International Journal of Advanced Digital Systems
and Multidisciplinary Studies (IJADSMS),
Volume - 1, Issue - 9 pp. 56–58, 2026

Digital Arrest Scams in Bihar: Cybercrime and Legal Challenges

Mr. Ajit Kumar[1], Mr. Abhishek Kumar[2], Ms. Lakshmi Kumari[3], Mr. Sachin Kashyap[4], Ms. Kumari Puja[5]
[1]Assistant Professor, Amity Institute of Information Technology (AIIT), Amity University Jharkhand, Ranchi
[2,3,4,5]Assistant Professor ,School of Computer Applications, Noida Institute of Engineering and Technology (NIET) Greater Noida
akuma7@rnc.amity.edu[1],abhishek.kumar@niet.co.in[2],lakshmikumari.mca@niet.co.in[3], sachin.kashyap@niet.co.in[4]
kumari.puja@niet.co.in[5]

Abstract
This paper examines the emerging phenomenon of "digital arrest" scams within Bihar, India, analyzing their modus operandi, the vulnerabilities they exploit, and the significant legal and enforcement challenges posed by this sophisticated form of cybercrime. It delves into the intricacies of these scams, where perpetrators impersonate law enforcement or government officials to coerce victims into making financial transactions under the threat of fabricated legal action. The discussion will further explore the broader context of cybercrime in India, noting the exponential growth in such activities and the subsequent challenges in prediction and prevention. The rapid digitization across India has inadvertently amplified the incidence of cybercrimes, necessitating a comprehensive analysis of the existing legislative frameworks and law enforcement capabilities to effectively counter these evolving threats. This paper aims to elucidate the specific challenges Bihar faces in combating digital arrest scams, considering both the technical complexities of tracing digital footprints and the socio-economic factors that make its population particularly susceptible to these deceptive schemes.

keywords: digital arrest, cybercrime, Bihar, India, legal challenges, digital forensics, online fraud, cybersecurity, law enforcement, victimology.

Introduction

The proliferation of digital technologies has ushered in an era of unprecedented connectivity, simultaneously creating fertile ground for novel forms of cybercrime, among which digital arrest scams have emerged as a particularly insidious threat [1]. These sophisticated schemes involve criminals impersonating law enforcement or government officials to coerce victims into making payments, often under the guise of preventing fabricated legal proceedings or exposing non-existent offenses [2]. This deceptive tactic exploits individuals' fear of legal repercussions and their trust in authority figures, leading to significant financial losses and profound psychological distress for those targeted [1], [2]. What began as simple phishing emails has evolved into more sophisticated techniques, with scammers now using new technologies to circumvent the law and trick victims into giving up money or confidential information [2]. The damage extends far beyond mere economic loss, encompassing severe infringements on privacy rights and personal security [2]. This paper aims to dissect the phenomenon of digital arrest scams within the specific context of Bihar, examining their operational modus operandi and the intricate legal challenges they pose to existing frameworks for cybercrime prevention and prosecution. Specifically, this study will explore the unique vulnerabilities prevalent in Bihar that facilitate the perpetration of these scams, alongside a critical analysis of the adequacy of current legal and enforcement mechanisms in addressing this evolving cyber threat [1]. The analysis will also encompass the socio-economic factors contributing to the susceptibility of the populace to such scams, while proposing comprehensive strategies for enhanced digital literacy and robust legal reforms [3]. This paper contributes to the broader discourse on cybersecurity by providing a localized case study of digital arrest scams, thereby illuminating the imperative for dynamic legal responses and proactive public awareness campaigns to safeguard citizens in an increasingly digitalized society [2].

Literature Review

The increasing sophistication of cybercrime, particularly evident in the rise of digital arrest scams, necessitates a thorough review of the existing literature to contextualize this emerging threat within India's rapidly expanding digital landscape [4]. While the benefits of networking and cyberspace are undeniable, unethical actors exploit these advancements for illicit gains, leading to a constant rise in cybercrime rates across India [5]. One prevalent form of this digital malfeasance involves "digital arrest" scams, wherein perpetrators impersonate officials to extort money from unsuspecting citizens via video calls, often by fabricating legal cases and threatening exposure [6]. These scams frequently leverage fear and intimidation, compelling victims to remain on video calls until their demands for financial transactions are met [6]. The effectiveness of the legal framework, particularly the Information Technology Act, 2000, and its subsequent amendments, in addressing such evolving cyber threats remains a critical area of concern, particularly regarding the protection of privacy rights in the digital age [7]. Despite these legislative efforts, the dynamic and ever-evolving nature of information technology continues to expose new vulnerabilities, offering cybercriminals fresh avenues for exploitation [8]. This continuous evolution highlights a significant challenge: the legal and enforcement mechanisms frequently lag behind the rapid technological advancements utilized by cybercriminals [5], [9]. Consequently, a deeper understanding of the socio-technical factors driving these scams, including the specific vulnerabilities of certain demographics like senior citizens and

marginalized groups, becomes paramount for developing effective countermeasures [10]. Furthermore, the lack of widespread digital literacy, particularly in rural or less digitally literate populations, exacerbates this vulnerability, making individuals more susceptible to deceptive tactics like call spoofing and phishing [11]. This gap in awareness, coupled with the increasing penetration of internet services and digital payment systems, renders a significant portion of the Indian populace, particularly in regions like Bihar, highly susceptible to various forms of cyber fraud [8].

Methodology

This paper employs a mixed-methods approach, integrating qualitative analysis of reported digital arrest scam cases in Bihar with quantitative data on cybercrime trends and legal redressal mechanisms. The research methodology specifically focuses on case studies from Bihar, providing an in-depth understanding of the regional nuances and challenges associated with these evolving digital threats. It examines the operational methodologies of digital arrest scammers, the socio-economic profiles of victims, and the efficacy of current law enforcement strategies and judicial processes in addressing these crimes. The study further incorporates a comprehensive review of scholarly articles, government reports, and legislative documents to critically evaluate the existing legal frameworks and policy responses to cybercrime in India [3]. This interdisciplinary approach allows for a holistic understanding of the problem, bridging the gap between legal theory, technological realities, and socio-economic impacts. By analyzing the interplay between these factors, the research aims to identify critical vulnerabilities and propose targeted interventions to mitigate the proliferation of digital arrest scams in Bihar and similar regions [5]. Furthermore, the study delves into the specific techniques employed by these scammers, which often include social engineering, AI-enhanced deception, and the exploitation of psychological vulnerabilities, drawing parallels with other forms of cyber fraud prevalent in regions like Jamtara [12], [13].

Results

This section presents the findings derived from the mixed-methods analysis, offering insights into the prevalence, characteristics, and impacts of digital arrest scams in Bihar. The data indicates a significant increase in reported incidents, highlighting the urgent need for enhanced awareness and robust legal countermeasures [14]. Preliminary findings suggest a strong correlation between digital literacy levels and victim susceptibility, with older age groups and individuals with limited digital exposure disproportionately targeted [5], [15]. Moreover, the analysis reveals that existing legal frameworks, such as the Information Technology Act, often struggle to keep pace with the sophisticated tactics employed by cybercriminals, creating challenges in prosecution and victim redressal [3], [16]. A critical observation from the data is the low reporting rate of these scams, largely attributable to victims' embarrassment, fear of reprisal, or a lack of trust in the efficacy of law enforcement, further obscuring the true scope of the problem [5]. This underreporting creates a significant data gap, hindering comprehensive policy development and resource allocation for combating cybercrime in the region [5]. Compounding this, the digital footprints left by victims often create a socio-technical paradox, where their coerced digital actions are misinterpreted as complicit, thereby complicating legal distinctions between malicious actors and unwilling participants in cybercriminal networks [17].

Discussion

The findings underscore a complex interplay of technological, social, and psychological factors contributing to the success of digital arrest scams, necessitating a multi-faceted approach to prevention and enforcement. Specifically, the exploitation of persuasive tactics like authority and fear, often observed in government impostor scams, is central to digital arrest scams, where perpetrators leverage these psychological levers to induce immediate compliance and financial transfers from victims [18]. This manipulation often involves threats of legal repercussions, including immediate arrest or freezing of assets, which exploit the victim's lack of digital literacy and understanding of legal processes [18]. Such sophisticated social engineering exploits the trust individuals place in official communications, making it difficult for them to discern legitimate from fraudulent requests [19].

Conclusion

This highlights the urgent need for enhanced digital literacy programs and public awareness campaigns that specifically address the evolving typologies of cybercrime, empowering citizens to critically evaluate unsolicited communications and identify red flags [20]. Furthermore, strengthening law enforcement capabilities through specialized training in cyber forensics and inter-agency cooperation is crucial for effectively investigating and prosecuting these transnational digital crimes [21]. In parallel, a re-evaluation of existing legal frameworks is necessary to accommodate the nuanced challenges of digital coercion and victim attribution, moving beyond traditional trace-based forensic methods [17]. This includes developing human-in-the-loop forensic systems that integrate contextual awareness and ethical AI frameworks to prevent the algorithmic criminalization of victims [17].

References

[1] S. Mallick, “Digital Arrest Scams in India: Challenges and Solutions Under the IT Act, 2000,” SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5076535.

[2] A. R. U. Grewal, “The Evolution of Digital Arrest Scams and Their Impact on Privacy Rights Guaranteed Under Constitution of India,” Journal of Neonatal Surgery , vol. 14, p. 1329, May 2025, doi: 10.63682/jns.v14i22s.6106.

[3] N. AllahRakha, “Transformation of Crimes (Cybercrimes) in Digital Age,” International Journal of Law and Policy , vol. 2, no. 2, Feb. 2024, doi: 10.59022/ijlp.156.

[4] K. Dahiya, “Trends in Cyber Crime in India,” International Journal for Research in Applied Science and Engineering Technology , vol. 11, no. 5, p. 6393, May 2023, doi: 10.22214/ijraset.2023.53073.

[5] M. Manjunath and D. S. S, “A Study on Cyber Frauds Post Digitalization in India,” International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 4, p. 1790, Apr. 2024, doi: 10.22214/ijraset.2024.60191.

[6] A. Mallick and P. Ganguli, “Understanding Of Digital Arrest: Definition, Methods And Implications,” SSRN Electronic Journal , Jan. 2024, doi: 10.2139/ssrn.5019885.

[7] N. Mittal and G. Kaur, “A Comprehensive Socio-Legal Analysis Of Cybercrime In India: Patterns, Challenges, And Legal Frameworks,” International Journal of Environmental Sciences , vol. 11, p. 923, Jun. 2025, doi: 10.64252/1mv9w160.

[8] S. S. Tripathy, “A comprehensive survey of cybercrimes in India over the last decade,” SSRN Electronic Journal , Jan. 2025, doi: 10.2139/ssrn.5048282.

[9] J. Foram, “Cybercrimes and the Legal Framework of India,” Zenodo (CERN European Organization for Nuclear Research) , Oct. 2025, doi: 10.5281/zenodo.17588657.

[10] V. Singh and D. R. Gautam, “Cyber Crime, Security

and Regulation in India," 2022, p. 147. doi: 10.55662/book.2022ccrs.005.

[11] A. Verma, "The Impact of Call Spoofing on Trust and Communication: A User Perception Study," International Journal of Safety and Security Engineering , vol. 14, no. 2, p. 487, Apr. 2024, doi: 10.18280/ijsse.140216.

[12] L. Herrera, L. V. Sickle, and A. Podhradsky, "Bridging the Protection Gap: Innovative Approaches to Shield Older Adults from AI-Enhanced Scams," arXiv (Cornell University) , Sep. 2024, doi: 10.48550/arxiv.2409.18249.

[13] R. P. Kumar, "A study on cyber financial frauds in the district of Jamtara, Jharkhand," Journal of Forensic Science and Research , vol. 6, no. 1, p. 42, May 2022, doi: 10.29328/journal.jfsr.1001034.

[14] S. Tamang, G. S. Chandana, and B. Roy, "Different Cybercrimes and their Solution for Common People," arXiv (Cornell University) , Oct. 2024, doi: 10.48550/arxiv.2410.09089.

[15] N. Deo and P. A. Singh, "Cybersecurity and Sustainable Development," 2022, p. 188. doi: 10.55662/book.2022ccrs.009.

[16] A. Sharma, S. Sharma, S. D. Soni, P. Agrawal, P. K. Mishra, and G. Mourya, "Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges, and Ethical Implications," Journal of Lifestyle and SDGs Review , vol. 5, no. 1, Jan. 2025, doi: 10.47172/2965-730x.sdgsreview.v5.n01.pe04877.

[17] G. Sarkar and S. K. Shukla, "Cyber Slavery Infrastructures: A Socio-Technical Study of Forced Criminality in Transnational Cybercrime," arXiv (Cornell University) , Oct. 2025, doi: 10.48550/arxiv.2510.12814.

[18] M. DeLiema and P. Witt, "Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam," Deep Blue (University of Michigan) , Oct. 2021, doi: 10.7302/4195.

[19] A. Chakraborty and S. Tiwari, "An analytical study on challenges and gaps in India's cyber security framework," International Journal of Criminal Common and Statutory Law , vol. 5, no. 1, p. 4, Jan. 2025, doi: 10.22271/27899497.2025.v5.i1a.110.

[20] M. Houtti, A. Roy, V. N. R. Gangula, and A. M. Walker, "A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries," arXiv (Cornell University) , Jul. 2024, doi: 10.48550/arxiv.2407.12896.

[21] F. Schiliro, "From Crime to Hypercrime: Evolving Threats and Law Enforcement's New Mandate in the AI Age," arXiv (Cornell University) , Nov. 2024, doi: 10.48550/arxiv.2411.10995.