ISSN: 3139-3179(Online)
Aviradha International Journal of Law and Legal Studies (AIJLLS)
© AIJLLS | Vol. 2 | Issue 3 | April-June 2026
Available online at: https://aijlls.com/
DOI: https://doi.org/10.65785/aijlls.v2i3.17

Investigation of Cyber Frauds in India: Legal and Digital Forensic Challenges in the Era of UPI and Online Banking

Shilpa KL [1] and Dr. Manindra Singh Hanspal [2]

[1] *LL.M. (Criminal Law), School of Law, Presidency University, Bengaluru.*

[2] *Assistant Professor, LL.M. Coordinator, School of Law, Presidency University, Bengaluru.*

Corresponding Author Email: *shilpaslg10@gmail.com*

ABSTRACT:

India's financial system has been rapidly digitised, with the ubiquitous use of Unified Payment Interface (UPI) and online banking now creating unprecedented convenience for transactions, and an expanded attack surface for cyber-enabled financial crime. The paper examines the legal and digital-forensic issues that plague detection, investigation and prosecution of cyber frauds in the UPI/online-banking ecosystem. It explores the most prevalent fraud typologies, such as phishing, vishing, smishing, QR code manipulation, SIM-swap and remote-access fraud, and how this fit into the now revamped statutory framework, including the Information Technology Act, 2000 and the new criminal laws of 2023. The Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita and the Bharatiya Sakshya Adhiniyam. The study examines the contribution of digital forensics in the context of admissibility of electronic evidence in the light of the certification process under Section 63 of Bharatiya Sakshya Adhiniyam and the judicial evolution from *Anvar P.V.* to *Shafhi Mohammad to Arjun Panditrao Khotkar*. It identifies the mismatch between the pace of fraud in the UPI and the evidentiary process in criminal adjudication and argues that coordinated legal, institutional, technological and capacity building reforms by regulators, law enforcement agencies, the judiciary and the banking sector are required to effectively combat cyber fraud.

Keywords: *Cyber Fraud; UPI; Digital Forensics; Electronic Evidence; Bharatiya Sakshya Adhiniyam.*

1. INTRODUCTION:

In just one decade, India has made the transition to a real-time payments powerhouse. UPI was launched by the National Payments Corporation of India (NPCI) in April 2016 under instructions from the Reserve Bank of India (RBI) and formed the bedrock of India's retail payment system.[1] Its design a non-proprietary, interoperable layer on the top of the Immediate Payment Service which only requires users know from

[1] National Payments Corporation of India, *About UPI* (NPCI, 2024); UPI launched 11 April 2016 under RBI regulatory oversight.

whom to what their Virtual Payment Address for instant inter-bank settlements, was historically frictionless enough to allow hundreds-of-millions of net-new users into the formal financial system. Annual transaction volume grew from around two crore transactions per year in FY 2016-17 to more than 24,162 crore transactions in FY 2025-26, while value increased to about ₹314 lakh crore during the same timeframe.[2] UPI processed a whopping 21.63 billion transactions worth ₹27.97 lakh crore in December 2025, the highest monthly figure yet, which translates to almost 698 million transactions per day on an average.[3] UPI, by transaction volume, is the largest real-time payment system globally, a new recognition of it as an instrument of India's digital diplomacy that even the International Monetary Fund has not escaped. Internet penetration has also increased, with over 86 per cent of households now connected to the internet[4], bringing digital finance within reach of rural and semi-urban India.[5]

However, this same convenience that drives the rapid adoption has also led to a parallel epidemic of cyber-enabled financial crime. The very characteristics that make UPI appealing speed, ubiquity, irreversibility and easy onboarding are exactly the traits fraudsters leaped on. As per data laid before Parliament by the Ministry of Home Affairs, cyber crimes against individuals in India caused losses of around ₹22,845 crore last year 400 times more than the actual amount correctly handed back to victims.[6] The rise in number of complaints on the portal went up from approximately 4.52 lakh in 2021 to over 22 lakh by the year 2024, more than quadrupling victims not only indicate an increase in victimisation but also strengthen reporting.[7] The Reserve Bank's own ON-SITE supervisory database on cases of card, internet & digital-payment frauds of ₹1 lakh or more registered23 stood at 29,082 (₹1,457 crores) in 2023-24.[8] Broken down, investment-related scams now make up around three-quarters of all reported monetary losses, followed by rapidly-expanding "digital custody" and impostor frauds.[9] In 2023, the National Crime Records Bureau registered a total of 86,420 cybercrime cases from 52,974 in 2021 with fraud being the most common motive for competition.[10] The State has reacted by setting up a helpline (1930) and the Citizen Financial

[2] Press Information Bureau, "UPI Completes 10 Glorious Years, Emerges as World's Largest Real-Time Payments Platform," PIB Release No. 2257087 (30 April 2026).

[3] "UPI Records 21.63 Billion Transactions Worth ₹27.97 Lakh Crore in December 2025," *Elets BFSI* (2 January 2026); daily average of approximately 698 million transactions.

[4] International Monetary Fund, cited in PIB Release No. 2257087 (30 April 2026) (UPI recognised as the world's largest real-time payment system by volume).

[5] Press Information Bureau, *Curbing Cyber Frauds in Digital India* (PIB, 8 October 2025), Note ID 155384 (over 86 per cent of households connected).

[6] Ministry of Home Affairs data placed before Parliament, reported in "India's Cybercrime: 22.68 Lakh Cases in 2024, ₹22,845 Crore Lost" (December 2025).

[7] Indian Cyber Crime Coordination Centre / National Cyber Crime Reporting Portal data, Ministry of Home Affairs (Rajya Sabha replies, 2025).

[8] Reserve Bank of India frauds data, cited in IndiaSpend, "How India's Cyber Crime Incidence Is Rising" (6 December 2025); frauds of ₹1 lakh and above reached 29,082 cases in 2023-24 involving ₹1,457 crore.

[9] I4C data reported in *The Indian Express*; investment-related scams account for approximately 77 per cent of reported cyber-fraud losses.

[10] National Crime Records Bureau, *Crime in India*; registered cybercrime cases rose from 52,974 (2021) to 86,420 (2023).

Cyber Fraud Reporting and Management System, but still the difference between victimisation and successful prosecution remains great, the conviction rate stayed low.[11]

The research problem that this work addresses is the structural dissonance between the rapid and anonymous nature of UPI era fraud and the slow-moving evidence-heavy practices associated with criminal investigation and adjudication. A transaction is generated and transacted in seconds, funds are quickly laundered through a series of so called "mules" and often the perpetrator is based outside any jurisdiction that could be accessed by an investigating officer. Investigation, on the other hand, relies on the lawful collection, faithful preservation and eventual admissibility of perishable electronic evidence a process governed by procedural and evidentiary rules that have traditionally been designed to suit a paper environment. The present study has three main objectives. The first objective is to identify the main cyber-fraud schemes working in the UPI and online-banking ecosystem, classifying them based on human nature or technical aspects exploitation. Secondly, it analyzes whether the existing legal framework for investigating such frauds, is adequate considering the extensive recodification of Indian criminal law in 2023. Third, it evaluates the digital- forensic and evidentiary hurdles that in practice dictate the success or failure of prosecutions. Thus, the relevant research questions are these: Is the existing statutory and regulatory architecture up to the task of addressing high-velocity digital fraud; what reforms legal, institutional and technological are needed to bolster investigation and prosecution?

The methodology used is doctrinal and analytical. It is based on primary legal sources statutes, subordinate legislation, regulatory circulars and the judicial decisions of the Supreme Court and High Courts supported by official statistical data from NPCI, RBI, I4C and NCRB. Secondary academic and institutional analysis contextualizes and critiques the primary material. The study focus under examination is purposely kept narrow across financial cyber frauds on digital payments and online banking; it does not have scope on data-protection breaches, online content offences or unless relevant to the scrutiny of fraud any form of cyber-terrorism. The study is national in scope, with comparative observations introduced only to the extent that gaps in domestic practice are illuminated through comparison, and mainly focuses on the investigative and evidentiary stages, rather than focusing on sentencing or victim compensation as stand-alone issues.

2. Cyber Frauds in India's Digital Payment Ecosystem

Cyber fraud in the context of digital-payment, could be defined as an instance of deception carried out through electronic platforms usually unauthorised access, identity misuse or social engineering made with the purpose of causing wrongful financial loss to a victim and corresponding wrongful gain to the offender.[12] Most notably, it is fundamentally different and easily distinguished from traditional cheating: it occurs with extraordinary rapidity, scales to thousands of victims at once, provides the criminal access

[11] Ministry of Home Affairs, Citizen Financial Cyber Fraud Reporting and Management System and National Helpline 1930.

[12] Press Information Bureau, *Curbing Cyber Frauds in Digital India* (PIB, 8 October 2025).

to a high degree of anonymity, constitutes a very low marginal cost per attempt and routinely transgresses state and national borders. Combined, these characteristics make traditional, geographically defined investigative practices obsolete and require a wholly unique evidentiary response and forensic response. UPI and online-banking frauds are almost always carried out through social engineering on the human user, rather than through breaking the underlying crypto protocol. UPI frauds usually involve perpetrators posting links containing "collect request", and fake *payee* handles in addition to the rampant misconception that entering a UPI PIN is necessary to *receive* money, whereas it is only needed while *sending*.[13] A victim who is convinced to initiate or authorise a "collect" request, or the authorisation for the credit rather than debit of an apparent transaction, gives their own authentication of the fraud. In contrast, online-banking frauds often revolve around intercepting the login credentials and the one-time password (OTP) for second-factor authentication, which are tricked or technically intercepted from the victim by an attacker.

Phishing, vishing and smishing are most common attack vectors. *Phishing* uses faked emails or copycat banking websites to obtain credentials and card data. In *vishing*, a voice-fraud tactic in which the calling party impersonates a bank officer, payment-service representative or other official in order to leverage that authority and get targeted individuals to reveal sensitive information. An example of this is *Smishing*, which uses misleading SMS messages to fool them into clicking on malicious links or offerings fake rewards and prizes.[14] Alongside the normalisation of merchant QR payments, similarly related are QR-code scams, where a victim scans a code under the apprehension that this is crediting their account and, in fact, it authorises a debit; such scams have flourished.[15] The common thread among those techniques is that they use cognitive bias and misplaced faith rather than any technical vulnerabilities, making both prevention and later legal proof of intent to defraud more difficult.

Two more approaches have been especially nasty because they foiled the second half of the authentication process on which banking security relies. In *SIM-swap fraud*, criminals get a hold of the duplicate copy of the SIM card associated with the mobile number registered to a victim who unwittingly falls prey, as it allows them to access OTPs and transaction alerts and de-activate two-factor authentication in place by stealing thousands literally before one gets to know.[16] *Remote-access application fraud* involves tricking victims into authenticating downloads of screen-sharing tools like AnyDesk or TeamViewer under the guise of addressing a technical problem or refund, allowing criminals to control their devices in real-time and access their banking applications.[17] Early indications now show a definitive change towards organised, psychologically based and ever more trans-national operations rather than purely technical exploitation.

[13] National Payments Corporation of India, *UPI Safety and Awareness Guidelines* (NPCI).

[14] Reserve Bank of India, *BE(A)WARE — A Booklet on Modus Operandi of Financial Fraudsters* (RBI, 2022).

[15] *Ibid.* (QR-code collect-request frauds).

[16] CERT-In advisory on SIM-swap and OTP-interception frauds; RBI, *BE(A)WARE* (2022).

[17] Reserve Bank of India, *BE(A)WARE* (2022) (remote-access / screen-sharing application frauds).

Fraudsters impersonating police, customs or other enforcement officials in this "digital arrest" scam who psychologically plant a victim to be watched for an extended period of time on audio-visual surveillance and have them coercing the funds under threat of elaborately concocted prosecution has seen the biggest increase of any category.

As Indian law does not even acknowledge the existence of a "digital arrest," reported incidents increased from just 39,925 in 2022 to approximately 1,23,672 by May 2024 which led to losses measured in terms of nearly ₹1,935 crore.[18] Most of these operations are managed from organised scam compounds based in South-East Asia, and rely on a network of mule bank accounts to clean proceeds. Though it was launched in September 2024, the I4C's suspect registry has identified over 24.67 lakh mule accounts and helped block a total of ₹8,031 crore worth of fraudulent transactions.[19] The enforcement agencies have also blocked lakhs of SIM cards and IMEIs related to frauds and deactivated thousands of Skype accounts and WhatsApp accounts linked to cyber-fraud rackets.[20] These scams too have progressed down into the Tier-2 and Tier-3 cities, even as more first-time digital users in India least capable of identifying warning signs make this threat, if anything, as much a socio-economic challenge as it is one theoretically addressed.[21]

Table 1: Typology of UPI and Online-Banking Fraud Schemes in India

Fraud Type	Attack Mechanism	Primary Vector	Target Vulnerability	Typical Loss Scale	Geographic Origin
Phishing	Fake emails/copycat websites	Credential harvesting	User authentication weakness	₹5,000-₹50,000 per victim	Domestic + International
Vishing	Voice impersonation	Social engineering via phone	Authority exploitation	₹10,000-₹100,000 per victim	Organized compounds (SE Asia)
Smishing	Malicious SMS messages	Fake links/reward offers	Cognitive bias	₹2,000-₹30,000 per victim	Domestic + International
QR Code Manipulation	Fraudulent QR codes at merchant locations	Debit authorization reversal	UPI PIN misunderstanding	₹500-₹5,000 per victim	Localized (Tier-2/3 cities)

[18] J. Bhandekar, quoted in IndiaSpend, "How India's Cyber Crime Incidence Is Rising" (6 December 2025); digital-arrest incidents rose from 39,925 (2022) to 1,23,672 (2024), with losses of approximately ₹1,935 crore; Indian law recognises no concept of "digital arrest."

[19] Ministry of Home Affairs, Suspect Registry data (launched September 2024), reported December 2025; over 24.67 lakh mule accounts flagged and over ₹8,031 crore in fraudulent transactions stopped.

[20] Ministry of Home Affairs / I4C data, reported December 2025 (blocking of fraud-linked SIM cards and IMEIs; deactivation of Skype and WhatsApp accounts linked to fraud syndicates).

[21] *InsightsonIndia*, "Cybercrime in India 2025" (21 February 2026) (penetration into Tier-2 and Tier-3 cities).

SIM-Swap Fraud	Duplicate SIM card acquisition	OTP/2FA interception	Telecom operator vulnerability	₹50,000-₹500,000+ per victim	Organized compounds (SE Asia)
Remote-Access Fraud	Screen-sharing tool exploitation (AnyDesk/TeamViewer)	Real-time device control	Social trust in technical support	₹1,00,000-₹10,00,000 per victim	Organized compounds (SE Asia)
Digital Arrest Scam	Impersonation of police/customs/enforcement	Psychological coercion over extended period	Fear-based manipulation	₹2,00,000-₹50,00,000+ per victim	Organized compounds (SE Asia)

"Taxonomy of prevalent UPI and online-banking fraud typologies, categorized by attack mechanism and exploitation methodology. The table delineates the technical and social-engineering vectors through which perpetrators operate, distinguishing between credential-interception schemes, identity misuse tactics and psychological manipulation strategies. Each fraud type is mapped against its primary vulnerability exploitation pattern and target population characteristics. This classification framework illustrates the heterogeneous nature of cyber-fraud attacks in India's digital payment ecosystem and underscores the difficulty in developing uniform preventive and investigative responses."

3. Legal Framework for Investigation of Cyber Frauds

India's core cyber-fraud law is still the Information Technology Act, 2000 (IT Act), which established envelope India's first sector specific scheme of e-crime. Section 43 of the Act provides for civil liabilities arising out of unauthorised access and damage to computer resources and Section 66 intensifies this very conduct to a criminal offence when dishonest/fraudulent.[22] For frauds in relation to the payments, Section 66C dealing with identity theft i.e., fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature and Section 66D for cheating by personation using computer resource or communication device has been made operative.[23] These two provision are regularly used in OTP-interception, vishing and impersonation cases. Section 65 deals with the concealment or destruction of computer source documents, while further provisions have been made in the Act on privacy violation, cyber-terrorism and looking-reaching charges for receipt of stolen computer resources.[24] Courts have judicially limited the ambit of the statute for instance, in *Shreya Singhal v. Union of India*, the Supreme Court declared Section 66A was unconstitutional and struck it down as vague and overbroad in violation of Article 19(1)(a) which guarantees free speech.[25] This provision was then also formally repealed

[22] Information Technology Act, 2000, ss. 43 and 66.
[23] Information Technology Act, 2000, ss. 66C (identity theft) and 66D (cheating by personation using computer resource).
[24] Information Technology Act, 2000, ss. 65, 66B, 66E and 66F
[25] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

by means of Jan Vishwas (Amendment of Provisions) Act Friday bringing to an end a long journey rife with its ongoing abuse.[26]

The 2023 revision of the system provided an exhaustive recodification of substantive and procedural criminal law, including the environment within which cyber frauds are punishable. The substantive offenses encapsulating the deception intrinsic to a bulk of economic frauds are furnished by the Bharatiya Nyaya Sanhita, 2023 (BNS), which has come into force from July 1, 2024 and replaced the Indian Penal Code. Section 318: Cheating; section 319 during the given act of the form that is aggravated by cheating with dishonest delivery of property; Section 336 to Punishes forgery.[27] The mapping to the former Code is broadly continuous (e.g. the old offence of cheating by personation under Section 419 parallels BNS Section 319; and cheating with dishonest inducement under Section 420 parallels BNS Section 318(4)) which preserves the significant body of precedent developed under the predecessor provisions.[28] Section 1-11 is of particular relevance to syndicated fraud; it creates a new offence organised crime, which lends itself with greater applicability to the structured, multi-actor mule-account networks and scam-compound type operations that typify modern cyber fraud.[29]

The BNSS, which replaces the Code of Criminal Procedure, 1973 updates the procedural architecture of investigation. The Sanhita nudges the police and courts to exercise their authority by introducing provisions that permit them to compel compliance through the production of documents or electronic records, whereas sections 94 strengthen powers to seize documents; digital methods are provided directly within the investigative process, through provisions around audio-visual recording of searches and seizures.[30] These are not, in sum, just formal procedural reforms: the validity of any eventual forensic analysis and its future admissibility as evidence hinge upon lawful seizure, with meticulous documentation from this initial stage on. Thus, the Supreme Court has strongly stressed on a general police training related to extraction and presentation of computer-generated evidence so that procedural lapses do not invalidate otherwise just convictions.[31]

The banking dimension of regulatory governance is driven by Reserve Bank of India. The landmark 2017 circular on Customer Protection, Limiting Liability of Customers in Unauthorised Electronic Banking Transactions by the Reserve Bank of India (RBI) defines a tiered "zero liability" and a "limited liability" regime where in case of fraud, loss is not onus on a customer if it occurs due to any negligence or deficiency

[26] Jan Vishwas (Amendment of Provisions) Act, 2023 (formal repeal of s. 66A).

[27] Bharatiya Nyaya Sanhita, 2023, ss. 318 (cheating), 319 (cheating by personation) and 336 (forgery), in force 1 July 2024

[28] Mapping of IPC s. 419 to BNS s. 319 and IPC s. 420 to BNS s. 318(4); see CyberPeace, "The Data Behind India's Digital Fraud Surge" (11 March 2026).

[29] Bharatiya Nyaya Sanhita, 2023, s. 111 (organised crime).

[30] Bharatiya Nagarik Suraksha Sanhita, 2023, s. 94 (production and seizure of documents and electronic records) and provisions on audio-visual documentation of search and seizure.

[31] *William Stephen v. State of Tamil Nadu* (Supreme Court) (need for police training in handling electronic evidence).

by the bank itself, or arises from third-party breach reported within timeframe stipulated by RBI.[32] This circular rebalanced the fiduciary relationship by not requiring the victim to prove harm, but rather treating the institution as if it had to prove innocence. This framework has found active articulation in courts: the mere authentication of transactions through OTP was not sufficient where deep-rooted technical manipulation along with social engineering had been used to extract bank details and passwords from the victim, as demonstrated by the Delhi High Court's ruling in *Hare Ram Singh v. Reserve Bank of India*[33]; on the other hand, in *Suresh Chandra Negi v. Bank of Baroda*, mobile banking transactions that were self-initiated via a person whom they know through own net-banking credentials could not be converted into IT fraud under zero-liability policy, held Allahabad High Court.[34] Collectively these decisions carve out the unresolved boundary between true third-party breach, and customer fault.

Enforcement is institutionally layered. First-information reports are registered and field investigation carried out by state cyber-crime police stations; the Indian Cyber Crime Coordination Centre (I4C) set up under the Ministry of Home Affairs provides it overarching inter-agency coordination framework, capacity-building support, technical-tool development and real-time financial-fraud reporting and freezing.[35] through Section 70B of the IT Act, and not only identifies CERT-In as the national nodal agency for cyber-incident response but also empowers it to collect, analyse and disseminate threat information and conduct readiness exercises across sectors[36] by Section 70A establishes NCIIPC for protection of designated critical systems, which now expressly include core banking, payment and UPI infrastructure notified under successive Gazette orders.[37]

Table 2: Evolution of Legal Framework for Cyber-Fraud Investigation (2000-2024)

Legal Instrument	Year	Core Provision	Applicability to Cyber-Fraud	Key Limitation	Amendment/Successor
Information Technology Act, 2000 - Section 43	2000	Civil liability for unauthorized access	Establishes foundational e-crime framework	Slow civil process; lacks criminal teeth	Superseded by IT Act Sec. 66
Information Technology Act, 2000 - Section 66	2000	Criminal liability for dishonest/fraudulent conduct	Makes fraud via computer systems criminal offense	Narrowly interpreted by courts	Continues under BSA framework

[32] Reserve Bank of India, "Customer Protection — Limiting Liability of Customers in Unauthorised Electronic Banking Transactions," Circular DBR.No.Leg.BC.78/09.07.005/2017-18 (6 July 2017).

[33] *Hare Ram Singh v. Reserve Bank of India*, W.P.(C) 13497/2022 (Delhi High Court).

[34] *Suresh Chandra Negi v. Bank of Baroda*, Writ-C No. 24192 of 2022 (Allahabad High Court, 2025).

[35] Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C) framework.

[36] Information Technology Act, 2000, s. 70B (CERT-In as national nodal agency for cyber-incident response).

[37] Information Technology Act, 2000, s. 70A (NCIIPC); notification of banking, payment and UPI infrastructure as critical information infrastructure through successive Gazette orders

Information Technology Act, 2000 - Section 66C	2000	Identity theft via electronic signature/password misuse	Directly addresses OTP-interception and vishing	Limited scope to "unique identification features"	Continues under BSA framework
Information Technology Act, 2000 - Section 66D	2000	Cheating by personation via computer resource	Covers impersonation-based frauds	Jurisdictional delays in enforcement	Continues under BSA framework
Information Technology Act, 2000 - Section 66A	2000 - 2015	Offensive online content	Broad application to cyber-crime	**STRUCK DOWN** as unconstitutional (Shreya Singhal v. UoI)	Formally repealed by Jan Vishwas Act, 2023
RBI Circular on Customer Protection	2017	Zero-liability/limited-liability regime	Rebalances risk between bank and customer	Interpretive conflicts in judiciary (Hare Ram Singh v. RBI vs. Suresh Chandra Negi v. BoB)	Continues; awaits Supreme Court final word
Bharatiya Nyaya Sanhita, 2023 - Sections 318-319	2023	Cheating; aggravated cheating with dishonest delivery	Maps to old IPC Sec. 420/419; preserves precedent	Still requires proof of dishonest intention	Primary substantive offense for cyber-fraud
Bharatiya Nyaya Sanhita, 2023 - Section 1-11	2023	Organized crime offense	New provision enabling multi-actor mule-account prosecution	Requires proof of organized structure	Significantly strengthens prosecution toolkit
Bharatiya Nagarik Suraksha Sanhita, 2023 - Sections 91-94	2023	Production/seizure of documents and electronic records	Modernizes investigative powers; enables audio-visual recording of searches	Procedural compliance critical to admissibility	Mandatory compliance for forensic integrity
Bharatiya Sakshya Adhiniyam, 2023 - Section 61	2023	Electronic records equal to	Grants equivalent legal status to digital documents	Definition ambiguity re:	Primary evidentiary framework for cyber-fraud cases

		documentary evidence		"electronic records" scope	
Bharatiya Sakshya Adhiniyam, 2023 - Section 63	2023	Computer output admissibility via expert certification	Replaces contentious Sec. 65B of Indian Evidence Act, 1872	Hash-value certification requirement; interpretive tension on "copies"	Mandatory certification for secondary electronic evidence
Judicial Evolution: Anvar P.V. v. P.K. Basheer	2014	Certificate mandatory; source/authenticity as twin pillars	Established strict compliance doctrine for electronic evidence	Created conflicts with Shafhi Mohammad	Superseded by Arjun Panditrao
Judicial Evolution: Shafhi Mohammad v. State of Himachal Pradesh	2018	Relaxed certificate requirement where device not in possession	Provided exception for third-party evidence custody	Conflicted with Anvar P.V. precedent	Overruled by Arjun Panditrao
Judicial Evolution: Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal	2020	Reaffirmed certificate mandate; clarified device-owner exception	Decisively resolved conflict; clarified court-order mechanism for certificates	Remains subject to interpretive litigation on copies	Current binding precedent for electronic evidence admissibility

"Comparative legal framework analysis: mapping substantive and procedural cyber-fraud provisions from the Information Technology Act, 2000 (pre-2023 regime) to the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam (post-2023 regime). The table demonstrates legislative continuity while identifying substantive amendments and procedural modernisations introduced through the 2023 recodification. Particular attention is accorded to provisions governing identity theft, cheating by personation, organised crime, digital evidence admissibility, and certification requirements under Section 63, illustrating the statutory evolution."

4. Digital Forensics and Electronic Evidence in Cyber Fraud Cases

Digital forensics is the scientificbedrock upon which rests the entire investigatory and evidentiary superstructure incyber-fraud cases. Its core purpose is to discover, obtain, store, analyse and communicate electronic data in a way that retains its integrity and makes it admissible and compelling evidence in a

court of law.[38] In a context in which the offence typically gives rise to no tangible physical evidence, where the perpetrator may never be brought to justice in person, and where the only lasting memorial of the crime, its data trail is left behind, the prosecution's case rises or falls upon how soundly forensic foundations have been laid. Digital forensics thus has a significance that goes beyond the technical recovery: it is the process through which ephemeral digital actions are transformed into legally recognisable evidence of identity, behaviour and intention.

Digital Evidence in UPI and banking frauds are highly diversified spread across various custodians. These include, transaction logs and audit trails kept by banks and payment-service providers, records of beneficiary and mule accounts whereby the proceeds are funneled through; mobile-device artefacts such as SMS messages, application data, browsing history, and stored credentials in-browser. IP-address allocation and login metadata which may localise the offender down to a few feet, closed-circuit television (CCTV) footage from an automated teller machine used at cash-out stage. Finally, telecom records capable of establishing the fact & timing of a SIM-swap event.[39] For any of these sources to be relied upon as evidence, it must be obtained lawfully from the appropriate custodian, satisfactorily attributed to an identifiable actor and linked in time to the impugned transaction. The disciplined gathering, securing and examination of such material must be consistent with accepted technical standards for sound forensic methodology. Volatile data that could be overwritten or erased in the 10 seconds after an incident, for example, needs to be collected as soon as possible and original storage device must be forensically imaged so that analysis takes place on a copy only; finally authenticity and integrity of captured data need to have been verified via cryptographic *hash values* which act like digital fingerprints revealing any modification by even a single bit thereafter.[40] Likewise essential is that there be an unbroken chain of custody a record that tracks each individual who handles the evidence and details the circumstances of each transfer; any unexplained break in that chain invites speculation about tampering, with serious negative consequences for the admissibility and weight to be afforded to the evidence. Mishandling at any level along that chain, no matter how inconsequential it may seem has the potential to destroy the evidentiary value of an entire forensic endeavor.[41]

Much of the evidentiary regime concerning this material has been extensively reshaped by the Bharatiya Sakshya Adhiniyam, 2023 (BSA) which repealed the Indian Evidence Act, 1872. Under section 2(1)(d) electronic and digital records (including email, server logs, messages and documents stored on computer systems, laptops and smartphones) are directly included within the definition of "document", giving them

[38] Standard digital-forensics literature on identification, preservation, analysis and presentation of electronic evidence

[39] Compiled from RBI, *BE(A)WARE* (2022) and I4C investigative guidance on sources of digital evidence

[40] Corpotech Legal, "Admissibility of Electronic Evidence, Certificate and Hash Value under Section 63 BSA" (2024) (hash values verify integrity and detect tampering).

[41] National judicial-academy training materials on chain of custody for electronic and digital records (2024)

equivalent status to standard documentary evidence.[42] Section 61 asserts that electronic or digital record cannot be denied admissibility on the ground that it is in electronic form and gives equal legal effect, validity and enforceability to such record as any document Subordinate to Section 63.[43] Information in the form of "computer output" which is an admissible document and may be produced in evidence without proving its contents or producing the original, and is governed by Section 63, the reader would note that section 89 deals with digital documents being a successor to the highly litigated provision of section 65B under old Act.[44] Significantly, the Schedule mandates that on every occasion when an electronic record is tendered, accompanying it shall be a certificate. Which must now be signed not only by the person in charge of the computer or communication device but also by an expert; and there is provision of hash value to secure integrity.[45] There is some interpretive tension in that the explanation for Section 57 treats specific originals and copies of electronic records as primary evidence, but it still raises whether or not those specified copies must always pass through the Section 63 certification route, but then again, the non-obstante clause in Section 63(1) suggests that we continue to be ruled by *Arjun Panditrao* logic even with respect to copies.[46]

The judicial approach to admissibility has evolved through a clearly discernible arc that any investigator must understand. In *State (NCT of Delhi) v. Navjot Sandhu*, the Supreme Court initially permitted electronic records to be proved through secondary evidence without strict compliance with the certificate requirement.[47] That permissive position was decisively reversed by a three-judge bench in *Anvar P.V. v. P.K. Basheer*, which held that the certificate is a mandatory condition precedent to the admissibility of secondary electronic evidence, and that source and authenticity are the twin pillars of such evidence.[48] A subsequent two-judge decision in *Shafhi Mohammad v. State of Himachal Pradesh* relaxed this requirement where the party tendering the evidence was not in possession of the device,[49] creating a conflict that was finally resolved in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*. There, the Court conclusively reaffirmed the mandatory nature of the certificate, overruled *Shafhi Mohammad*, and clarified the important practical exception that no certificate is required where the original device is itself produced and proved by its owner, while also providing a mechanism to seek the certificate by court order where a party cannot procure it.[50] This line is reinforced by *Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao*

[42] Bharatiya Sakshya Adhiniyam, 2023, s. 2(1)(d) (definition of "document" includes electronic and digital records).

[43] Bharatiya Sakshya Adhiniyam, 2023, s. 61.

[44] Bharatiya Sakshya Adhiniyam, 2023, s. 63 (admissibility of electronic records / computer output).

[45] Bharatiya Sakshya Adhiniyam, 2023, s. 63(4) and the Schedule (two-part certificate by device-in-charge and expert, incorporating hash value).

[46] Bharatiya Sakshya Adhiniyam, 2023, s. 57, Explanations 4–7; SCC Online, "Electronic Evidence in Focus: Navigating Legal Shifts under the BSA, 2023" (23 October 2024).

[47] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600 (overruled on this point)

[48] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

[49] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801 (overruled).

[50] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

Phalke, emphasising source and authenticity[51] by *Sonu @ Amar v. State of Haryana*, on the stage at which objections to the mode of proof must be raised[52] by *P. Gopalkrishnan v. State of Kerala*, recognising stored video footage as a "document" of which a cloned copy must be furnished to the accused[53] and by *Tukaram S. Dighole v. Manikrao Shivaji Kokate*, which insists that the standard of proof for electronic evidence be more accurate and stringent than for ordinary documents.[54] The cumulative effect of this jurisprudence is to subordinate the admissibility of cyber-fraud evidence to demanding procedural discipline, so that forensic and certification failures, rather than the absence of culpable conduct, frequently determine the outcome of a prosecution.

5. Challenges and the Way Forward

Notwithstanding this elaborate framework, the investigation of cyber frauds confronts persistent and interlocking obstacles. The technical challenges are formidable: digital traces are volatile and easily deleted; offenders routinely employ virtual private networks, encrypted messaging channels, anonymised payment rails and disposable virtual identities; and investigators face chronic delays in securing records from banks, payment aggregators, telecom operators and intermediaries, by which time crucial data may have been purged.[55] Jurisdictional and cross-border issues are especially acute. Proceeds are layered within seconds across mule accounts spread over multiple states, and a substantial proportion of the most damaging frauds are orchestrated from organised scam compounds located abroad, particularly in South-East Asia, placing the perpetrators beyond the immediate reach of domestic process and necessitating slow and uncertain mutual-legal-assistance procedures.[56]

Privacy, encryption and data-access concerns introduce a genuine constitutional tension between the investigative imperative to access communications and devices and the fundamental right to privacy recognised in *K.S. Puttaswamy v. Union of India*, now reinforced by the data-minimisation and purpose-limitation safeguards of the Digital Personal Data Protection Act, 2023; lawful access must therefore be proportionate rather than indiscriminate.[57] The capacity constraints of cyber-forensic laboratories compound these difficulties: laboratories operate with heavy backlogs and limited specialised personnel, and many investigators and prosecutors lack the technical training to acquire, interpret and present digital evidence competently, which contributes directly to low conviction rates.[58] The way forward demands a coordinated programme of legal, institutional and technological reform: the adoption of uniform forensic

[51] *Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke*, (2015) 3 SCC 123.

[52] *Sonu @ Amar v. State of Haryana*, (2017) 8 SCC 570.

[53] *P. Gopalkrishnan v. State of Kerala*, (2020) 9 SCC 161.

[54] *Tukaram S. Dighole v. Manikrao Shivaji Kokate*, (2010) 4 SCC 329 (stricter standard of proof for electronic evidence).

[55] Press Information Bureau, *Curbing Cyber Frauds in Digital India* (8 October 2025) (technical and procedural challenges).

[56] *InsightsonIndia*, "Cybercrime in India 2025" (21 February 2026); links to scam compounds in South-East Asia.

[57] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1; Digital Personal Data Protection Act, 2023.

[58] National Crime Records Bureau, *Crime in India* data on enforcement and conviction; capacity constraints of cyber-forensic laboratories

standards and certified procedures. Faster, structured data-sharing protocols between banks, telecom operators and law-enforcement agencies, the establishment of dedicated cyber courts and specialised prosecution cells. The use of tamper-proof, potentially blockchain-based, evidence-storage systems and sustained investment in training and laboratory infrastructure all directed at strengthening every link in the chain from detection to conviction.[59]

6. Conclusion

This Study finds that although India's transition to a UPI dominated digital economy is a tremendous progress in public digital infrastructure, there is also an upsurge of cyber enabled financial crimes in terms of loss and substantial volume of complaints. The study shows that those types of frauds are not necessarily the result of loopholes in the technological system but rather the result of social engineering, deception and organised cybercrime networks. The big investigative challenge is thus establishing human intent, following digital evidence and linking fragmented cyber trails across jurisdictions. The analysis also finds that while India has a robust legal and forensic framework, such as the Information Technology Act, Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam, RBI regulations, and jurisprudence on electronic evidence, it is still largely ineffective because of delays, limited forensic capabilities, difficulties in jurisdiction and unevenness in enforcement. An integrated approach is needed in addressing the issue of sustainable action for regulators, financial institutions, telecom agencies, cybercrime units, forensic laboratories, and courts, with a coordinated real-time action with regards to detection, prevention, investigation, and prosecution. Investing in cyber-forensic capabilities, building up prevention and deterrent measures (like the helpline 1930, suspect registries, mule-account monitoring), and streamlining the collection and handling of electronic evidence can greatly contribute to cyber resilience. In conclusion, safeguarding India's digital economy requires robust legal frameworks as well as efficient institutional collaboration, technological advancements, and a proactive approach to preventing cybercrime, rather than reactive recovery.

Cite this Article:

***Shilpa KL & Dr. Manindra Singh Hanspal, "Investigation of Cyber Frauds in India: Legal and Digital Forensic Challenges in the Era of UPI and Online Banking"**, Aviradha International Journal of Law and Legal Studies (AIJLLS), ISSN: 3139-3179 (Online), Volume 2, Issue 3, pp. 12-25, April-June 2026.*
Journal URL: https://aijlls.com/

DOI: https://doi.org/10.65785/aijlls.v2i3.17

[59] Press Information Bureau, *Curbing Cyber Frauds in Digital India* (8 October 2025) (recommended legal, institutional and technological reforms).