IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14156

The Role of Six States Police to Mitigating the Cyber Crime in India: A Case Study

Varinder Kaur Attri[1], Teena Jaiswal[2], Ram Narayan Jaiswal[3], Vidhu Baggan [4]

Assistant Professor, CSE Dept, GNDU, RC Jalandhar, India[1]

Research Scholar, CS Dept, GNDU, Amritsar, Punjab, India[2]

Research Scholar, Bundelkhand University Jhansi, India[3]

Professor, CSE Dept, Chitkara University, Himachal Pradesh, India [4]

Abstract: Cybercrime has become a major challenge in India, as digital platforms continue to evolve. With increasing incidents of financial fraud, hacking, identity theft, online bullying, and more, the role of state police forces has become critical in addressing cybercrime. This research paper examines the role of six Indian state police forces—Madhya Pradesh, Maharashtra, Delhi, Tamil Nadu, Karnataka, and Punjab—in mitigating cybercrime. Through a case study approach, the paper highlights specific incidents in each state, focusing on how police forces responded to cases of cybercrime, their strategies, technological advancements, collaborations with other agencies, and the challenges they faced. The research sheds light on both successes and areas for improvement in the fight against cybercrime in India.

Keywords: Cybercrime**,** State-Specific Approaches, Police, Indian Penal Act.

I. INTRODUCTION

Cybercrime, as defined by the United Nations, refers to criminal activities that are conducted through digital platforms or involve a computer as the target or tool for committing the crime. The surge in internet usage, especially through mobile devices, has provided new avenues for criminals to exploit vulnerable users. Madhya Pradesh, being a populous state with a growing urban-rural divide, faces unique challenges in dealing with these crimes. The MP Police, through the Cyber Crime Cell and other specialized units, have adopted several measures to combat cybercrimes. With the rapid growth of digital technology, cybercrime has emerged as one of the most pressing challenges for law enforcement in India [1,2]. The rise of cybercriminal activities—ranging from financial fraud to online harassment—has left many citizens vulnerable. State police forces across the country have been adapting to these new threats, establishing specialized cybercrime units and collaborating with national and international agencies to address the rising menace. This paper focuses on the police forces of Madhya Pradesh, Maharashtra, Delhi, Tamil Nadu, Karnataka, and Punjab, analyzing their efforts to combat cybercrime through case studies of notable cybercrime incidents. These case studies will showcase the methods, technologies, and strategies employed by the police to mitigate cybercrime in their respective states.

A. Types of Cyber Crimes in India

Cybercrime refers to illegal activities conducted through the internet or other forms of computer networks. In India, with the increasing use of the internet and digital platforms, cybercrimes have escalated, affecting individuals, businesses, and government institutions alike. Below are the major types of cybercrimes prevalent in India:

TABLE 1: TYPES OF CYBERCRIME IN INDIA

Sno	Cyber crime	Definition	Example	Legal Reference
1.	Hacking	Hacking involves unauthorized access to computer systems or networks to steal, modify, or destroy data. This can be done for malicious purposes or personal gain.	A hacker breaking into a bank's database to transfer funds or manipulate records.	Section 66 of the Information Technology Act, 2000.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14156

2.	Identity Theft	Identity theft occurs when an individual's personal information (such as Social Security number, credit card details, or personal identification) is stolen and used for fraudulent purposes.	A cybercriminal stealing someone's bank account details to withdraw money.	Legal Reference: Section 66C of the Information Technology Act, 2000.
3.	Cyberbullying	: Cyberbullying refers to the use of digital platforms to harass, intimidate, or harm others. It involves sending abusive or threatening messages, spreading rumors, or engaging in online shaming	A teenager receiving harmful, abusive messages through social media platforms, leading to emotional distress.	Section 66A of the Information Technology Act (for sending offensive messages), and the Indian Penal Code (IPC) sections for harassment and defamation.[4]
4.	Phishing	Phishing is a method used by cybercriminals to trick individuals into revealing personal information, such as passwords, bank account details, or credit card numbers, by pretending to be legitimate entities (banks, websites, etc.).	A user receiving an email claiming to be from their bank, asking them to click a link and enter their account details to avoid "suspicious activity."	Section 66D of the Information Technology Act, 2000.
5.	Financial Fraud (Online Fraud)	Financial fraud involves the use of online platforms to deceive individuals or organizations into transferring money or sensitive financial information for criminal purposes. This can include credit card fraud, online banking fraud, or fake e-commerce websites.	A cybercriminal setting up a fake online shopping website that collects payments but delivers no goods.	: Section 420 of the Indian Penal Code (IPC) for cheating and fraud.[4]
6.	Cyber Stalking	Definition: Cyberstalking is the use of the internet to stalk or harass an individual by sending threatening emails, making repeated online threats, or spreading false information	An individual constantly receiving threatening emails or being monitored through social media.	Section 66A of the Information Technology Act and Section 354D of the IPC.
7.	Online Child Sexual Abuse (Child Pornography)	This category of cybercrime includes the creation, distribution, and possession of child pornography or the	: A person sharing explicit content involving minors or attempting to groom a child for sexual	Section 67B of the Information Technology Act, 2000, and the Protection of Children

DOI: 10.17148/IJARCCE.2025.14156

		exploitation of children for sexual purposes via the internet.	exploitation via online platforms.	from Sexual Offences (POCSO) Act, 2012
8.	Cyber Terrorism	Cyber terrorism involves the use of the internet to carry out acts of terrorism, such as spreading terror, disrupting critical infrastructure, or attacking national security systems.	A cyberattack on a country's power grid, which causes widespread disruption.	Section 66F of the Information Technology Act, 2000.
9.	Data Theft and Privacy Violations	Data theft refers to the unauthorized access and theft of personal, financial, or confidential data for malicious purposes. This can include stealing data from government databases, companies, or individuals.	A hacker breaking into a company's database to steal sensitive client information or government secrets	Section 43 of the Information Technology Act and Section 72A for privacy violations.
10.	Online Impersonation	Online impersonation is the act of creating fake profiles or accounts to pretend to be someone else, often with the intent to defraud or harm that person's reputation.	A person creating a fake social media profile pretending to be someone else to defraud others or harass them.	Section 66C of the Information Technology Act and Section 419 of the Indian Penal Code (IPC).[4]
11.	Software Piracy	Software piracy involves the unauthorized reproduction, distribution, or use of software, often with the intent to avoid paying for legitimate licenses.	Downloading cracked or pirated versions of paid software from illegal websites.	Copyright Act of 1957 and Section 63 of the Information Technology Act.
12.	Spreading Malware or Ransomware	Malware or ransomware involves the use of malicious software to damage or gain unauthorized access to computer systems. Ransomware is a form of malware that locks a system or encrypts data and demands a ransom for its release.	A cybercriminal sending a malicious email attachment that locks a victim's files and demands payment to unlock them.	Section 66 of the Information Technology Act (for hacking and causing harm) and Section 383 of the IPC (for extortion)[4]
13.	Fake News and Defamation	The spreading of false information or rumors online, often with the intent to harm a person's reputation or incite unrest. This can include fake news or defamatory content posted on social	Someone creating a fake news story about a politician or public figure and sharing it online to damage their reputation.	Section 66A of the Information Technology Act and Section 499 of the IPC for defamation. [4]

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025
DOI: 10.17148/IJARCCE.2025.14156

		media, blogs, or websites.		

II. LITERATURE SURVEY

The role of police in mitigating cybercrime across six Indian states is multifaceted, involving legal frameworks, technological advancements, and collaborative efforts. The increasing prevalence of cybercrime necessitates a robust response from law enforcement agencies, which includes not only enforcing existing laws but also adapting to the evolving nature of cyber threats.The Information Technology Act, 2000, serves as the primary legal framework for addressing cybercrime in India, yet it faces challenges in enforcement and prosecution[13][14]. There is a critical need for a comprehensive legislative framework to address the unique challenges posed by cybercrime, as highlighted by various studies[15]. States like Kerala and Maharashtra have implemented technology infusion in their policing strategies, enhancing their capabilities to combat cybercrime[12]. The development of cybercrime cells and the use of digital tools for intelligence gathering are essential for proactive measures against cyber threats. Effective mitigation of cybercrime requires collaboration among various stakeholders, including government agencies, private sectors, and international partners[13,14]. Public awareness and education on cybersecurity are crucial components of a comprehensive strategy to reduce cybercrime incidents[14]. While the police play a vital role in combating cybercrime, the effectiveness of their efforts can be hindered by inadequate resources and the rapid evolution of cyber threats. Continuous adaptation and investment in technology and training are essential for law enforcement to keep pace with these challenges. The Madhya Pradesh State Police plays a crucial role in mitigating cybercrime through various strategies and initiatives. Their approach encompasses prevention, investigation, and public awareness, which are essential in addressing the complexities of cyber threats. Integrated Approach: Madhya Pradesh Police employs a comprehensive strategy that combines legislative measures, technical tools, and community engagement to combat cybercrime. Continuous training for police personnel is emphasized to enhance their skills in handling electronic evidence and utilizing new technologies effectively [16]. Community Engagement: Initiatives aimed at educating the public about cyber threats and preventive measures are crucial. The police provide resources and guidance to help citizens protect themselves online[17].Partnerships with schools and universities facilitate the dissemination of knowledge regarding cyber safety, fostering a culture of awareness among students[18]. Use of Technology: The police utilize advanced software and databases for timely information gathering, which is vital for preventing and investigating cybercrimes .Operational units conduct investigations using both public and secret methods to effectively suppress and disclose cybercriminal activities[19].

While the Madhya Pradesh State Police has made significant strides in combating cybercrime, challenges remain, particularly in keeping pace with rapidly evolving cyber threats and ensuring public trust in their capabilities. The role of police in mitigating cyber crime across Maharashtra, Punjab, Delhi, Karnataka, and Tamil Nadu is critical, given the increasing prevalence of cyber threats. These states have adopted various strategies to enhance their cyber policing capabilities, focusing on training, cooperation, and public awareness. Police forces in these states are investing in specialized training programs to equip officers with the skills necessary to handle cyber crime effectively [16]. Continuous professional development is essential, as the landscape of cyber crime is rapidly evolving, necessitating updated knowledge and techniques[17]. Effective cyber crime mitigation requires collaboration between law enforcement, private sector entities, and the community [16]. Initiatives that foster partnerships with technology companies can enhance investigative capabilities and resource sharing[17]. Increasing public awareness about cyber crime and its reporting mechanisms is vital to reduce unreported cases [20]. Educational campaigns can empower citizens to recognize and report cyber threats, thereby improving overall community safety[21]. While these states are making strides in cyber crime mitigation, challenges remain, such as the need for more robust legislative frameworks and the integration of advanced technologies in policing efforts. Addressing these issues will be crucial for enhancing the effectiveness of cyber crime prevention strategies.

III.CASE STUDY APPROACH

This paper employs a case study approach to explore the role of state police forces in India in mitigating cybercrime. Each case study will Identify a significant cybercrime case handled by the state police. Discuss the investigation methods, technological tools, and collaboration with other agencies. Analyze the strategies employed to resolve the case and mitigate the effects of cybercrime. Address the challenges faced by law enforcement agencies in investigating and prosecuting cybercrimes.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025
DOI: 10.17148/IJARCCE.2025.14156

A. Role of Madhya Pradesh Police in Mitigating Cybercrime

Madhya Pradesh (MP) has seen a significant rise in cybercrimes, especially financial frauds and cyberbullying. The MP Police have worked actively to establish specialized Cyber Crime Cells in major cities, with a focus on digital forensics and public awareness.

- Case Study: Bhopal Phishing Scam (2023)

In 2023, the MP Police responded to a phishing scam that affected over 50 residents in Bhopal. Victims received messages from a fake banking app designed to steal personal and banking details. The Cyber Crime Cell investigated the issue, traced the perpetrators, and collaborated with banks to freeze accounts and prevent further fraud.

B. Role of Maharashtra Police in Mitigating Cybercrime

Maharashtra is one of the most advanced states in terms of addressing cybercrime, particularly in Mumbai, which is a financial hub and a prime target for cybercriminals. The Maharashtra Police have established the Cyber Crime Investigation Cell (CCIC) to handle complex cases[7].

- Case Study: Ransomware Attack on a Hospital (2022)

In 2022, a hospital in Mumbai was hit by a ransomware attack that encrypted sensitive patient data and demanded a ransom for its release. The Maharashtra Cyber Crime Cell, in collaboration with international agencies, successfully investigated the case, decrypted the data, and arrested the cybercriminals involved in the attack.

C. Role of Delhi Police in Mitigating Cybercrime

Delhi, as the national capital, faces a wide range of cybercrimes, including cyberbullying, financial fraud, and data theft. The Delhi Police have set up a specialized Cyber Crime Unit to address these issues[8] .

- Case Study: Cyberbullying and Online Harassment (2021)

In 2021, Delhi Police investigated a series of cyberbullying incidents involving young women. Victims were targeted on social media, receiving abusive and threatening messages. The Cyber Crime Unit worked closely with social media platforms to trace the perpetrators, identify their locations, and prevent further harassment. The police arrested the offenders and conducted outreach campaigns to educate the public about online safety.

D. Role of Tamil Nadu Police in Mitigating Cybercrime

Tamil Nadu, with a large population and growing tech industry, faces increasing cybercrime, especially related to financial fraud. The Tamil Nadu Police have been proactive in establishing the Tamil Nadu Cyber Crime Unit (TNCU) to address these issues[9].

- Case Study: Online Financial Fraud (2020)

In 2020, several people in Chennai fell victim to an online scam promising high returns on investments. The perpetrators used fake websites and social media ads to trick individuals into investing money. The Tamil Nadu Cyber Crime Unit investigated the case and arrested the suspects, recovering a portion of the stolen funds.

E. Role of Karnataka Police in Mitigating Cybercrime

Karnataka, particularly Bengaluru, is a major tech hub, and the state's police have developed strong mechanisms to handle the increasing number of cybercrimes.

- Case Study: Data Breach at an IT Firm (2019)

In 2019, an IT firm in Bengaluru suffered a significant data breach that compromised sensitive customer information. The Karnataka Cyber Crime Unit, in collaboration with the firm's internal cybersecurity team, traced the breach to an insider who had sold data to external hackers. The police arrested the culprit and secured the stolen data[10].

F. Role of Punjab Police in Mitigating Cybercrime

Punjab has faced increasing cybercrime, particularly drug trafficking through the dark web and financial fraud. The Punjab Police have adapted to these threats through the establishment of a Cyber Crime Investigation Cell.

- Case Study: Online Drug Trafficking Network (2021)

In 2021, Punjab Police uncovered a dark web-based drug trafficking network operating in the state. The criminals used encrypted communication channels to sell narcotics to customers across the country. The Punjab Police, through digital forensics, managed to break the encryption and apprehend several members of the network [11].

IV. COMPARATIVE ANALYSIS OF STRATEGIES AND CHALLENGES

Across the six states—Madhya Pradesh, Maharashtra, Delhi, Tamil Nadu, Karnataka, and Punjab—the case studies reveal both common and unique strategies to combat cybercrime:

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025
DOI: 10.17148/IJARCCE.2025.14156

A. **Common Strategies**:
Establishment of specialized Cyber Crime Units in each state. Collaboration with national agencies and international law enforcement to handle cross-border cybercrimes. Public outreach and digital literacy campaigns to prevent online fraud and harassment. Utilization of advanced technologies like digital forensics, AI, and machine learning.

B. **State-Specific Approaches:**
Maharashtra's focus on ransomware attacks, particularly in the healthcare sector. Delhi's proactive approach to tackling cyberbullying and online harassment. Punjab's efforts in addressing dark web-based drug trafficking.

C. **Challenges Faced:**
Technological limitations in tracking cybercriminals who use VPNs and encrypted messaging systems.
Legal complexities, especially regarding data privacy and cross-border jurisdictional issues.High public reluctance to report cybercrimes due to fear of embarrassment or financial loss.

TABLE:2 CASE STUDY OF SIX STATES OF INDIA

SNO	Case Study	State	Key Strategies	Challenges
2023,[5,6]	Bhopal Phishing Scam (2023)	Madhyapradesh Police	Use of digital forensics tools to trace the origin of the fraudulent app. Collaboration with banking institutions to track and prevent further fraudulent activities. Launching public awareness campaigns about phishing scams.	Limited technological infrastructure to track cybercriminals using VPNs and encrypted communication. Reluctance among citizens to report cybercrime due to fear of financial loss.
2022,[7]	Ransomware Attack on a Hospital (2022)	Maharashtra Police	The formation of the Cyber Crime Investigation Cell (CCIC) for specialized handling of cybercrimes. Cross-border cooperation with international law enforcement agencies like Interpol. Rapid response to ransomware attacks to mitigate damage.	Difficulties in tracking cybercriminals who use international VPNs and anonymous networks. Balancing speed and accuracy in resolving ransomware cases while ensuring that digital evidence remains intact.
2021,[8]	Cyberbullying and Online Harassment (2021)	Delhi Police	Establishment of a dedicated Cyber Crime Unit to investigate various online crimes. Active monitoring and reporting of harmful content on social media platforms. Collaboration with social media companies to track and remove offensive content.	Jurisdictional issues regarding the access of data from social media platforms. Legal complexities surrounding online harassment and the balance between privacy and safety.
2020[9]	Online Financial Fraud (2020)	Tamil Nadu Police	Formation of the Tamil Nadu Cyber Crime Unit	High volume of online financial

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025
DOI: 10.17148/IJARCCE.2025.14156

			(TNCU) to investigate online fraud. Collaboration with financial institutions to track fraudulent transactions. Public education campaigns to raise awareness about online investment scams.	fraud cases and resource constraints in handling them. Difficulty in tracing cybercriminals who use fake identities and operate from multiple locations.
2019,[10]	Data Breach at an IT Firm (2019)	Karnataka Police	Collaboration between the police and private companies to address cybersecurity incidents. Use of machine learning and artificial intelligence to predict and identify potential threats. Implementation of stronger cybersecurity practices in both public and private sectors.	Jurisdictional issues in handling cases that involve international data breaches. Difficulty in recovering encrypted or stolen data that has been disseminated online.
2021[11]	Online Drug Trafficking Network (2021)	Punjab Police	Digital forensics is essential for tracing dark web transactions. Collaborating with national agencies like the Narcotics Control Bureau helps dismantle drug trafficking networks. Ongoing training for law enforcement is vital to keep up with new cybercriminal techniques.	The anonymity of the dark web makes it difficult to trace and apprehend criminals. Limited public awareness of emerging cybercrimes such as dark web trafficking.

Despite the efforts made by the Police, various challenges hinder the effective mitigation of cybercrime:

- Lack of Public Awareness

A significant portion of the population in Madhya Pradesh remains unaware of the risks associated with cybercrime. Many individuals are vulnerable to phishing attacks, online fraud, and identity theft due to the lack of understanding regarding digital security.

- Limited Technological Resources

While the MP Police have made advancements in their capabilities, there is still a shortage of advanced cyber forensic tools and highly skilled personnel to deal with complex cybercrimes, particularly those involving emerging technologies like cryptocurrency.

- Jurisdictional Issues

Cybercriminals often operate across state and national borders, which complicates the investigation and prosecution process. While collaborations with national agencies help, jurisdictional challenges remain a significant barrier.

- Slow Legal Process

The legal framework for prosecuting cybercrimes is still evolving, and the judicial process often lags in keeping up with the rapid pace of technological advancement. Delays in investigations and prosecutions can discourage victims from reporting crimes.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025
DOI: 10.17148/IJARCCE.2025.14156

V. RECOMMENDATIONS FOR STRENGTHENING CYBERCRIME MITIGATION EFFORTS

To further enhance the MP Police's ability to combat cybercrime, the following recommendations are proposed:

A. Expanding Public Awareness Programs
Increased efforts should be made to target underserved rural areas with awareness programs on digital security, including workshops in schools and community centers. These programs should focus on creating a digital-savvy population that can recognize and avoid cyber threats.

B. Investment in Training and Technology
MP Police should continue to invest in cutting-edge technologies and advanced training programs for their personnel. Specialized units should be equipped with the latest tools for digital forensics, data recovery, and social media monitoring to stay ahead of cybercriminals.

C. Strengthening Inter-State and International Collaboration
Cybercrime is a global issue, and MP Police must strengthen their partnerships with law enforcement agencies in other states and countries to track down international perpetrators. Collaboration with private tech companies and cybersecurity firms is also vital in developing proactive strategies.

D. Collaboration with National Agencies
Recognizing the complexity of tracking down cybercriminals who may have been operating from different states or even countries, the MP Police escalated the case to the National Cyber Crime Reporting Portal and sought collaboration from the Central Bureau of Investigation (CBI) and other state police forces.
This inter-state cooperation was essential in tracing the criminal's location and narrowing down suspects involved in the scam. The police also received technical assistance from cybersecurity companies specializing in data breach investigations.

E. Speeding up Legal Reforms
There is a need for faster judicial processes in cybercrime cases. Special courts and fast-track tribunals should be established to handle cybercrime cases more efficiently, ensuring that offenders are brought to justice promptly.

VI. CONCLUSION

Cybercrime in India has become a serious issue, affecting individuals, businesses, and government sectors. As technology continues to evolve, new forms of cybercrime will likely emerge, requiring constant vigilance and updates to legal frameworks. India's laws, such as the Information Technology Act, 2000, along with provisions in the Indian Penal Code (IPC), aim to curb these crimes, but awareness and prevention remain key to mitigating cyber risks. Both individuals and organizations need to prioritize cybersecurity measures to protect themselves from the growing threat of cybercrime.Cybercrime poses a significant threat to Madhya Pradesh, as it does across the globe. However, the Police's efforts to mitigate these crimes through specialized units, technological advancements, and public awareness initiatives have made significant progress. While challenges persist, the collaboration with national and international law enforcement agencies, along with continuous investments in training and technology, will ensure that states Police are well-equipped to tackle the evolving threat of cybercrime. Further policy reforms and increased public awareness will also be key in reducing the vulnerability of citizens to cybercrime .This case study of the 2023 financial fraud in Madhya Pradesh illustrates the proactive role of the MP Police in mitigating cybercrime. Through collaboration, technological advancements, and public outreach, the MP Police were able to successfully address the crisis, recover stolen funds, and deter future cybercriminal activities. Despite facing challenges such as technological gaps and jurisdictional issues, their multi-faceted approach provides valuable lessons for improving cybercrime mitigation strategies across the state. The ongoing efforts of the States Police serve as a model for other regions in India dealing with similar issues.

REFERENCES

[1]. Rishi Bhargava. (2020). Cyber Crime and Cyber Security in Madhya Pradesh.
[2]. MP Police Official Website. (2024). Cyber Crime Cell and Initiatives.
[3]. National Cyber Crime Reporting Portal. (2024). Annual Report on Cyber Crime Statistics.
[4]. Indian Penal Code. (1860). Relevant Sections on Cyber Crime.
[5]. Madhya Pradesh Cyber Crime Prevention Scheme. (2023). State Government Initiatives.
[6]. Madhya Pradesh Police Official Website. (2023). Cyber Crime Prevention in Madhya Pradesh

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 1, January 2025

DOI: 10.17148/IJARCCE.2025.14156

[7]. Maharashtra Cyber Crime Investigation Cell. (2022). Annual Report on Cybercrime Trends.
[8]. Delhi Police Cyber Crime Unit. (2021). Report on Social Media-Based Harassment and Cyberbullying.
[9]. Tamil Nadu Police Cyber Crime Unit. (2020). State Cyber Crime Awareness and Prevention Program.
[10]. Karnataka Police Cyber Crime Unit. (2019). Data Breach Response and Mitigation.
[11]. Punjab Police Cyber Crime Cell. (2021). Combatting Online Drug Trafficking and Cybercrime.
[12]. Rajput, B., Gada, D., & K, A. (2024). Efforts Taken by Law Enforcement Agencies Across India (pp. 87–97). Springer International Publishing. https://doi.org/10.1007/978-3-031-45697-8_7
[13]. Rani, K. (2023). Cybercrime and Legal Responses in the Indian Jurisdiction. 1(1), 35–41. https://doi.org/10.36676/ijl.2023-v1i1-05
[14]. S.Thangamayan, E. al. (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. https://doi.org/10.17762/ijritcc.v11i9.9379
[15]. Nakkeeran, S. and Dr. Dharamveer Singh. "Challenges in Cybercrime Prevention and Legal Frameworks in India: An Analytical Study." Journal of Advances and Scholarly Researches in Allied Education (2024): n. pag.
[16]. Tropina, T. (2017). Cyber-policing: the role of the police in fighting cybercrime. 2, 287–294. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/232
[17]. Staniforth, A. (2017). Preventing Cyber Crime. Oxford University Press. https://doi.org/10.1093/oso/9780198723905.003.0005
[18]. Malathi, B., Munesh, P., & Chandra Sekharaiah, K. (2020). PGF Cyberpolicing to Defuse Fake Government of Telangana (FGoT), Fake Government of India (FGoI) and Cybercriminal Legacy (pp. 181–191). Springer, Singapore. https://doi.org/10.1007/978-981-16-3660-8_17
[19]. Sidorova, E., & Usov, E. G. (2024). The main measures to prevent digital crime. https://doi.org/10.29039/2312-7937-2024-2-38-43
[20]. Patel, P. B., Thakor, H. P., & Iyer, S. (2019). A Comparative Study on Cyber Crime Mitigation Models. International Conference on Computing for Sustainable Global Development.
[21]. Karali, Y., Panda, S., & Panda, C. S. (2015). Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. International Journal of Engineering and Management Research, 5(2), 43–48. https://www.indianjournals.com/ijor.aspx?target=ijor:ijemr&volume=5&issue=2&article=009