JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cybercrime in India: A Review of Digital Arrest Scams

Rahul Kumar[1], Dr. Gurvinder Singh[2]

[1]Assistant Professor, Department of Computer Science & Applications, Arni University, Kangra, Himachal Pradesh, India, rahulmahajan480@gmail.com

[2]Associate Professor, Arni School of Technology, Arni University, Kangra, Himachal Pradesh, India, drkahlon29@gmail.com

ABSTRACT

The rapid growth of digital technology and internet-based services has transformed communication, financial transactions, and access to information, but it has also created new opportunities for cybercriminals. India has witnessed increasing incidents of phishing, identity theft, hacking, online financial fraud, and digital extortion. Among these emerging threats, digital arrest scams have become a serious concern, using impersonation, intimidation, and psychological manipulation to deceive victims and obtain money.This paper reviews the emergence and development of digital arrest fraud in India during 2022–2025. Based on government sources, law-enforcement records, and credible media reports, the study examines the common techniques adopted by offenders, including caller-ID spoofing, AI-enabled video impersonation, fabricated legal proceedings, and coercive communication. The review also examines reported complaints and financial losses associated with these scams, along with factors such as limited public awareness, increasing digital dependence, and challenges in cybercrime enforcement. Further, the study discusses the role of the Indian Cyber Crime Coordination Centre (I4C) and the national helpline 1930, together with measures introduced by the Government of India. The paper concludes by highlighting legal, technological, and awareness-based measures required to reduce digital arrest fraud.

Keywords: Digital Arrest Fraud, Cybercrime, Online Fraud, Cyber Extortion, Cybersecurity.

INTRODUCTION

India is experiencing rapid expansion in digital connectivity, online services, and technology-driven communication. While this transformation has contributed significantly to economic and social development, it has simultaneously increased the country's vulnerability to sophisticated forms of cybercrime. The frequency and complexity of internet-based fraud have continued to grow, with phishing and other forms of digital deception becoming increasingly common. One of the emerging methods is the so-called “digital arrest scam,” in which criminals exploit digital communication channels to deceive individuals and obtain money through intimidation. Fraudsters commonly impersonate police officials, the Central Bureau of Investigation (CBI), or other government authorities and contact potential victims through telephone calls, WhatsApp, or video conferencing platforms. During these interactions, victims may be falsely accused of involvement in serious offences, including cybercrime, drug trafficking, or activities involving illegal online content. The perpetrators then create a sense of urgency and fear by threatening immediate arrest or legal action, subsequently demanding money as a supposed penalty, verification fee, or settlement to avoid prosecution.

WHAT IS A "Digital Arrest" SCAM?

A "digital arrest" scam is a form of cyber fraud in which criminals impersonate law-enforcement personnel, commonly presenting themselves as police officers, CBI officials, or representatives of other government agencies. The victim is falsely told that an arrest warrant, criminal complaint, or legal proceeding has been issued against them, usually involving allegations of serious offences. Communication is generally established through telephone calls, WhatsApp, or video-conferencing applications such as Skype (The News Minute, n.d.; The Hindu, 2024). The fraudsters use threats of arrest, investigation, or prosecution to frighten victims and pressure them into transferring money. It is important to note that Indian law does not recognise arrest through a telephone or video call. Therefore, the concept of a "digital arrest" has no legal validity and is entirely based on deception and intimidation (The Hindu, 2024).

METHODOLOGY

This study employs a narrative or descriptive review approach rather than a systematic review, primarily because research specifically addressing digital arrest fraud is still developing and much of the available evidence comes from non-academic sources. Information and case-related material were collected from three major source groups: (i) official government databases and publications, including the Open Government Data Platform India and information released by the Ministry of Home Affairs and the Indian Cyber Crime Coordination Centre (I4C); (ii) parliamentary documents, particularly written responses presented in the Rajya Sabha; and (iii) reports published by established national media organisations such as The Hindu, NDTV, and Digit.in, along with an academic case study concerning digital arrest fraud in Gujarat (Sapovadia, n.d.). Sources were considered when they provided information on reported incidents, financial losses, or specific cases between January 2022 and mid-2025. Reports lacking sufficient supporting evidence or independent corroboration were excluded. Since different organisations follow different reporting schedules, 2025 figures represent only a portion of the calendar year and are identified accordingly in Section 6. This methodology enables the study to integrate governmental, media-based, and case-specific evidence, although it does not provide the methodological depth associated with a systematic review based on pre-defined and registered search protocols (see Section 10, Limitations).

MODUS OPERANDI

First Contact: The fraud generally begins with an unexpected telephone call, WhatsApp message, or email from an individual falsely claiming to be associated with a senior police official, CBI officer, income-tax department, customs authority, or another government agency.

Psychological Manipulation: Fear and intimidation form the central elements of the scam. Fraudsters exploit victims' concerns about arrest, damage to their reputation, social humiliation, and criminal prosecution. To strengthen their credibility, they may produce forged legal notices, fabricated warrants, and other official-looking documents. During video calls, criminals sometimes appear in uniforms and create backgrounds resembling police stations, courtrooms, or government offices to reinforce the impression of authenticity.

Isolation and Intimidation: Once contact is established, perpetrators may keep victims engaged in prolonged video or telephone conversations. They instruct them to remain at home and avoid informing relatives, friends, or colleagues, thereby preventing access to external advice or assistance while the fraud is being carried out.

Financial Extortion: After establishing fear and apparent authority, scammers demand money by presenting it as a verification charge, legal clearance payment, security deposit, or bail-related amount. Victims are usually instructed to transfer the money through UPI, bank accounts, or cryptocurrency platforms within a specified period. Continued threats of arrest are used to ensure compliance. The combined use of impersonation, technological deception, psychological pressure, and financial coercion makes digital arrest fraud particularly effective and difficult for victims to recognise in time.

SCALE AND IMPACT

The growing seriousness of digital arrest fraud in India can be understood through several reported cases involving substantial financial losses and prolonged psychological harassment.

On 5 August 2025, a 70-year-old woman from Koparkhairane, Navi Mumbai, was contacted through a video call by an unknown individual posing as a police commissioner. She was falsely accused of misusing her Aadhaar details to assist another person in opening a Canara Bank account allegedly connected with terrorist financing. The fraudster further claimed that she had received ₹20 lakh as commission. Fearing arrest, the victim transferred a total of ₹21 lakh in several instalments to the bank account specified by the caller (Digit.in, 2025).

In another incident reported on 21 August 2025, a married couple was defrauded of ₹50 lakh, representing their accumulated savings, over a period of 13 days. The perpetrators posed as police officials and accused the couple of being connected with murder, kidnapping, and financial fraud involving a SIM card allegedly registered in their names.

A 78-year-old man from Thippasandra, HAL 3rd Stage, reportedly remained under a fabricated "digital arrest" for almost two months, from 21 May until July. A caller claiming to represent the Mumbai Cyber Crime Branch accused him of being the principal suspect in a bank fraud investigation, resulting in a loss of approximately ₹83.2 lakh from his lifetime savings.

In Bengaluru, a retired engineer and his wife were subjected to a similar fraudulent "digital arrest" for nearly two and a half months. The perpetrators accused them of money laundering and credit-card-related offences and used a counterfeit arrest warrant to demand ₹4.79 crore as purported bail money (NDTV, n.d.).

FINANCIAL IMPACT

Reported incidents and associated financial losses by year are summarised below, drawing on the Open Government Data Platform India (n.d.).

Sl. No.	Year	Number of Incidents	Amount Defrauded (₹ Crore)
1	2025*	17,718	210.21
2	2024	1,23,672	1,935.51
3	2023	60,676	339.03
4	2022	39,925	91.14

**2025 figures reflect a partial calendar year based on data available at the time of writing and are not directly comparable, on a year-on-year basis, to the full-year totals for 2022–2024.*

ROOT CAUSES AND UNDERLYING VULNERABILITIES

Psychological Exploitation: Psychological pressure is a central component of digital arrest fraud. Criminals deliberately create fear and urgency by threatening imprisonment, legal proceedings, reputational harm, and social consequences. The use of official-looking logos, documents, uniforms, and increasingly AI-generated voices or video content further strengthens the false appearance of legitimacy and encourages victims to comply (Kenstone Capital, n.d.).

Limited Public Awareness: Many individuals have limited knowledge of legal procedures and the methods used in digital financial fraud. A significant number are also unaware that Indian law does not provide for an arrest to be conducted through a telephone or video call. Elderly people, individuals with limited digital literacy, and those placed under emotional stress may therefore be particularly vulnerable to such deception.

Fear of Social Consequences: Concern about embarrassment, reputational damage, and possible criticism from family or society can prevent victims from seeking immediate assistance. Some individuals avoid sharing the incident with relatives or friends because they fear being judged. This secrecy can increase their vulnerability and allow criminals more time to exert pressure and extract money.

Law-Enforcement Difficulties: Identifying and apprehending perpetrators remains challenging because criminals frequently use false identities, temporary accounts, encrypted communication platforms, and networks of intermediary bank accounts. Delays in reporting incidents can reduce the possibility of tracing or freezing transactions at an early stage. Recovery becomes even more difficult when stolen funds are transferred through multiple accounts or converted into cryptocurrency.

LEGAL FRAMEWORK AND INSTITUTIONAL RESPONSES

The Government of India has established institutional mechanisms to strengthen the country's response to cybercrime. The Ministry of Home Affairs established the Indian Cyber Crime Coordination Centre (I4C) in 2021 as a central framework for coordinating efforts against different forms of cybercrime. The government has also undertaken targeted awareness initiatives to educate citizens about digital arrest scams, including public communication through the Prime Minister's *Mann Ki Baat* programme (Ministry of Home Affairs, n.d.). In collaboration with the Department of Telecommunications (DoT), I4C introduced a caller-tune awareness campaign encouraging citizens to use the national cybercrime helpline (1930) and the National Cyber Crime Reporting Portal (cybercrime.gov.in), administered by the Ministry of Home Affairs. According to government information, I4C has blocked more than 3,962 Skype IDs and 83,668 WhatsApp accounts associated with digital arrest fraud. Government agencies and telecom operators have also taken measures against spoofed international calls. By 28 February 2025, law-enforcement agencies had identified and deactivated more than 7.81 lakh SIM cards and 2,08,469 IMEIs. Since its establishment, I4C has facilitated the registration of approximately 13.36 lakh cybercrime complaints through the national portal, helping prevent potential financial losses of more than ₹4,386 crore (Ministry of Home Affairs, n.d.). In addition, all Indian states and union territories have dedicated cybercrime units. TRAI and DoT work with telecom service providers to identify fraudulent numbers and address spoofed calls, phishing messages, and other forms of telecommunications-based fraud.

FUTURE DIRECTIONS

Strengthening Public Awareness: Cybersecurity education should be incorporated into school and higher-education curricula and supported through community programmes, workplace training, and sustained public-awareness campaigns. Information regarding official helplines and reporting platforms should be regularly disseminated across government, public-sector, and private-sector organisations.

Industry Collaboration: Financial institutions, telecom companies, payment platforms, and technology providers should implement existing guidance, including NPCI measures concerning digital arrest scams, to identify suspicious communications and transactions. Common protocols for detecting unusual customer activity, responding to incidents, and supporting affected customers should also be developed.

Rapid Response Systems: Artificial intelligence and machine-learning technologies can be employed to identify fraudulent activity across SMS, voice calls, online platforms, and social-engineering channels. Real-time analysis of abnormal transaction behaviour should enable payment providers to flag, delay, or temporarily block suspicious transactions before funds are transferred further.

Cross-Border Coordination: Since many cyber-fraud networks operate across national boundaries, stronger cooperation with international law-enforcement agencies is required. Joint investigative mechanisms, timely intelligence sharing, coordinated action against organised fraud networks, and common databases of suspicious accounts and identifiers could improve both detection and recovery of stolen funds.

Enhanced Cybersecurity: Financial institutions and digital platforms should strengthen multi-factor authentication, encryption, access controls, and regular security assessments. Periodic security audits and penetration testing can help identify vulnerabilities before they are exploited by cybercriminals.

Victim Assistance: Dedicated support mechanisms should be established to help victims address the psychological, financial, and legal consequences of digital arrest fraud. Such services could provide counselling, guidance on filing complaints, assistance with financial recovery procedures, and information regarding available legal remedies and compensation mechanisms.

LIMITATIONS OF THE REVIEW

This review is primarily based on secondary sources, including government publications, parliamentary records, official data releases, and media reports, rather than primary surveys of victims or direct law-enforcement case records. Consequently, the findings may be influenced by reporting practices, source-selection limitations, and differences in the availability of documented cases. Underreporting remains a significant concern in cybercrime research, particularly because victims may hesitate to report incidents due to fear, embarrassment, or social stigma, as discussed in Section 7. Therefore, the reported figures for incidents and financial losses may not represent the actual magnitude of digital arrest fraud in India. The review also relies on a limited number of illustrative cases rather than a statistically representative sample. These cases help demonstrate common characteristics and consequences of the fraud but cannot be considered sufficient for making broad generalizations about all victims or incidents. The patterns discussed in Section 5 should therefore be interpreted cautiously. Furthermore, government and media databases are periodically revised as new complaints and financial-loss figures become available, meaning that the statistics presented in this review may change over time. The data for 2025 are provisional and represent information available up to the time of preparation of this paper. Readers should therefore treat the 2025 figures as indicative rather than final.

CONCLUSION

The rapid expansion of digital services in India has been accompanied by the emergence of sophisticated cyber threats, among which digital arrest fraud has become a particularly concerning form of financial deception. These scams combine technological impersonation with psychological manipulation and limited public understanding of legal procedures to create fear and compel victims to transfer money. Beyond direct financial losses, such incidents can cause considerable emotional distress, anxiety, and loss of confidence in digital services.

The persistence of digital arrest scams demonstrates the need for a coordinated and multi-dimensional response involving legal enforcement, technological safeguards, public awareness, and international cooperation. Institutions such as the Indian Cyber Crime Coordination Centre (I4C), the national cybercrime helpline 1930, and the National Cyber Crime Reporting Portal have strengthened the country's ability to respond to reported incidents. However, continued public education and stronger preventive mechanisms remain necessary.

Greater emphasis should be placed on cyber-safety education, coordination among law-enforcement agencies, rapid identification of fraudulent transactions, and effective information sharing among banks, payment platforms, and telecom operators. Accessible victim-support systems are equally important to encourage timely reporting and assist affected individuals.

Ultimately, digital arrest fraud is not merely a technological challenge. It represents a wider social, economic, psychological, and institutional problem that requires sustained cooperation among citizens, government agencies, financial institutions, technology companies, and law-enforcement authorities.

References

1. Digit.in. (2025). *Elderly woman loses Rs 21 lakh in digital arrest scam: Here's what happened.* https://www.digit.in/news/general/elderly-woman-loses-rs-21-lakh-in-digital-arrest-scam-heres-what-happened.html
2. Drishti IAS. (n.d.). *Rising digital arrests.* https://www.drishtiias.com/daily-updates/daily-news-analysis/rising-digital-arrests
3. Kenstone Capital. (n.d.). *What is digital arrest? Trends, tactics, and measures.* https://www.kenstonecapital.in/digital-arrest
4. Ministry of Home Affairs, Government of India. (n.d.). *Steps taken to address the issue of digital arrest scams* [Written reply by Shri Bandi Sanjay Kumar, Minister of State for Home Affairs, Rajya Sabha].
5. NDTV. (n.d.). *Bengaluru couple loses Rs 4.79 crore in cyber fraud; 'digital arrest' scamster visits Sri Lankan casino.* https://www.ndtv.com/india-news/bengaluru-couple-loses-rs-4-79-crore-in-cyber-fraud-digital-arrest-scamster-visits-sri-lankan-casino-8639564.
6. Open Government Data Platform India. (n.d.). *Year-wise number of incidents, digital arrest scams and related cyber crimes reported, national.* https://www.data.gov.in/resource/year-wise-number-incidents-digital-arrest-scams-and-related-cyber-crimes-reported-national.
7. Sapovadia, V. (n.d.). *Unraveling digital arrest scams in Gujarat: A deep dive into fraud, systems, and society.* National Forensic Sciences University, Gandhinagar.
8. The Hindu. (2024). *What is a 'digital arrest scam' and how can you protect yourself?* https://www.thehindu.com/news/national/digital-arrest-scam-how-to-protect-yourself/article68806494.ece.
9. The News Minute. (n.d.). *What is a 'digital arrest' scam? Explained.* https://www.thenewsminute.com/news/what-is-a-digital-arrest-scam-explained.