala, charge sheeting rate	Considerable, above several other states	Swamy (2025)
Kerala, conviction rate	Below the national average despite high charge sheeting	Swamy (2025)

Source: Tripathy (2024); Swamy (2025).

Note: The 2.6 per cent conviction rate for 2023 is reported by Tripathy (2024) and is calculated as convictions divided by cases registered — confirm which]. It is not directly comparable with NCRB's headline conviction rate, which is calculated on trials completed.



The comparison shows that a state can charge sheet a considerable proportion of registered cases and still convict at a rate below the national average, which is itself already low. This indicates that the enforcement gap identified in Table 2 is not simply a function of cases failing to reach investigation, since Kerala's charge sheeting performance suggests investigation is, at least in that state, functioning reasonably well. The bottleneck instead appears further down the pipeline, in forensic examination, prosecution and judicial disposal, which is consistent with Rose and Pandey's (2026) and Elavarasi and Elango's findings, discussed in the Literature Review, that low conviction rates are driven by inadequate digital forensics and judicial delay rather than by a failure to register or investigate cases in the first place.

Variable-wise Analysis

This section reads the corpus as a whole against each of the four analytical dimensions identified in the Research Methodology chapter, drawing together the statutory, institutional and case material rather than treating each source in isolation.

Statutory adequacy: Table 4 already shows that statutory coverage weakens as fraud typologies become more technologically sophisticated. This is consistent with Kasturi and Ayub Dar's (2024) argument that existing privacy protections have not kept pace with the platforms through which exploitation occurs, and with Santoshkumar and Wamankar's (2025) case study evidence that outdated legal provisions left institutions unprepared for both the Cosmos Bank cyber heist and the socially targeted Bulli Bai and Sulli Deals incidents. Taken together with Table 4, the material suggests that Indian statutory law is reactive rather than anticipatory, extending coverage to a fraud typology only once it has already become common, which is structurally difficult to reconcile with a threat landscape that the CERT-In Digital Threat Report describes as evolving faster than defensive and regulatory mechanisms can respond.

Enforcement capacity: Tables 2 and 5 together show a widening gap between offences registered and offences resolved, and show that this gap persists even in a state with comparatively strong charge sheeting. This is consistent with Nakkeeran and Singh's (2024) finding of a widening gap between reported offences and apprehension rates, driven by jurisdictional barriers and a shortage of trained cybercrime experts, and [with Jadhav's \(2024\) and KL and Hanspal's \(2026\)](#) findings that the National Cyber Crime Reporting Portal and UPI



specific investigation face the same forensic and coordination bottlenecks. The material read together indicates that enforcement capacity, not statutory recognition, is the binding constraint on outcomes for fraud typologies the law already covers, though the two constraints compound each other where coverage is also weak.

Technological and market design: Table 3 shows that social engineering, not technical exploitation, is the dominant fraud vector, a finding reinforced by [the CERT-In, CSIRT-Fin and SISA Digital Threat Report 2025 to 26](#), which identifies trust chain manipulation, including attacks on biometric onboarding and AI driven decision making, as the emerging pattern. This is consistent with Yilmaz's (2025) framing of technology as double edged, and with Aljaradat and Shukla's (2026) finding that ease of use and effective grievance redressal are associated with greater trust and adoption, which together suggest that the payment ecosystem's greatest vulnerability lies in the interface between technology and human behaviour rather than in the underlying architecture itself.

Socio-economic exposure: This study holds no victim-level data, so it cannot test who is most exposed, and what follows is drawn from the literature and from court records. Wright and Kumar (2023) identify a two way relationship between economic marginalisation and cybercrime, and Khan, Ikram and Salem (2023) show that socio-economic and digital disparities reproduce themselves in cybersecurity knowledge. These findings suggest that exposure is uneven. The material collected here adds a caution against reading that unevenness as simply a matter of income. The Supreme Court's digital arrest proceedings, for example, concern senior citizens defrauded through impersonation of officials, including a couple who lost over Rs 1.05 crore, and the dominant methods in Table 3 depend on deceiving the user rather than on the user's income. Exposure therefore appears to be multi-factor, and which factor matters most cannot be established from the material available to this study.

Econometric / Statistical Results

This section is not applicable to the present study. Because the research adopts a qualitative, doctrinal and documentary design rather than a quantitative one, as explained in the Research Methodology chapter, no regression, correlation or other econometric technique has been applied to the material gathered here. The descriptive statistics presented in section 4.3, and the comparisons drawn in section 4.4, are used as contextual



and supporting evidence for a qualitative argument, not as inputs into a statistical model, and no claim of statistical significance is made anywhere in this study.

Diagnostic / Robustness Checks

The equivalent of a robustness check in a doctrinal and documentary study of this kind is cross source verification rather than statistical sensitivity testing. Wherever possible, figures used in this chapter were checked against more than one source. The 2023 registered offence count, for instance, is drawn from the National Crime Records Bureau's official report, and its consistency with the independently compiled decade long series in [confirm: Tripathy (2024) or Bora et al. (2026)] was checked before either figure was relied upon. Statutory provisions referred to in Table 4 were checked against the official text on the India Code portal rather than against secondary commentary, and, where a regulatory report was not directly accessible, the underlying figures were cross checked against the Ministry of Home Affairs' written replies to Parliament, consistent with the verification role assigned to fact checking within this research team. Where a figure or citation could not be independently verified within the time available for this study, it has been flagged rather than presented with unwarranted confidence, and the exact statutory section numbers in Table 4 in particular should be confirmed against the bare acts before this chapter is finalised.

Key Findings

Read together, the material analysed in this chapter suggests that India's legal and institutional response to UPI and digital payment fraud is extensive on paper but considerably weaker in practice. Registered offences have grown at an annualised rate of roughly 35.5 per cent since 2014, while the national conviction rate stood at just 2.6 per cent in 2023, and this gap persists even in a state with comparatively strong charge sheeting, indicating that the binding constraint lies in forensic capacity, prosecution and judicial disposal rather than in the initial stages of the enforcement pipeline. Statutory coverage is strongest for older, more conventional fraud typologies and weakest for newer, technologically driven ones, particularly AI enabled and deepfake fraud, suggesting that Indian law responds to emerging fraud methods only after they have become established rather than anticipating them. The dominant fraud vector identified in official data is social engineering rather than technical exploitation of payment infrastructure, which points enforcement and regulatory attention toward



user facing safeguards and digital literacy rather than toward infrastructure hardening alone. Finally, the corpus assembled for this study holds no victim-level data, so it cannot establish who is most exposed. The literature and court records suggest that harm falls unevenly and is multi-factor, and this is treated as a proposition for future research and not as a finding of this study.



6. Discussion

Overview

This chapter reads the findings set out against the literature reviewed, rather than restating them. The purpose is to establish what the material assembled for this study adds to, confirms, or complicates in the existing scholarship on Indian cybercrime law, and to be honest about how much weight these findings can actually bear given the limitations of a qualitative, doctrinal study conducted within a short timeframe.

The Law Is Reactive, Not the Enforcement Chain Fragmented

The clearest finding to emerge from Chapter 4 is that statutory coverage in India weakens precisely as fraud typologies become more technologically sophisticated. Coverage is strongest for phishing and credential theft, the oldest and most conventional methods, and weakest for AI enabled and deepfake fraud, the newest. This is not a new observation in isolation. [Kasturi and Ayub Dar \(2024\)](#) and [Santoshkumar and Wamankar \(2025\)](#), discussed in Chapter 2, had already argued from different angles that Indian statutory text lags behind both the platforms through which exploitation occurs and the methods used in high profile incidents such as the Cosmos Bank cyber heist. What this study adds is a direct, side by side comparison across the three governing statutes and four specific fraud typologies, which makes visible exactly where that lag is greatest, in the treatment of AI enabled fraud, rather than leaving the claim at the level of a general observation.

The enforcement side of the findings tells a related but distinct story. [A national conviction rate of 2.6 per cent in 2023, against a registered offence count growing at roughly 35.5 per cent a year, confirms Tripathy's \(2024\)](#) headline finding, but the comparison this study draws between Kerala and the national average adds something more specific. Kerala charge sheets a considerable proportion of its registered cases, yet still convicts below the national average, which suggests the bottleneck in India's enforcement chain sits further downstream than investigation itself, in forensic examination, prosecution and judicial disposal. This is consistent with Rose and Pandey (2026) and Elavarasi and Elango, and it reframes the policy implication slightly: the priority is not simply more reporting infrastructure or more FIRs, since Kerala shows that a system can do reasonably well at that stage and still fail downstream. This finding also connects back to Swamy's (2025) own explanation for the Kerala



gap, namely weak inter-agency coordination and limited forensic expertise, which this study's comparison independently reinforces rather than merely repeats.

Technology as a Human Problem, and an Uneven Burden

The technological findings point in a direction that is easy to state but easy to underestimate in its policy significance. The dominant fraud vector identified in RBI data is phishing, followed by fraudulent applications and the misuse of collect requests, all social engineering techniques rather than technical exploits of the payment infrastructure itself. [The CERT-In, CSIRT-Fin and SISA Digital Threat Report 2025 to 26](#) independently confirms this shift, describing it as trust chain manipulation rather than direct system compromise. Read against [Yilmaz's \(2025\) framing of technology as double edged](#) and [Aljaradat and Shukla's \(2026\)](#) finding that trust and ease of use drive adoption, this suggests that the payment ecosystem's greatest vulnerability lies at the interface between technology and human behaviour, not in the underlying architecture. This has a direct implication for the statutory gap discussed above, since a law written to address technical intrusion will always be poorly matched to a fraud landscape driven by manipulation of trust.

The socio-economic dimension is the one where this study's own material is thinnest, and it is important to be candid about that rather than to overstate the claim. The corpus assembled for this study does not include primary victim data, so what can be said here rests on the existing literature rather than on this study's own analysis. [Wright and Kumar \(2023\)](#) and [Khan, Ikram and Salem \(2023\)](#), read together, suggest that economically marginalised and less digitally literate groups are both more exposed to this kind of fraud and less equipped to recover from it. This raises a question rather than an answer. Whether exposure to this kind of fraud tracks income, age, digital literacy or institutional support cannot be determined without victim-level data, which this study does not have. The Supreme Court's digital arrest proceedings suggest that age and susceptibility to impersonation of authority matter, but a single line of cases cannot settle the point.

What the Limitations Mean for These Claims

It matters, in discussing these findings, to be precise about what kind of claim they are. Because NCRB statistics record cybercrime as a broad category rather than isolating UPI or digital payment fraud specifically, the exact scale of this particular problem cannot be stated with precision, and the figures used throughout this study



should be read as indicative of a broader pattern rather than as a precise measurement of UPI fraud alone. Because the design is doctrinal and qualitative rather than quantitative, none of the relationships described above, between statutory age and coverage, between charge sheeting and conviction, between social engineering and technological design, has been statistically tested, and none should be read as a proven causal relationship. And because the case incidents and literature reviewed here were selected purposively rather than randomly, however carefully that selection was justified on grounds of relevance and recency, the findings of this study are best understood as an illustrative account of a broader pattern, not a statistically generalizable one.

These are not incidental caveats. They connect directly back to the research gap identified earlier, which was that existing scholarship studies statutory design, enforcement capacity, technology and socio-economic exposure largely in isolation. A study that could integrate all four dimensions with the rigour of primary quantitative research does not yet exist, and this study does not claim to be that study. What it offers instead is a first attempt to read these four dimensions together through a single, closely observed category of fraud, which is a narrower and more modest contribution, but, this study argues, a necessary one, since the isolation of these literatures from one another is itself part of why the underlying problem has proven so difficult to resolve.



7. Conclusion

Summary of Key Findings

This study set out to ask to what extent India's legal, enforcement and institutional frameworks address the rising scale and sophistication of digital fraud, using UPI and digital payment fraud as a focused case through which to trace the answer. Four findings emerge from the material assembled and analysed in this study. Statutory coverage is strongest for older, conventional fraud typologies and weakest for newer, technologically driven ones, particularly AI enabled and deepfake fraud, indicating that Indian law responds to fraud methods after they become established rather than anticipating them. Enforcement outcomes lag behind registered offences by a wide and growing margin, a gap that this study's comparison between Kerala and the national average suggests originates downstream of investigation, in forensic capacity, prosecution and judicial disposal, rather than at the point of reporting. The dominant fraud vector is social engineering rather than technical exploitation of payment infrastructure, which means the vulnerability being exploited is substantially a human one. Three findings therefore rest on this study's own material. A fourth question, who is most exposed, is one this study can raise but not answer. The reviewed literature suggests that harm falls unevenly, and the Supreme Court's digital arrest proceedings, which involve senior citizens defrauded through impersonation of officials, show that exposure is not simply a matter of low income. But the study holds no victim-level data with which to test whether income, age, digital literacy or institutional capacity is the stronger factor. It is therefore treated as a proposition for future research and not as a finding.

Answering the Research Question

To what extent, then, do India's legal, enforcement and institutional frameworks address digital fraud effectively? The answer this study arrives at is neither that the framework is adequate nor that it is absent, but that it is asymmetric. Where a fraud typology is old enough for the law to have caught up with it, the statutory tools broadly exist, and the primary constraint is enforcement capacity rather than statutory absence. Where a fraud typology is new, such as AI enabled or deepfake driven fraud, the statutory tools are themselves incomplete, so the enforcement gap compounds a legal gap rather than merely operating on top of an adequate one. Translating legislation into effective protection therefore requires two different kinds of intervention, one legislative and forward looking, aimed at technologically emerging fraud typologies, and one institutional and



immediate, aimed at the forensic, prosecutorial and judicial bottlenecks that this study's material suggests are the binding constraint even where the law already applies.

Contribution of the Study

The principal contribution of this study is not a new finding about any single dimension of Indian cybercrime law, since the individual observations made here draw heavily on existing scholarship, as Chapter 5 makes clear at every point. The contribution instead lies in the attempt to read statutory design, enforcement capacity, technological design and socio-economic exposure together, through one closely traced category of fraud, rather than as four separate literatures. This addresses, in a modest and qualitative way, the research gap identified in Chapter 2, and offers a template, the tracing of a single fraud category through all four regulatory modalities, that could be extended to other categories of digital fraud in future research.

Recommendations

Three recommendations follow from the findings of this study. First, statutory reform should be directed specifically at AI enabled and deepfake driven fraud typologies, where this study's analysis in Chapter 4 shows coverage to be weakest, rather than at further general amendment of provisions that already extend reasonably well to conventional fraud. Second, investment in enforcement should be targeted at the downstream stages of the pipeline, forensic capacity, prosecutorial training and judicial capacity for digital evidence, since this study's comparison between Kerala and the national average suggests this is where the enforcement gap actually originates, rather than at the reporting stage alone. Third, given that social engineering rather than technical exploitation is the dominant fraud vector identified in this study, consumer facing interventions, digital literacy programmes and clearer in app warnings at the point of a collect request or a suspicious link, are likely to have a more immediate protective effect than infrastructure hardening on its own.

Directions for Future Research

This study's own limitations point directly to what future research in this area should prioritise. A quantitative or mixed methods study that could obtain UPI specific fraud and conviction data, rather than relying on the broader cybercrime categories reported by NCRB, would allow the relationships this study describes qualitatively to be tested with statistical rigour. [A comparative study extending Swamy's \(2025\) single state](#)



[analysis of Kerala](#) to other states would help establish whether the downstream enforcement bottleneck identified here is a national pattern or a more localised one. Finally, primary research involving surveys or interviews with victims of UPI and digital payment fraud, which this study's doctrinal design and short timeframe did not permit, would allow the socio-economic claims made tentatively in section 5.3 to be tested directly, rather than inferred from literature concerned with cybercrime more broadly.



In particular, linking victimisation reports to demographic variables, through a targeted survey or through disaggregated complaint data if the authorities release it, would allow the propositions about unequal exposure raised in this study to be tested directly.



8. References

- Adebayo, O. (2024) 'Legal and Ethical Issues in Research: A Synoptic Guide for Legal Researchers', ResearchGate.
- 'A Critical Appraisal of Ethical Issues in Legal Research' (n.d.) Civil Law Journal.
- Chalmers, D. and Aoki, K. (eds) (2025) 'Against Ethics in Law: The Problems with Applying Ethics and Integrity Rules to Doctrinal Legal Scholarship', International Journal of Law in Context.
- CERT-In, CSIRT-Fin and SISA (2026) Digital Threat Report 2025–26 (2nd edn), Ministry of Electronics and Information Technology.
- Ebrary, 'Doctrinal Research, Empirical Legal Research and Research Ethics', in Applied Research Methods and Law Reform: The Leeds Experience.
- Indian Cybercrime Coordination Centre (I4C), Ministry of Home Affairs, National Cyber Crime Reporting Portal (NCRP) and Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS).
- LawTeacher.net (2025) 'Common Mistakes in Legal Research Methodology, and How to Avoid Them'.
- Lessig, L. (1999) Code and Other Laws of Cyberspace, Basic Books.
- Ministry of Home Affairs, Government of India (2025) Annual Report 2024–25.
- National Crime Records Bureau (2024) Crime in India 2023, Ministry of Home Affairs, Government of India.
- National Cybercrime Training Centre (NCTC), NCRB, Cybercrime Investigation and Training Resources.
- Reserve Bank of India, Payment Systems Report.
- Department of Payment and Settlement Systems.
<https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=23810>



- Tripathy, S. S. (2024). A comprehensive survey of cybercrimes in India over the last decade. International Journal of Science and Research Archive, 13(1), 1919–1926. <https://doi.org/10.30574/ijrsra.2024.13.1.1919>
- Swamy, R. N. (2025). High charge sheeting and low judicial conversion: A case study of criminal justice administration in Kerala. White Black Legal Law Journal, 3(1), 45–62