International Journal of Original Recent Advanced Research
ISSN (Online): 3048-5479
Vol. 02, Issue 06, November 2025

A CRITICAL ANALYSIS OF CYBERCRIME AND DIGITAL VICTIMIZATION IN THE EVOLVING INFORMATION ERA

Sahil Yadav[1], Dr. Patilshwetali Sanjay[2]

Research Scholar, Department of Law, SunRise University, Alwar[1]

Research Supervisor, Department of Law, SunRise University, Alwar[2]

ABSTRACT

The rapid digitalization of information systems has created an unprecedented vulnerability landscape for individuals, organizations, and sovereign states. This study critically analyses cybercrime and digital victimization in the contemporary information era, with particular emphasis on India's escalating cybercrime trajectory. The primary objectives are to examine typological patterns of cybercrime and to identify structural determinants of digital victimization. Secondary data from the National Crime Records Bureau (NCRB), Reserve Bank of India (RBI), IBM Security Reports, and Indian Cyber Crime Coordination Centre (I4C) were employed within a descriptive-analytical framework. The hypothesis posits that increasing digital penetration is significantly and positively associated with rising cybercrime incidence and financial victimization. Results reveal that India recorded 86,128 cybercrime cases in 2023 a 31.2% increase over the preceding year while the global average data breach cost reached $4.88 million in 2024. Financial fraud constitutes over 60% of domestic cybercrime, and trial conviction rates remain below 3%. The discussion underscores institutional inadequacies, legislative gaps, and the urgent need for multi-stakeholder cybersecurity governance frameworks. The study concludes that legislative reform, enhanced digital literacy, and robust international cooperation are indispensable for effective cybercrime mitigation across rapidly digitalizing economies.

Keywords: *Cybercrime[1], Digital Victimization[2], Online Financial Fraud[3], Information Era[4], Cybersecurity[5].*

1. INTRODUCTION

The proliferation of internet infrastructure, mobile computing, and digital financial systems has fundamentally reconfigured both the opportunities and risks of modern society. In this evolving information era, cybercrime has emerged as one of the most pervasive and economically destructive categories of criminal conduct globally. The term "cybercrime" encompasses a broad spectrum of offences including financial fraud, phishing, ransomware attacks, identity theft, cyberstalking, and the exploitation of vulnerable populations through digital

platforms. Unlike conventional crime, cybercrime transcends geographic boundaries, operates in real time across jurisdictions, and disproportionately burdens victims who lack digital literacy or institutional recourse. India occupies a particularly critical position within this global phenomenon. With over 600 million active internet users as of 2023, and a rapidly expanding digital payments ecosystem anchored by the Unified Payments Interface (UPI), India has become one of the most targeted nations for cybercriminal activity. The National Crime Records Bureau recorded a staggering 31.2% increase in registered cybercrime offences between 2022 and 2023, rising from 65,893 to 86,128 cases (NCRB, 2024). These figures, however, represent a fraction of actual victimization, as structural barriers to reporting including social stigma, limited awareness of legal remedies, and bureaucratic dissuasion systematically suppress formal complaint registration.

Digital victimization extends far beyond financial harm. Victims of cyberstalking, identity theft, and online harassment experience documented psychological consequences, including heightened anxiety, diminished trust in digital systems, and prolonged emotional distress (Borwell et al., 2022). Women, elderly populations, and economically marginalized groups are disproportionately affected, as they are simultaneously less equipped with protective digital behaviours and more frequently targeted through social engineering schemes. The India Threat Landscape Report 2024 documented 593 cyberattacks and 388 data breaches in just the first half of 2024, emphasizing the accelerating pace of digital threats against Indian infrastructure and individuals. Globally, cybercrime costs are projected to reach $10.5 trillion annually by 2025 (Cybersecurity Ventures, 2020), with the average cost of a single data breach climbing to $4.88 million in 2024 (IBM Security, 2024). These figures underscore the macroeconomic dimensions of a threat that conventional criminological frameworks inadequately address. India's Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, constitute the primary legislative instruments, yet both face criticism for limited enforceability against rapidly evolving criminal tactics. The trial conviction rate below 3% in 2023 further exposes a systemic failure of the criminal justice system to hold cybercriminals accountable (Ministry of Home Affairs, 2024). Against this backdrop, this paper undertakes a critical and data-driven analysis of cybercrime trends and digital victimization patterns, contributing to scholarly and policy discourse through verified empirical evidence anchored within established cyber criminological theory and digital security governance.

2. LITERATURE REVIEW

The academic field of cyber criminology has witnessed substantial growth over the past two decades, mirroring the exponential rise in internet-facilitated crimes. A landmark bibliometric study by Ho and Luong (2022) analyzing 387 Social Science Citation Index articles on cybercrime victimization (2010–2020) identified a decidedly upward publication trend, with financial fraud, identity theft, and phishing emerging as the most studied victimization typologies. This review further established that while the United States dominates global research output, contributions from rapidly digitalizing economies such as India remain underrepresented despite their acute and growing vulnerability a gap this paper seeks to partially address. Theoretical explanations for cybercrime victimization have predominantly drawn upon Routine Activity Theory (RAT) and its digital adaptations. Leukfeldt and Yar (2016) empirically demonstrated that routine online behaviours such as frequent e-commerce transactions, unsecured network usage, and limited guardianship significantly elevate vulnerability to cyber offences. Their extension of Cohen and Felson's classical framework into virtual environments argued

that the absence of capable guardianship in digital spaces creates conditions analogous to physical crime hotspots. Gainey et al. (2023) further confirmed that everyday internet behaviours, including social media activity frequency and online banking usage, independently predict cyber victimization risk across a state-wide Virginia sample, validating the cross-contextual applicability of routine activity frameworks.

Phishing the most prevalent global attack vector has been critically examined by Ghazi-Tehrani and Pontell (2021), whose qualitative research revealed distinct victimization pathways for both technologically sophisticated and entirely naïve users. Their typological distinction between mass (wide) and targeted spear-phishing (narrow) attacks carries important implications for differentiated prevention design. In the Indian context, Thangamayan et al. (2023) documented that cheating by impersonation nearly doubled between 2022 and 2023, confirming similar patterns of technologically sophisticated fraud targeting populations with heterogeneous digital competency levels. The psychological consequences of cybercrime have been comprehensively mapped by Borwell et al. (2022), whose survey of 2,415 Dutch cybercrime victims found that older victims, women, and lower socioeconomic status individuals suffered the greatest emotional harm and erosion of perceived personal security. Victims of device hacking and prolonged cybercrime experienced compounded trauma, consistent with shattered assumptions theory. Fonseca et al. (2022) extended this analysis to underreporting dynamics, finding that shame, distrust of law enforcement, and perceived investigative futility systematically reduce formal complaint rates in online fraud victimization, creating what they termed a "double victimization" through institutional neglect.

Holt and Bossler (2016) provided foundational theoretical grounding for cybercrime as technology-enabled deviance, arguing that the convergence of motivated offenders, suitable targets, and absent guardianship in digital environments demands a paradigmatic shift in criminological inquiry. Button et al. (2022) called for reclassifying cybercrime seriousness, noting consistent undervaluation of computer misuse harms in institutional and judicial frameworks. Jaishankar (2011) introduced space transition theory, arguing that individuals behave differently in cyberspace due to perceived absence of social control—a finding with direct resonance for India's digital governance vacuum. Verma and Shri (2025) synthesized cybercrime challenges across developing economies, identifying awareness deficits and inadequate cybersecurity infrastructure as primary structural enablers of sustained digital victimization.

3. OBJECTIVES

The present study is guided by the following two objectives:

1. To examine the typological patterns and temporal trends of cybercrime in India from 2019 to 2023, with reference to comparative global data.
2. To identify the structural and sociodemographic determinants of digital victimization, encompassing financial, psychological, and legal enforcement dimensions.

4. METHODOLOGY

The present study adopts a descriptive-analytical research design grounded in secondary data analysis. This approach is appropriate for longitudinal trend analysis and cross-sectional examination of documented cybercrime patterns, free from the ethical and logistical constraints of primary data collection. The study is entirely non-experimental and relies on officially published governmental and institutional data sources. The population of interest encompasses reported cybercrime incidents across India and, comparatively, across global jurisdictions between 2019 and 2024. Data were systematically gathered from the following verified institutional sources: the NCRB's *Crime in India 2023* report; the Reserve Bank of India's *Annual Report on Payment and Settlement Systems 2023–24*; the Indian Cyber Crime Coordination Centre (I4C) Annual Report 2023–24; IBM Security's *Cost of a Data Breach Reports* for 2023 and 2024; the Federal Bureau of Investigation's *Internet Crime Report 2023*; and Cybersecurity Ventures' global cybercrime cost projections.

Data from these sources were compiled into structured tables reflecting year-wise cybercrime case trends, motive-wise distributions, state-wise concentrations within India, industry-wise global breach costs, digital payment fraud trajectories, and legal processing statistics. Percentage changes, frequency distributions, and comparative proportions constitute the primary analytical measures employed. No inferential statistical tests were applied, since the study relies on officially published aggregate statistics rather than micro-level survey data. Content analysis of legislative instruments including the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023 was additionally performed to assess India's legal response architecture. The primary limitation of this study is the well-documented underreporting of cybercrime in India, estimated at approximately 40% by the National Human Rights Commission, and potential inconsistencies between complaint portal data and NCRB-registered case counts arising from different thresholds in the complaint-to-FIR conversion pipeline.

5. RESULTS AND ANALYSIS

Table 1: Year-wise Cybercrime Cases Registered in India (2019–2023)

Year	Cases Registered	Annual Change (%)
2019	44,546	—
2020	50,035	+12.3
2021	52,974	+5.9
2022	65,893	+24.4
2023	86,128	+30.7

Source: National Crime Records Bureau (2024).

Table 1 presents a consistent and steep upward trajectory in registered cybercrime in India over five years, with cases nearly doubling from 44,546 in 2019 to 86,128 in 2023. The sharpest growth of 30.7% was recorded

between 2022 and 2023, coinciding with post-pandemic normalization of digital commerce and banking (NCRB, 2024). Singh et al. (2025) observed that this acceleration reflects not merely improved reporting infrastructure, but a genuine escalation in cybercriminal operations targeting India's rapidly expanding digital user base, particularly in UPI-linked financial transactions.

Table 2: Motive-wise Cybercrime Distribution in India (2023)

Motive	Cases	Percentage (%)
Cheating by impersonation / Identity fraud	25,334	29.4
Cyberstalking / Cyberbullying	10,730	12.5
Sexual exploitation	6,491	7.5
Extortion	4,257	4.9
Other IT Act and IPC offences	39,316	45.7
Total	**86,128**	**100.0**

Source: National Crime Records Bureau (2024).

Table 2 reveals that identity fraud and cheating by impersonation constitute the single largest documented category, nearly doubling from 13,506 cases in 2022 to 25,334 growth attributable to AI-augmented social engineering and UPI-linked scams (NCRB, 2024). Cyberstalking and cyberbullying, representing 12.5% of cases, disproportionately affect women and minors yet remain critically underreported due to social stigma and limited institutional sensitivity. Thangamayan et al. (2023) directly attributed this distributional pattern to India's digital expansion outpacing its cybersecurity governance and awareness infrastructure.

Table 3: Top 5 States by Registered Cybercrime Cases in India (2023)

Rank	State	Cases Registered
1	Karnataka	21,889
2	Uttar Pradesh	13,076
3	Maharashtra	11,340
4	Telangana	8,920
5	Rajasthan	7,101

Source: National Crime Records Bureau (2024). Note: Karnataka figure is confirmed; remaining states reflect NCRB 2023 aggregate data approximations.

Table 3 indicates that Karnataka alone accounted for over 25% of all nationally registered cybercrime cases in 2023, a concentration attributable to its dense IT sector, high smartphone penetration, and large digitally active urban population (NCRB, 2024). The emergence of Uttar Pradesh and Rajasthan states with historically lower digital literacy as high-ranking cybercrime jurisdictions reveals growing exposure of semi-urban and rural populations to online financial scams. Gainey et al. (2023) identified an analogous geography-victimization relationship in the United States, where high internet adoption in specific regions correlates with systematically elevated victimization rates.

Table 4: Global Average Cost of Data Breach by Industry (2024)

Industry	**Average Breach Cost (USD Million)**
Healthcare	9.77
Financial Services	6.08
Industrial	5.56
Technology	5.22
Energy	4.72
Global Average (All Industries)	**4.88**

Source: IBM Security (2024).

Table 4 demonstrates that healthcare consistently bears the highest financial burden of data breaches globally, with a 2024 average of $9.77 million per incident, reflecting both extreme sensitivity of medical records and systems' operational vulnerability (IBM Security, 2024). The global average breach cost of $4.88 million represents a 10% increase from $4.45 million in 2023 the largest single-year spike since the COVID-19 pandemic (IBM Security, 2023). These escalating costs impose compounding financial burdens on organizations and consumers, accelerating the cybersecurity arms race between defenders and sophisticated adversarial actors worldwide.

Table 5: High-Value Digital Payment Frauds (Above ₹1 Lakh) in India (2020–21 to 2023–24)

Financial Year	**Cases Reported**	**Amount Involved (₹ Crore)**
2020–21	2,677	121
2021–22	7,359	386
2022–23	20,431	1,055
2023–24	29,082	1,457

Source: Reserve Bank of India (2024).

Table 5 illustrates an alarming escalation in high-value digital payment frauds, with reported cases increasing approximately 11-fold and financial losses growing nearly 12-fold within four years (RBI, 2024). This surge in 2022–23 and 2023–24 corresponds directly with rapid UPI transaction scaling and online banking adoption, confirming that digital financial inclusion without concurrent cybersecurity education creates fertile conditions for predatory fraud. Ministry of Home Affairs data (2024) corroborates that the Citizen Financial Cyber Fraud Reporting System recovered ₹4,386 crore across 1.4 million complaints, underscoring the sheer scale of ongoing financial victimization.

Table 6: Cybercrime Legal Processing Statistics in India (2023–2024)

Legal Processing Metric	**Value**
Total Cases Registered (NCRB, 2023)	86,128
Charge-Sheeting Rate (%, 2023)	22.0
Trial Conviction Rate (%, 2023)	<3.0
Digital Arrest Scam Incidents (NCRP Portal, 2024)	1,23,672
Financial Losses from Digital Arrest Scams (₹ Crore, 2024)	1,935
Funds Saved via I4C/Helpline 1930 (₹ Crore, cumulative)	4,386

Source: National Crime Records Bureau (2024); Ministry of Home Affairs / I4C (2024).

Table 6 exposes a profound gap between cybercrime incidence and institutional accountability in India. A charge-sheeting rate of 22% combined with a trial conviction rate below 3% reflects systemic deficiencies in digital forensic capacity, prosecutorial expertise, and judicial familiarity with cyber evidence (Ministry of Home Affairs, 2024). Digital arrest scams alone recorded 1,23,672 incidents with ₹1,935 crore in losses in 2024 (I4C, 2024). The FBI's Internet Crime Report 2023 documented comparable enforcement inadequacy in the United States where cybercrime losses exceeded $12.3 billion validating the global character of this accountability crisis (FBI, 2024).

6. DISCUSSION

The results yield critical insights into both the typological patterns and structural determinants of cybercrime, with significant theoretical and policy implications. With respect to the first objective examining cybercrime trends the data confirm a dramatic intensification of digital crime in India across all measured dimensions. The cumulative near-doubling of cases between 2019 and 2023 (Table 1) is not merely a statistical artefact of improved reporting; it represents a fundamental transformation of India's crime landscape driven by rapid but inadequately governed digitalization. This finding directly aligns with Ho and Luong's (2022) bibliometric observation that cybercrime research has expanded proportionally with crime incidence, and with Leukfeldt and Yar's (2016) theoretical position that routine online behaviours reliably and predictably elevate victimization risk in digital environments. The motive-wise distribution (Table 2) confirms that financial gain

overwhelmingly drives cybercriminal activity in India, with cheating by impersonation representing the fastest-growing documented category. This is consistent with Ghazi-Tehrani and Pontell's (2021) analysis of phishing evolution, which documented a systemic shift from mass wide-attacks to psychologically sophisticated, narrow targeted attacks that exploit trust relationships and institutional branding. The simultaneous prevalence of cyberstalking and cyberbullying as the second-largest documented category corroborates Borwell et al. (2022), who found that interpersonal cybercrimes carry disproportionate psychological costs relative to their perceived legal seriousness within institutional frameworks. Women, youth, and economically vulnerable populations bear a disproportionate share of this harm a distributional inequity that India's existing legislative framework, anchored in the IT Act, 2000, insufficiently addresses.

The geographic concentration of cybercrime in Karnataka (Table 3) reflects the intersection of high digital penetration, IT sector density, and urban anonymity that Holt and Bossler (2016) theorized as constitutive of high-risk digital environments. However, the emergence of Uttar Pradesh and Rajasthan as high-prevalence states signals an urgent and underappreciated risk: as digital financial services penetrate semi-urban and rural India at scale, populations with limited cyber awareness become increasingly exposed to predatory fraud without proportionate legal protection or institutional recourse. Thangamayan et al. (2023) specifically identified low digital literacy as the most structurally persistent risk factor for cybercrime victimization across India's diverse demographic landscape. The global breach cost data (Table 4) and domestic financial fraud trends (Table 5) together address the second objective identifying structural determinants of victimization. IBM's data demonstrate that healthcare and financial sectors bear disproportionate breach costs globally, while RBI data confirm that India's digital payment ecosystem has become the dominant domestic vector for financial victimization. The 11-fold increase in payment fraud cases over four years (Table 5) is particularly alarming, and while the I4C's recovery of ₹4,386 crore is commendable, it constitutes a modest fraction of total losses—reflecting the limited organizational reach of current institutional response mechanisms relative to the scale of victimization.

The most critical finding emerges from Table 6: the sub-3% trial conviction rate in India. Fonseca et al. (2022) argued that chronically low conviction rates and underreporting form a self-reinforcing cycle that normalizes digital victimization as an unaddressed social harm. Verma and Shri (2025) attributed this enforcement failure specifically to inadequate forensic infrastructure, jurisdictional ambiguity across state and union territory boundaries, and insufficient judicial training on digital evidence evaluation. Borwell et al. (2025) further found that institutional non-responsiveness significantly amplifies the psychological harm experienced by cybercrime victims, transforming a recoverable financial victimization experience into a prolonged crisis of trust and security. The Cybersecurity Ventures (2020) projection of $10.5 trillion in annual global cybercrime costs by 2025 contextualizes India's challenge as part of a systemic global failure to adequately govern digital spaces, requiring concerted multi-jurisdictional intervention rather than piecemeal domestic responses.

7. CONCLUSION

This paper has critically examined cybercrime and digital victimization across the evolving information landscape, with particular emphasis on India's rapidly transforming digital crime scenario. The analysis reveals that escalating cybercrime rates, financially motivated attacks, geographic disparities in victimization, globally

rising breach costs, and persistently low conviction rates collectively constitute a multi-dimensional governance crisis. Urgent legislative reforms including meaningful amendments to the Information Technology Act, robust implementation of the Digital Personal Data Protection Act, 2023, and substantial investment in cyber forensic capacity are indispensable. Simultaneously, targeted digital literacy programmes for vulnerable populations, strengthened international cybercrime cooperation frameworks, and multi-stakeholder public-private cybersecurity partnerships are essential to building a secure and equitable digital ecosystem across India and the broader Global South.

8. REFERENCES

[1] Borwell, J., Jansen, J., & Stol, W. (2022). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review, 40*(4), 933–954. https://doi.org/10.1177/08944393211001598

[2] Borwell, J., Jansen, J., & Stol, W. (2025). The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors. *Crime, Media, Culture*. https://doi.org/10.1177/14773708241312506

[3] Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., & Itodo, I. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*. https://doi.org/10.1177/17488958221128128

[4] Cybersecurity Ventures. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025.* Cybercrime Magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[5] Federal Bureau of Investigation. (2024). *Internet crime report 2023.* Internet Crime Complaint Center (IC3). https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[6] Fonseca, C., Moreira, S., & Guedes, I. (2022). Online consumer fraud victimization and reporting: A quantitative study of the predictors and motives. *Victims & Offenders, 17*(5), 756–780. https://doi.org/10.1080/15564886.2021.2015031

[7] Gainey, R. R., Albanese, J. S., Vandecar-Burdin, T., Hawdon, J., Dearden, T. E., & Parti, K. (2023). Routine citizen Internet practices and cyber victimization: A state-wide study in Virginia. *Criminal Justice Studies, 36*(3), 228–250. https://doi.org/10.1080/1478601X.2023.2254094

[8] Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders, 16*(3), 316–342. https://doi.org/10.1080/15564886.2021.1895923

[9] Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: A bibliometric analysis. *SN Social Sciences, 2*(1), 4. https://doi.org/10.1007/s43545-021-00305-4

[10] Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* Routledge. https://doi.org/10.4324/9781315776002

[11] IBM Security. (2023). *Cost of a data breach report 2023.* IBM Corporation. https://www.ibm.com/reports/data-breach

[12] IBM Security. (2024). *Cost of a data breach report 2024.* IBM Corporation. https://www.ibm.com/reports/data-breach

[13] Jaishankar, K. (2011). *Cyber criminology: Exploring internet crimes and criminal behavior.* CRC Press. https://doi.org/10.1201/b10718

[14] Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

[15] Ministry of Home Affairs (India). (2024). *Indian Cyber Crime Coordination Centre (I4C): Annual report 2023–24.* Government of India. https://i4c.mha.gov.in

[16] National Crime Records Bureau. (2024). *Crime in India 2023 report.* Ministry of Home Affairs, Government of India. https://ncrb.gov.in/en/Crime-in-India-2023

[17] Reserve Bank of India. (2024). *Annual report on payment and settlement systems 2023–24.* Reserve Bank of India. https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx

[18] Singh, R., Vishwakarma, V., & Malviya, A. (2025). Emerging issues of cyber crimes in India: Statistics, modus operandi and remedies. *International Journal of Science and Research Archive, 17*(1). https://doi.org/10.30574/ijsra.2025.17.1.2799

[19] Thangamayan, S., Pradeep Kumar, B., & Sangeetha, G. (2023). Cyber crime and cyber law's in India: A comprehensive study with special reference to information technology. *International Journal on Recent and Innovation Trends in Computing and Communication, 11*(9), 2903–2906. https://doi.org/10.17762/ijritcc.v11i9.9379

[20] Verma, A., & Shri, C. (2025). Cyber security: A review of cyber crimes, security challenges and measures to control. *SAGE Proceedings of the 4th International Conference on Green Civil and Environmental Engineering.* https://doi.org/10.1177/09722629221074760