International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Emerging Cyber Crimes in India: Trends, Impact & Regulatory Evaluation

Sarthak Ray[1], Dr. Soumya Ranjan Nayak[2]

[1]2nd Year (Master of Science Information Security), School of Vocational Education and Training, Indira Gandhi National Open University, Maidan Garhi, New Delhi, Mail ID: kakun.sarthak08@gmail.com
[2]Associate Prof., IGNOU Academic Counsellor Code: AIYPN0305M/001, Regional Centre (IGNOU) Bhubaneswar

ABSTRACT:
India's rapid digitalization has transformed banking, commerce, governance, and public services, but it has also increased the risk of cybercrime. This study examines major cybercrime incidents in India, including the Cosmos Bank cyber heist, Aadhaar data breaches, ransomware attacks on AIIMS Delhi and Tata Technologies, and phishing scams. The research analyzes the methods used by cybercriminals, identifies common vulnerabilities, and highlights emerging cyber threats. The study evaluates the social and economic impact of cybercrime on individuals, organizations, and critical infrastructure. It also examines the roles of law enforcement agencies, cybersecurity institutions, and government bodies in responding to cyber incidents. Furthermore, the effectiveness of existing cybersecurity laws, policies, and technological safeguards is reviewed. The research identifies key challenges in cybercrime prevention and investigation, such as limited awareness, inadequate digital literacy, and evolving attack techniques. Based on the findings, it recommends stronger cybersecurity practices, improved public awareness, enhanced legal frameworks, and greater collaboration among stakeholders. The study emphasizes that a coordinated effort by government, institutions, and citizens is essential to strengthen cyber resilience and ensure a secure digital future for India.

KEY WORDS: Cyber frauds, Identity theft, Cyber terrorism, Aadhaar data breach, Cyber Terrorism, Ransomware attacks, Phishing scams, UPI frauds, Deepfake phishing, NCRB Crime Statistics, CERT-In advisories, I4C, IT (Amendment) Act, 2008¸ Digital forensics, Judicial challenges; Cyber hygiene awareness; Public-private partnerships, AI-driven scams, Policy Modernization

1. INTRODUCTION:

The rapid growth of digital technologies has transformed India into one of the largest digital economies in the world. With over 800 million internet users, widespread smartphone penetration, and ambitious government initiatives such as Digital India, the country has embraced digitalization across education, and healthcare. This transformation has created immense opportunities for innovation and efficiency, but it has also exposed individuals, businesses, and institutions to new vulnerabilities. Cybercrime has emerged as a critical challenge, threatening not only financial stability but also national security and public trust in digital systems. **[1]**

Cybercrime refers to unlawful activities carried out using computers, networks, or digital devices. It encompasses a wide range of offenses, including hacking, phishing, identity theft, ransomware, cyber

terrorism, and online financial fraud. In India, incidents have ranged from large-scale data breaches affecting millions of citizens to targeted attacks on banks, e-commerce platforms, and government databases. The anonymity of cyberspace, coupled with the global reach of the internet, makes detection and prevention particularly complex. **[2]**

The increasing sophistication of cybercriminals, who often operate in organized groups and exploit systemic loopholes, has made cybercrime a multidimensional issue. It is not merely a technological problem but also a social, economic, and legal challenge. The rise of cybercrime in India underscores the urgent need for systematic research and policy intervention. **[3]**

1.1.Rationale of the Study:

India's digital ecosystem is expanding at an unprecedented pace, but the frameworks to secure it have not always kept up. While the Information Technology Act, 2000 and its amendments provide a legal foundation, enforcement remains inconsistent. Institutions such as the Indian Cybercrime Coordination Centre (I4C) and state-level cybercrime cells have been established, yet challenges persist in terms of capacity, coordination, and awareness. Moreover, cybercrime in India is not limited to financial frauds or data breaches. It intersects with broader social issues such as misinformation, online harassment, and exploitation of vulnerable populations. It also has geopolitical dimensions, with state-sponsored cyberattacks targeting critical infrastructure and defence systems. **[4]**

A case study approach is particularly valuable in this context. By analyzing specific incidents, the study can uncover patterns, highlight systemic weaknesses, and evaluate institutional responses. This evidence-based analysis will contribute to both academic discourse and practical policymaking, bridging the gap between theory and practice.

1.2.Research article Aim:

India has experienced a rapid wave of digitalization in the past decade, and this transformation has created immense opportunities for economic growth and innovation. Online banking, e-commerce, and digital governance have become integral to everyday life, but this digital expansion has also introduced significant risks. Cybercrime has emerged as one of the most pressing challenges in this new era, with financial frauds increasingly targeting individuals and institutions alike. **[5]**

Ransomware attacks have disrupted businesses and critical services, while identity theft has become a common threat to citizens using online platforms. Cyber terrorism poses dangers to national security and public safety, and the overall number of cyber incidents in India has surged dramatically. These crimes exploit vulnerabilities in technology and human behavior, and the consequences range from financial losses to reputational damage. They also undermine trust in digital systems and institutions, making it harder for citizens to feel secure online. **[6]**

2. LITERATURE REVIEW:

India has experienced a rapid wave of digitalization in the past decade. In the year 2025 Samal A. & Samal S. in their article "Cyber threats and national security in India: Evaluating policy measures and emerging challenges" have examined the dominant cyber threats confronting Indian organizations and individuals, with particular emphasis on ransomware, phishing, and sophisticated malware campaigns. It underscores how India's rapid digital transformation, coupled with the widespread integration of Internet of Things (IoT) devices, has outpaced the deployment of adequate security safeguards. This imbalance has created exploitable vulnerabilities across both governmental and corporate domains. By mapping these risks, the

paper offers a holistic view of India's cyber security environment, identifies pressing challenges, and proposes proactive defense strategies tailored to the nation's evolving digital ecosystem. **[7]**

Cybersecurity in India has developed into a multi-dimensional policy and governance issue shaped by rapid digitization, institutional fragmentation, and the rising sophistication of cyber threats. The literature consistently shows that India's cybersecurity posture is not determined by technology alone; it also depends on legal frameworks, inter-agency coordination, public awareness, and private-sector participation. Kshetri N. (2015) argues that cybersecurity in India cannot be managed by the state alone because essential digital services, platforms, and infrastructure are increasingly owned or operated by private actors. **[8][9] (Kshetri N.; Markovic E).**

Recent policy discussions likewise emphasize that India must combine technical controls with coordinated governance if it is to protect citizens, businesses, and critical infrastructure effectively. The report by United Nations Office on Drugs & Crime named "Public-Private Partnerships on Cybercrime" similarly contends that information sharing, joint incident response, and trust-based cooperation are essential for a resilient cyber ecosystem. This perspective is reinforced in newer policy-oriented work, which notes that public-private partnerships are central to improving cyber preparedness, innovation, and threat intelligence exchange. Taken together, these studies suggest that India's cybersecurity governance must be networked rather than purely state-centric.

Another major theme is cyber hygiene and organizational readiness. Khanna A. highlighted that weak password practices, poor patch management, unsafe browsing behaviour and inadequate user awareness remain common vulnerabilities across Indian institutions. Their findings align with broader evidence that cyber incidents often exploit basic operational weaknesses rather than highly advanced technical flaws. The literature therefore implies that improving awareness, training, and routine security practices may yield substantial gains in reducing risk, especially in public institutions and smaller private organizations In this sense, cyber hygiene is presented not as a minor issue but as a foundational layer of defense. **[10]**

A further body of work examines institutional and policy shortcomings. Markovic E. argue that India's cybersecurity framework suffers from fragmented institutional responsibility, uneven enforcement, and limited operational coordination among agencies. He has gone further by questioning whether India's National Cyber Security Policy is still adequate for the current threat environment. More recent government measures, including CERT-In directives and sectoral guidelines, indicate that the state has recognized these gaps, but implementation remains uneven **(CERT-In, 2024).** The literature therefore portrays India's cyber governance as evolving, but still incomplete. **[9][11]**

Another important strand concerns awareness and capacity gaps. Bholane K.P., Jadhav T.P., Rathod Dr. V.M. have highlighted a rural-urban divide in cybersecurity awareness, showing that digital risks are not distributed evenly across populations. People in rural and semi-urban areas may have lower awareness of phishing, fraud, safe authentication practices, and reporting mechanisms. They have also identified a related shortage of cybersecurity skills, arguing that India needs a larger and more specialized workforce to meet rising demand. These studies imply that India's cyber resilience depends not only on institutions and laws, but also on education, training, and digital literacy at the user level. **[12]**

The protection of critical infrastructure is one of the most urgent concerns in this literature. It is argued that power, transport, communications, health, and other essential systems must be treated as high-priority cybersecurity domains because disruptions can produce national-scale consequences. Meccyjoy et. al extends this argument by showing that ransomware attacks on critical infrastructure can interrupt essential services, create financial losses, and expose gaps in recovery planning. CERT-In's threat reporting and

government statements similarly underline the rising volume and severity of attacks affecting essential services and public systems (CERT-In, 2024). This literature indicates that critical infrastructure protection requires specialized monitoring, segmentation, and incident response capacity. **[13][14][11]**

The emerging legal literature centres on data protection and cyber law reform. Dharmendra Kumar (2025)) evaluates the Digital Personal Data Protection Act and presents it as an important step toward a more structured privacy regime in India. However, the literature also notes that legal effectiveness depends on enforcement capacity, institutional readiness, and citizen awareness, not merely on statutory text. **[15]**

Malhotra, C., & Malhotra, U. (2024) argue that India's cybercrime laws still face practical problems related to jurisdiction, evidence collection, attribution, and case disposal. More recent analyses of the DPDP framework similarly note that privacy reform is significant but will only succeed if regulatory mechanisms and compliance systems mature alongside it. Thus, the literature suggests that legal modernization is necessary but not sufficient. **[16]**

Overall, the literature presents cybersecurity in India as a governance challenge shaped by interdependence among state agencies, private firms, legal institutions, and end users. Across the references, a consistent conclusion emerges: India needs a more integrated model that combines public-private partnership, stronger institutional coordination, better cyber hygiene, robust critical infrastructure protection, and modern data protection law (Kshetri N., Markovic E.). Recent policy and analytical sources also reinforce the idea that cyber resilience in India will depend on sustained cooperation, enforcement, and capacity building across sectors. **[8][9]**

3. RESEARCH METHODOLOGY:

This research seeks to analyze notable case studies of cybercrime in India, and each case study will highlight specific methods used by cybercriminals. It will also examine the social and economic impacts of these incidents, while understanding the causes behind these crimes remains a key objective. The research article will evaluate how law enforcement and institutions responded and the effectiveness of legal frameworks and technological measures will be assessed. Ultimately, the study aims to provide insights for stronger prevention and resilience against cybercrime, ensuring that India's digital future remains secure and trustworthy.

Objectives:

- To document and analyze major cybercrime incidents in India.
- To identify patterns and trends in cybercrime activities.
- To assess the legal and institutional frameworks addressing cybercrime.
- To propose preventive measures and policy recommendations.

3.1. Research Design:

The study adopts a descriptive and analytical research design using a case study approach to examine the emerging trends of cyber-crimes in India, their socio-economic impact, and the effectiveness of the existing legal and regulatory framework during the period 2022 -2024. It is based entirely on Secondary Data and follows a case study approach focussed in India, as the study aims to understand the trends, impact, and regulatory response to cybercrimes in the Indian context. **[7][17][18]**

The study mainly uses data from the National Crime Records Bureau (NCRB), which provides official and reliable statistics on different categories of cybercrimes. For analysis, the collected data were organized into tables, percentages, and bar diagrams to compare cyber crime trends across the three years

i.e. 2022, 2023 & 2024. The study examines three main aspects: trend., impact, and regulatory evaluation. The research combines both qualitative and quantitative methods to ensure comprehensive analysis.

The descriptive component focuses on identifying various forms of cyber-crimes such as phishing, identity theft, ransomware, cyber stalking, financial fraud, and data breaches. The analytical component evaluates the impact of these crimes and critically examines the adequacy of Indian cyber laws and enforcement mechanisms.

3.2. Nature of Study:

This research is primarily based on:

- Doctrinal Research – for examining cyber laws, judicial decisions, and regulatory policies.
- Empirical Research – for analysing cybercrime statistics, trends, and case data available from government and institutional sources.

The methodology also incorporates a socio-legal approach to understand how cyber-crimes affect society, businesses, and governance in India.

3.3. Sources of Data:

The study relies on secondary data sources.

Secondary data is collected from:

- National Crime Records Bureau (NCRB) reports
- CERT-In reports
- Research journals, books, and dissertations
- Government portals and legislative documents
- Articles related to the Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023
- Case laws and judicial precedents
- Published academic studies on cybercrime trends in India

3.4. Data Collection Methods:

Specific cybercrime incidents in India will be examined to understand:

a) Nature of attack
b) Modus operandi
c) Financial and psychological impact
d) Law enforcement response
e) Judicial outcomes

3.5. Data Analysis Techniques:

The collected data will be analysed using:

A) Quantitative Analysis:

Statistical tools such as:

a) Percentage analysis
b) Frequency distribution
c) Trend analysis
d) Graphs and charts

Cybercrime data from NCRB and other official reports will be used to identify patterns and growth trends in cyber offences.

B) Qualitative Analysis:

a) Content analysis

b) Comparative legal analysis
c) Thematic interpretation of case studies

This analysis helps evaluate the strengths and weaknesses of India's cyber regulatory framework.

3.6. Scope of the Study:

The study is limited to cyber-crimes occurring within India and focuses mainly on:

a) Financial cyber frauds
b) Social media crimes
c) Data theft and privacy violations
d) Cyber terrorism
e) Online harassment and identity theft
f) Regulatory mechanisms under Indian cyber laws

The research primarily covers developments from the last decade, particularly after rapid digitalization and expansion of online financial services in India.

3.7. Limitations of the Study:

a) Limited availability of accurate cybercrime reporting due to underreporting.
b) Restricted access to confidential investigation records.
c) Rapid technological changes may affect long-term relevance of findings.
d) Dependence on secondary statistical data for trend analysis.

3.8. Conclusion of Methodology:

The adopted research methodology provides a systematic framework for examining emerging cybercrimes in India through legal, statistical, and socio-economic perspectives. By combining doctrinal analysis with empirical investigation, the study aims to provide practical insights into cybercrime trends, their impact on society, and the effectiveness of India's evolving cybersecurity regulations.

4. ANALYSIS & INTERPRETATION:

The present analysis is based on various cyber-attacks from the data prepared by the National Crime Record Bureau (NCRB), Indian Computer Emergency Response Team (Cert-In), Ministry of Electronics & Information Technology. The following data are obtained from the Crime in India (NCRB) & Annual report (Cert-In) of the years 2022, 2023 & 2024. **[11][19]**

Before analysing the data, following keywords related to cybercrimes need to be understood.

4.1. Cybercrime Definition:

It refers to unlawful activities carried out using computers, networks, or digital devices. It encompasses a wide range of offenses, including hacking, phishing, identity theft, ransomware, cyber terrorism, and online financial fraud. **[2]**

4.2. Cyber fraud Definition:

There is no definition of "cyber fraud" under India's Information Technology Act-2000 or IT (Amendment) Act-2008. Nonetheless D. Bainbridge claims that the term "computer fraud" refers to "theft of money or property through the use of a computer that is employing a computer to fraudulently get assets such as cash and checks, credit card services, or to fraudulently avoid obligations or debossing a counterfeit bank card to get money from an automated teller machine or dishonestly instructing a computer to transfer money into a bank account". **[20]**

Types of Cyber Fraud:

4.2.1. Phishing:

- Definition: Fraudulent attempts to obtain sensitive information (like usernames, passwords, or credit card details) by disguising as a trustworthy entity in electronic communication.
- Example: Fake emails posing as a bank asking users to "verify" their account details.

4.2.2. Identity Theft:

- Definition: Stealing personal information (such as Aadhaar number, SSN, or PAN) to impersonate someone for financial gain.
- Example: Using stolen credentials to open a loan account in another person's name.

4.2.3. Online Banking Fraud:

- Definition: Unauthorized access to online banking systems to transfer or steal money.
- Example: Fraudsters exploiting weak OTP authentication to siphon funds from accounts.

4.2.4. Credit/Debit Card Fraud:

- Definition: Misuse of card details for unauthorized purchases or withdrawals.
- Example: Skimming devices at ATMs capturing card data, later used for online shopping.

4.2.5. E-Commerce Fraud:

- Definition: Manipulating online shopping platforms to deceive buyers or sellers.
- Example: Fake online stores collecting payments but never delivering products.

4.2.6. Social Engineering Fraud:

- Definition: Manipulating individuals into divulging confidential information by exploiting trust.
- Example: Fraudsters posing as IT support staff to trick employees into sharing login credentials.

4.2.7. Ransomware & Malware Fraud:

- Definition: Malicious software encrypts or locks data, demanding payment for restoration.
- Example: WannaCry ransomware attack that locked hospital systems worldwide.

4.2.8. Investment & Ponzi Schemes:

- Definition: Fraudulent schemes promising high returns with little risk, often paying old investors with new investors' money.
- Example: Online crypto scams promising "double your money in 30 days."

4.2.9. Business Email Compromise (BEC):

- Definition: Fraudulent emails sent to employees, often impersonating executives, to authorize fund transfers.
- Example: A fake CEO email instructing finance staff to urgently wire money to a "vendor."

4.2.10. Job & Lottery Frauds:

- Definition: Fake job offers or lottery wins used to extract money or personal details.
- Example: Emails claiming "You've won $1 million" but requiring a processing fee.

4.3. Types of Cyber Crime under information Technology (Amendment) Act, 2008:

Under India's Information Technology Act, 2000 (IT Act, 2000), several categories of cybercrimes are explicitly defined. The IT Act, 2000 was India's first cyber law framework, later amended in 2008 to expand coverage (e.g., identity theft, cyber terrorism). [21] Here's a clear breakdown with definitions and examples:

4.3.1. Tampering with Computer Source Documents (Section 65):

- Definition: Altering, concealing, or destroying computer source code required to be maintained by law.

- Example: Modifying source code of banking software to hide fraudulent transactions.

4.3.2. Hacking with Computer System (Section 66):

- Definition: Unauthorized access to computer systems with intent to cause damage, delete data, or disrupt services.
- Example: Breaking into a government server to steal confidential files.

4.3.3. Dishonestly receiving stolen computer resources or communication devices (Section 66B):

- Definition: Whoever dishonestly receives or retains any stolen computer resource or communication device, knowing or having reason to believe that it is stolen, shall be punished.
- Examples: Buying a stolen laptop that contains sensitive government data, Receiving a hacked smartphone from a fraudster and using it for personal gain, Retaining illegally obtained software or digital certificates knowing they were stolen.

4.3.4. Identity Theft (Section 66C):

- Definition: Fraudulent use of another person's electronic signature, password, or unique identification feature.
- Example: Using someone's Aadhaar-linked mobile number to access financial accounts.

4.3.5. Cheating by Personation using Computer Resources (Section 66D):

- Definition: Whoever, by means of any communication device or computer resource, cheats by personating another person, shall be punished under this section. In simple terms, it covers online impersonation with the intent to deceive or defraud.
- Examples: Fraudsters creating a fake bank website to trick customers into entering login details., Sending emails pretending to be from the Income Tax Department to collect personal data, impersonating a company executive via email to authorize fraudulent fund transfers (a form of Business Email Compromise), Fake job portals where scammers pose as HR managers of reputed firms to extract money from applicants.

4.3.6 Violation of Privacy (Section 66E):

- Definition: This section deals with the punishment for violation of privacy. It states that whoever intentionally captures, publishes, or transmits the image of a private area of any person without their consent, under circumstances violating their privacy, shall be punished.
- Examples: Secretly recording someone in a changing room and uploading the video online, Circulating intimate images of a person without their permission, Using hidden cameras to capture private acts and transmitting them via messaging apps.

4.3.7. Cyber Terrorism (Section 66F):

- Definition: Acts intended to threaten the unity, integrity, security, or sovereignty of India through computer resources.
- Example: Launching a malware attack on critical infrastructure like power grids.

4.3.8. Obscenity & Pornography (Section 67, 67A, 67B):

- Definition: Publishing or transmitting obscene material, sexually explicit content, or child pornography in electronic form. 67B IT Act deals with Child Pornography
- Example: Running a website that hosts illegal pornographic videos.

4.3.9. Publishing False Digital Certificates (Section 73):

- Definition: Issuing or publishing electronic certificates without proper authority.
- Example: Fake SSL certificates used to mislead users into trusting fraudulent websites.

4.3.10. Breach of Confidentiality & Privacy (Section 72):

- Definition: Unauthorized access and disclosure of electronic records, books, registers, or information.
- Example: A company employee leaking customer data to third parties.

4.3.11. Sending Offensive Messages (Section 66A – struck down in 2015):

- Definition: Sending offensive, menacing, or false information via electronic communication.
- Example: Abusive social media posts or threatening emails.

(Note: Section 66A was declared unconstitutional by the Supreme Court in Shreya Singhal v. Union of India, 2015.)

On the above part the various types of cyber fraud & the penal provisions defined in the Information Technology (Amendment) Act, 2008 are discussed. While imposing the penal provisions on the fraudster/criminals/accused persons along with the IT (Amendment) Act, 2008, the Bharatiya Nyaya Sanhita, 2023 (Earlier Indian Penal Code, 1860) are simultaneously applied by the law enforcing agencies. Similarly, the trials in the courts are done by the court procedures & the evidences are admissible in the court by the principles prescribed in the "Bharatiya Sakshya Adhiniyam, 2023". In this project I have taken four (04) number of objectives which I have already mentioned in the Introduction part which are as follows:

- To document and analyze major cybercrime incidents in India.
- To identify patterns and trends in cybercrime activities.
- To assess the legal and institutional frameworks addressing cybercrime.
- To propose preventive measures and policy recommendations.

The following tables are made from the Crime in India data (2022, 2023 & 2024) prepared by the NCRB, Ministry of Home Affairs to measure the intensity, patterns & trends of cybercrime incidents in India. **[19]**

Table 1: Year wise Cybercrime cases registered in India:

Year	Case registered
2022	65893
2023	86420
2024	101928

Figure 1: Year wise Cybercrime cases registered in India in Bar diagram:

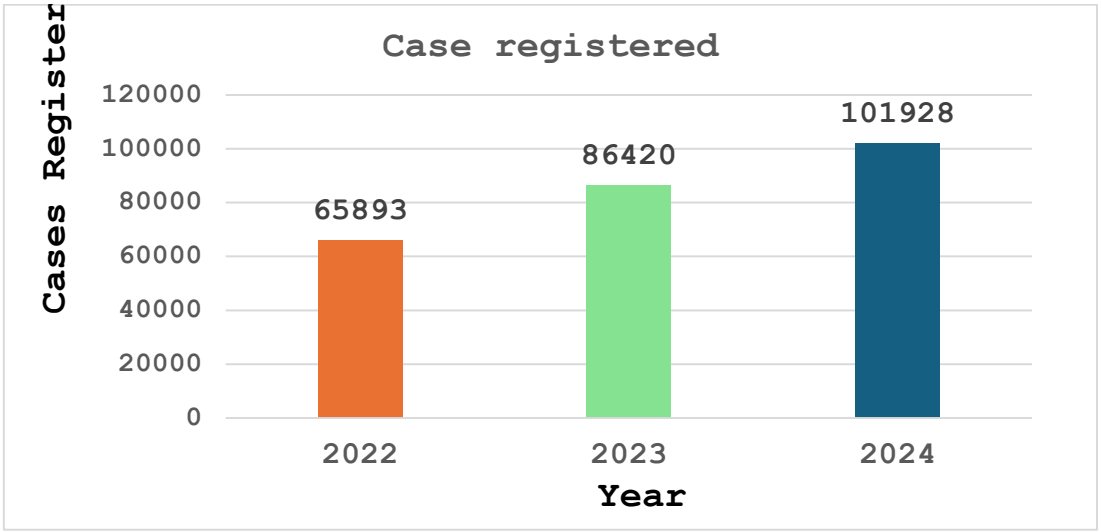


Figure 1 is an analytical interpretation of the **trend in cybercrime cases registered in India** between **2022 and 2024** based on the data in the **Table 1.** The data reveals a concerning and consistent rise in cybercrime cases over the three-year period. Cybercrime registrations increased by 31% in 2023 compared to 2022 and by a further 18% in 2024 compared to 2023. Overall, the number of cases grew from 65,893 in 2022 to 101,928 in 2024, representing an increase of more than 54% within just two years. This upward trend can be attributed to several factors, including rapid digital expansion through online banking, e-commerce, and UPI transactions, which has broadened the attack surface; increased public awareness of cybercrime reporting mechanisms such as the 1930 helpline and online complaint portals, resulting in higher reporting rates; the emergence of sophisticated threats like phishing, identity theft, ransomware, AI-driven scams, and social engineering attacks; and generally weak cyber hygiene among users, making them more vulnerable to fraud. The sharp rise between 2022 and 2023 reflects the post-pandemic surge in digital activities, while the continued increase in 2024 suggests that preventive measures and enforcement efforts have not yet kept pace with the growing misuse of technology. This trend has significant implications, including rising financial losses for individuals and businesses, declining public trust in digital platforms, and an urgent need for stronger cyber laws, enhanced cybersecurity awareness, and greater capacity building within law enforcement agencies.

Table 2: Year wise various Cybercrime offences (Under Information Technology (Amendment) Act, 2008):

Offence	**2022**	**2023**	**2024**	**Trend**
Ransomware (Sec. 66)	958	795	554	**Declining**
Identity Theft (Sec. 66C)	5,740	4,978	3,668	**Declining**
Cheating by Personation (Sec. 66D)	13,506	25,334	29,557	**Sharp Increase**
Violation of Privacy (Sec. 66E)	423	468	436	**Stable**
Cyber Terrorism (Sec. 66F)	12	11	18	**Low but Sensitive**
Sexually Explicit Acts (Sec. 67)	2,755	3,110	2,914	**Fluctuating**
Transmission of Sexually Explicit Act (Sec. 66A)	1,931	2,168	2,197	**Gradual Increase**
Child Pornography (Sec. 66B)	1,166	1,472	1,036	**Volatile**

Figure 2: Year wise various Cybercrime offences (Under Information Technology (Amendment) Act, 2008):

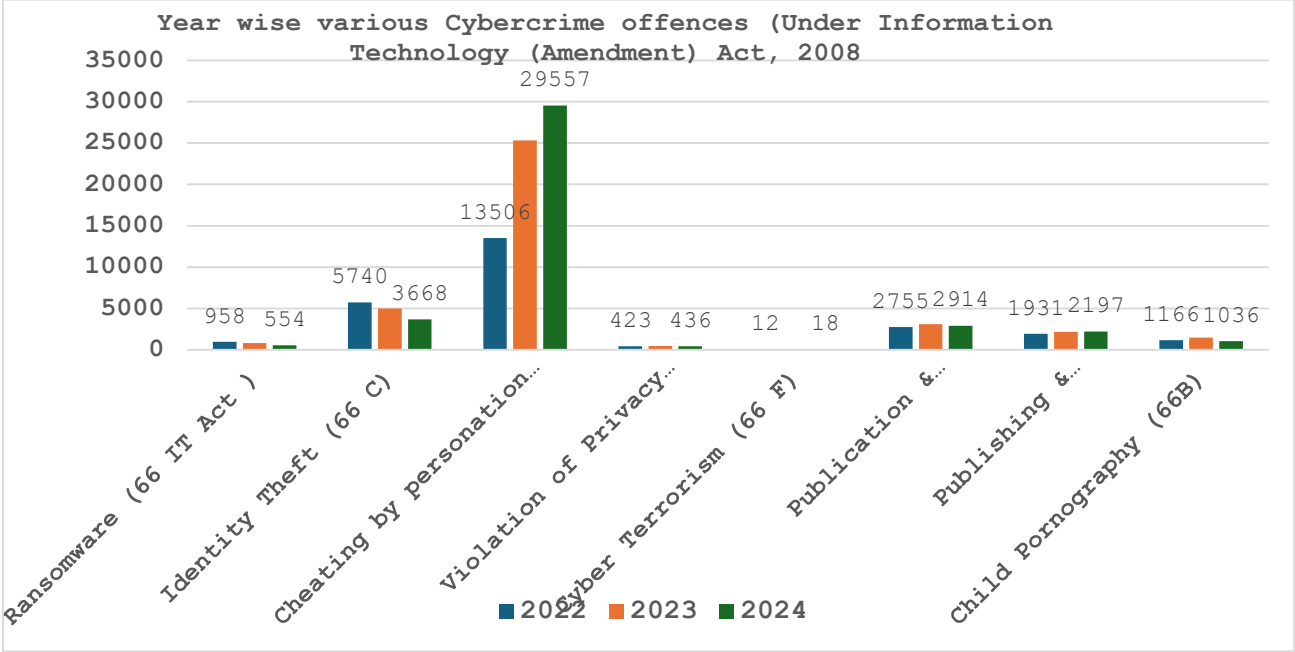


Figure 2 analyses **year-wise various Cybercrime offences (Under Information Technology (Amendment) Act, 2008)** data plotted above in the bar diagram from 2022–2024, along with practical suggestions for rectification:

The analysis indicates that **Cheating by Personation (Sec. 66D)** is the fastest-growing cybercrime category, with cases nearly doubling between 2022 and 2024 due to the rise in phishing, impersonation frauds, and fake job scams. While **identity theft and ransomware** cases show a declining trend, suggesting improved cybersecurity measures such as multi-factor authentication and enhanced threat detection, concerns of under-reporting remain. **Privacy violation (Sec. 66E)** cases continue at stable levels, reflecting persistent issues of digital voyeurism and non-consensual image sharing. Although **cyber terrorism (Sec. 66F)** cases remain low, even marginal increases are significant because of their national security implications. Cases involving **sexually explicit and illegal child-related online content** continue to remain consistently high, highlighting difficulties in controlling unlawful digital content. These trends underscore the need for stronger legal frameworks, faster cybercrime adjudication, AI-driven fraud detection, enhanced authentication systems, improved content monitoring, greater public awareness, cybersecurity education, and strengthened law enforcement capabilities. Overall, the surge in impersonation fraud represents the most urgent cyber threat, while sustained vigilance and a coordinated approach involving law, technology, awareness, and enforcement are essential to effectively address emerging cybercrime challenges.

Table 3: Year wise various cybercrime offences (IPC/BNS with IT Act):

Offence	2022	2023	2024	Trend
Cyber Stalking/Bullying of women/children (Sec 78 BNS/354 D IPC)	1,471	1,305	1,240	▼ Declining

Offence	2022	2023	2024	Trend
Fraud (Sec. 318(4)/336(2)(3)(4)/340(1)(2) BNS/420/ 465/468-471 IPC (Credit/Deceit card/ATMS/ Online Banking/OTP/Gaming-App/Website/Marketing/ Investment/ Fraud Call/ Vishing/ E-Wallet/UPI)	17,470	19,466	29,758	▲ Sharp Increase
Cheating only (318(4) BNS/420 IPC)	10,509	16,943	19,296	▲ Steady Increase
Only Forgery (338/336(3)(4), 340(2), 339 BNS/465, 468/ 471 BNS)	224	444	702	▲ Rising
Cyber Blackmailing/ Threatening (Sec 351(1,2 & 3), 308 BNS/ Section 506, 503, 384 IPC r/w BNS/SLL)	696	689	601	▼ Slight Decline
Fake news on Social-Media (Sec 353 BNS/505 IPC)	230	209	483	▲ Doubling in 2024

Figure 3: Year wise various cybercrime offences (IPC/BNS with IT Act) in visual representation:

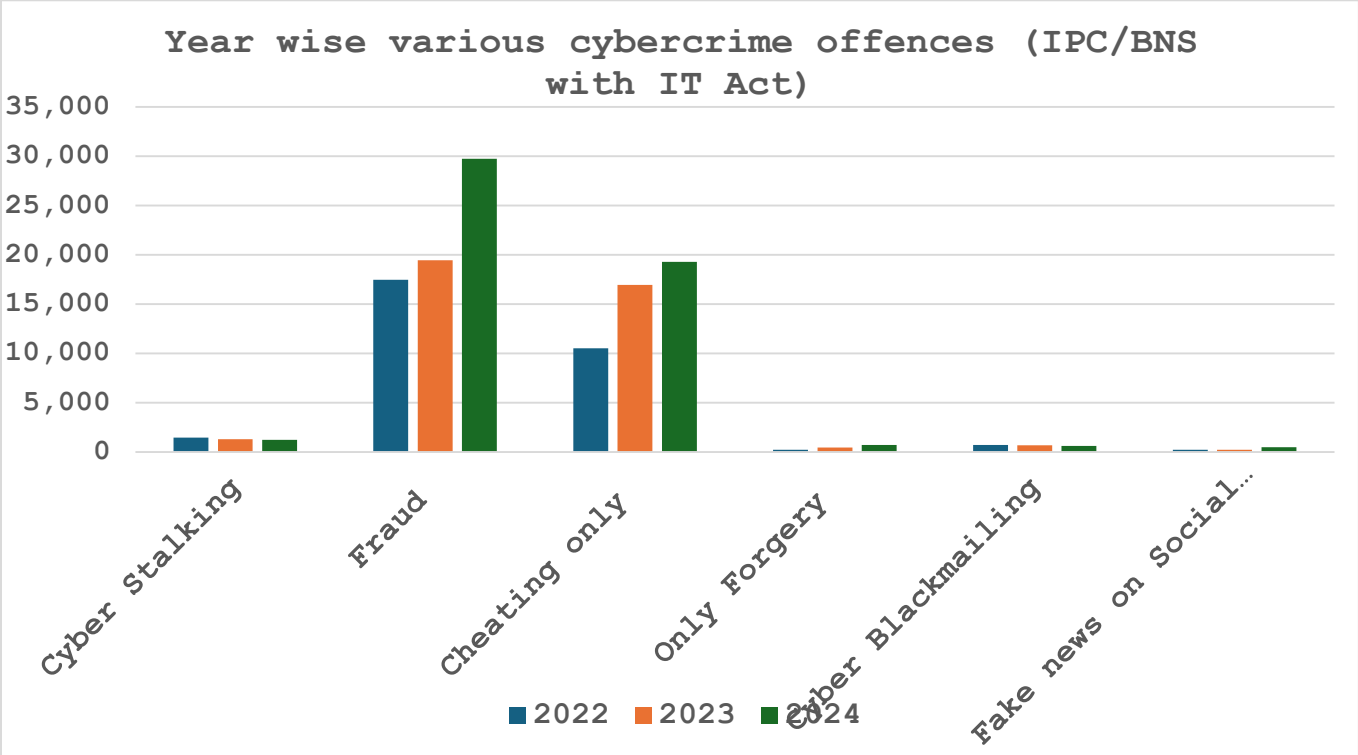


Figure 3 portrays a comprehensive **Year wise various cybercrime offences (IPC/BNS with IT Act)** (2022–2024) based on **Table 3** followed by **strategic suggestions** to address the rising trends:

Between 2022 and 2024, cybercrime trends indicate a significant shift toward financially motivated and information-related offences, with **fraud and cheating cases** increasing by **70%** and **83%** respectively, driven by the rapid growth of digital transactions and increasingly sophisticated online scams. **Forgery cases** more than **tripled**, highlighting the rising **misuse of fake documents, digital signatures, and**

identity manipulation, while **fake news incidents nearly doubled**, reflecting the growing threat of misinformation on social media and its potential social and political consequences. **Although cyber stalking, bullying, and blackmailing cases showed a slight decline**, they continue to pose serious risks, particularly to women and children. These trends underscore the need for a comprehensive response involving stronger cyber laws, dedicated cyber courts, AI-based fraud detection systems, mandatory multi-factor authentication, improved monitoring of misinformation, widespread public awareness and cyber safety education, and enhanced law enforcement capabilities through better-equipped cyber cells, forensic infrastructure, and strengthened reporting mechanisms such as the **1930** helpline. Overall, the data highlights a transition from harassment-based offences to financial fraud and misinformation-driven crimes, emphasizing the need for coordinated legal, technological, and awareness-based interventions to strengthen cyber resilience.

Table 4: Year wise Motives of Cyber Crimes (2022-2024):

Year/ Cybercrime Motives	Personal Revenge	Emotional Motives like Anger Etc	Fraud	Extortion	Prank	Sexual Exploitation	Political Motives	Terrorist Activities	Inciting Hate against Country
2022	857	792	42710	3648	173	3434	165	6	34
2023	1118	1110	59526	3326	190	4199	205	6	17
2024	1850	1336	73987	2536	247	3190	464	2	11

Figure 4: Year wise Motives of Cyber Crimes (2022-2024) in visual representation:

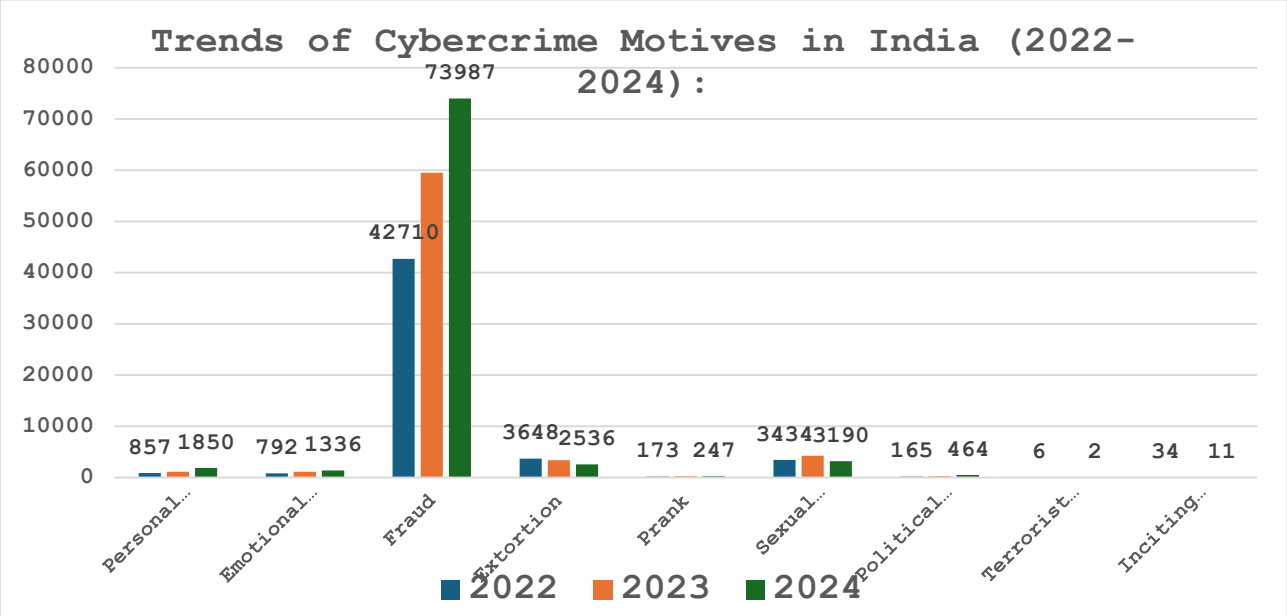


Figure 4 portrays a comprehensive analysis to **Motives of Cyber Crimes (2022-2024)** based on **Table 4** followed by **strategic suggestions** to address the rising trends:

Detailed Data:

Between 2022 and 2024, cybercrime motives in India increasingly shifted toward **profit-driven fraud and influence-based offences**, with fraud emerging as the dominant motive, rising from **42,710 to 73,987 cases**, reflecting growing **financial scams**, **phishing attacks** and **online transaction fraud**. **Personal revenge and emotional motives** also recorded **steady growth**, indicating increased misuse of digital platforms for **cyberbullying**, **harassment** and **interpersonal conflicts**, while **political motives** nearly **tripled,** highlighting the expanding **use of cyberspace for misinformation, propaganda, and influence operations**. Although **extortion, sexual exploitation, terrorism-related activities and hate-incitement** cases showed a **declining trend**, they continue to pose significant risks due to their social and national security implications. The trend underscores the need for a comprehensive strategy combining **AI-driven fraud detection, stronger authentication mechanisms, cyber ethics and digital literacy education, enhanced digital forensic capabilities, effective content moderation, robust law enforcement** and **updated policy frameworks.** Overall, the findings indicate that cybercrime is evolving from primarily personal and harassment-based offences to financially motivated and influence-driven activities, requiring coordinated technological, legal, educational, and enforcement measures to strengthen digital security and protect both individual and national interests.

Table 5: Year wise Police disposal of Cybercrime cases (2022-2024):

Year/ Police	Total case disposed of by police	Cases pending for investigation	Chargesheet rate	Pendency Percentage	Final Report
2022	63988	74751	29.60%	53.90%	44945
2023	60618	100621	33.90%	62.40%	39939

2024	77975	124988	31.90%	61.60%	53042

Figure 5: Year wise Police disposal of Cybercrime cases (2022-2024) in visual representation:

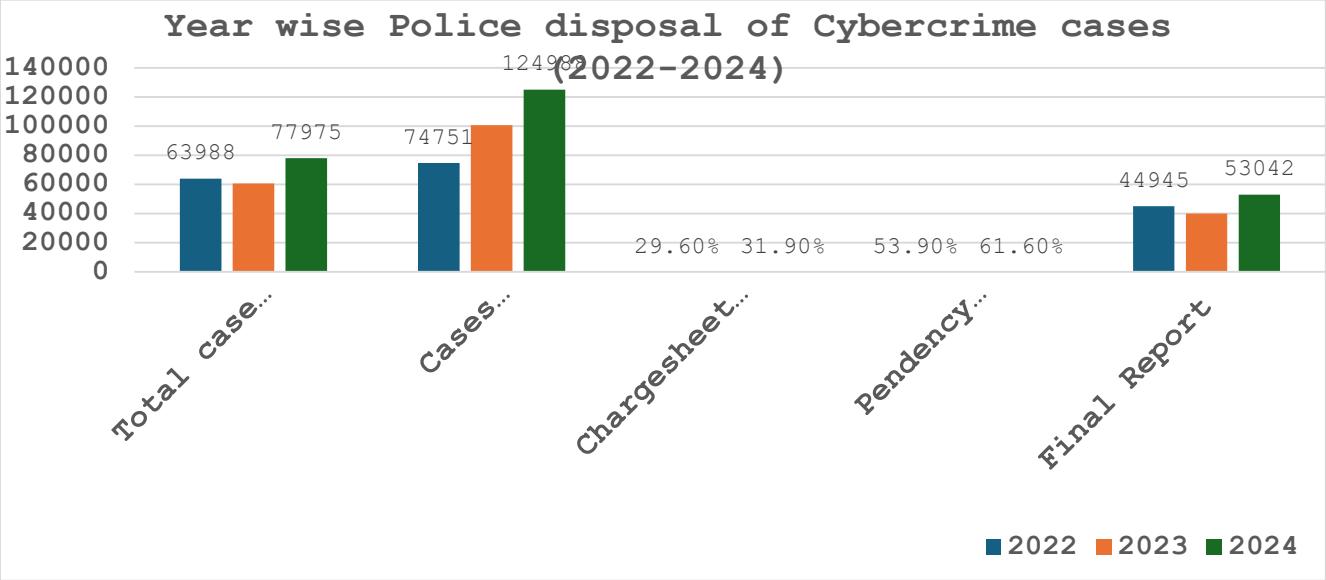


Figure 5 analyses the police data from 2022–2024 and the proportion of **Final Report cases** within total disposals based on **Table 5**:

Between 2022 and 2024, despite a modest improvement in police case disposal, **cybercrime investigations** continued to face significant challenges, with pendency rising from **53.9% to 61.6%**, indicating a growing backlog of unresolved cases. The **chargesheet rate** remained inconsistent, increasing slightly in 2023 before **declining to 31.9%** in 2024, reflecting difficulties in investigation, evidence collection, and prosecution preparedness. Moreover, nearly **two-thirds to 70%** of disposed cases were closed through final reports rather than chargesheets, suggesting that many cases remained undetected, lacked sufficient evidence, or could not be substantiated. These trends highlight the need for stronger investigative capacity through AI-assisted case management, specialized cybercrime units, improved digital forensic expertise, time-bound investigation protocols, enhanced coordination among police, forensic laboratories and the judiciary, and greater accountability in case closure processes to reduce pendency and improve conversion of cases into successful chargesheets.

Table 6: Year wise Court disposal of Cybercrime cases (2022-2024):

Year/ Court	Completed trail	Cases Disposed of by Courts	Cases Pending Trial at End of the Year	Conviction Rate
2022	2402	6685	60080	46.50%
2023	3210	5968	74638	27.60%
2024	4567	9063	90630	56.80%

Figure 6: Year wise Court disposal of Cybercrime cases (2022-2024) in visual representation:

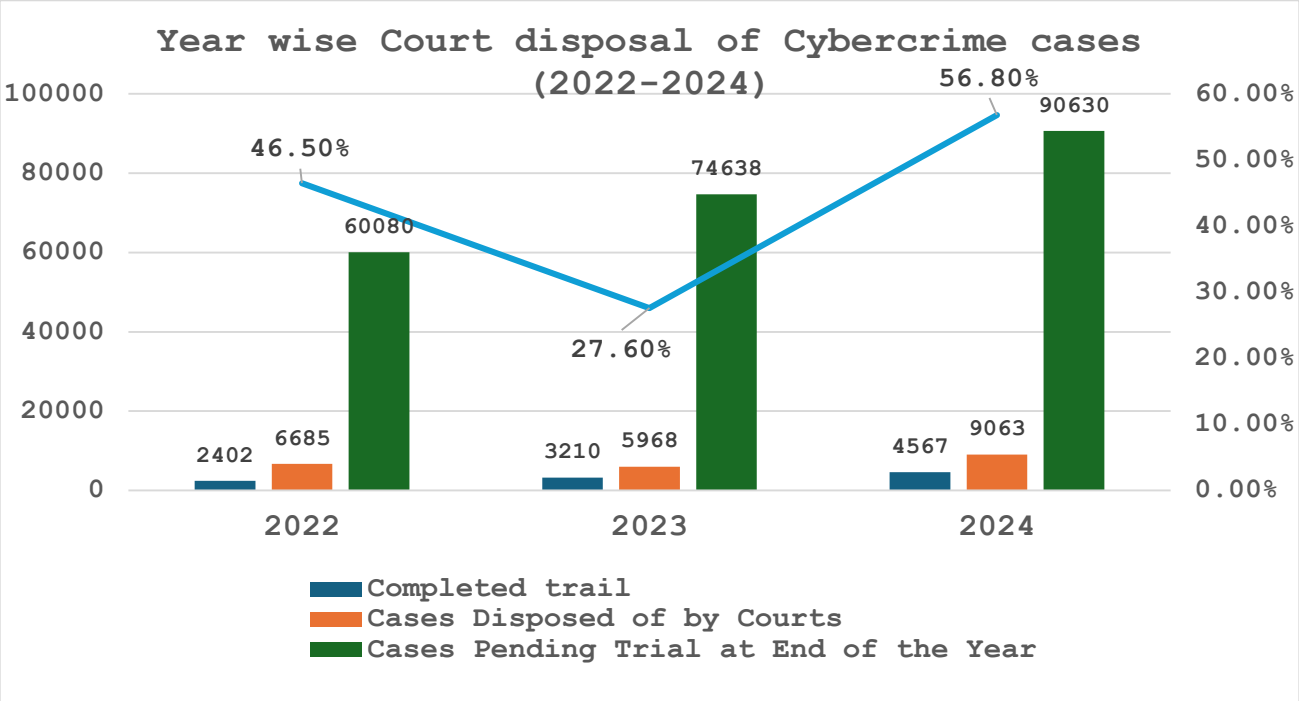


Figure 6 analyses the **Court disposal of Cybercrime cases (2022-2024)** based on **Table 6** and following inferences can be drawn from the data: **Between 2022 and 2024**, cybercrime adjudication showed mixed outcomes, with conviction rates fluctuating significantly from **27.6% in 2023** to **56.8% in 2024**, indicating inconsistencies in evidence presentation, witness support, and prosecution effectiveness. While the number of completed trials increased, reflecting improved judicial throughput, pending trials rose by **nearly 50%** from **60,080 to 90,630**, highlighting a growing backlog and pressure on the judicial system. These trends underscore the need for stronger digital forensic capabilities, timely and high-quality charge sheets, enhanced police-prosecution coordination, integrated case management systems, fast-track cybercrime courts, greater judicial capacity, witness support mechanisms, and improved legal awareness. A coordinated focus on evidence quality, efficient investigations, faster trials, and institutional capacity building is essential to improve conviction rates and ensure timely justice in an increasingly complex cybercrime landscape.

The following **two (02)** tables are made from **the Annual Report data (2022, 2023 & 2024)** of the **CERT-In, Ministry of Electronics and Information Technology (MeitY), Government of India** which is established with the objective of securing Indian cyber space. CERT-In has been operational since January, 2004. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services. CERT-In has been designated to serve as national agency for incident response under Section 70B of the Information Technology Act, 2000 (Amendment 2008). CERT-In operates 24x7 incident response Help Desk for providing timely response to reported cyber security incidents. CERT-In performs the following functions in the area of cyber security: **[11]**

- Collection, analysis and dissemination of information on cyber incidents.
- Indian Computer Emergency Response Team (CERT-In) handled incidents. The type of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements, Unauthorized Network Scanning/Probing activities, Ransomware

attacks, Data Breach and Vulnerable Services. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

- CERT-In tracks latest cyber threats and vulnerabilities. Security alerts, advisories and Vulnerability Notes are issued every year.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

CERT-In creates awareness on cyber security issues through dissemination of information on its websites (https://www.cert-in.org.in and https://www.csk.gov.in)

Table 7: Incident Handling Reports Year wise: [11]

Year/Incident Handling Reports	Security Incidents handled	Vulnerability Notes Published	Advisories Published	Security Alerts issued	Security Drills	Trainings Organized
2022	1391457	488	38	653	14	23
2023	1592917	397	52	657	22	26
2024	2041360	360	72	959	21	23

Figure 7: Visual representation of Incident Handling Reports (2022-24):

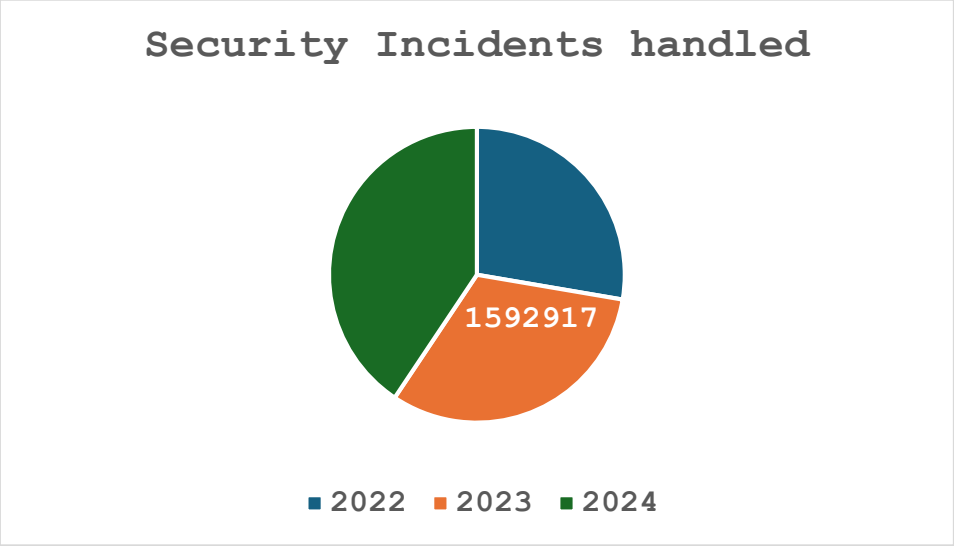


Figure 7 portrays a detailed explanation and analysis of the **Incident Handling Reports (2022–2024)** along with strategies to effectively deal with such incidents which are as follows.

Between **2022 and 2024**, the number of security incidents handled increased sharply from **1.39 million to 2.04 million**, reflecting a nearly **47%** rise in cyber threats driven by expanding digital adoption and increasingly sophisticated attacks. While vulnerability notes published declined, advisories and security alerts increased significantly, indicating enhanced threat monitoring and improved dissemination of

preventive guidance. Despite consistent security drills and training initiatives, the growing threat landscape demands stronger preparedness through greater training frequency, AI-driven threat detection, automated incident response, continuous monitoring, and effective threat intelligence sharing. A robust incident management framework encompassing preparation, detection, containment, recovery, and post-incident review, supported by digital forensics, regular vulnerability assessments, and awareness programs, is essential to strengthen cyber resilience, improve response efficiency, and mitigate the impact of evolving cyber threats.

Table 8: Abuse Statistics (The summary of various types of incidents handled by Cert-In is given below (2022-2024)):

Year/ Security Incidents	Phishing	Unauthorized Network Scanning /Probing	Vulnerable Services	Virus/ Malicious Code	Website Defacements	Website Intrusion & Malware Propagation
2022	1714	324620	875892	161757	19793	2164
2023	869	447720	941592	184131	10665	1045
2024	785	1610608	294908	119763	5496	1246

Figure 8: Visual representation of Abuse Statistics (The summary of various types of incidents handled by Cert-In is given below (2022-2024)):

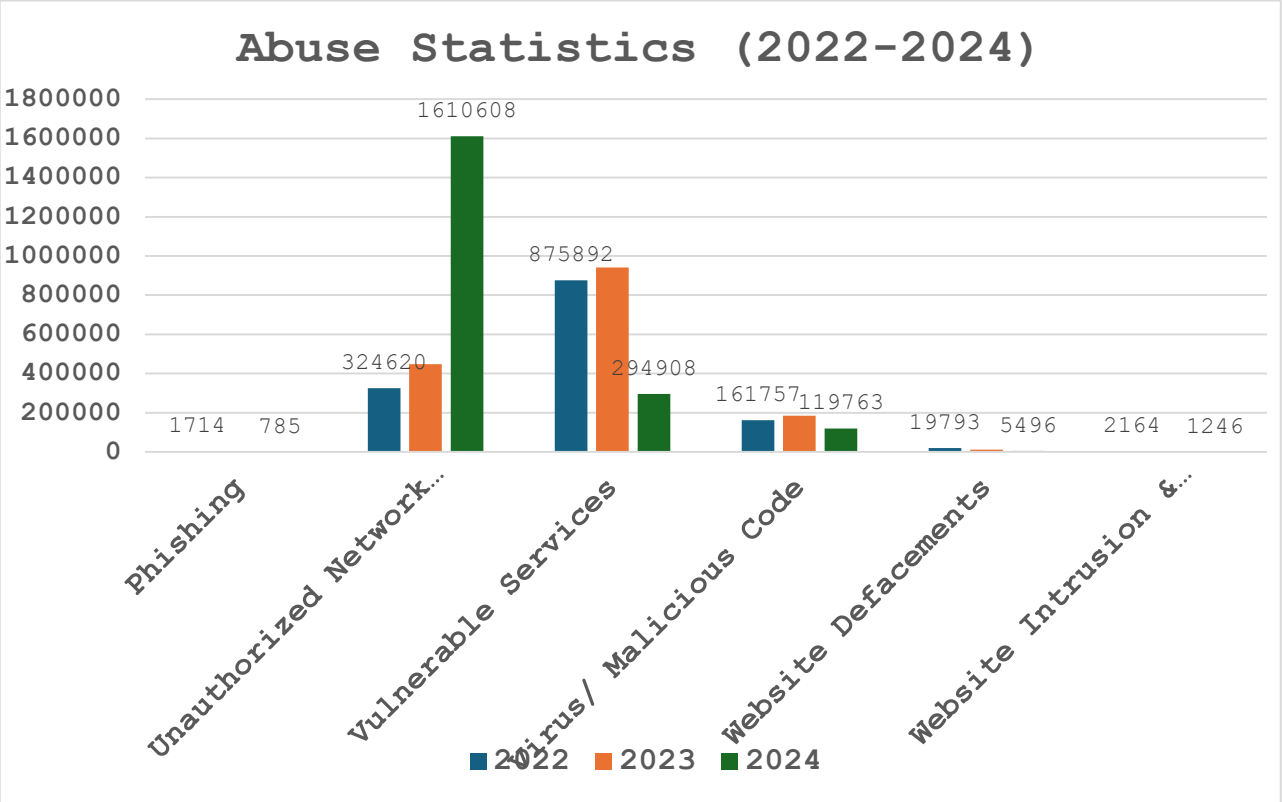


Figure 8 portrays a detailed explanation of the **security abuse statistics (2022–2024)** based on **Table 8** and following inferences are drawn.

The analysis indicates a rapidly evolving cyber threat landscape, characterized by a sharp rise in unauthorized network scanning and probing, which reached 1.61 million incidents in 2024 and signals intensified attacker reconnaissance activities. While phishing, website defacements, and intrusions have shown a declining trend, suggesting improved awareness, filtering mechanisms, and web security practices, phishing remains a key vector for credential theft and ransomware attacks. Vulnerable services continue to pose significant risks despite a decline in 2024, highlighting the need for robust patch management and secure system configurations, while fluctuating malware incidents reflect changing attack techniques and the impact of enhanced endpoint security measures. These trends underscore the importance of a comprehensive cybersecurity strategy involving AI-driven threat detection, continuous monitoring, intrusion prevention systems, zero-trust architecture, effective vulnerability management, strong website security controls, incident response readiness, regular security training, threat intelligence sharing, and mandatory security audits. Overall, organizations must adopt a proactive and collaborative approach to strengthen cyber resilience and effectively counter increasingly sophisticated cyber threats.

5. CONCLUDSION & SUGGESTION:

In the Analysis & Interpretation, total 8 tables are made from the secondary data i.e. data from NCRB & Cert-In in which various parameters of Cybercrimes are discussed in terms of numbers for the year 2022, 2023 & 2024. Following observations are structured observations from various perspective on the rising cybercrime trend.

OBSERVATIONS ON TYPES OF CYBER CRIME UNDER INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008:

The analysis indicates a rapidly evolving cyber threat landscape, characterized by a sharp rise in **unauthorized network scanning and probing**, which reached 1.61 million incidents in 2024 and signals intensified attacker reconnaissance activities. While **phishing**, **website defacements**, and **intrusions** have shown a declining trend, suggesting improved awareness, filtering mechanisms, and web security practices, phishing remains a key vector for credential theft and ransomware attacks. **Vulnerable services** continue to pose significant risks despite a decline in 2024, highlighting the need for robust patch management and secure system configurations, while fluctuating malware incidents reflect changing attack techniques and the impact of enhanced endpoint security measures. These trends underscore the importance of a comprehensive cybersecurity strategy involving AI-driven threat detection, continuous monitoring, intrusion prevention systems, zero-trust architecture, effective vulnerability management, strong website security controls, incident response readiness, regular security training, threat intelligence sharing, and mandatory security audits. Overall, organizations must adopt a proactive and collaborative approach to strengthen cyber resilience and effectively counter increasingly sophisticated cyber threats.

OBSERVATIONS ON MOTIVES OF CYBER CRIME:

Between 2022 and 2024, cybercrime motives in India shifted from personal and emotional causes to profit-driven fraud and politically motivated activities. Fraud emerged as the dominant motive with nearly 75% growth, while revenge- and emotion-based crimes also increased. Although extortion, sexual exploitation, terrorism, and hate-incitement cases declined slightly, they remain significant concerns. The rise in political misuse of digital platforms for misinformation further highlights emerging risks. These trends underscore the need for stronger legal frameworks, advanced cyber defenses, digital literacy, and enhanced law enforcement capabilities to address evolving cyber threats. **[22]**

OBSERVATIONS ON POLICE DISPOSAL OF CYBERCRIME CASES:

Between 2022 and 2024, cybercrime investigations faced growing challenges, with case pendency rising from 53.9% to 61.6% and chargesheet rates remaining inconsistent. A large proportion of disposed cases ended in Final Reports, indicating difficulties in evidence collection, case detection, and prosecution. Strengthening digital forensic capabilities, AI-assisted case management, investigator training, and inter-agency coordination is essential to reduce backlog, improve chargesheet quality, and enhance conviction outcomes.

OBSERVATION ON COURT DISPOSAL OF CYBERCRIME CASES:

Between 2022 and 2024, cybercrime courts witnessed rising pendency and fluctuating conviction rates despite an increase in completed trials, indicating that judicial capacity has not kept pace with growing caseloads. Strengthening digital evidence management, police-prosecution coordination, fast-track courts, and judicial infrastructure is essential for timely justice and sustained conviction outcomes.

OBSERVATION ON SECURITY INCIDENT HANDLING BY CERT-IN:

Between 2022 and 2024, security incidents increased by nearly 47%, highlighting a rapidly growing and more sophisticated cyber threat landscape. Although advisories and alerts improved, the pace of training and preparedness has not matched the rise in incidents. Strengthening automation, threat intelligence sharing, cybersecurity awareness, and incident response capabilities is essential to enhance resilience and effectively manage evolving cyber threats.

OBSERVATION ON SECURITY ABUSE STATISTICS BY CERT-IN:

Between 2022 and 2024, security abuse statistics highlight a shifting threat landscape where traditional attacks like phishing and website defacements show steady decline due to improved awareness and filtering, yet attackers are adapting with more targeted spear-phishing and persistent CMS vulnerabilities. The most alarming trend is the explosion of unauthorized network scanning and probing in 2024, reflecting massive automated reconnaissance efforts aimed at exploiting weak systems. Vulnerable services, though reduced after peaking in 2023, remain a significant risk due to outdated configurations, while malware activity continues to fluctuate with evolving tactics. Overall, the data underscores that while defensive measures are curbing some attack vectors, adversaries are scaling up reconnaissance and exploiting systemic weaknesses. This demands a comprehensive strategy combining stronger perimeter defences, continuous patch management, AI-driven detection, proactive incident response, and expanded awareness campaigns to build resilience against increasingly sophisticated cyber abuse patterns.

In conclusion, the overall cybercrime landscape in India between 2022 and 2024 demonstrates a rapid escalation in both scale and complexity, with financial fraud, impersonation, forgery, and misinformation emerging as dominant threats, while persistent offences such as privacy violations, sexual exploitation, and child pornography continue to expose deep social vulnerabilities. Motives have shifted decisively toward profit and political manipulation, while police and judicial data reveal systemic inefficiencies, rising pendency, inconsistent conviction rates, and heavy reliance on Final Reports. Simultaneously, CERT-In statistics highlight surging security incidents, massive reconnaissance activity, and evolving abuse patterns despite some progress in phishing and web security. Together, these trends underscore that technological misuse is outpacing enforcement and legal adaptation, demanding a synchronized, multi-layered response—modernized laws, AI-driven detection, stronger investigative and judicial capacity, proactive incident handling, and widespread awareness campaigns—to build resilience, restore trust in digital platforms, and safeguard both individual rights and national security.

Following are some suggestions to handle Cybercrime offences successfully.

PUBLIC AWARENESS AND CYBER LITERACY:

From the patterns of the cybercrimes that has occurred point to a major common problem i.e., lack of users' knowledge about online safety. Users simply believe whatever is being told to them without verifying its authenticity. For this a nationwide cyber awareness program needs to be conducted in all the educational institutions and workplaces. **[23]** Cyber security can be included in the school curriculum and can also be introduced as a paper in the college and university level. Through this safe internet practices can be taught such as strong password creation, two-factor authentication and identifying phishing emails or smishing messages on phones. Awareness can be spread through various media and social media platforms in regional languages by Ministry of Information and Broadcasting. **iGot karmayogi** provides many video lessons related to cyber security which can also be made available to the general public by designing them as public-facing courses.

STRENGTHENING CYBER SECURITY INFRASTRUCTURE:

From private individuals to government organizations the digital system should be made secured by using updated antivirus software and firewalls. Sensitive personal and financial data has to be always encrypted. Perform security scans such as running Microsoft Malicious Software Removal Tool for Windows; using Google play protect for android devices; trusted software like Malwarebytes or ESET Online Scanner also can be used. Unauthorized access can be checked through verifying logged in devices in users account; running **netplwiz** (Network Places Wizard) son Windows; dialling codes ***#62#** to check if the calls or messages are getting forwarded to another number. Private as well as Government organizations can conduct periodic security audits and vulnerability assessments.

CAPACITY BUILDING AND SKILLED WORKFORCE:

In the face of cyber threat police officers, judges, and investigators can be trained in handling cases of cybercrimes in grassroot level. Specialized cybercrime training labs for hands-on experience with forensic tools can be established. Collaboration between industries and universities to focus on practical cyber security courses based on current threat patterns like preventing financial frauds or securing govt. data is also a way out. Similarly, public-private partnerships is imperative for skill development.

STRONG REPORTING AND INCIDENT RESPONSE SYSTEMS:

Although **1930** serves as India's national cybercrime helpline, underreporting remains a challenge due to lack of awareness, fear, connectivity issues, busy lines, and difficulties in providing technical details. To improve cybercrime response, dedicated cyber crisis teams should be established across all states, and the National Cyber Crime Reporting Portal should be redesigned for greater accessibility and victim support. The **Indian Cyber Crime Coordination Centre (I4C)** should be empowered with greater operational autonomy, supported by regional hubs, standardized state-level protocols, and stronger international cooperation to address cross-border cybercrime. Enhanced collaboration with private technology firms and academic institutions can further strengthen India's cybercrime prevention, investigation, and response capabilities.

PROTECTION OF CRITICAL INFRASTRUCTURE:

Cyber-attacks on huge data base like in banking sector, healthcare sector, power grids, transportation sector creates national security risks. Hence there is a need for these critical sectors to develop advanced monitoring systems to prevent data theft. **[24]** Adding multifactor authentication for access is a strong step combined with network segmentation and continuous monitoring and finally having robust back-up and recovery plans. Regularly conducting cyber drills and simulations is crucial for testing an individual as

well as an organization's preparedness for potential cyber-attacks. **[25]** Zero Trust Security Architecture has the potential to be implemented. It is a modern cybersecurity framework built on the principle of "Never Trust, Always Verify". It eliminates implicit trust, continuously authenticates every user, device, and application, and assumes that breaches are inevitable, thereby minimizing risks and limiting damage.

REGULATION OF EMERGING TECHNOLOGIES:

Day by day technologies such as Artificial intelligence, deepfakes and cryptocurrency are increasingly misused. Standardized guidelines are to be developed for ethical AI usage. In social media platforms where most of the deepfake and AI generated contents are circulated; systems should be created to filter them out or flag such content. Transactions of cryptocurrency linked to illegal activities needs monitoring. Building healthier communities and stronger connections require responsible use of social media platforms.

6. REFERENCES:

1. Daxeshkumar J., "Emerging issues of cybercrimes in India: Statistics, Modus Operandi of online frauds & Remedies to curb Cyber Crimes", IJSRA, 2025, 17(01), 408-418, DOI:10.30574/ijsra
2. Yagati A.K., Sridevi M., Naidu S.T. (2023), "Emerging trends in cybercrime: challenges and countermeasures in India", South India Journal of Social Sciences ; 21(17); 149-155
3. Afzal A. & Singh A. (2026), Cyber Crimes in India: Challenges & legal Reform. IJSSR, 3(1), 243-253
4. Chakraborty A., Tiwari S. (2025), "An analytical study on challenges and gaps in India's cyber security framework", IJCCSL 2025; 5(1);04-07, DOI: https://doi.org/10.22271/27899497.2025.v5.i1a.110
5. Kushwaha K. (2025), "Cyber laws in India: Issues & Challenges", Indian Journal of Legal Review, 5(7), 361-371
6. Naveen kumar C.G., Dr. Sanjay Pande M. (2017), "A study on Ransomware & it's effect on India & rest of the world", International Journal of Engineering Research & Technology, 5(22), DOI: 10.17577/IJERTCONV5IS22042
7. Samal A. & Samal S. (2025), "Cyber threats and national security in India: Evaluating policy measures and emerging challenges". IJPSG, 7(1); 232-240, DOI: https://www.doi.org/10.33545/26646021.2025.v7. i1c.523
8. Khetri N. (2015), "India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership". IEEE Security … Privacy, Volume 13, Issue 3, pp. 16-23, 8 pp., DOI: 10.1109/MSP.2015.61
9. Markovic E, (2026). "Recalibrating Cybercrime Investigation and Digital Evidence Governance: A Comparative Legal-Operational Framework with Insights from India and Selected Arab Jurisdictions". International Journal of Law and Criminology 6(3), 1-13
10. Khanna A., (2025), "Implementing effective cyber hygiene practices", IJARET, 16(1), 01-09, DOI:https://doi.org/10.34218/IJARET_16_01_001
11. CERT-In. Annual Report 2022, 2023, 2024. Ministry of Electronics and Information Technology.
12. Bholane K.P., Jadhav T.P., Rathod Dr. V.M. (2024), "Bridging The Digital Divide: Understanding Consumer Awareness Towards Cyber Security in Rural and Urban Communities", SSRN Electronic Journal 20(1(19)):96-100, DOI: 10.2139/ssrn.5100525
13. Haridas R., Sharma S., Bhakar R. and Chenghong Gu (2025), "Cybersecurity Threats to Critical Energy Infrastructure in India: Challenges, Opportunities and Insights for Developing Nations." Commonwealth Cyber Journal,\ 53 Print ISSN 2959-3018, online ISSN 2959-3026

14. Meccyjoy, Zion, Mark M., Mohammed S., Ahmed M. (2019), "Ransomware Attacks on Critical Infrastructure: Effects and Prevention Strategies", Journal of research, innovation & Technologies; 4(6);20
15. Kumar Dharmendra. (2025), "Constitutional privacy meets legislative protection: evaluating the digital personal data protection act through the lens of fundamental rights", IRJMETS, 7(8), 998-1005
16. Malhotra, C., & Malhotra, U. (2024). Putting interests of digital nagriks first: Digital Personal Data Protection (DPDP) Act 2023 of India, Sage Journal, 70(3), https://doi.org/10.1177/00195561241271575
17. Patel D., Pandey A., Singh S., Tiwari P. (2025), "A comparative study of Cybercrime cases on Social media in India : Technical & Legal Aspects", IJESRR, 12(4);33-45
18. Shelar A., Zanzane A., Salunkhe Y., Kamble K. (2025), "Cybercrime Trends in India: A data-driven analysis using power BI", IRJMETS, 7(10), 906-913
19. Crime in India 2022, 2023, 2024 (Statistics Volume II), National Crime Record Bureau, Ministry of Home Affairs
20. Vashisth S., Pankisha, Mehta P. (2025), "A study on Emerging Trends of Cyber Frauds & Digitalization in India Including Financial Cybercrime Legal Implications", Journal of Information Systems Engineering & Management, 10(47s), 690-696
21. INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008 (No. 10 of 2009) by Ministry of Law & Justice (Legislative Department), Govt. of India (An Act further to amend the Information Technology Act, 2000)
22. Chawki M. (2026), "Legal foundations and future directions of AI-enabled cybersecurity: a cross-jurisdictional analysis", 12(1), https:// doi.org/10.1080/23311886.2026.2614015
23. Mokha A.K. (2017), "A study on Awareness of Cybercrime & Security", Research Journal of Humanities & Social Sciences, 8(4), 459-464, DOI: 10.5958/2321-5828.2017.00067.5
24. Admass W., Munaye Y.Y., Diro A.A., (2024), "Cyber security: State of the art, challenges and future directions", KeAi Chinese Roots Global Impact (ScienceDirect) Vol 2, https://doi.org/10.1016/j.csa.2023.100031
25. Prummer J., Steen T.V., Berg B., (2024), "A Systematic review of current cybersecurity training methods", Computers & Security (ScienceDirect), Volume 136, https://doi.org/10.1016/j.cose.2023.103585