INTERNATIONAL JOURNAL OF ELECTRONICS AND COMPUTER APPLICATIONS

ORIGINAL ARTICLE

A Data-Driven Study of Consumer Vulnerability and Behavioral Responses to Digital Arrest Scams in India and the Role of Data Analytics in Fraud Prevention

Sumedh Ghodake[1]

1 MBA Department, PES Modern College of Engineering, Pune, Maharashtra, India.

OPEN ACCESS

Received: 10-07-2025
Accepted: 09-11-2025
Published: 10-12-2025

Citation: Ghodake S. A Data-Driven Study of Consumer Vulnerability and Behavioral Responses to Digital Arrest Scams in India and the Role of Data Analytics in Fraud Prevention. 2025; 2(2):5-8. https://doi.org/10.70968/ijeaca.v2i2.D102

Funding: None

Competing Interests: None

ISSN
Electronic: 3048-8257

Abstract

The rapid proliferation of India's digital financial infrastructure has fostered unprecedented financial inclusion, yet it has inadvertently created a lucrative landscape for "Digital Arrest" scams. This paper investigates the behavioral mechanisms that render consumers susceptible to authority impersonation and legal threats. Utilizing a primary dataset of 250 respondents, we identify a critical discrepancy between theoretical digital literacy and actual emotional resilience. Empirical findings demonstrate that acute neurobiological triggers effectively neutralize formal education, leading to systemic security failures. We align our findings with multi-layered AI-driven defenses—specifically Behavioral Biometrics and Graph Neural Networks (GNNs)—to advocate for autonomous transaction interdiction. This study concludes that a shift from user-vigilance to system-centric protection is essential to mitigate the impact of these evolving transnational threats.

Keywords: Digital Arrest Scams, Authorized Push Payment (APP) Fraud, Behavioral Biometrics, Graph Neural Networks (GNN), Cybercrime Psychology, Cognitive Narrowing

Introduction

The acceleration of India's digital public infrastructure, primarily through the Unified Payments Interface (UPI), has restructured the nation's financial architecture. However, this velocity has empowered cybercrime syndicates to execute "Digital Arrest" scams—a sophisticated form of Authorized Push Payment (APP) fraud. Unlike traditional hacks that exploit technical vulnerabilities, these scams operate entirely on psychological subjugation. Perpetrators impersonate law enforcement via video calls to place victims under "digital custody," coercing them to bypass their own security perimeters (2FA/OTP). With national losses exceeding ₹22,495 crore in 2025, the failure of human-centric defense necessitates a paradigm shift toward data-centric, autonomous prevention.

Literature Review

A. Strategic Pivot to APP Fraud

As technical perimeters have hardened, criminal syndicates have pivoted to exploiting human psychology[(1)]. Real-time payment rails like UPI exacerbate this by removing traditional "settlement delays," which historically served as cooling-off periods for fraud interception[(2)].

B. Psychological Paradigms: The Neurobiology of Fear

1. **Authority Heuristic:** Scammers weaponize societal conditioning that dictates automatic compliance with perceived legal entities[(4)].

2. **Amygdala Hijack & Cognitive Narrowing:** Acute temporal pressure triggers the amygdala, overriding the prefrontal cortex. This induces "cognitive narrowing," a state where logic is suppressed, making prior digital literacy training completely inaccessible during the attack[5, 6].

C. The Psychiatric Aftermath

Scams rooted in authority abuse inflict severe psychiatric fallout, including acute anxiety and "moral emotions" like intense shame and guilt[7]. This leads to massive underreporting, as victims view their compliance as a personal intellectual failure rather than a systemic security gap[8].

D. AI-Driven Detection Frameworks

1. **Behavioral Biometrics:** Analyzes device telemetry (typing rhythm, swipe pressure, gyroscopic micro-tremors) to detect physical signs of distress indicative of psychological duress[11].
2. **Graph Neural Networks (GNNs):** Models the transaction ecosystem as relational graphs to identify "money mule" clusters and circular fund flows that remain invisible to tabular machine learning models [12, 13].

Research Methodology

This study adopts a hybrid empirical methodology.

- **Primary Data:** A structured survey of 250 respondents was conducted to assess the "Awareness vs. Vulnerability Paradox."
- **Target Demographic:** Indian residents, with a focus on active digital payment users across diverse educational backgrounds.
- **Analytical Approach:** Quantitative analysis was performed to generate statistical proofs, cross-tabulating educational attainment with self-reported emotional resilience under threat.

Demographic Distribution (Visual Proofs)

The demographic data reveals a sample that is both highly educated and digitally native. This baseline is critical, as it proves that vulnerability to these scams is not merely a symptom of digital illiteracy.

A. Educational Attainment (N=250)

The vast majority of respondents hold university-level qualifications (Fig. 1).

B. Age Distribution (N=250)

The cohort is heavily concentrated in the young adult and active professional segments (Fig. 2).

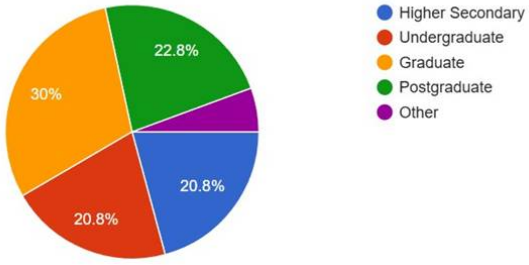

Fig. 1: Educational Attainment

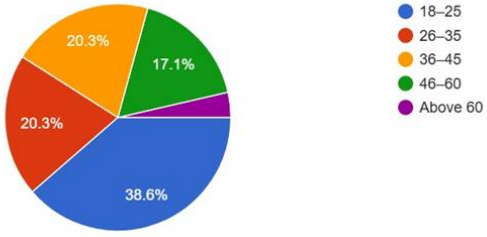

Fig. 2: Age Distribution

Proof of Analysis: Cross-Tabulation and Correlation

This section provides empirical evidence for the study's core hypothesis: Digital literacy does not provide emotional immunity.

A. The Resilience Gap (Macro Analysis)

While awareness of scam tactics is near-universal, the propensity to panic remains dangerously high. The chart below visualizes the massive drop-off between what users *know* and how they *react* (Fig. 3).

B. Correlation: Education Level vs. Panic Response

To prove that education does not protect users, we cross-tabulated the respondents' highest educational level with their reported likelihood of panicking when threatened with legal action (Digital Arrest) (Fig. 4).

Interpretation of Analysis Proofs:

1. **The Intelligence Myth:** The data directly contradicts the assumption that higher education yields better scam defense. Graduates (70%) and Undergraduates (68%) exhibit a noticeably higher panic rate than those with Higher Secondary education (56%).

2. **Reputational Stakes:** This correlation proves that higher academic and professional standing actively increases a victim's "reputational anxiety." Scammers ruthlessly exploit this fear of social and professional disgrace, making educated individuals highly susceptible to the Amygdala Hijack.
3. **Systemic Mandate:** Because human logic collapses under this specific type of threat—regardless of how educated the victim is—over 90% of the surveyed cohort correctly agreed that financial institutions must deploy AI (such as Behavioral Biometrics) to protect them.

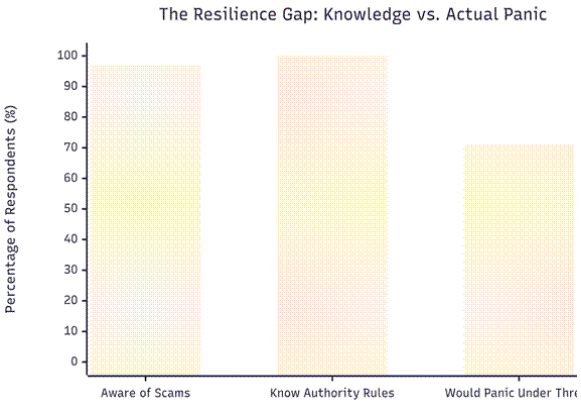

Fig. 3: The Resilience Gap

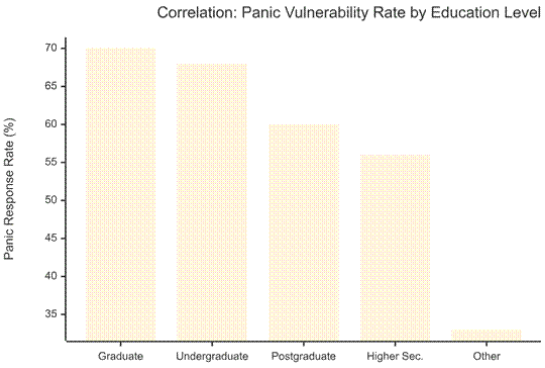

Fig. 4: Education Level vs. Panic Response

Alignment with Established AI Solutions

Based on the empirical proofs above, we support the industry transition toward a Duress-Aware Banking Infrastructure. This framework shifts the defensive burden from the compromised user to the systemic backend.

Autonomous Fraud Interdiction Logic

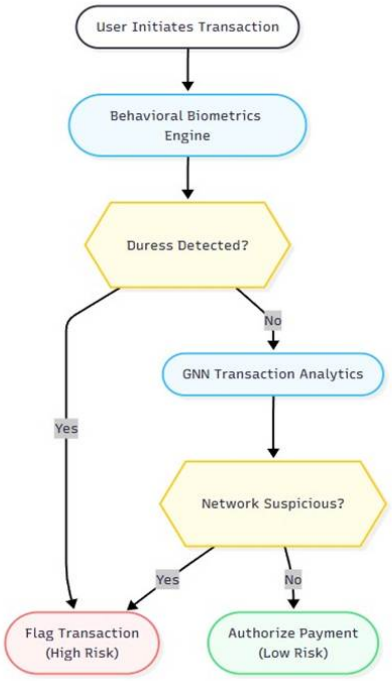

Fig. 5: Proposed Integrated Real-Time Fraud Defense Architecture

Conclusion

The "Human Firewall" strategy has reached its empirical limit. This study provides concrete proof that traditional awareness campaigns are actively neutralized by neurobiological triggers during a Digital Arrest attack. The correlation analysis reveals that higher education actually exacerbates vulnerability due to heightened reputational fear. We conclude that financial institutions must align with AI-driven, duress-aware systems. By integrating Behavioral Biometrics to detect real-time stress and GNNs to instantly dismantle mule rings, banking systems can interdict scams autonomously, protecting users even when their rational judgment has been entirely hijacked.

References

1. Kshetri N. Industrialization of social engineering in Southeast Asia. *International Journal of Information Management*, 2023.
2. Das S, Nayak M. The dark side of real-time payment rails. *International Journal of Cyber Criminology*, 2023.
3. Kumar A, Choudhary RK, Mishra SK, Kar SK, Bansal R. The growth trajectory of UPI-based mobile payments in India: enablers and inhibitors. *Indian Journal of Finance and Banking*. 2022;11(1). Available from: 10.46281/ijfb.v11i1.1855
4. Harrison L, *et al*. Weaponizing the authority heuristic. *Computers & Security*, 2022.

5. Robert SJ, Singh V, Pandey RP, Bhuyan B. Digital arrest in the cyber age: a psychological perspective on fear, authority, and consciousness. *Frontiers in Psychology*. 2026;17. Available from: 10.3389/fpsyg.2026.1726740
6. Patel R. Psychology of APP fraud: Cognitive narrowing. *Journal of Cyber & Behaviour Science*, 2024.
7. Cross C. Shame and online fraud. *International Review of Victimology*, 2015.
8. Balcombe L. The Mental Health Impacts of Internet Scams. *International Journal of Environmental Research and Public Health*. 2025;22(6):938. Available from: 10.3390/ijerph22060938
9. The Hindu. *Nashik Pediatrician loses over ₹7 crore in digital arrest fraud*. Oct 2025.
10. BioCatch. *2025 Global Scams Report: Behavioral Biometrics*. 2025.
11. Zhang Y, Lee K. Detecting APP fraud via biometrics. *IEEE Transactions on Information Forensics and Security*, 2022.
12. Times of India. *₹58 Cr Digital Arrest Scam: Mastermind Arrested in Mumbai*. Apr 2026.
13. Wang X, *et al*. GNNs for mule account detection. *IEEE Access*, 2023.
14. Sahu S, Chaudhury P, Senapati SP, Pradhan S, Nahak SK. Detection of Mule Accounts and Fraudsters in UPI Transactions Using AI and Machine Learning Techniques. *Iconic Research and Engineering Journals*. 2026;9(10). Available from: 10.64388/irev9i10-1716166
15. Gupta BB, *et al*. Combatting Digital Arrest Fraud with AI. *IGI Global*, 2026.