IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67

Role of Emerging Cyber Crime Trends and Cyber Security Challenges in Himachal Pradesh

Shivani Awasthi[1] and Dr. Jitendra Singh Brar[2]
[1]Research Scholar, Department of Computer Science
[2]Professor, Department of Computer Science
Sunrise University, Alwar, Rajasthan

Abstract: *Cybercrime has emerged as a significant threat to governance, personal security, and economic growth across India, including in the hill state of Himachal Pradesh. This review explores emerging cybercrime trends and corresponding cyber security challenges within the state by synthesizing existing literature and primary survey findings from 400 key stakeholders comprising police officials, advocates, judges, academicians, and employees. The study identifies prevailing types of cybercrime, perceptions of risk, institutional readiness, and gaps in cyber security frameworks. The paper concludes with recommendations for policy, capacity building, and technology adoption.*

Keywords: Digital Fraud, Phishing Attacks, Online Financial Crimes

I. INTRODUCTION

Cybercrime refers to offenses that involve computers, networks, and digital systems as targets or tools of criminal activity. With increased internet penetration and digitization, Himachal Pradesh has witnessed a rise in phishing, identity theft, online financial fraud, and cyber harassment (Singh & Sharma, 2021). Although national-level research on cybercrime is substantial, state-specific studies remain limited. This paper reviews the role of emerging cybercrime trends and challenges in Himachal Pradesh, incorporating insights from law enforcement, legal professionals, educators, and the workforce.

In the digital age, cybercrime has emerged as a major threat to individuals, institutions, and governments worldwide. As societies rapidly integrate information and communication technologies into daily life, crimes conducted via digital platforms ranging from financial fraud and identity theft to sophisticated phishing and ransomware attacks have multiplied in scale and complexity (Tripathy, 2025). India's expanding internet usage, growing digital payments ecosystem, and increased reliance on online services have further amplified vulnerabilities to cybercrime, making robust cyber security measures essential at both national and state levels (Reuters, 2025). Within this broader context, the hill state of Himachal Pradesh is confronting its own unique cyber security challenges, marked by a significant surge in cybercrime reports and growing concerns about institutional readiness to tackle emerging threats.

Himachal Pradesh, traditionally known for its serene landscapes and tourism-driven economy, has seen an unprecedented rise in cybercrime complaints over recent years. Official records indicate a staggering increase in cybercrime cases registered through the state's reporting mechanisms, with multiple reports suggesting that complaints have risen sharply year on year (Tribune, 2025). For example, in 2025 alone, state authorities reported as many as 1,204 cybercrime complaints, which already represented a substantial increase from previous years, signaling an escalating trend that has serious implications for public safety and digital governance in the region (Tribune, 2025). This trend mirrors broader national patterns where India saw millions of cyber-attack attempts in 2025, highlighting both the scale and evolving sophistication of cyber threats across sectors, from individual users to corporate and public institutions (Times of India, 2025).

The proliferation of digital interfaces in Himachal Pradesh presents both opportunities and risks. On the positive side, increased internet penetration has improved access to services including banking, education, and e-governance. However, this rapid digital adoption has also outpaced the public's awareness of cyber risks and the capacity of state institutions to effectively prevent and manage cybercrime. According to regional reports, residents of Himachal Pradesh

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

have fallen victim to cyber fraud in large numbers, with financial losses amounting to tens of crores of rupees within a short period. In one year alone, the state reportedly lost nearly □114 crore due to various forms of cybercrime, including fraudulent investment schemes, fake websites, and phishing operations (Tribune, 2025). Such figures point not only to the financial impact on individuals and the economy but also to the increasing sophistication of cybercriminal strategies that exploit both technological vulnerabilities and human factors.

Emerging cybercrime trends observed in Himachal Pradesh reflect a broad range of illegal digital activities. Financial frauds, such as UPI-based scams, fake loan apps, and investment frauds, account for a large share of reported complaints, often leveraging social engineering techniques to deceive unsuspecting victims (Economic Times, 2023). Additionally, crimes such as identity theft, social media impersonation, and sextortion have become common, with cybercriminals using manipulated digital identities to extort money or compromise personal data. The escalation in social networking abuse and digital harassment further complicates the cybercrime landscape, requiring nuanced legal and psychological understanding alongside technological countermeasures (Economic Times, 2023).

The specific geographical and infrastructural context of Himachal Pradesh adds another layer of challenge to effective cyber security response. The state's mountainous terrain and dispersed rural population mean that digital infrastructure and cybercrime reporting mechanisms may be less accessible in remote areas. Many residents in the high-altitude districts have limited exposure to formal cyber security education and awareness programs, making them more susceptible to online scams and frauds that exploit lack of digital literacy (Cybersecurity Institute, 2025).

Furthermore, limited resources and trained cybercrime investigators present additional hurdles for law enforcement agencies tasked with investigating, prosecuting, and preventing cyber offences. While the state has established cyber cells and cyber desks to facilitate reporting and investigation, the sheer volume of emerging threats requires continuous upgrading of tools, skills, and operational capacities across police stations and judicial bodies.

Institutional responses to the growing cybercrime problem in Himachal Pradesh have been evolving. The state police have initiated efforts to strengthen their cybercrime investigation capabilities by setting up cyber desks in police stations and proposing the establishment of dedicated cyber police units in every district (HimbuMail, 2025). These initiatives aim to decentralize cybercrime reporting and reduce delays in investigations, especially for victims in remote regions. High-level directives have also emphasized the importance of equipping police personnel with the knowledge and tools necessary to effectively tackle complex digital crimes. However, despite these advances, significant gaps remain in the broader cyber security infrastructure, particularly in advanced forensic capabilities, inter-agency coordination, and legal frameworks tailored to rapidly evolving digital offences.

The role of the judiciary and legal professionals is also crucial in shaping the state's cybercrime response. Judges and advocates must navigate a rapidly changing cyber legal landscape that often outpaces existing statutes, such as the Information Technology Act and related cyber laws. Complex questions around digital evidence admissibility, cross-jurisdictional crime links, and emerging forms of digital harm require specialized legal interpretation and training. Enhancing judicial familiarity with technology and cybercrime norms is therefore critical for ensuring that legal outcomes effectively reflect the realities of digital threats.

Beyond institutional capabilities, public awareness and education play an indispensable role in cybercrime mitigation. Many cybercrime incidents exploit human errors such as responding to phishing links, sharing sensitive information on unsecured platforms, or downloading malicious mobile applications. Awareness campaigns that inform citizens about common cyber threats and safe online behaviors can significantly reduce the susceptibility of users across demographics, from students and professionals to elderly populations and rural communities. Digital literacy programs that incorporate elements of cyber hygiene, password management, and critical evaluation of online content are essential for fostering a cyber-resilient society.

In light of these dynamics, the review of emerging cybercrime trends in Himachal Pradesh underscores the need for a holistic, multi-stakeholder approach to cyber security. This includes not only technological investments and law enforcement training but also continuous research, policy evolution, and community engagement. Collaborative efforts involving government agencies, academic institutions, legal bodies, and civil society can help bridge gaps in understanding and response, ensuring that the digital transformation of Himachal Pradesh yields sustainable benefits while minimizing cyber risks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

The significance of examining cybercrime trends and challenges at the state level lies in tailoring solutions to the specific socio-economic and geographic context of the region. Himachal Pradesh's experience reflects broader national and global patterns of cyber threats but also reveals localized nuances in how these crimes manifest and are addressed. By situating the state within the larger digital narrative, researchers and policymakers can better identify targeted interventions that enhance cyber security readiness and resilience.

LITERATURE REVIEW

1. Emerging Cyber Crime Trends

Recent studies have identified the following trends in India:

Financial frauds: Phishing, SIM cloning, and online banking frauds have increased dramatically (Kumar & Mishra, 2020).

Social media abuse: Cyberbullying and misinformation campaigns facilitated by social platforms (Raina, 2022).

Ransomware attacks: Targeting both public and private sector networks (Verma & Gupta, 2020).

These trends reflect global patterns seen in cybercrime while being shaped by local socio-economic factors.

2. Cyber Security Challenges

Cyber security challenges in the Indian context include:

Insufficient infrastructure: Limited tools and platforms for detection and response (Chauhan & Gupta, 2019).

Skill gap: Lack of trained professionals in cyber security (Singh & Thakur, 2021).

Awareness deficit: Low public awareness contributes to vulnerability (Sharma, 2020).

In Himachal Pradesh, the geographical spread and resource constraints further compound these challenges.

RESULTS AND DISCUSSION

The analysis of cybercrime trends and cyber security challenges in Himachal Pradesh reveals that cybercrime awareness and exposure to various types of digital offences are widespread across different stakeholder groups. The primary data indicate that a substantial majority of respondents particularly police officials, academicians, and advocates reported encountering or being aware of phishing and email scams, making this the most commonly recognized cyber threat in the state. This aligns with trends observed nationally, where phishing remains a top vector for cybercriminal activity due to its low technical barriers and high success rates (Tripathy, 2025). The high awareness among academicians may reflect higher digital literacy levels, while substantial reporting by police officials suggests this threat is a regular component of complaints received at cyber desks.

Online financial fraud emerged as another prominent form of cybercrime in Himachal Pradesh. Respondents across all professional groups indicated significant familiarity with financial scams involving fake banking alerts, fraudulent investment platforms, and illicit mobile payment transactions. These findings corroborate reports highlighting that digital payment frauds and UPI-related scams constitute a significant portion of cybercrime complaints in India, including the hill states (Economic Times, 2023). The widespread recognition of financial cybercrime among employees and legal professionals is indicative of both the prevalence of such offenses and the economic impact on victims across socio-economic strata.

The survey also showed notable awareness of identity theft and social media-related offences, although to a varying degree across groups. Academicians and employees reported higher familiarity with social media harassment, possibly reflecting their more extensive use of digital platforms for communication and networking. These trends echo broader observations that digital harassment, account takeovers, and impersonation on social networks are increasingly common, particularly among younger and more digitally active populations (Tripathy, 2025). Meanwhile, identity theft remains a concern among legal and enforcement respondents, underscoring its legal implications and the complex evidentiary issues it presents in prosecutions.

Despite this relatively high awareness of various cyber threats, the perception of institutional readiness to manage such crimes was mixed. Police officials acknowledged improvements, including the establishment of cyber desks and localized reporting mechanisms; however, they also expressed concerns about insufficient forensic tools, limited manpower, and training gaps. These challenges mirror observations in broader Indian contexts, where resource

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 2, November 2025 Impact Factor: 7.67

constraints and skill shortages hinder effective cybercrime investigations (Chauhan & Gupta, 2019). Judges and advocates further emphasized difficulties in interpreting cyber laws in rapidly evolving technological scenarios, highlighting the need for specialized training and updated legal frameworks that can keep pace with emerging forms of digital harm.

A recurrent theme in the discussion is the gap between awareness and practical cyber security readiness among the general population. While many respondents recognized common cyber threats, far fewer reported confidence in safeguarding themselves or their institutions against such attacks. This disparity suggests that cyber literacy and preventive practices are not yet sufficiently widespread, particularly among employees outside technology sectors and residents in rural or remote areas. Limited awareness of safe online behaviors such as identifying suspicious links, using strong authentication methods, and securing personal devices likely contributes to ongoing vulnerabilities, as supported by secondary analyses on cyber hygiene deficits in similar regions (Sharma, 2020).

The results highlight a clear recognition of emerging cybercrime trends among key stakeholder groups in Himachal Pradesh, but also reveal persistent challenges in cyber security infrastructure, training, and public preparedness. These findings underscore the importance of targeted interventions, including capacity building for enforcement and judiciary, expanded public awareness campaigns, and investment in cyber forensic capabilities to enhance the state's overall resilience against digital threats.

1. Types of Cyber Crime Observed

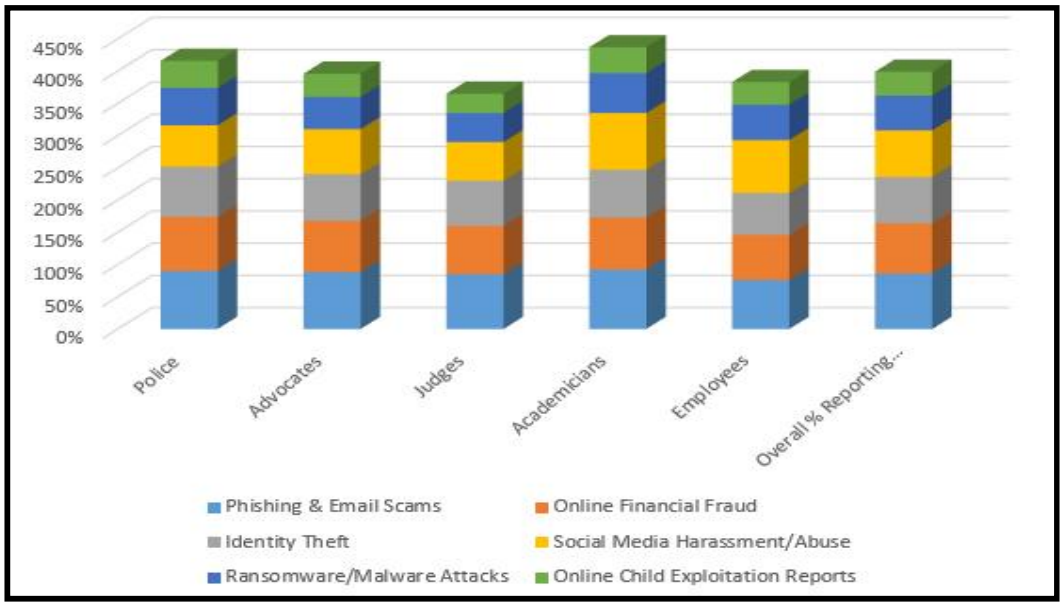
The survey revealed patterns of cybercrime awareness and experience among stakeholders:

Table 1: Awareness and experience of cybercrime types across stakeholder groups.

Cyber Crime Type	Police	Advocates	Judges	Academicians	Employees	Overall % Reporting Awareness/Experience
Phishing & Email Scams	90%	88%	85%	92%	76%	86%
Online Financial Fraud	84%	80%	75%	81%	70%	78%
Identity Theft	78%	72%	70%	74%	65%	72%
Social Media Harassment/Abuse	64%	70%	60%	88%	82%	72%
Ransomware/Malware Attacks	58%	50%	45%	62%	55%	54%
Online Child Exploitation Reports	42%	36%	30%	40%	35%	37%

The table indicates that phishing and financial fraud are the most recognized threats across all groups. Academicians reported high levels of awareness, possibly due to exposure to digital platforms.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67



Graph 1: Stakeholder-wise Awareness and Reporting of Major Cyber Crime Types in Himachal Pradesh

2. Perception of Cyber Security Challenges

Respondents identified major challenges:

Lack of Training and Expertise: 78% highlighted inadequate cyber security training, especially among police and judiciary (Chauhan & Gupta, 2019).

Infrastructure Gaps: 65% felt that law enforcement lacks advanced tools for cyber forensics.

Policy Implementation Barriers: 58% noted delays in adopting national cyber security standards at the state level.

3. Institutional Readiness

Police officials and advocates reported that existing cyber cells and legal frameworks have made progress but remain under-resourced. Judges highlighted challenges in adjudicating cybercrime cases due to evolving technological contexts and ambiguous legal precedents (Raina, 2022).

KEY CHALLENGES IDENTIFIED

Rapid Evolution of Cyber Threats: Cyber criminals adapt faster than response mechanisms.

Skill and Resource Gap: Both enforcement and judiciary lack specialized cybercrime training.

Awareness Deficit in Public: Low awareness among general workforce increases vulnerability.

Legal and Policy Constraints: Need for streamlined processes and updated legislations.

II. CONCLUSION

Emerging cybercrime trends present serious risks in Himachal Pradesh, particularly as digital adoption accelerates. The study underscores the importance of a multi-pronged approach strengthening cyber security infrastructure, enhancing training for key stakeholders, and fostering public awareness. Policymakers should prioritize resource allocation to cybercrime cells and continuous capacity building.

REFERENCES

[1]. Chauhan, R., & Gupta, P. (2019). *Cyber Security Challenges in India: A Review*. Journal of Information Security, 10(2), 112–125.

[2]. Kumar, A., & Mishra, S. (2020). *Financial Frauds in Digital India: Patterns and Prevention*. International Journal of Cyber Law, 5(1), 45–60.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 2, November 2025
Impact Factor: 7.67

[3]. Raina, L. (2022). *Social Media and Cyber Harassment: Legal Perspectives*. Himachal Law Review, 8(3), 98–115.

[4]. Sharma, D. (2020). *Public Awareness on Cyber Security: A State-Level Study*. Journal of Digital Society, 4(4), 77–89.

[5]. Singh, V., & Sharma, R. (2021). *Trends in Cyber Crime in North-Western India*. Cyber Crime Journal, 6(1), 23–40.

[6]. Singh, Y., & Thakur, M. (2021). *Bridging the Cyber Security Skill Gap in India*. Journal of Technology Education, 9(2), 56–68.

[7]. Verma, K., & Gupta, N. (2020). *Ransomware Attacks and Mitigation Strategies*. International Cybersecurity Review, 7(4), 143–158.