

Digital Play, Criminal Pay: Exploring the Impact of Online Gaming Fraud and Countermeasures on Indian Youth

(A Study Based on Actual Victim Incidents in the State of Maharashtra)

Dr. Prajakta R. Patil

KCES's College of Engineering & Management, Jalgaon, Maharashtra, India

prpatil.coem@kces.in

Orchid id: 0009-0004-4118-1976

ABSTRACT

The exponential growth of digital technology and internet connectivity has transformed the online gaming landscape in India into a multi-billion-dollar ecosystem, simultaneously creating fertile ground for sophisticated cybercriminal activity. This paper investigates the nature, scale, and socio-economic impact of online gaming fraud on Indian youth, with a particular focus on real victim incidents documented in Maharashtra — the state reporting the highest volume of cybercrime complaints in India. Drawing on six case studies from Maharashtra between 2022 and 2025, secondary crime data from the National Crime Records Bureau (NCRB) and the Indian Cyber Crime Coordination Centre (I4C), and a synthesis of contemporary scholarly literature, the study examines how deceptive strategies — including phishing, fake reward mechanisms, account manipulation, and psychological pressure — are deployed against young and semi-literate digital users. The findings reveal that victims range from rural farmers to urban businesspersons, and that financial losses span from a few lakh to several crore rupees per individual, with aggregate state-level losses running into thousands of crore. The paper further identifies critical gaps in legal enforcement, digital literacy, and victim support infrastructure. Building on these findings, actionable policy recommendations are presented, covering regulatory reform, law enforcement capacity-building, platform accountability, and victim rehabilitation. The study contributes a ground-level, context-specific perspective to the growing body of literature on digital fraud in developing economies.

Keywords: *online gaming fraud, cybercrime, Indian youth, Maharashtra, digital literacy, phishing, IT Act, online betting, cyber safety, financial fraud*

JEL Classification: K42, L86, O33

1. INTRODUCTION

India stands at a pivotal crossroads in its digital journey. With over 86 per cent of households now connected to the internet and nearly 500 million active online gaming users as of 2025, the country has emerged as one of the world's fastest-growing digital entertainment markets (PIB, 2025; The Bridge Chronicle, 2025). Yet this remarkable expansion has carried an uncomfortable shadow: a staggering and accelerating wave of cybercrime that targets the very population driving the digital revolution — Indian youth.

Between 2022 and 2024, reported cybersecurity incidents in India surged from approximately 10.29 lakh to 22.68 lakh, with 2025 projected to exceed 28 lakh cases (PIB, 2025; Insights on India, 2026). Maharashtra, India's financial capital and a state with exceptionally high digital penetration, consistently records the highest volume of complaints — over 3.03 lakh cases in 2024 alone, with cybercrime-linked financial losses running into hundreds of crore rupees (Medianama, 2025). Online gaming platforms have emerged as a particularly insidious vector within this larger crime ecosystem, exploiting the psychological vulnerabilities of young users through engineered excitement, fabricated winning streaks, and manufactured trust.

The scholarly literature has documented how gaming-related fraud typically operates through deceptive strategies such as phishing links, fake reward systems, account takeovers, malware injection, and unauthorised financial transactions — mechanisms that cause both monetary and emotional harm to victims (Samuel & Latha, 2025; Chen et al., 2005). Researchers have also highlighted how the deep integration of digital media into daily life, combined with insufficient awareness of online risks, leaves young users disproportionately exposed (Bharadwaj & Arora, 2025; Tomczyk et al., 2020). The psychological appeal of gaming — escapism, social belonging, the thrill of achievement — can additionally lower a user's critical defences, making them more susceptible to manipulation (Marques et al., 2023).

Despite growing scholarly attention to cybercrime in India, localized, victim-centred investigations that combine qualitative case analysis with policy evaluation remain relatively sparse, particularly for Maharashtra. This paper, titled "Digital Play, Criminal Pay: Exploring the Impact of Online Gaming Fraud and Countermeasures on Indian Youth," addresses that gap. It seeks to: (i) document and analyse the lived experiences of fraud victims in Maharashtra; (ii) identify the mechanisms through which gaming platforms are weaponized; (iii) evaluate the adequacy of existing legal and institutional responses; and (iv) propose actionable, evidence-based recommendations for creating a safer digital gaming environment for Indian youth.

The remainder of the paper is organized as follows. Section 2 reviews the relevant literature. Section 3 articulates the research gap. Section 4 describes the methodology and presents the six case studies. Section 5 discusses the findings. Section 6 offers conclusions and recommendations.

2. REVIEW OF LITERATURE

The intersection of online gaming, youth behaviour, and cybercrime has attracted increasing academic attention over the past two decades, though the literature remains fragmented across disciplines including criminology, psychology, information systems, and public policy.

2.1 Online Gaming Growth and its Dual Character

The Indian online gaming industry has been described as one of the most dynamic segments of the country's digital economy. Dey (2021) provides a foundational analysis of the gaming industry in India, noting its rapid revenue growth driven by affordable smartphones, low-cost mobile data, and a young demographic with a strong appetite for digital entertainment. The industry's commercial success, however, has not been accompanied by commensurate regulatory oversight, creating conditions that criminal actors have readily exploited. Brar, Singh Balhara, and Bhargava (2025) extend this analysis by examining public health implications, noting that the same commercial algorithms designed to maximize user engagement also foster addictive behaviour, which increases vulnerability to financial manipulation.

At a global level, observers from the Observer Research Foundation (ORF, 2024) have documented how gaming companies themselves are frequent targets of cyberattacks — including the notorious social engineering breaches at Rockstar Games in 2022 and Riot Games in 2023 — with the resulting stolen data subsequently used for identity theft and account takeovers targeting end users. This "trickle-down victimization" pattern is particularly relevant to the Indian context, where users are frequently unaware that their credentials may have already been compromised.

2.2 Typology of Online Gaming Fraud

Chen, Chen, Hwang, Korba, Song, and Yee (2005) conducted one of the earliest systematic analyses of crime in online gaming environments, examining hundreds of reported cases and identifying fraud and theft as the dominant offense categories. Their study found that both perpetrators and victims were predominantly young individuals, and that offenses were commonly carried out through identity deception and social engineering — findings that retain striking relevance two decades later. More recently, Kristiansen and Jensen (2023) examined victimization in online gaming trade scams, demonstrating how peer trust within in-game economies creates predictable opportunities for deception. Their work shows that the social fabric of gaming communities — built on reciprocity and assumed good faith — is itself weaponized against players.

The mechanisms of fraud identified in the literature include: phishing through deceptive links shared via messaging platforms; fake gaming websites engineered to mirror legitimate platforms; artificial winning streaks designed to build

trust before larger deposits are requested; account manipulation where accumulated points are covertly erased; demands for fictitious "tax payments" before withdrawals are permitted; and the use of international servers and virtual private networks (VPNs) to obscure the operators' identities (ORF, 2024; Samuel & Latha, 2025). Each of these tactics maps directly onto cases documented in Maharashtra, which are analysed in Section 4.

2.3 Psychological Dimensions of Youth Vulnerability

A growing body of research examines why young people are particularly susceptible to online fraud. Marques, Uchida, Aguiar, Kadri, Santos, and Barbosa (2023) conducted a systematic review of virtual gaming and mental health, finding that escapism, social validation, and the pursuit of achievement are primary motivators for gaming engagement. While these motivations are not inherently harmful, the same emotional needs — particularly the desire to "win back" losses or to achieve the status signalled by large winnings — are actively exploited by fraudulent platforms.

Tomczyk et al. (2020) situate youth vulnerability within a broader framework of problematic internet use, linking excessive digital engagement with impulsivity, emotional dysregulation, and reduced capacity for critical risk assessment. These psychological characteristics dovetail with the conditions of manufactured urgency and social pressure that fraudulent gaming platforms deliberately create. Research on cognitive dimensions of phishing susceptibility further suggests that heuristic decision-making — relying on mental shortcuts rather than systematic evaluation — is a primary pathway through which online fraud victims are drawn in (Shang et al., 2023; Iacis, 2023).

2.4 Regulatory and Legal Responses

India's primary legislative instrument for addressing cybercrime remains the Information Technology Act, 2000 (amended 2008), supplemented by provisions of the Bharatiya Nyaya Sanhita, 2023. The UNICEF and Cyber Peace Foundation (2022) collaborative report with the Government of India provides structured guidelines for investigating gaming-related cybercrimes, including reporting mechanisms, applicable legal sections, and investigative procedures. However, scholars and practitioners have consistently noted enforcement gaps: slow FIR-to-investigation timelines, limited forensic capacity for tracing digital transactions across international servers, and low conviction rates that embolden repeat offenders (Insights on India, 2026).

A significant legislative development occurred in August 2025 when the Indian government enacted the Promotion and Regulation of Online Gaming Act, 2025, which bans Real Money Games (RMG) and introduces KYC requirements, advertising restrictions, and payment processing controls for gaming platforms (ORF, 2025). The Act also addresses national security concerns, including the use of gaming platforms as communication and recruitment tools by extremist organizations. While the legislation represents a meaningful step forward, its implementation and enforcement infrastructure remains nascent.

2.5 Bibliometric Context: Digital Fraud Research Trends

Laxman et al. (2024) conducted a bibliometric review of digital banking fraud research, finding a strong upward trend in scholarly output post-2021, with emerging focus areas including artificial intelligence-based detection, blockchain forensics, and identity theft analysis. Notably, India ranks among the top contributing nations in this literature, reflecting both the scale of the problem domestically and the growing engagement of Indian researchers. The same review identified a persistent gap in the integration of technical fraud detection systems with behavioural and socio-legal frameworks — precisely the integration this paper seeks to advance.

3. RESEARCH GAP

The existing scholarship on digital fraud has made substantial contributions, particularly in the domains of technological detection systems and broad epidemiological mapping of cybercrime trends. However, several critical lacunae persist that this paper is specifically positioned to address.

First, the dominant research paradigm in digital fraud studies remains technology-centred: the majority of published work focuses on algorithmic solutions — machine learning classifiers, blockchain audit trails, intrusion detection systems — with comparatively little attention to the human experience of victimization and the socio-behavioural

pathways that lead individuals into fraud situations (Laxman et al., 2024). Understanding why a young farmer or a small businessman deposits crores of rupees into a manipulated gaming platform requires a different analytical lens than optimizing a fraud detection algorithm.

Second, existing literature is predominantly drawn from Western contexts or aggregated national-level analyses of India, with limited attention to state-level or community-specific dynamics. Maharashtra presents a particularly rich and underexplored case: it is simultaneously India's most cyber-crime-reporting state, home to both its largest metropolis and extensive rural and semi-urban populations, and a state where the government itself has contemplated broad bans on online gaming in response to rising social harms (The Bridge Chronicle, 2025).

Third, most bibliometric and survey-based studies rely on English-language databases and formal reporting channels, which systematically undercount victimization in populations where reporting barriers are high — including shame, lack of awareness of legal recourse, and distrust of authorities.

Finally, while policy analysis of India's regulatory evolution is beginning to appear (ORF, 2025), there remains little work that connects legislative developments directly to documented victim experiences, and still less that translates this analysis into operationally specific recommendations for law enforcement, educators, and platform regulators.

This paper addresses these gaps by combining victim-centred case analysis with regulatory review and a synthesis of multi-disciplinary scholarly literature, offering both conceptual and practical contributions to the field.

4. RESEARCH METHODOLOGY

This study adopts a qualitative, interpretive methodology grounded in secondary case analysis. Given that online gaming fraud is a sensitive phenomenon involving vulnerable victims, collecting primary survey data poses significant ethical and practical barriers. Instead, the paper draws on a structured analysis of six documented victim incidents from Maharashtra, supplemented by official crime statistics from the National Crime Records Bureau (NCRB), I4C, and publicly available investigative reports. This approach aligns with established traditions of crime case study research, which treats real incidents as data units from which patterns, mechanisms, and policy implications can be derived (Yin, 2018).

The six cases were identified through a systematic scan of credible journalistic sources, official cybercrime unit press releases, and parliamentary records between 2022 and 2025. Cases were selected to achieve diversity across: victim demographic profile (age, occupation, location); fraud mechanism; financial magnitude; and investigative outcome. Each case was analysed for: the entry point of fraud; the trust-building mechanisms employed; the escalation pattern; the point of victim recognition; and the legal and institutional response.

Secondary literature was synthesized thematically. Search terms included: online gaming fraud India; Maharashtra cybercrime youth; phishing gaming platforms; digital literacy India; IT Act enforcement gaming. Databases consulted included Google Scholar, Scopus, and ResearchGate. Only peer-reviewed articles, official government publications, and high-credibility policy research were included.

5. CASE STUDIES: DOCUMENTED VICTIM INCIDENTS IN MAHARASHTRA

Case 1: The Investment-Gaming Hybrid Fraud — Maharashtra State-Wide (2019–2025)

The Economic Offences Wing of Thane police arrested Sameer Narvekar, his wife Neha, and associate Amit Palaw for allegedly defrauding over 11,000 investors across Maharashtra of approximately ₹500 crore (The Hindu, 2026). Operating through their Pune-based entity "Trade with Jazz" from 2019, the accused blended gaming investment aesthetics with Ponzi mechanics, promising monthly returns of 4 per cent from stock market trading. The scheme's credibility was artificially reinforced by the enrolment of approximately 1,500 police personnel and government officials as investors. After accumulating substantial funds, the company abruptly ceased operations and became unresponsive, triggering a wave of complaints. The accused were eventually traced to Gujarat and booked under the Maharashtra Protection of Interest of Depositors (MPID) Act and the Bharatiya Nyaya Sanhita, 2023. Financial investigations into linked accounts remain ongoing.

This case illustrates how the veneer of financial technology and gaming legitimacy can be used to attract not only financially naive victims but also informed professionals, demonstrating the broad demographic reach of sophisticated fraud operations.

Case 2: The Rigged Card Gaming Platform — Jalgaon (2023)

A 27-year-old civil contractor from Jalgaon was contacted via WhatsApp with a link to what appeared to be a legitimate online card gaming platform. After creating an account, his initial games produced small but real winnings, including approximately ₹7 lakh credited to his bank account — a deliberate trust-building mechanism. Over ten days between December 8 and 18, 2023, he transferred a total of ₹78.90 lakh, believing he was investing in a profitable activity. When he attempted to withdraw his balance, he discovered the platform had been manipulating outcomes: won games reduced rather than increased his points. Platform operators subsequently demanded additional "tax payments" as a precondition for withdrawals. Upon recognizing the fraud, he filed a cybercrime complaint, and a case was registered under cheating provisions and the IT Act.

This case exemplifies the "salami-slicing" trust escalation pattern — small initial rewards that build confidence before large-scale financial extraction — which has been identified in the academic literature as one of the most psychologically effective mechanisms in online fraud (Chen et al., 2005).

Case 3: Gaming Addiction and Agricultural Community Loss — Rural Maharashtra

A young horticulture farmer became progressively entangled in online gaming platforms that initially appeared innocuous and entertaining. The platforms employed reward mechanics — bonuses, achievement milestones, and the promise of rapid financial gains — to sustain engagement and incentivize escalating financial commitment. Losses compounded progressively: the farmer initially used personal savings, then agricultural income, and ultimately borrowed funds from within his community. Total estimated losses reached approximately ₹84 lakh, with severe consequences for his household's financial stability and family relationships.

The case carries particular significance because it demonstrates how gaming fraud and gaming addiction are not always clearly separable phenomena. The platform was not necessarily rigged in an obvious technical sense; rather, its design exploited well-documented psychological vulnerabilities — the sunk cost fallacy, loss-chasing behaviour, and reward anticipation — to sustain financially destructive engagement. This dynamic is consistent with Marques et al.'s (2023) findings on escapism and emotional vulnerability as drivers of problem gaming, and with Brar et al.'s (2025) analysis of addictive platform design. The case also foregrounds the particular risks faced by rural and semi-urban youth, who may have less robust social and institutional safety nets than their urban counterparts.

Case 4: International Server Fraud — Navi Mumbai (2022–2025)

A 42-year-old businessman from Koparkhairane, Navi Mumbai, lost approximately ₹2.74 crore over more than two years of participation on a gaming platform called satsports.com, which offered games including Teen Patti and Casino. The platform initially showed winnings and facilitated a withdrawal of approximately ₹50 lakh — again, a trust-building mechanism — before the victim's account balance ceased registering wins. Total transfers from the victim's bank accounts reached approximately ₹3.25 crore across multiple linked accounts. Following inconclusive responses from platform operators, the victim approached Navi Mumbai cyber police. Investigators registered an FIR under the IT Act and established that the platform operated through an international server using a VPN, with recipient bank accounts already identified for further investigation.

This case highlights a structural enforcement challenge: the deployment of international hosting infrastructure and VPN masking to prevent jurisdictional accountability. The pattern mirrors the "trickle-down victimization" model noted by ORF (2024), where gaming platforms registered in foreign jurisdictions — often small island nations — channel victim funds through Indian proxy accounts before remitting proceeds abroad.

Case 5: Criminal Network Disruption — Gondia, Vidarbha

Nagpur police executed raids at six locations in Gondia district in connection with an online gaming fraud investigation, recovering 2.4 kg of gold and approximately ₹70 lakh in cash. The operation followed the surrender of

Anant alias Sontu Navratan Jain, a Gondia resident accused of defrauding a Nagpur-based businessman of approximately ₹58 crore through an orchestrated online gaming scheme. Jain had evaded arrest for approximately three months before surrendering. Police sources identified Jain as a local coordinator for a larger illegal betting network, with suspected links to underground gaming applications. The seized assets were treated as potential proceeds of crime under applicable forfeiture provisions.

This case underscores the organized criminal infrastructure underlying gaming fraud: individual operators are embedded within layered networks that include local coordinators, money mules, and internationally registered platform entities. The scale — ₹58 crore from a single victim — illustrates that gaming fraud can reach levels of financial magnitude comparable to major commercial fraud cases.

Case 6: Institutional Complicity — Banking System Exploitation, Daund

The manager of a State Bank of India branch in Daund identified suspicious transaction patterns across several current accounts. Investigation revealed that 84 individuals had opened current accounts under various business names, which were then used exclusively for large-volume unauthorised online gaming transactions — each account handling transfers of approximately ₹20–25 lakh or more. The irregular fund flows were identified through cross-referencing with cybercrime helpline complaints. The matter was referred to the Economic Offences Branch. Investigators noted the strong probability of money laundering given the nature and scale of the transactions. As of the reporting date, investigations were ongoing with no arrests made.

This case reveals a dimension of gaming fraud that receives relatively limited attention in the scholarly literature: the laundering infrastructure. Gaming platforms do not merely defraud individual victims; they also generate illicit financial flows that pass through the legitimate banking system, creating systemic risks that extend well beyond the gaming ecosystem.

6. DISCUSSION AND ANALYSIS

6.1 Cross-Case Patterns

Across the six cases, several recurring patterns emerge that are consistent with the international and Indian scholarly literature on gaming fraud. The first and most consistent is the trust-building sequence: an initial period of genuine or simulated small winnings that establish credibility before escalating financial demands are made. This pattern appears in Cases 2, 3, and 4, and mirrors what Chen et al. (2005) and Kristiansen and Jensen (2023) describe as the foundational mechanism of gaming-related fraud.

The second pattern is demographic breadth. Victims in the Maharashtra cases span a young rural farmer, a 27-year-old civil contractor, a 42-year-old businessman, and a city-wide population of small business account holders. This contradicts the common assumption that online fraud primarily targets the digitally inexperienced or very young; it suggests instead that the fraud mechanisms are sufficiently sophisticated to exploit cognitive biases and emotional vulnerabilities across education and income levels.

Third, the cases collectively illustrate the structural impunity available to operators who deploy international hosting, VPN masking, and proxy bank accounts. Legal jurisdiction becomes ambiguous, digital evidence is difficult to preserve, and money has often been moved beyond recovery before investigators are engaged. This infrastructure challenge is documented in the policy literature (ORF, 2024, 2025) but remains inadequately addressed by existing legal frameworks.

6.2 Regulatory Adequacy

India's Information Technology Act, 2000, and its 2008 amendment provide a foundational legal architecture for addressing gaming fraud through provisions on identity theft, data theft, cheating, and financial fraud. The Bharatiya Nyaya Sanhita, 2023, further strengthens provisions for organized financial fraud. The enactment of the Promotion and Regulation of Online Gaming Act, 2025 — banning Real Money Games, introducing KYC requirements, and mandating platform transparency — represents the most significant regulatory development to date (ORF, 2025).

However, the gap between legislative intent and enforcement reality remains significant. Maharashtra's cyber police units, though among the better-resourced in India, face structural constraints: the state recorded 3.03 lakh complaints in 2024, but conviction rates remain low (Insights on India, 2026). The Chief Minister's own acknowledgement that the state's legal framework is "ill-equipped for the digital age" and that action against foreign-registered platforms requires central government coordination suggests that regulatory convergence has not yet been achieved (The Bridge Chronicle, 2025).

7. CONCLUSIONS AND RECOMMENDATIONS

Online gaming fraud in India is not a marginal phenomenon. It is a large-scale, systematically organized form of financial crime that targets the emotional and psychological vulnerabilities of young digital users, causes severe and often irrecoverable financial harm, and is enabled by structural inadequacies in regulation, enforcement, and digital literacy. Maharashtra's experience — as India's most cyber-crime-affected state, and one in which real losses measured in crore rupees have been experienced by individuals across the socio-economic spectrum — provides a compelling case study for the national policy conversation.

The following recommendations emerge directly from the case analysis and literature synthesis:

7.1 Digital Literacy and Awareness

Age-appropriate digital safety curricula should be integrated into school education at secondary and higher secondary levels across Maharashtra, with particular emphasis on recognizing rigged platforms, understanding reporting mechanisms, and the psychology of online trust manipulation. State-funded awareness campaigns should specifically target semi-urban and rural communities, where digital adoption is growing faster than digital safety awareness. Maharashtra's Cyber Department has already initiated school and social media campaigns; these should be scaled and evaluated for impact (The Bridge Chronicle, 2025).

7.2 Law Enforcement Capacity

Dedicated cyber units at the district level — not only in metropolitan areas — are needed to reduce the time between FIR filing and active investigation. Training should focus on three technical domains: tracing multi-layered digital payment chains; conducting and executing cross-border evidence requests under mutual legal assistance treaties (MLATs); and identifying and immobilizing proxy bank accounts used for money laundering. Since 2017, over 3,200 Maharashtra police officers have received digital crime training (The Bridge Chronicle, 2025); this programme should be expanded and updated to address VPN-based anonymization and international platform jurisdiction.

7.3 Victim Support Infrastructure

The emotional and financial consequences of gaming fraud are severe and compounding. Victims frequently experience shame, debt, family breakdown, and in some cases suicidal ideation. A 24/7 dedicated victim support helpline — distinct from the general cybercrime reporting helpline — should be established, staffed by both legal advisors and mental health counsellors. Debt counselling services that can help victims navigate loan obligations should also be made available. Reducing stigma around reporting is essential to improving official case counts and enabling more effective law enforcement responses.

7.4 Platform Accountability and Regulatory Enforcement

The Promotion and Regulation of Online Gaming Act, 2025 provides a strong foundation. Its implementation should be prioritized through: mandatory KYC verification for all gaming accounts with real-money functionality; expedited takedown mechanisms for platforms identified by I4C or state cyber units as predatory; international cooperation frameworks — particularly with jurisdictions such as Curacao, Malta, Cyprus, Cambodia, Myanmar, and Laos, where many fraudulent platforms are registered; and financial liability provisions for payment gateway operators who knowingly or negligently facilitate fraud transactions. The NCRP and I4C's recent achievement of blocking fraudulent transactions worth over ₹8,031 crore (PIB, 2025) demonstrates that real-time financial intervention is both feasible and effective at scale.

7.5 Research and Data Infrastructure

Official data on gaming-specific cybercrime should be disaggregated from general cybercrime statistics to enable better tracking of trends and policy evaluation. Victim demographics, fraud mechanisms, financial magnitudes, and recovery rates should be recorded systematically. Academic researchers should be provided structured access to anonymized case data to support evidence-based policy development — an approach that has been successfully adopted in the UK and Australia for financial crime research.

In closing, the digital revolution that has brought entertainment, connectivity, and economic opportunity to millions of young Indians cannot be allowed to simultaneously serve as an open field for organized criminal exploitation. Protecting India's youth in digital spaces requires a coherent, collaborative effort across government, law enforcement, educational institutions, the private sector, and civil society. The cases documented in this paper represent not merely individual tragedies but a systemic failure that demands systemic solutions.

REFERENCES

- Bharadwaj, A., & Arora, S. (2025). Digital media integration and youth safety: Emerging challenges in India's online ecosystem. *Journal of Digital Society*, 14(1), 23–41.
- Brar, M. K., Singh Balhara, Y. P., & Bhargava, R. (2025). Balancing play and protection: Public health risks and regulatory measures in India's online gaming landscape. *Simulation & Gaming*. <https://doi.org/10.1177/10468781251388867>
- Chen, K. T., Chen, J. Y., Hwang, C., Korba, L., Song, R., & Yee, G. (2005). An analysis of online gaming crime characteristics. *Internet Research*, 15(3), 246–261. <https://doi.org/10.1108/10662240510602956>
- Dey, K. (2021). An analysis of the gaming industry in India. *International Journal of Science and Research (IJSR)*. <https://doi.org/10.21275/sr21520124120>
- Insights on India. (2026, February 21). Cybercrime in India 2025: 24% spike, ₹22,495 crore lost. Retrieved from <https://www.insightsonindia.com/2026/02/21/cybercrime-in-india/>
- Kristiansen, S., & Jensen, M. (2023). Victimization in online gaming trade scams among young users. *Journal of Cybercrime and Deviance*, 7(2), 118–136.
- Laxman, K., Bhat, S., & Rao, N. (2024). Digital banking fraud: A bibliometric analysis and thematic review. *International Journal of Finance and Banking Studies*, 13(1), 45–63.
- Marques, S., Uchida, H., Aguiar, M., Kadri, S., Santos, L., & Barbosa, F. (2023). Escaping through virtual gaming: What is the association with emotional, social and mental health? A systematic review. *Journal of Behavioral Addictions*, 12(4), 890–910. <https://www.researchgate.net/publication/375463853>
- Medianama. (2025, August 1). India sees 500% increase in cybercrime cases from 2021 to 2024. Retrieved from <https://www.medianama.com/2025/08/223-india-cybercrime-500-percent-increase-2021-2024/>
- Microsoft Source Asia. (2025, December 12). A race against time: Maharashtra police get an AI copilot to fight cybercrime. Retrieved from <https://news.microsoft.com/source/asia/features/a-race-against-time-maharashtra-police-get-an-ai-copilot-to-fight-cybercrime/>
- Observer Research Foundation [ORF]. (2024, January 11). Cybersecurity threats in online gaming: Learnings for India. Retrieved from <https://www.orfonline.org/research/cybersecurity-threats-in-online-gaming-learnings-for-india>
- Observer Research Foundation [ORF]. (2025, September 3). Online gaming regulation in India: A preliminary review — Building a regulatory framework. Retrieved from <https://www.orfonline.org/research/building-a-regulatory-framework-for-online-gaming-in-india>
- Press Information Bureau [PIB], Government of India. (2025). Curbing cyber frauds in Digital India. Retrieved from <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3®=3&lang=2>

Samuel, R., & Latha, K. (2025). Online fraud and Indian youth: An empirical inquiry into victimization patterns and digital risk awareness. *Journal of Cyber law and Information Security*, 6(1), 55–72.

Shang, Y., Wang, Z., Tian, X., Zhou, R., Ma, B., & Liu, Y. (2023). Theoretical basis and occurrence of internet fraud victimization: Based on two systems in decision-making and reasoning. *Frontiers in Psychology*, 14, 1087463. <https://doi.org/10.3389/fpsyg.2023.1087463>

The Bridge Chronicle. (2025, July). Maharashtra plans ban on online games over youth addiction worries. Retrieved from <https://www.thebridgechronicle.com/amp/story/tech/maharashtra-ban-online-games-youth-addiction-2025>

The Hindu. (2026). EOW arrests trio in Maharashtra gaming-investment fraud. [News report].

Tomczyk, L., Watt, M., Tomczyk, M., & Guardiola, J. (2020). Problematic internet use among youth. *Educational Research and Review*, 15(9), 497–512. <https://www.researchgate.net/publication/342173936>

UNICEF & Cyber Peace Foundation. (2022). Online gaming cyber safety: Standard operating procedures and legal framework for India. Government of India.

Yadav, R., Sharma, P., & Kapoor, A. (2025). Online gaming fraud and socio-economic impact on Indian youth: A digital addiction perspective. *International Journal of Emerging Technologies in Society*, 9(2), 112–129.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.