INTEGRATION OF INDIA'S MULTI-STAKEHOLDER RESPONSE TO DIGITAL ARREST SCAMS: LAW ENFORCEMENT, NPCI, AND INTERNATIONAL COOPERATION

K Aakash Jayandan, Guest Faculty, Department of Public Administration, Sree Vivekananda College, Kunnamkulam, Thrissur, Kerala, India

Aalan Joe Edwin J J, Practicing Advocate, District Court, Nagercoil, Tamilnadu, India

ABSTRACT

Digital arrest scams have emerged as one of the most alarming forms of cyber-enabled fraud in India, exploiting fear, impersonation, and real-time payment systems to coerce victims into transferring money. This paper examines India's multi-stakeholder response to digital arrest scams by integrating three critical domains: law enforcement, financial systems led by the National Payments Corporation of India (NPCI), and international cooperation frameworks. Using a structural-conceptual methodology, the study systematically reviews secondary data from government portals, RBI advisories, NPCI circulars, legal frameworks under the IT Act and Bharatiya Nyaya Sanhita, and international cybercrime cooperation models. A layered conceptual model is proposed, comprising four functional tiers—detection and reporting, coordination and data exchange, enforcement and prosecution, and prevention and awareness—mapped to the roles of I4C, NPCI, state cyber cells, telecom regulators, and Interpol. The findings reveal that while initiatives such as the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), helpline 1930, and NPCI-led advisories have enhanced reporting and facilitated partial recovery of defrauded funds, significant challenges persist. These include fragmented coordination between central and state agencies, delays in FIR registration, inconsistent real-time transaction blocking, and slow cross-border legal assistance. The paper highlights the need for secure API-driven data-sharing infrastructure, streamlined FIR and evidence admissibility procedures, and enhanced capacity building for cyber forensics. Internationally, faster mutual legal assistance processes and expanded participation in joint operations such as INTERPOL's HAECHI are recommended. The study concludes that an integrated, proactive, and victim-centric model can transform India's approach from reactive to preventive, reducing financial losses, strengthening public trust, and positioning India as a global leader in

cybercrime response. Future research should empirically validate the model through stakeholder interviews, victim surveys, and forensic case studies to refine operational effectiveness.

Keywords: Digital Arrest Scams, Cybercrime Prevention, Law Enforcement, National Payments Corporation of India, and International Cooperation

Introduction

Digital arrest is a scam that uses intimidation, lies, and terror to extract money from victims. Fraudsters pose as law enforcement officers and threaten victims with arrest, bank account freezing, and passport cancellation in order to get them to pay a "fine" or "security deposit" in order to avoid going to court (Major Sadhna Singh, 2024). A digital arrest fraud is, to put it simply, an internet swindle. In this scam, con artists deceive victims into believing that law enforcement or government officials have detained them (Arora, 2025). To make people think they are in real legal jeopardy, they utilise phoney paperwork, phoney video calls, and other tactics.

The scam often starts with a phone call that is ordinary and can range from a request for KYC verification to receiving a minor parcel delivery (Union Bank of India, 2024). After some fear, as they gain familiarity with the victim, the fraudster tends to become more assertive when offering the emotional reasons for the request, and often alleges the victim has some form of connection with significant crimes, such as drug trafficking, money laundering, or cybercrime (Union Bank of India, 2024). The scammers all provided legitimacy by using false documents, edited videos, and sometimes spoof phone numbers to convince victims to comply with their requests.

Modus Operandi:

- The Scammers/Cheaters pretend to act like law enforcement or government officials (Police, ED, CBI, Interpol, Customs, etc.) via emails, phone calls, WhatsApp messages, or fake official letters.

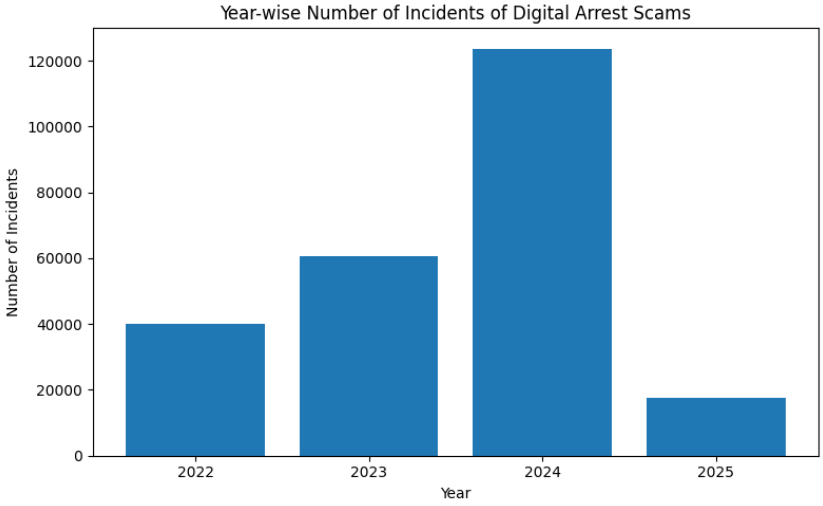
- Scammers then create a panic to tell the victim of a supposed arrest warrant in the victim's name for tax evasion, customs violations, or other violations like pornography, unauthorized site usage, etc…,

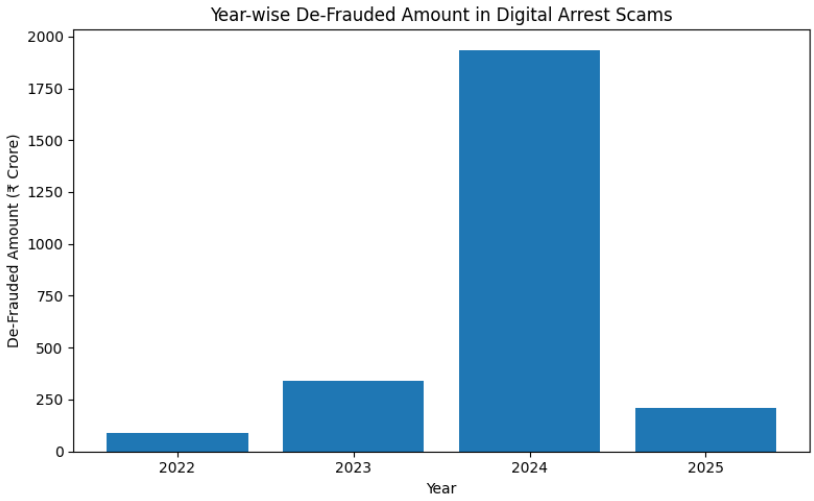
- To show credibility to the victim, the scammers send fake documents, fake videos, or fake arrest warrants, making the claim as real. And they threatened the victim not to approach the advocate.

- Then the scammers forced the victims to turn on a video call through WhatsApp or Skype to make the interaction look real. Scammers will set up a fake police station to convince the victim to gain trust.

- Then, the Scammers say something like, "Let's settle the matter," and pressure the victim to pay money through the UPI ID or cryptocurrency, or prepaid gift cards, or bank transfer to avoid arrest.

- Once the victim paid the amount, the scammers disappear immediately and leaving the victim to realize he has been deceived and cheated, and that situation was not real.





The data, sourced from the National Cyber Crime Reporting Portal and made available through data.gov.in , shows a sharp year-on-year escalation in digital arrest scam activity, with 2022 serving as the baseline. In 2022, there were 39,925 reported incidents, leading to a total de-frauded amount of ₹91.14 crore. This figure almost doubled in 2023, with incidents rising to 60,676 and losses climbing more than three-fold to ₹339.03 crore, indicating that scams became both more frequent and more financially damaging. The situation worsened dramatically in 2024, which recorded 123,672 incidents—more than double the previous year—and a staggering ₹1,935.51 crore in losses, suggesting either higher value transactions were targeted or victim compliance increased due to more sophisticated social-engineering tactics. Interestingly, the partial data available for 2025 already reports 17,718 incidents and ₹210.21 crore in losses, which—if extrapolated—could indicate either a moderating trend due to stronger counter-measures or simply incomplete reporting for the year. Overall, the "Number of Incidents" represents the count of reported digital arrest scam cases, while the "De-Frauded Amount (in Crore)" quantifies the total monetary losses suffered by victims in each year. Together, these metrics highlight both the scale and economic impact of the crime over time.

A multi-stakeholder response is critical because digital arrest scams operate at the intersection of law, finance, technology, and international borders. Legal measures alone are not enough even if a police case is registered, money can be siphoned off in seconds through instant payment systems, mule accounts, or cross-border transfers (The Financial Express, 2025). Without real-time financial safeguards, such as the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) and NPCI-led dispute resolution frameworks, victims would have no practical way to freeze fraudulent transactions before funds disappear (TechGig, 2025). Moreover, digital arrest scams often exploit telecom networks (via spoofed calls, VoIP, or encrypted messaging), which means telecom operators and regulators like DoT must actively block spoofed caller IDs, disable fraudulent SIMs, and provide citizens with tools like Sanchar Saathi/Chakshu to report scam communications (Xiong & Qiu, 2024). Finally, because many of these scams originate from overseas call centres or scam hubs, global cooperation is essential. Agreements like the MoU between India's I4C and U.S. Homeland Security Investigations enable intelligence sharing, coordinated takedowns, and faster legal assistance across borders (Policy Circle, 2024).

Despite the rising incidence of digital fraud in India, there is limited academic work examining how stakeholders coordinate to counter scams such as digital arrest. Existing studies

focus mainly on technical solutions, legal provisions under the IT Act and IPC, or awareness campaigns by institutions like RBI and CERT-In. What remains underexplored is a comprehensive assessment of coordination among law enforcement agencies, financial regulators (RBI, NPCI), telecom providers, international policing bodies, and private technology platforms. While international models such as the UK's National Economic Crime Centre and Europol's EC3 highlight the benefits of joint task forces and shared fraud registries, similar research in the Indian context is scarce. Initiatives like the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), I4C's Cyber Crime Coordination Centre, and NPCI's UPI fraud prevention protocols are rarely studied collectively, and India's participation in global mechanisms such as JCCTs and Interpol's Cyber Fusion Centre remains under-evaluated. This article addresses this gap by offering a multi-stakeholder analysis of India's response to digital arrest scams and proposing recommendations to strengthen integrated, scalable response mechanisms.

Literature Review

In the period of the digital era, the form of crimes also evolved, and the criminals too are adopting the new technology to commit different kinds of crimes. In the era of AI, it's very easy for scammers to commit cybercrime against a person using the technology. Among those, one is cybercrime. Cybercrime includes phishing, hacking, data theft, virus attacks, ransom ware, etc. In this list, the new one is digital arrest. This article is trying to integrate Law Enforcement, National Payments Corporation of India, and International Cooperation for better response to digital arrest scam.

This paper is trying to make a conceptual framework that will help in better response to digital arrest by reviewing the body of literature already written on this topic. The NITI Aayog India's think tank has released a report "Digital Arrest: The Modern-Day Cyber Scam by Major Sadhna Singh, Consultant, NITI Aayog. (n.d.). Retrieved August 2, 2025, from https://www.niti.gov.in/node/1642 details I4C's efforts to integrate state cyber cells, establish the National Cyber Crime Reporting Portal, and facilitate Joint Cybercrime Coordination Teams (JCCTs), which have played critical roles in detecting and blocking fraudulent digital assets such as SIM cards, bank accounts, and messaging handles" (Major Sadhna Singh, 2024).

The article "The Case of "Digital Arrest Scam": Cybercrimes In India And Its Ordeal-Crime-India.(2024). Retrieved September 6, 2025, from

https://www.mondaq.com/india/crime/1607658/the-case-of-digital-arrest-scam-cybercrimes-in-india-and-its-ordeal - provides a structural overview of tools such as the Suspect Registry, Financial Cyber Fraud Reporting and Management System (FCFRMS), and telecom coordination efforts that allow for real-time response " (Mondaq, 2024). From the legal perspective, this article "Digital Arrest Scams In India: A New-Age Cyber Threat and A Growing Concern » Lawful Legal. (2024). Retrieved September 6, 2025, from https://lawfullegal.in/digital-arrest-scams-in-india-a-new-age-cyber-threat-and-a-growing-concern/ - notes that while the Information Technology Act, 2000 and the Indian Penal Code address fraud and impersonation, they do not explicitly define or penalize coercive digital arrest scams" (LawfulLegal, 2024). On the financial ecosystem this article "*Digital Arrest Frauds on Rise: NPCI Cautions People on How to Identify and Protect Themselves from Frauds*. Retrieved September 6, 2025, from https://economictimes.indiatimes.com/news/india/digital-payment-agency-npci-highlights-common-tactics-used-by-fraudsters-shares-tips-to-stay-safe/articleshow/116365462.cms with was published in Economic Times document's NPCI's scam-prevention advisories, which aim to increase public awareness about common fraud tactics and provide clear reporting pathways " (The Economic Times, 2024). Finally "The Interpol Global Cybercrime Conference 2023 - advisories and Cybercrime Directorate reports highlight the global dimension of such frauds, stressing the importance of cross-border cooperation. Operations such as HAECHI-III and First Light demonstrate that coordinated intelligence sharing and rapid asset-freezing through mechanisms like the Anti-Money Laundering Rapid Response Protocol (ARRP) can be effective " (Interpol, 2023).

These studies point to a critical gap in the literature: the absence of a fully integrated conceptual model that links law enforcement, financial networks (NPCI and banks), and international cooperation frameworks into a unified response system. This paper seeks to bridge this gap by proposing a structural model that maps these interactions and identifies opportunities for strengthening coordination and response in India.

Methodology

This study employs a structural-conceptual methodology to analyze and propose an integrated multi-stakeholder response to digital arrest scams in India. The methodology proceeds in three interrelated stages.

The secondary data was systematically reviewed. These included news reports, RBI

guidelines, case law under the Information Technology Act and Bharatiya Nyaya Sanhita (BNS), government advisories, Ministry of Home Affairs (MHA) policy documents, National Payments Corporation of India (NPCI) circulars, international cybercrime frameworks like the Budapest Convention, and Interpol advisories. A thorough grasp of the institutional functions of law enforcement, participants in the financial system, and foreign partners was established by this review.

In order to determine the main nodes and connections inside the response network, a structural mapping exercise was conducted. A multilayered system was envisioned with law enforcement organisations (I4C, state cyber cells, JCCTs), financial institutions (NPCI, banks, payment service providers), and international stakeholders (Interpol, CERT equivalents, foreign law enforcement) as nodes. Structural relationships were used to depict their interactions, which included victim reporting, transaction blocking, sharing of evidence, coordinating investigations, and awareness programs.

On the basis of this mapping, a conceptual integration model was created. (i) detection and reporting; (ii) coordination and data exchange; (iii) enforcement and prosecution; and (iv) prevention and international collaboration comprise the four functional layers that make up the model. By visualising information flows, decision points, and feedback loops across layers, the structural approach makes it possible to identify areas with strong integration and those that need work.

Conceptual Framework

In order to combine detection, coordination, enforcement, and prevention functions across law enforcement, NPCI, and international partners, the suggested model conceptualises India's multi-stakeholder response to digital arrest frauds as a layered and linked system. The structural elements and interactions depicted in the model are explained in this section.

Detection - The model specifies several entry points at the detection and reporting layer where a scam can be reported, including telecom surveillance of spoof calls, real-time fraud detection by NPCI and banks, and victim reports via the National Cybercrime Reporting Portal or helpline 1930. The Indian Cyber Crime Coordination Centre (I4C), the main national centre for cybercrime intelligence, is linked to these nodes (NITI Aayog, 2025).

Coordination - I4C and the Joint Cybercrime Coordination Teams (JCCTs), which compile

information from telecom operators, state police, and NPCI, serve as representatives of the coordination and data exchange layer. Secure data-sharing interfaces facilitate inter-state and inter-agency cooperation and enable the prompt freezing of problematic transactions. This layer is essential for establishing a cohesive operating picture and avoiding jurisdictional delays (Mondaq, 2024).

Enforcement - A uniform investigative workflow connects state cyber cells, local police, and central agencies like the Central Bureau of Investigation (CBI) at the enforcement and prosecution layer. This part of the model focusses on cross-jurisdictional FIR registration, standardisation of digital evidence collecting, and court admissibility of electronic records—all of which are necessary for a successful prosecution (LawfulLegal, 2024).

International Cooperation - India's cooperation with worldwide cybercrime networks, such as Interpol's Cybercrime Directorate, Mutual Legal Assistance Treaties (MLATs), and bilateral agreements with nations that host scam call centres, is represented by the international cooperation layer. This layer makes sure that intelligence is shared promptly, that actions are coordinated, and that cross-border scam networks are disrupted (Interpol, 2023).

Prevention - NPCI advisories, RBI rules, and public campaigns like MHA's Cyber Dost effort are all connected into a single communication framework by the prevention and awareness layer. By coordinating communications across media, law enforcement, and financial institutions, this layer seeks to increase public awareness and lessen vulnerability to frauds (The Economic Times, 2024).

Discussion

The suggested layered conceptual approach aims to create a structurally integrated framework for India's currently disjointed response to digital arrest frauds, involving law enforcement, financial institutions, and foreign partners. This rethinking highlights the interdependence of detection, coordination, enforcement, and prevention in order to develop a system that can handle the intricacy of international cybercrime.

Law enforcement integration exhibits both possibilities and constraints. While saving crores of rupees, the Indian Cyber Crime Coordination Centre (I4C) has centralised coordination through tools like Joint Cybercrime Coordination Teams (JCCTs) across hotspot

regions and has blocked over 1,700 Skype IDs, 59,000 WhatsApp accounts, SIMs, and IMEIs used in scams. However, because of irregular interagency contact between central organisations and state cyber cells, delays in filing FIRs and freezing accounts frequently continue. In order to effectively and swiftly disable scammers, interoperability and quicker evidence sharing are still essential.

The National Payments Corporation of India (NPCI) is an important player in the Financial System & NPCI space. Its advisories have played a key role in raising awareness by pointing up warning signs such phoney official calls, fear mongering, and urgent payment demands. They have also urged victims to report suspicious behaviour to the telecom portal or helpline 1930. More comprehensive data also demonstrates corrective action, with the Financial Cyber Fraud Reporting System Business Standard barring over 6.69 lakh SIMs and 1.32 lakh IMEIs and aiding in the recovery of over ₹3,431 crore. The effectiveness of reaction is still limited by the inconsistency in communication between law enforcement and the financial ecosystem about real-time transaction blockage and quick victim support.

India's involvement in worldwide law enforcement operations has made significant contributions to international cooperation. For example, operations such as INTERPOL's HAECHI and First Light have resulted in international arrests and the freezing of illicit assets under the Anti-Money Laundering Rapid Response Protocol. More importantly, India's recently developed Bharatpol portal under the CBI allows for real-time coordination with Interpol, accelerating access to global notices, extradition help, and logistical support in cyber investigations. Despite these advances, obstacles remain: MLAT processes are slow, bilateral agreements with scam-hosting countries are restricted, and prosecuting abroad criminals under Indian law lags behind.

This leads to systemic gaps in integration. The response system now operates in silos, with fragmented legal and procedural frameworks, poor technical integration, and insufficient mutual awareness preventing quick action. For victims, this frequently translates into complexity—delayed FIRs, inconsistent transaction redress, and slow public messaging all contribute to ongoing losses. Between January and May 2025, digital arrest frauds in Pune caused ₹9.21 crore in damages, despite increased awareness initiatives. This emphasises the necessity for a united, centralised structure that can act on detection, enforcement, prevention, and international interaction.

There are numerous opportunities to strengthen the model. Technically, creating secure API links between I4C, NPCI, banks, and telecom authorities can allow for real-time flagging and freezing of suspicious accounts. Legally, simplifying FIR rules and improving digital evidence admissibility could reduce investigative latency. Institutionally, increasing capacity through expanded forensic infrastructure, training, and financing will strengthen enforcement. Internationally, fast-track treaties, increased participation in INTERPOL operations, and optimised platforms such as Bharatpol can encourage cross-border prosecutions. Preventively, incorporating fraud alerts into UPI apps and conducting regional-language awareness campaigns can effectively reach underprivileged groups.

From a policy standpoint, implementing an integrated model has strategic benefits. It contributes to national cybercrime strategy by providing a proactive, coordinated, and victim-centered response. Multi-agency coordination yields scalable effects, including discouraging repeat offenders and increasing public trust. Furthermore, the model serves as a core framework for future academic and policy research, providing a baseline for evaluating the efficacy of integrated digital crime prevention systems. Finally, the scope of this study is limited. The model is built on secondary literature, advisory, and structural mapping rather than primary, field-collected empirical data. To enhance this paradigm, future research should include primary stakeholder interviews, victim surveys, and forensic case studies to validate linking dynamics and operational effectiveness.

Legal Framework for Digital Arrests

a) Constitutional Provisions:

- **Article 20 (3**) protects individuals from self-incrimination. In the context of digital arrest, this means that individuals cannot be compelled to provide passwords or other information that could be used against them in a criminal proceeding.

- In the landmark ruling of **Justice K.S. Puttaswamy v. Union of India**[1]The Supreme Court recognised the right to privacy as a fundamental right under the Indian Constitution - it expressly stated that under Article 21, the right to privacy is part of the right to life and personal liberty. Restrictions of any digital

[1] AIRONLINE 2018 SC 237

arrest must apply the principles of proportionality that do not infringe on the privacy rights of people. **The Personal Data Protection Bill, 2019,** promotes a broader regime concerning the protection of individuals' personal data in India in addition to the constitutional right to privacy. The Bill includes provisions on consent, data processing, and more broadly, data rights that are relevant to the construction of digital arrest.

b) Information and Technology (IT) Act, 2000 –

- **Section 66C. Punishment for identity theft. –**Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment which may extend to **three years and shall also be liable to fine which may extend to rupees one lakh**[2]

- **Section 66D. Punishment for cheating by personation by using computer resources. –**Whoever, using any communication device or computer resource, cheats by personation, shall be punished with imprisonment of either description for a term which may extend **to three years** and shall also be liable to a fine which may extend to **one lakh rupees**[3]**.**

- **Section 72** speaks about the Penalty for Breach of confidentiality and privacy[4].

c) The Bhartiya Nyaya Sanhita (BNS)Provisions:

- **Section 111** addresses organized crime and its penalties. It entails engaging in any illegal conduct, **including cybercrimes**, either alone or in concert. Organized crime syndicates are also covered.

- **Section 318 of BNS,2023(IPC 415), speaks about cheating and its punishments**.

- Section 318(1) - Whoever, by **deceiving any person, fraudulently or**

[2]https://www.legalserviceindia.com/legal/article-16939-identity-theft-and-indian-laws.html
[3] ibid
[4] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

> **dishonestly induces the person** so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is **likely to cause damage or harm to that person in body, mind, reputation or property, is said to "cheat"[5].**

Conclusion

The emergence of digital arrest scams highlights the increasing sophistication of cyber-enabled fraud and the critical need for an integrated, multi-stakeholder response in India. This study proposed a structural model that connects three essential domains—law enforcement, financial systems led by the NPCI, and international cooperation—to demonstrate how collaboration may turn the present fragmented response into a unified, real-time ecosystem.

According to the analysis, India has taken important measures to counter the threat: NPCI advisories have raised public awareness, the Indian Cyber Crime Coordination Centre (I4C) and 1930 helpline have enhanced reporting and coordination, and India's increasing involvement in international operations like Interpol's HAECHI has made cross-border enforcement possible. However, there are still issues with state and federal law enforcement agencies' inability to communicate with one another, delays in banning financial transactions, and sluggish procedures for exchanging legal aid with other countries.

The creation of a secure API-driven data-sharing interface between I4C, NPCI, banks, and telecom operators is suggested in this paper as a solution to these issues. It also suggests expediting the filing of FIRs and the admissibility of evidence for cybercrimes, establishing interagency task forces, and extending bilateral agreements with nations that are known to engage in scams in order to facilitate quicker extradition and evidence sharing. Public-facing approaches, such as implementing victim-centric compensation systems, conducting multilingual awareness programs, and directly integrating scam alarms into UPI apps, are equally important.

By implementing this integrated paradigm, India may shift from a reactive to a

[5] https://devgan.in/bns/section/318

proactive posture, reducing financial losses, increasing public trust, and positioning itself as a global leader in cybercrime prevention. Future research should focus on empirically testing the model using stakeholder interviews, victim surveys, and forensic case studies, allowing for continuous refinement of the national cybercrime response system.

Reference

1. CFCFRMS prevents ₹600 crore scams, sets benchmark | TechGig. (n.d.). Retrieved September 6, 2025, from https://content.techgig.com/technology/cfcfrms-prevents-600-crore-scams-sets-benchmark/articleshow/105374313.cms

2. Digital Arrest: The Modern-Day Cyber Scam by Major Sadhna Singh, Consultant, NITI Aayog. (n.d.). Retrieved August 2, 2025, from https://www.niti.gov.in/node/1642

3. Digital Arrest: Trends, Tactics & Safety Measures-Union Bank Of India. (n.d.). Retrieved September 6, 2025, from https://www.unionbankofindia.co.in/en/blog/Digital-Arrest-Understanding-Modus-Operandi-Current-Trends-and-Safety-Tips

4. Digital arrest frauds on rise: NPCI cautions people on how to identify and protect themselves from frauds - The Economic Times. (2024). https://economictimes.indiatimes.com/wealth/save/digital-arrest-frauds-on-rise-npci-cautions-people-on-how-to-identify-and-protect-themselves-from-frauds/articleshow/116290568.cms?utm_source=chatgpt.com&from=mdr

5. DIGITAL ARREST SCAMS IN INDIA: A NEW-AGE CYBER THREAT AND A GROWING CONCERN » Lawful Legal. (n.d.). Retrieved September 6, 2025, from https://lawfullegal.in/digital-arrest-scams-in-india-a-new-age-cyber-threat-and-a-growing-concern/

6. Interpol. (2023). INTERPOL GLOBAL CYBERCRIME CONFERENCE 2023 "CREATING COMMUNITIES TO PROTECT COMMUNITIES" Outcome Report.

7. Major Sadhna Singh. (2024). Digital Arrest: The Modern-Day Cyber Scam. Table 10, 4–6. https://securitylinkindia.com/eMagazine/February2025.php

8. Massive spike in digital arrest scams,cybercrimes almost tripled: Govt - India News | The Financial Express. (n.d.). Retrieved September 6, 2025, from https://www.financialexpress.com/india-news/massive-spike-in-digital-arrest-scamscybercrimes-almost-tripled-govt/3775959/?utm_source=chatgpt.com

9. The Case Of "Digital Arrest Scam": Cybercrimes In India And Its Ordeal - Crime - India. (n.d.). Retrieved September 6, 2025, from https://www.mondaq.com/india/crime/1607658/the-case-of-digital-arrest-scam-cybercrimes-in-india-and-its-ordeal

10. The digital fraud epidemic calls for stronger cybersecurity measures | Policy Circle. (n.d.). Retrieved September 6, 2025, from https://www.policycircle.org/policy/why-are-digital-frauds-rising/?utm_source=chatgpt.com

11. Xiong, Y., & Qiu, M. (2024). Research on the Criminal Law Response to Telecom Fraud in the Digital Society. Economics, Law and Policy, 7(3), p33. https://doi.org/10.22158/elp.v7n3p33

12. Bharatiya Nagarik Suraksha Sanhita (BNSS)

13. The Bharatiya Nyaya Sanhita, 2023 (BNS)

14. Information and Technology Act, 2000.

15. AIR 2018 SC 237. (2018). Supreme Court of India. Retrieved from https://www.aironline.in/legal-judgements/AIR+2018+SC+237

16. Tare, P. (n.d.). Identity Theft and Indian Laws. Legal Service India. Retrieved September 8, 2025, from https://www.legalserviceindia.com/legal/article-16939-identity-theft-and-indian-laws.html

17. Information Technology Act, 2000, Act No. 21 of 2000 (India). Retrieved from https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

18. Devgan, R. (n.d.). Section 318 – Cheating. *Bharatiya Nyaya Sanhita, 2023.* Retrieved September 8, 2025, from https://devgan.in/bns/section/318