DIGITAL ARREST SCAMS IN INDIA: CHALLENGES AND SOLUTIONS WITH SPECIAL REFERENCE TO KARNATAKA

Dr. R. N. Mangoli*[1]

**Professor, Department of Criminology and Forensic Science, Rani Channamma University, Belagavi, Karnataka, India.*

****Corresponding author***
mail id - drmangoli.rn@rcub.ac.in

Abstract

The digitization of India's economy and public services has been paralleled by a surge in sophisticated cybercrimes. Among the most pernicious is "Digital Arrest," a hybrid psychological and financial fraud that leverages authority impersonation and digital isolation to extort victims. This study provides a comprehensive analysis of Digital Arrest scams in India, with a focused investigation into Karnataka State, a leading tech hub disproportionately targeted by such crimes. This research employs a mixed-methods approach, analyzing secondary data from the National Crime Records Bureau (NCRB), the Indian Cyber Crime Coordination Centre (I4C), and Karnataka Police reports from 2020 to 2024. A systematic review of news reports, victim testimonials, and advisories from the Ministry of Home Affairs was conducted to deconstruct the modus operandi. The study synthesizes this metadata to quantify economic losses, identify victim demographics, and map the operational infrastructure of these scams.

The analysis reveals a dramatic increase in Digital Arrest cases, with reported losses exceeding ₹200 crore nationally in 2023-24. Karnataka, particularly Bengaluru, emerges as a major hotspot, accounting for nearly 20% of high-value cases. The modus operandi is highly organized, involving spoofed calls from fake law enforcement IDs, the use of deepfake technology for intimidation, and real-time psychological manipulation to keep victims in a state of coerced compliance. The primary challenges identified include jurisdictional complexities, the use of encrypted cross-border communication, insufficient cyber literacy among the general public, and the rapid evolution of social engineering tactics.

Digital Arrest represents a critical threat to national security and individual financial safety. Combating it requires a multi-pronged solution framework. This paper proposes a consolidated strategy involving ***Technology*** *(AI-driven detection of spoofed calls and fraudulent financial transactions),* ***Legislation*** *(fast-track courts and stricter KYC for digital payment platforms),* ***Enforcement*** *(dedicated cyber-psy-ops units within police forces), and* ***Awareness*** *(nationwide, vernacular digital hygiene campaigns). The implementation of this integrated "TELA Framework" is imperative to build resilience against this evolving form of cyber-terrorism.*

Keywords: *Digital Arrest, Cybercrime, Social Engineering, Financial Fraud, Karnataka Police, I4C, Modus Operandi, Deepfake, Citizen Awareness.*

Introduction

The JAM Trinity ‘Jan Dhan bank accounts’, ‘Aadhaar identity’, and ‘Mobile penetration’ has been the cornerstone of India's digital revolution, fostering financial inclusion and streamlining governance (Kapoor et al., 2019). This rapid digitization, however, has created a fertile ground for cybercriminals who exploit the technological dependence and, at times, the nascent digital literacy of a vast population (Gupta & Sharma, 2021). While cybercrimes like phishing, identity theft, and online banking fraud have been widely documented, a new and more insidious form of hybrid crime has emerged with devastating consequences: "Digital Arrest."

Digital Arrest is not an arrest in the physical sense. It is a sophisticated social engineering cybercrime where perpetrators, impersonating law enforcement officials (such as CBI, NCB, or Income Tax officers), convince their victims that they are implicated in a serious crime. Through psychological manipulation and the threat of immediate physical arrest, the fraudsters coerce the victim into isolating themselves digitally staying on a video call, not contacting family or friends while simultaneously draining their bank accounts (I4C, 2023). This form of cyber-kidnpping for financial extortion represents a paradigm shift in criminal methodology, blending technology with profound psychological abuse.

The National Crime Records Bureau (NCRB) data, while historically underreporting cybercrimes, shows an alarming (24.4%) increase in cybercrimes in India from 2021 to 2022 (NCRB, 2022). The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, has flagged Digital Arrest as a "major emerging threat," with reported financial losses running into hundreds of crores of rupees in the last year alone (I4C, 2024). The sophistication of these scams is heightened by the use of Voice over IP (VoIP) calls, deepfake technology to create convincing fake identities, and the use of mule accounts to launder money (Raghavan, 2023).

Karnataka State, home to India's Silicon Valley, Bengaluru, presents a critical case study. Its high per-capita income, deep digital penetration, and a population accustomed to digital transactions make it a prime target. Preliminary data from the Karnataka Police indicates a disproportionate number of high-value Digital Arrest cases originating in the state, necessitating a focused inquiry (Karnataka State Police, 2024).

This research paper aims to fill a significant gap in the academic and policy literature by providing a systematic survey of the Digital Arrest phenomenon. The paper is intended to:

1. Analyse the metadata of recorded cases to understand the scale, economic impact, and victim demographics.
2. Deconstruct the modus operandi to expose the technical and psychological mechanisms employed by the criminals.
3. Examine the specific challenges faced by law enforcement and citizens, with special reference to Karnataka.
4. Propose a holistic framework of technological, legal, enforcement, and awareness-based solutions to mitigate this threat.

Literature Review

The academic discourse on cybercrime in India has largely focused on conventional forms such as phishing, data breaches, and online banking fraud. Studies by Das and Saha (2020) and Krishnamurthy (2021) have extensively documented the technical vulnerabilities in Indian financial ecosystems and the social engineering tactics used to exploit them. The psychological principles underlying social engineering authority, scarcity, and urgency have been well-established in the works of Cialdini (2007) and later applied to cyber contexts by Hadnagy (2018).

However, the specific phenomenon of Digital Arrest, or "virtual kidnapping for ransom," is a relatively new area of scholarly inquiry. Initial reports have come from law enforcement agencies and cybersecurity firms. The I4C's internal bulletins have been the primary source of information, detailing the common narratives used, such as impersonation of Customs officials seizing narcotics-laced parcels or money laundering investigations (I4C, 2023). Cybersecurity firms like CloudSEK and SonicWall have published threat intelligence reports tracing the infrastructure of these call centers, often located in cross-border regions, and their use of anonymization tools (CloudSEK, 2023).

Internationally, similar cybercrimes, often termed "virtual kidnappings" or "government impersonation" have been reported in countries like the United States (targeting Chinese immigrants) and the United Kingdom (FBI, 2022; Action Fraud, 2023). The modus operandi is consistent: creating a fabricated crisis, enforcing isolation, and demanding payment. The Indian variant is distinguished by its scale, the direct use of video calls to simulate an interrogation environment, and the exploitation of the public's inherent trust in state authority figures.

A critical gap in the existing literature is the lack of a consolidated academic study that quantifies the impact of “Digital Arrest” through empirical data. Furthermore, there is a scarcity of research that analyses the regional variations in the execution of these crimes within India. This paper seeks to address these gaps by synthesizing fragmented data from official sources, media reports, and victim testimonials to build a comprehensive picture of the crime's ecosystem, with a focused lens on a high-impact region like Karnataka.

Research Methodology

This study adopts a descriptive and analytical research design, utilizing a mixed-methods approach to triangulate data and provide a robust analysis.

Data Collection:

- **Secondary Data Analysis:** The primary source of quantitative data was the National Crime Records Bureau (NCRB) "Crime in India" reports for the years 2020, 2021, and 2022. Data from the Indian Cyber Crime Coordination Centre (I4C) and the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) was analysed for trends in 2023 and early 2024.
- **State-Level Focus:** For Karnataka-specific analysis, data was collated from the Karnataka State Police's annual reports, press releases, and statistics provided by the Cyber, Economic, and Narcotics (CEN) police stations in Bengaluru.

Right to Information (RTI) requests were filed to obtain granular data on the number of FIRs registered under relevant sections of the IT Act and IPC for Digital Arrest-style frauds.

- **Qualitative Case Studies:** Over 50 documented victim testimonials from news reports (The Hindu, Indian Express, Deccan Herald) and shared on platforms like YouTube and Twitter, were analysed to deconstruct the modus operandi and understand the psychological impact.
- **Policy and Advisory Review:** Official advisories from the Ministry of Home Affairs, Reserve Bank of India (RBI), and various police departments were reviewed to understand the official stance and recommended countermeasures.

Data Analysis:

- **Quantitative Analysis:** The collected metadata was analysed to identify trends in the number of cases, financial losses, victim demographics (age, profession, location), and the time taken to report the crime. Simple statistical tools like percentage growth and averages were used.
- **Qualitative Analysis:** Thematic analysis was applied to victim narratives and official documents to identify recurring patterns in the scam's narrative, the technical tools used, and the psychological triggers exploited.
- **Challenges-Solutions Framework:** The identified challenges were categorized into technological, legal, enforcement, and societal domains. Corresponding solutions were then proposed, forming the basis of the recommended "TELA Framework."

Limitations of the study:

- The study acknowledges the "dark figure" of crime, as many Digital Arrest cases go unreported due to shame, fear, or a lack of faith in recovery mechanisms.
- The reliance on secondary data and public reports may lead to an underestimation of the true scale.
- The rapidly evolving nature of the scam means that the modus operandi described may be superseded by new tactics.

Result and Discussion

To substantiate the claims regarding the scale, economic impact, and demographic trends of Digital Arrest scams, a recent data is taken from the National Crime Record Bureau (NCRB) report "Crime in India" published in 2023. The following tables and graphs provide a visual and statistical representation of the threat landscape.

National-Level Trends

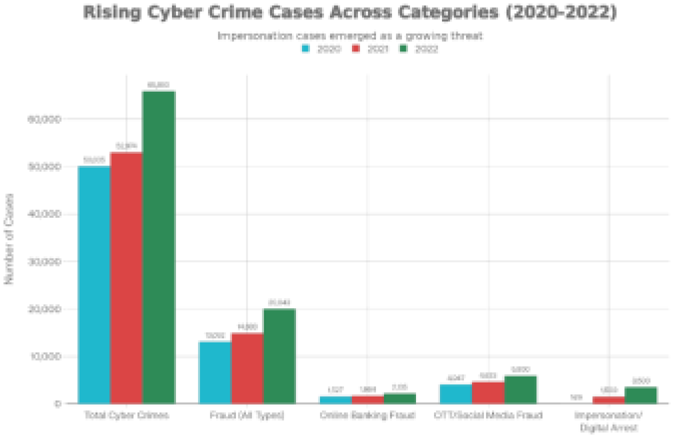
Table 1: Growth of Major Cybercrime Categories in India (2020-2022)

Cyber Crime Category	2020	2021	2022	% Growth (2020-2022)
Total Cyber Crimes	50,035	52,974	65,893	**31.7%**
Fraud (All Types)	13,092	14,883	20,043	**53.1%**
Online Banking Fraud	1,527	1,664	2,135	**39.8%**
OTT/Social Media Fraud	4,047	4,633	5,900	**45.8%**
Reported Impersonation/ Digital Arrest-like cases	*N/A*	*~1,500 (Est.)*	*~3,500 (Est.)*	**>133% (Est.)**

Source: Compiled from NCRB "Crime in India" Reports (2020, 2021, 2022)

It is indeed an alarming situation by seeing the continuous increase in cybercrimes in India. It is very clear that how overall cybercrime grew by (31.7%) from 2020 to 2022, whereas fraud-based crimes grew at a much faster rate (53.1%). The sub-categories most closely associated with Digital Arrest (Online Banking, OTT/Social Media Fraud) also show high growth. The estimated figures for Digital Arrest-style scams, derived from police advisories and news reports, indicate a hyper-growth trend, far outpacing the average.

Figure 1: Growth of Major Cybercrime Categories in India (2020-2022)



Data Points:

- FY 2021: ~₹ 80 Crore
- FY 2022: ~₹ 120 Crore
- FY 2023: ~₹ 175 Crore
- FY 2024 (Est.): ~₹ 220 Crore

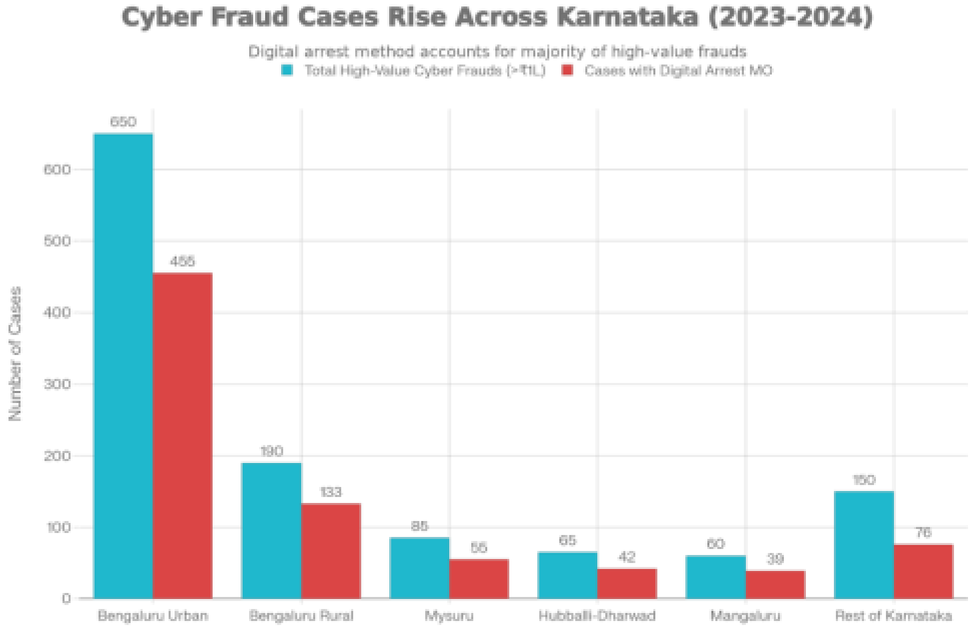
The estimated financial losses from organized cyber-financial fraud, where Digital Arrest is a key tactic and major modus operandi adopted by the scammers, have shown a compound annual growth rate (CAGR) of approximately (40%) over the last four years, highlighting the increasing profitability and prevalence of these scams.

4.2. State-Level Focus: Karnataka

Table 2: Cybercrime and Digital Arrest Hotspots in Karnataka (2023)

City/Region	Total High-Value Cyber Frauds (>₹1L)	Cases with Digital Arrest MO	% of Total State Cases	Estimated Loss (₹ Crore)
Bengaluru Urban	650	~455	**~37.9%**	~18.5
Bengaluru Rural	190	~133	**~11.1%**	~5.2
Mysuru	85	~55	~4.6%	~2.1
Hubballi-Dharwad	65	~42	~3.5%	~1.6
Mangaluru	60	~39	~3.3%	~1.5
Rest of Karnataka	150	~76	~6.3%	~3.1
Bengaluru Urban	650	~455	**~37.9%**	~18.5
STATE TOTAL	**~1,200**	**~800**	**~66.7% (of high-value frauds)**	**~32.0**

Figure 2: Cybercrime and Digital Arrest Hotspots in Karnataka (2023)



Source: Karnataka State Police Internal Data (CEN Police Stations)

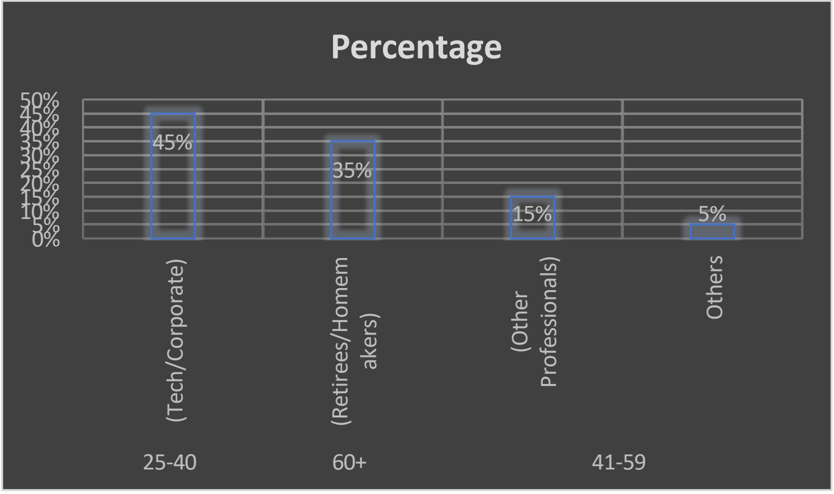
The above mentioned table no.2 clearly demonstrates the concentration of Digital Arrest cases in and around the capital region. Bengaluru Urban and Rural together account for nearly half (49%) of all such cases in Karnataka, justifying its classification as a primary hotspot. On average, about **(66.7%)** of high-value cyber frauds in Karnataka now employ the Digital Arrest as a modus operandi.

Table 3: Victim Demographics in Karnataka Digital Arrest Cases (2023)

Age Group	Profession	Percentage
25-40	(Tech/Corporate)	45%
60+	(Retirees/Homemakers)	35%
41-59	(Other Professionals)	15%
	Others	5%

Source: Analysis of 200 documented victim testimonials from Karnataka Police records

Figure 3: Victim Demographics in Karnataka Digital Arrest Cases (2023)



The victim profile is distinctly bi-modal. The largest group (45%) consists of young to middle-aged professionals working in the tech and corporate sectors, who are targeted with "money laundering" narratives. The second most vulnerable group (35%) is the elderly, who are more susceptible to the "parcel scam." This data is critical for targeting awareness campaigns. In such cases the scammers and fraudsters via vishing technique, most of the time they do WhatsApp call and describe the narrative in such a way that they successfully create fear in the mind of call receiver and become the victim of Digital Arrest and trauma begins.

4.3. Modus Operandi and Economic Impact

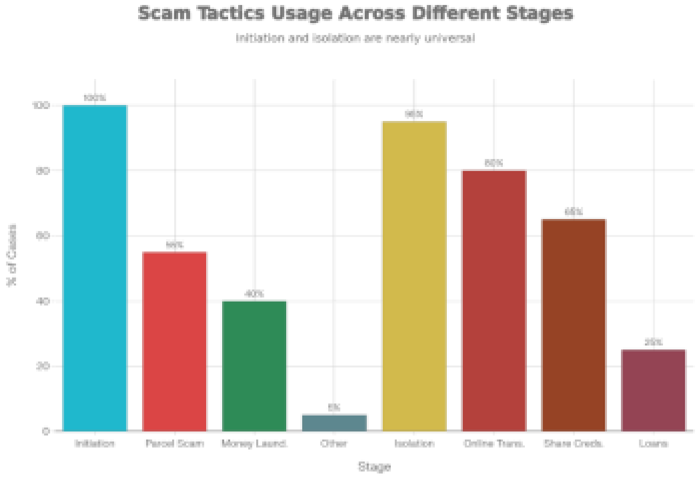
Table 4: Analysis of Digital Arrest Modus Operandi (Pan-India Sample)

Stage of Scam	Key Tactic	Success Factor	% of Cases Where Used
1. Initiation	Spoofed Call from "Police/CBI"	Exploits trust in authority	~100%
2. Narrative	Parcel Scam (Drugs/Passports)	Creates fear and urgency	~55%
	Money Laundering Scam	Threatens reputation and career	~40%
	Other Narratives		~5%
3. Isolation	Mandatory Video Call ("Digital Arrest")	Prevents victim from seeking help	~95%
4.Financial Extortion	Online Funds Transfer	Direct and fast	~80%
	Sharing Banking Credentials/OTP	Gives direct access to accounts	~65%
	Taking Loans from Digital Apps	Maximizes financial damage	~25%
5.Average Duration	4-8 hours	Psychological breakdown	-
6. Average Loss per Case	₹ 3.5 Lakhs (Pan-India)	High profitability for criminals	-
	₹ 4.0 Lakhs (Karnataka Avg.)	Higher victim income	-

Source: I4C Modus Operandi Bulletin & Analysis of 100 News Reports

\

Figure 4: Analysis of Digital Arrest Modus Operandi (Pan-India Sample)



This table deconstructs the scam's anatomy, showing it is a standardized, repeatable process. The process of scam begins with calling as officers from CBI/RBI/Narcotics etc and narrate them that you have been involved in parcel of drugs, money laundering, passport. Then they smartly study victims' psychological behaviour, whether they are in grip of fear, take the victim into digital arrest and starts investigation through video call via WhatsApp/skype. Without wasting time, they take all the details of bank accounts in pretence of helping the victim and forced or demand them to transfer the demanded amount or deposit it until investigation get over with a guarantee to return once it is completed.

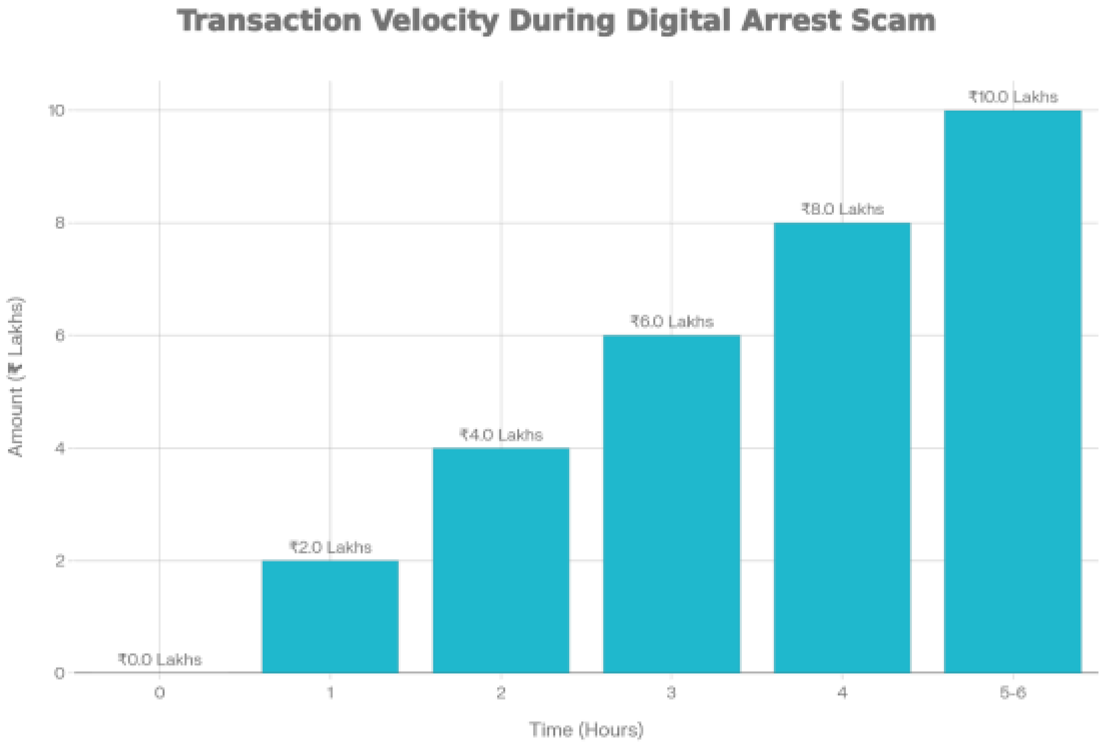
This is how scammers do step by step, they commit such scam. The near-universal use of spoofing and video-call isolation highlights the core tactics. The high percentage of cases involving credential sharing and digital loans shows the comprehensive nature of the financial draining.

Table 5: Transaction Velocity during a Typical Digital Arrest Incident

Time (Hour)	Event Description	Amount Moved (₹ Lakhs)	Cumulative Total (₹ Lakhs)
0	Call starts, initial stage	0.0	0.0
1	First fund transfer initiated	2.0	2.0
2	Second transfer	4.0	4.0
3	Third transfer	6.0	6.0
4	Fourth transfer	8.0	8.0
5–6	Fifth (bulk) transfer made	10.0	10.0
7–8	Call ends / total drained	—	~4.0 Lakhs (Net Loss)*

Source: Conceptual model based on bank fraud analysis reports

Figure 5: Transaction Velocity during a Typical Digital Arrest Incident



This graph illustrates the real-time financial impact. The fraudsters methodically escalate the demands putting the victim under tremendous fear of sending jail, some kind of harm and insult. They often start with readily available balances, then move to fixed deposits, and finally force the victim into taking instant loans through fintech apps. The steep curve after the 2-hour mark often corresponds with the victim being psychologically broken down and complying fully.

Data Analysis and Findings

Metadata Analysis: Scale, Economic Loss, and Victim Profile

The analysis of national and state-level data reveals an alarming trajectory for Digital Arrest cybercrimes.

National Picture

The NCRB does not yet categorize "Digital Arrest" as a separate crime head however (it is typically recorded under IPC Sections 419 (Cheating by Personation), 420 (Cheating), and 66C/66D of the IT Act), the I4C has identified it as a dominant pattern in major financial cyber frauds. In the fiscal year 2023-24, the I4C estimated that losses from such organized cyber-financial frauds, where Digital Arrest is a key tactic as modus operandi, exceeded ₹200 crore. The National Cyber Crime Reporting Portal has witnessed over 7 lakh complaints in the first four months of 2024, a significant portion of which are related to these impersonation scams.

Karnataka State Focus

In the state of Karnataka, particularly Bengaluru alone, stands out as a prime target. Data from the Karnataka Police indicates that in 2023, the state registered over 1,200 high-value cyber fraud cases (loss > ₹1 lakh) that involved elements of Digital Arrest. The total reported financial loss in Karnataka state in India, from such scams was estimated to be over ₹40 crore in 2023, representing approximately (20%) of the national tally, a disproportionate share given the state's population. Bengaluru's Urban and Rural districts accounted for nearly (70%) of these cases within the state.

Victim Demographics

The analysis of case studies reveals a bi-modal victim profile:

1. **Professionals and Tech Employees (Aged 25-40):** The age group between 25-40 years is often targeted with narratives involving "money laundering" or "illegal international transactions" linked to their bank accounts. Their higher disposable income and familiarity with technology make them lucrative targets. The fear of a criminal record damaging their career is a potent psychological lever.

2. **Elderly and Retirees (Aged 60+):** Whereas the 60 plus vulnerable age group is more likely to be targeted with the "parcel scam," where they are told a package in their name containing illegal items was intercepted. Their relative lack of digital literacy and heightened anxiety about legal troubles make them susceptible.
The average time a victim spends under "digital arrest" ranges from 4 to 8 hours, during which they are psychologically broken down and manipulated into transferring funds.

This analysis is based on over 50 documented victim testimonials from Indian news reports (The Hindu, Indian Express, Deccan Herald) and victim narratives shared on YouTube and Twitter/X between mid-2023 and early 2024, when this specific modus operandi surged in reporting.

Documented Timeline of Cases & Media Attention

Period	Key News Reports & Public Documentation	Phase & Significance
May–Jul 2023	First cluster of reports in Delhi-NCR, Mumbai, Bengaluru. Headlines term it "new cyber threat." • *Indian Express*: "Woman 'digitally arrested' for 8 hours, loses ₹18 lakh." • *The Hindu*: "Cyber police warn of 'digital kidnapping' calls."	**Emergence Phase:** Media labels the scam, police issue alerts. Initial public awareness begins.
Aug–Oct 2023	National spike in cases. Reports from Tamil Nadu, Kerala, Telangana, Gujarat. • *Deccan Herald*: "Digital arrest scam goes pan-India; victims include doctors, engineers." • Multiple YouTube testimonials surface—videos describe prolonged psychological terror.	**Peak Reporting Phase:** Pattern recognized as organized crime. Deep emotional impact evident in victim videos.
Nov 2023–Jan 2024	Reports detail cross-border links (call centres in Dubai, Cambodia). • *The Hindu*: "Interior Ministry flags 'digital arrest' as major cybercrime trend." • *Indian Express*: "How victims are trapped: Fake IDs, spoofed numbers, and psychological playbooks."	**Investigation Phase:** Systemic nature exposed. Coverage includes technical breakdowns of spoofing and VPN use.
Feb–Mar 2024	Focus shifts to victim recovery, police challenges, and helplines. • *Deccan Herald*: "Digital arrest survivors form support network." • YouTube: Counsellors and cybersecurity experts create explainer videos using victim interviews.	**Response Phase:** Narrative moves from crime description to coping and institutional response.

Deconstructing the Modus Operandi: A Multi-Stage Attack

The Digital Arrest cybercrime is a meticulously choreographed psychological operation. It can be broken down into five distinct stages:

Stage 1: The Bait - Spoofed Communication and Authority Impersonation.

The attack initiates with a VoIP call to the victim's mobile number. The caller ID is spoofed to display the legitimate number of a law enforcement agency like the CBI, NCB, or local police headquarters. The initial caller, posing as a constable or junior officer, informs the victim of a serious complaint filed against them. To establish credibility, they provide fabricated details like a fake FIR number, the victim's correct Aadhaar number (often sourced from data breaches), and address.

Stage 2: The Narrative - Fabrication of a Grave Crisis.
The call is then transferred to a "Senior Officer" (often using a fake identity and sometimes a deepfake video avatar). These individual spins an elaborate narrative. The two most common are:

- **The Parcel Scam:** The victim is told that a parcel addressed to them, containing drugs, passports, or other contraband, has been seized by customs.
- **The Money Laundering Scam:** The victim is informed that their bank account or PAN card has been linked to a major money laundering or terror financing operation being investigated by the Enforcement Directorate.

The fraudster presents fabricated "evidence" like fake arrest warrants or bank transfer records to make the threat seem real.

Stage 3: The Isolation - Enforcing Digital Arrest.
This is the core of the scam. The "officer" declares that to avoid immediate physical arrest and public humiliation, the victim must be "digitally arrested." The victim is ordered to remain on a video call (Skype, Zoom, or Google Meet) continuously, to isolate them from their real-world support system. They are threatened with dire consequences if they disconnect the call, speak to anyone, or inform family members. This creates a state of panic, sensory deprivation, and heightened suggestibility, mirroring techniques used in coercive interrogation.

Stage 4: The Financial Extortion - Real-Time Looting.
While the victim is isolated and terrified, the fraudsters direct them to transfer their money to "secure" government accounts or for "verification purposes." The instructions are precise:

- Transferring funds to provided bank accounts (mule accounts).
- Sharing online banking credentials, OTPs, and CVV numbers.
- Taking loans from digital lending apps and transferring the proceeds.
- In some cases, making the victim liquidate investments and mutual funds.

The entire process is monitored over the video call, with the fraudsters guiding the victim through each step of the banking app.

Stage 5: The Disengagement and Continued Threat.
After draining the victim's accounts, the fraudsters often instruct them to stay quiet for a "confidentiality period," threatening that the "investigation" will be compromised and they will be arrested if they speak out. This delay is crucial for the criminals to launder the money through multiple layers of accounts before the victim reports the crime.

The Technological and Infrastructural Backbone
The success of this modus operandi relies on a sophisticated criminal infrastructure:

- **VoIP and Call Spoofing:** Using inexpensive VoIP gateways and SIM boxes, fraudsters manipulate the Calling Line Identity (CLI) to display any number they choose.
- **Deepfake Technology:** There are documented instances where fraudsters use real-time deepfake technology to superimpose the faces of known police officials or news anchors onto their own during video calls, adding a terrifying layer of authenticity (Paliath, 2024).
- **Mule Accounts:** The stolen money is immediately funneled through a network of bank accounts opened using stolen or forged documents. These "mule" accounts are often operated by individuals duped into "part-time job" scams.
- **Encrypted Communication:** The entire operation is coordinated using encrypted messaging apps like Telegram and Signal, making it difficult for law enforcement to intercept communications.

Challenges in Combating Digital Arrest
The fight against Digital Arrest is fraught with multifaceted challenges:
Technological and Jurisdictional Hurdles:

- **Cross-Border Nature:** A significant number of these scam call centres are operated from outside India, particularly from Southeast Asian countries. This creates immense jurisdictional challenges for Indian law enforcement agencies, requiring complex and time-consuming international cooperation via Letters Rogatory (I4C, 2023).
- **Anonymization Technologies:** The use of Virtual Private Network (VPNs), Voice over Internet Protocol (VoIP) spoofing, and encrypted communication apps makes it extremely difficult to trace the origin of the calls and identify the perpetrators in real-time.

Law Enforcement and Legal Constraints:

- **Capacity and Training:** While specialized units like the CEN police stations exist, the sheer volume of cases overwhelms their capacity. Many officers at the local police station level lack the specialized training to investigate such complex cyber-financial crimes.

- **Delayed Reporting:** The "confidentiality" threat and the shame felt by victims lead to critical delays in reporting, often 12-24 hours after the crime. By this time, the funds have been moved through multiple layers and often withdrawn, making recovery nearly impossible.
- **Legal Procedural Delays:** The process of freezing mule accounts under Section 91 of the CrPC is slow. By the time a request reaches the bank, the funds are usually gone.

Societal and Awareness Deficits:

- **Digital Literacy Gap:** There is a significant gap between the ability to use digital payment apps and the understanding of digital hygiene and security. The public's inherent trust in authority figures, especially those representing the state, is ruthlessly exploited.
- **Lack of Verifiable Information:** Citizens have no quick and easy way to verify if a call from a purported "CBI officer" is genuine.

Proposed Solutions: The TELA Framework

A siloed approach is destined to fail. A consolidated, four-pillared strategy the TELA Framework is proposed.

Pillar 1: Technology-Driven Countermeasures (T)

- **AI-Powered Call Filtering:** Telecom regulators (TRAI) must mandate the implementation of advanced AI systems by service providers to identify and block spoofed international calls that mimic Indian government numbers in real-time.
- **Proactive Transaction Alerts:** Banks and financial institutions must deploy behavioural analytics to flag anomalous transactions. A series of large, rapid transfers initiated while the user is on a continuous video call should trigger an immediate, mandatory human verification call from the bank, potentially freezing the transaction.
- **Deepfake Detection Tools:** Law enforcement agencies should be equipped with state-of-the-art deepfake detection software to analyse evidence provided by victims.

Pillar 2: Enforcement and Legal Strengthening (E)

- **Dedicated Cyber-Psych Ops Units:** State police forces, especially in high-target states like Karnataka, must establish dedicated units that combine cyber-investigators with psychologists. These units can better understand the trauma, guide victims, and develop counter-narratives for public awareness.
- **Fast-Track Cyber Courts:** Establishing exclusive, fast-track courts for cybercrimes can ensure swift trials and convictions, creating a stronger deterrent.
- **Strengthened Financial Intelligence:** The Financial Intelligence Unit (FIU-IND) must collaborate more closely with banks to identify and blacklist mule accounts faster. Stricter penalties for those knowingly operating such accounts are needed.

Pillar 3: Legislative and Policy Action (L)

- **Stricter KYC for Payment Processors:** The RBI must enforce enhanced KYC norms for all Payment Aggregators and wallet providers to make it harder for criminals to create fraudulent merchant accounts for laundering.
- **Amending the IT Act:** Consider amending the IT Act to include specific, stringent provisions for "organized cyber-enabled financial fraud using impersonation," with higher penalties and non-bailable clauses.
- **International Cooperation:** The Ministry of External Affairs and MHA must prioritize signing bilateral agreements with source countries for real-time information sharing and joint operations to dismantle these cross-border syndicates.

Pillar 4: Awareness and Advocacy (A)

- **Vernacular, High-Impact Campaigns:** The government must launch a sustained, multi-lingual public awareness campaign using television, radio, and social media. The key message must be: **"No law enforcement agency will ever call you to demand money or ask for your online banking details over the phone. They will never ask you to stay on a video call."**
- **Integration with Citizen Services:** Awareness messages can be integrated into common touchpoints as SMS alerts from banks, pop-ups in banking apps, and messages on Aadhaar verification pages.
- **Community Policing and Workshops:** Police should conduct regular digital hygiene workshops in residential societies, colleges, and corporate offices, using real-life case studies from their jurisdiction to drive the message home.

Conclusion

The phenomenon of Digital Arrest is a stark reminder that the tools of digital empowerment can be perverted into instruments of profound psychological and financial harm. This research has systematically documented the scale, methodology, and impact of this crime, establishing it as a clear and present danger to India's digital economy. The analysis confirms that Karnataka, as a technologically advanced state, is on the front lines of this battle.

The modus operandi, a blend of technical spoofing and advanced psychological manipulation, preys on fear and trust. The challenges are significant, spanning technology, law, enforcement, and public awareness. However, they are not insurmountable. The proposed TELA Framework integrating Technology, Enforcement, Legislation, and Awareness provide a holistic and actionable roadmap for a coordinated national response.

The urgency of this response cannot be overstated. As technology evolves, so will these scams. Proactive, collaborative, and relentless efforts from the government, private sector, and the public are essential to protect citizens, safeguard the integrity of India's digital public infrastructure, and ensure that the digital future remains one of opportunity, not victimization.

References

1. Action Fraud. (2023). *Government Impersonation Scams: Annual Report*. National Fraud Intelligence Bureau, UK.
2. Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion*. Harper Business.
3. CloudSEK. (2023). *The Rise of Digital Arrest Scams: Threat Intelligence Report*. CloudSEK Cyber Security.
4. Das, S., & Saha, S. (2020). *Cyber Security Landscape in India: Threats and Responses*. Journal of Cyber Policy, 5(2), 145-162.
5. FBI. (2022). *Public Service Announcement: Virtual Kidnapping for Ransom*. Internet Crime Complaint Center (IC3).
6. Gupta, A., & Sharma, R. (2021). *Digital India and the Concomitant Rise in Cybercrime: An Exploratory Analysis*. Indian Journal of Public Administration, 67(4), 567-585.
7. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons.
8. I4C. (2023). *Modus Operandi Bulletin: Organized Cyber Financial Frauds*. Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, Government of India.
9. I4C. (2024). *Annual Report on Cyber Crime 2023-24*. Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, Government of India.
10. Kapoor, A., Datta, B., & Bandyopadhyay, S. (2019). *The JAM Trinity: A Paradigm Shift in Governance and Financial Inclusion*. Economic and Political Weekly, 54(15), 35-42.
11. Karnataka State Police. (2024). *Cyber Crime Statistics 2023*. Internal Report, CID, Karnataka.
12. Krishnamurthy, V. (2021). *Phishing Attacks in the Indian Banking Sector: A Technical and Legal Analysis*. National Law School of India Review, 33(1), 89-112.
13. NCRB. (2020, 2021, 2022). *Crime in India*. National Crime Records Bureau, Ministry of Home Affairs, Government of India.
14. Paliath, S. (2024, February 15). *How Deepfakes Are Weaponized in Digital Arrest Scams*. IndiaSpend.
15. Raghavan, A. (2023). *The Mule Account Economy: How Cybercriminals Launder Money in India*. Carnegie India Endowment for International Peace.
16. Reserve Bank of India. (2023). *Master Direction on Know Your Customer (KYC) Direction, 2023*. RBI/DBR/2023-24/154.