
CYBER FRAUD IN JHARKHAND: SOCIO-ECONOMIC DRIVERS, VICTIM VULNERABILITIES AND SPATIAL CONCENTRATION

Satya Prakash, Research Scholar, Faculty of Law,
Swami Vivekanand Subharti University, Meerut, Uttar Pradesh, India

Prof. Vaibhav Goel Bhartiya, Professor, Faculty of Law,
Swami Vivekanand Subharti University, Meerut, Uttar Pradesh, India

ABSTRACT

Cyber fraud in Jharkhand presents a distinctive socio-legal problem because digital victimisation coexists with locally concentrated offender networks, uneven digital literacy, rapid expansion of mobile payments, and a long-standing public association of districts such as Jamtara with social-engineering fraud. This article examines the prevalence and changing pattern of cyber fraud in Jharkhand, with particular emphasis on socio-economic drivers and victim vulnerability. The study uses a structured secondary-data design drawing on National Crime Records Bureau figures, Ministry of Home Affairs parliamentary material, the National Cyber Crime Reporting Portal framework, and recent peer-reviewed research concerning Jamtara and cyber-fraud victims in Jharkhand. NCRB data show that total registered cyber-crime cases in Jharkhand increased from 953 in 2021 to 1,079 in 2023, while the narrower fraud-for-cyber-crime category fluctuated from 79 cases in 2021 to 98 in 2022 and 43 in 2023. The divergence demonstrates why police registration statistics cannot be treated as a direct measure of underlying victimisation. Recent evidence further identifies Deoghar, Jamtara and Dumka among important places of cyber-crime origination and highlights the interaction of unemployment, local peer learning, social engineering, weak verification habits and digital opportunity structures. The article develops an integrated vulnerability pathway that distinguishes offender-side opportunity from victim-side exposure. It argues that prevention in Jharkhand should combine targeted digital-literacy interventions, behavioural verification routines, community-level deterrence, employment-linked prevention in high-risk districts, and rapid reporting through 1930/NCRP. The contribution is a state-specific framework that moves beyond the stereotype of a single “phishing hub” and treats cyber fraud as a dynamic socio-economic ecosystem requiring both victim protection and local structural intervention.

Keywords: Cyber fraud, Jharkhand, Jamtara, victim vulnerability, social engineering, digital literacy, socio-economic factors, cybercrime patterns.

I. Introduction

Digital financial services have lowered transaction costs and widened access to banking, commerce and public services, but the same infrastructure has expanded the attack surface for deception-based crime. In Jharkhand, the cyber-fraud problem has a dual character. The state records substantial victimisation and complaint activity, while some districts have also acquired national visibility as places from which social-engineering fraud is organised. The doctoral synopsis on which this article is based identifies the need to study prevalence, offender and victim demographics, socio-economic conditions, technology access and diversity of cyber threats within Jharkhand. The present article concentrates on these socio-economic and pattern-related objectives and develops a coherent state-level analysis.

The empirical challenge is that no single dataset measures cyber fraud completely. Police registration data reflect reporting, classification and enforcement practices; national portal complaints capture a wider range of reported incidents but are not identical to FIRs; and qualitative studies capture mechanisms rather than population prevalence. Accordingly, the paper triangulates official trend data with recent victim and offender research. The objective is not to infer that poverty or low education causes cybercrime. Instead, the analysis asks how structural disadvantage, digital opportunity, local learning networks and victim exposure can interact to create a durable fraud ecosystem.

This distinction matters for policy. A response centred only on arrests may displace operations without changing recruitment incentives, while awareness campaigns that blame victims can ignore the industrialised and adaptive character of fraud. Effective prevention requires a model that treats offenders, victims, digital platforms and local institutions as parts of the same risk environment.

II. Research Objectives and Questions

This article addresses three objectives derived from the broader synopsis: (i) to assess recent prevalence and patterns of cybercrime and cyber fraud in Jharkhand; (ii) to examine socio-economic and technology-related conditions associated with offending and victim vulnerability; and (iii) to identify prevention priorities that can be tailored to high-risk groups and districts. The guiding questions are: What do recent official statistics reveal about the scale and direction of cybercrime in Jharkhand? Which offender-side and victim-side mechanisms

are supported by current research? How can prevention be designed without reducing the problem to a single district stereotype?

III. Methodology

The study adopts a structured secondary-data and socio-legal review design. It uses official NCRB statistics reproduced in Ministry of Home Affairs/Press Information Bureau materials for 2021-2023; parliamentary information identifying major places of cybercrime origination in 2024; the Government of India cybercrime-reporting architecture; and peer-reviewed studies published between 2023 and 2026. Sources were selected for direct relevance to Jharkhand, victim vulnerability, organised fraud, or socio-economic impacts. Descriptive comparison is used for trend analysis; qualitative synthesis is used to identify mechanisms. Because the source synopsis proposes later interviews and surveys but does not contain completed primary data, this paper does not invent survey results or claim original field findings.

Table 1. Registered cyber-crime and cyber-fraud cases in Jharkhand

Indicator	2021	2022	2023	Interpretive note
All registered cyber-crime cases	953	967	1079	Steady increase across the three-year series.
Fraud-for-cyber-crime cases	79	98	43	Volatile series; narrower classification than all cybercrime.
Three-year direction	Baseline	+1.5% vs. 2021	+13.2% vs. 2021	Registration growth does not equal underlying incidence.

IV. Prevalence and Spatial Pattern

Jharkhand recorded 953 registered cyber-crime cases in 2021, 967 in 2022 and 1,079 in 2023. The increase from 2021 to 2023 is approximately 13.2 percent. This is meaningful but should be interpreted cautiously: changes in registration can reflect reporting awareness, police capacity, classification practice and access to complaint channels in addition to changes in offending. The fraud-specific subset is even more volatile, rising from 79 in 2021 to 98 in 2022 and falling to 43 in 2023. A narrow statutory or motive category therefore should not be used as a proxy for the whole digital-fraud environment.

Spatial concentration is more informative when combined with other evidence. A 2024 parliamentary reply, based on suspect mobile numbers reported on the National Cyber Crime Reporting Portal, listed Deoghar, Jamtara and Dumka among major places of origination of cybercrime in India. This pattern supports the synopsis's decision to treat Jharkhand as a distinctive field setting, but it also shows that the phenomenon extends beyond Jamtara. Policy that labels one district as the problem may miss mobility, network diffusion and displacement across district borders.

The most recent peer-reviewed study focused directly on Jamtara describes an evolution from relatively simple phishing toward organised, role-specialised fraud networks. Interviews and document analysis in that research identify social engineering, concealment, peer transmission of know-how, informal training, rapid financial returns and local support structures as important mechanisms. These findings are consistent with a broader literature showing that contemporary cybercrime can resemble an industry with division of labour rather than an activity carried out only by technically advanced lone offenders.

V. Socio-Economic Drivers on the Offender Side

Economic disadvantage should be treated as a contextual risk factor rather than a deterministic explanation. Jharkhand contains regions where formal employment opportunities are limited and where the visible returns from fraud can sharply exceed local legal earning opportunities. In such settings, successful offenders can create demonstration effects: techniques become locally teachable, proceeds create status incentives, and recruitment costs decline when trust already exists within friendship or kinship networks. The 2026 Jamtara study is especially important because it reports organised networks, family-linked participation, peer learning and cybercrime-as-a-service dynamics rather than merely individual deviance.

Technology access also has a paradoxical role. Cheap smartphones, SIM availability, digital payments and remote communication support legitimate inclusion while simultaneously reducing entry barriers for deception-based offending. Many social-engineering schemes do not require advanced malware development. They require scripts, lists of targets, impersonation skill, account or mule access, and an ability to create urgency. This lowers the technical threshold for participation and permits division of labour between callers, account handlers, recruiters and cash-out actors.

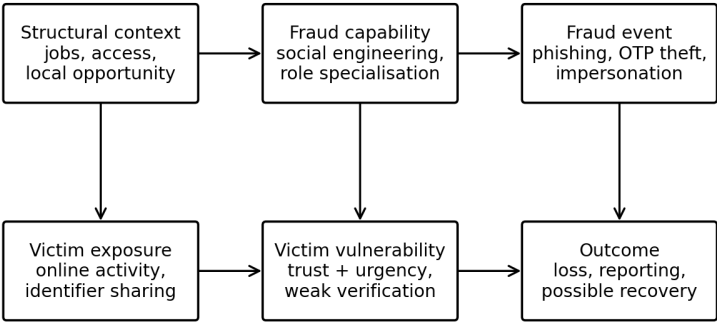
Local normalisation can further reduce perceived moral and enforcement costs. Where illegal income becomes socially visible but punishment appears uncertain or delayed, deterrence weakens. The policy implication is not mass suspicion of communities. It is the opposite: prevention should focus on specific recruitment pathways, illicit service markets, money-mule networks and repeated identifiers while creating legitimate skill and employment alternatives for youth.

VI. Victim-Side Vulnerability and Exposure

Cyber fraud depends on a successful interaction between an offender's technique and a victim's moment of exposure. A 2025 study of older cyber-fraud victims drawn from cyber police stations in Ranchi and Jamshedpur provides rare Jharkhand-specific evidence. Among the older victim subsample, pre-fraud digital behaviour included sharing identifiers and participating in online activities that created opportunities for manipulation. The authors caution that their sample is limited and not population-representative, but the study is valuable because it shifts attention from static demographic labels to behaviours and contexts of exposure.

Age, income, education and location can influence vulnerability, but none should be treated as a simple risk score. Digital confidence without verification habits can be as dangerous as low digital literacy. Fraud scripts often exploit authority, scarcity, fear, speed and trust: a bank impersonation, a KYC warning, a police or courier threat, an investment promise, or a request to install remote-access software. The relevant protective behaviour is therefore not merely knowing that cybercrime exists; it is having an automatic verification routine before sharing credentials, transferring funds or acting on an unsolicited instruction.

Victimisation also imposes non-financial harm. Recent socio-economic impact research emphasises stress, fear, loss of trust and broader social consequences. In Jharkhand, these harms may be amplified when victims are reluctant to report because of embarrassment, uncertainty over jurisdiction or fear that recovery is unlikely. Prevention policy should therefore measure reporting speed and victim support, not only the number of awareness events conducted.



The model treats offender opportunity and victim exposure as interacting risk pathways rather than deterministic causes.

Fig. 1. Integrated socio-economic and victim-vulnerability pathway for cyber fraud in Jharkhand.

VII. A Risk Matrix for Jharkhand

Table 2. Mechanism-based risk matrix

Risk mechanism	Observable indicator	Likely effect	Priority response
Peer transmission of fraud skills	Repeated local clusters; shared scripts or identifiers	Lower entry cost for new offenders	Network-focused investigation and youth diversion.
Money-mule availability	Rapid movement through multiple accounts	Weakens traceability and recovery	Bank analytics, mule awareness, rapid freeze requests.
Impersonation and urgency	Calls/messages claiming bank, police, courier or authority identity	Reduces verification time	Behavioural prompts: stop, verify, call official number.
High digital exposure	Frequent online participation and sharing of identifiers	Expands attack opportunities	Segmented awareness for older users and new digital adopters.

Under-reporting or delayed reporting	Large gap between fraud and complaint time	Reduces fund-recovery probability	Immediate 1930/NCRP reporting protocol.
--------------------------------------	--	-----------------------------------	---

VIII. Prevention Framework

First, Jharkhand should move from generic cyber-awareness messaging to behavioural prevention. Campaigns should teach a short verification sequence: do not act on urgency; independently verify the caller or sender; never disclose OTP, PIN or remote-access permission; and report suspected financial fraud immediately through 1930 or the National Cyber Crime Reporting Portal. The sequence should be repeated in banks, panchayats, colleges, self-help groups and community centres.

Second, prevention should be geographically differentiated. Districts repeatedly associated with origination patterns require network-disruption strategies, money-mule detection, school and college interventions, and livelihood-linked diversion measures. Victim-heavy urban locations such as Ranchi and Jamshedpur need strong reporting assistance, senior-citizen outreach and bank-platform coordination. A single statewide campaign cannot address both sides of the ecosystem with equal effectiveness.

Third, evaluation should focus on outcomes. Useful indicators include median time from fraud to 1930 reporting, share of complaints with attempted transaction holds, repeat use of suspect identifiers, victim awareness of independent verification, and the proportion of high-risk institutions providing standardised response instructions. These measures are more informative than counting pamphlets or seminars.

Finally, public communication should avoid glamorising or stigmatising Jamtara. The district's notoriety can unintentionally reinforce a criminal brand and obscure victims and law-abiding residents. A research-informed approach should describe the mechanisms of fraud, the changing geography of networks, and the routes through which young people are recruited, while preserving community legitimacy and cooperation.

IX. Discussion

The evidence supports a layered explanation of Jharkhand cyber fraud. Official cases show persistence rather than a simple linear surge; parliamentary data point to multiple origination

districts; offender research shows role specialisation and local learning; and victim research demonstrates that online habits and situational exposure matter. These layers challenge two common errors: treating cyber fraud only as a technical hacking problem, and treating it only as a poverty problem. The more useful unit of analysis is the interaction between digital opportunity, social organisation, behavioural manipulation and response speed. This also explains why interventions should combine law enforcement with financial-sector controls, community prevention and targeted digital-literacy design.

X. Limitations and Future Research

The study is based on secondary data. NCRB registered cases are not equivalent to true prevalence, and portal-origin data based on suspect mobile numbers do not establish offender residence or guilt. The Jharkhand-specific victim study is valuable but has a limited sample, while qualitative research on Jamtara cannot be generalised mechanically to the whole state. Future work should implement the synopsis's proposed interviews and surveys, with district-stratified sampling, separate victim and offender instruments, and measures of reporting delay, digital practices, occupation, income band, education and prior awareness. A longitudinal design would help distinguish changing fraud techniques from changes in reporting behaviour.

XI. Conclusion

Cyber fraud in Jharkhand is best understood as a socio-technical ecosystem. The state's registered cyber-crime caseload increased between 2021 and 2023, while fraud-specific registration fluctuated; at the same time, Deoghar, Jamtara and Dumka appeared among nationally important origination locations. Recent research demonstrates how local opportunity structures and organised social-engineering networks can coexist with diverse victim vulnerabilities. The policy response should therefore join rapid financial-fraud reporting, behavioural verification, geographically targeted enforcement, money-mule disruption and locally credible prevention. Such a framework directly advances the synopsis's objectives on prevalence, socio-economic factors and threat diversity while providing a self-contained basis for future empirical fieldwork.

REFERENCES:

- [1] Ministry of Home Affairs, Government of India, “Cyber Crime Cases,” Press Information Bureau, 17 Mar. 2026, Annexure-I (NCRB Crime in India 2023 data).
- [2] Ministry of Home Affairs, Government of India, Rajya Sabha Unstarred Question No. 553, “Fraud for Cyber Crimes,” 4 Feb. 2026, Annexure.
- [3] Ministry of Home Affairs, Government of India, Rajya Sabha Unstarred Question No. 1029, 31 Jul. 2024 (major places of origination based on suspect mobile numbers reported on NCRP).
- [4] G. Sarkar, V. S. C. Putrevu, and S. K. Shukla, “Understanding Jamtara cybercriminals: poverty, opportunity, and the rise of organized criminal networks,” *Humanities and Social Sciences Communications*, vol. 13, art. 1365, 2026, doi:10.1057/s41599-026-07703-0.
- [5] S. Kumar and M. Patel, “Digital habits and cyber vulnerabilities among older victims of cyber fraud,” *Working with Older People*, vol. 29, no. 4, pp. 433-443, 2025, doi:10.1108/WWOP-04-2025-0018.
- [6] Q. Luo, “Cybercrime as an industry: examining the organisational structure of Chinese cybercrime,” *Humanities and Social Sciences Communications*, vol. 11, art. 1554, 2024, doi:10.1057/s41599-024-04042-w.
- [7] A. Collier, D. R. Thomas, R. Clayton, and A. Hutchings, “Bootling the booters: evaluating the effects of police interventions in the market for denial-of-service attacks,” *Internet Policy Review*, vol. 11, no. 4, 2022.
- [8] C. Cross, “Romance fraud,” in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Cham: Palgrave Macmillan, 2020.
- [9] European Commission Joint Research Centre et al., “Assessing the socio-economic impacts of cybercrime,” *Societal Impacts*, vol. 1, 2023, 100013, doi:10.1016/j.socimp.2023.100013.
- [10] Ministry of Home Affairs, Government of India, “National Cyber Crime Reporting Portal,” cybercrime.gov.in, accessed Oct. 4, 2026.

- [11] Ministry of Home Affairs, Government of India, Annual Report 2023-24, section on Indian Cyber Crime Coordination Centre and Citizen Financial Cyber Fraud Reporting and Management System.
- [12] National Crime Records Bureau, Crime in India 2023, Ministry of Home Affairs, Government of India.
- [13] R. Leukfeldt and M. Yar, "Applying routine activity theory to cybercrime: a theoretical and empirical analysis," *Deviant Behavior*, vol. 37, no. 3, pp. 263-280, 2016.
- [14] J. Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge, MA: Harvard University Press, 2018.
- [15] K. Jaishankar, Ed., *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC Press, 2011.