Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44)** : 1–21.
ISSN-0037-8712
doi:10.5269/bspm.78912

An Analysis of Cybercrime Trends in India with a Focus on Tripura (Pre and During COVID-19)

Nirdesh Deb, Sharad Shekhawat, Sanjib Debnath and Rakhal Das*

ABSTRACT: The COVID-19 pandemic has drastically reshaped the digital ecosystem, resulting in a notable surge in cybercrime across the globe. This study focuses on the state of Tripura in northeastern India to analyze the impact of the pandemic on cybercrime incidents in the region. The research investigates the underlying factors contributing to the escalation of cybercrime during the pandemic, examines the operational patterns of cybercriminal activities, and compares trends in cybercrime before and during the COVID-19 period.Adopting a mixed-method approach that incorporates data from law enforcement records, interviews, and inputs from key stakeholders, the study identifies key drivers such as increased internet penetration, low levels of cyber awareness, and inadequate cybersecurity infrastructure. The findings highlight a marked rise in cybercrime cases during the pandemic in Tripura, with phishing, online fraud, and identity theft emerging as the most prevalent threats.The study concludes with a set of actionable recommendations to mitigate future risks, including the implementation of robust cyber awareness programs, the strengthening of cybersecurity practices among individuals and organizations, and the promotion of coordinated efforts among law enforcement agencies, the judiciary, intermediaries, government bodies, and financial institutions to foster a more secure digital environment in Tripura. This study also includes the statistical analysis between different data sets and the analysis by regression line for the cybercrime trends study.

Key Words: Cybercrime, financial fraud, social media crime, hacking, data breach, cyber security, cyber awareness.

Contents

1. Introduction and Preliminaries

Cybercrime has emerged as one of the most challenging and devastating threats in the digital age. As the world becomes increasingly dependent on digital technology, cybercrime has proliferated at an alarming rate. Every day, hundreds of cybercrime-related complaints are registered at police stations and

[*] Corresponding author.
2020 *Mathematics Subject Classification:* 55N31, 68T10, 62R07.

Submitted September 11, 2025. Published January 20, 2026

cyber cells across different states and countries worldwide. Cybercrime broadly refers to any criminal activity that involves the use of computers, networks, or digital devices either as tools, targets, or both. The term encompasses a wide range of illicit activities, including crimes committed against computer systems and networks, as well as traditional crimes facilitated or amplified through the use of the internet and digital technologies [6].

In the context of Tripura, a northeastern state of India, several forms of cybercrime are frequently reported. These include cyber financial frauds—such as cheating, identity theft, phishing attacks, sextortion, and investment scams—as well as the publication of obscene or defamatory content on online platforms, hacking of digital accounts and devices, and the misuse of compromised accounts.

Tripura is located in one of the remotest parts of India's North-Eastern Region and has historically faced challenges in terms of communication and connectivity. However, in recent years, the state has achieved significant progress in infrastructure, including improved access to railways, highways, airways, and digital connectivity via an internet gateway. Despite its geographical remoteness, Tripura boasts one of the highest literacy rates in India at 94.65% [16].

As of 2019, the financial and digital infrastructure in Tripura has also shown promising trends. The state has achieved 115% bank account penetration, surpassing the North-East average of 101%, although still trailing behind the national average of 126%. Smartphone and internet penetration stand at 57%, higher than both the North-East average (47%) and national average (48%). Furthermore, 81.9% of bank accounts are linked with mobile numbers, Aadhaar penetration is 89%, and 94% of bank accounts are linked with Aadhaar, which is well above the national average of 85% and North-East average of 64% [15].

Despite this progress in education and digital access, the level of digital literacy in Tripura remains significantly below the national average. Recognizing this gap, both central and state governments have initiated various efforts to improve digital literacy in the region. For instance, Tripura now hosts India's third international internet gateway—after Mumbai and Chennai—located in Agartala [3]. Additionally, premier institutions such as the Indian Institute of Information Technology (IIIT), National Institute of Technology (NIT), and National Institute of Electronics and Information Technology (NIELIT) have been established in the state to serve as Centers of Excellence in digital education and cybersecurity.

The COVID-19 pandemic dramatically altered the socio-economic landscape across the globe. The first case of COVID-19 in India was reported on January 30, 2020, in Kerala, where three medical students returning from Wuhan, China, tested positive for the virus [2]. In Tripura, the first confirmed case was reported on April 6, 2020, involving a 45-year-old woman who had traveled from Guwahati on March 18, 2020 [9]. The Government of India announced a nationwide lockdown on March 25, 2020, initially planned for 21 days but later extended in phases [21]. Tripura enforced a complete lockdown starting July 5, 2020 [20]. During the lockdown, most organizations, except for essential services such as police, hospitals, electricity, and fire services, were either fully or partially shut down. Markets operated with time restrictions, and public movement was severely limited.

As a consequence of lockdowns and social distancing measures, individuals, businesses, and government institutions increasingly shifted to online platforms for communication, education, commerce, and essential services. This surge in digital dependency exposed users to various cyber threats, particularly among those newly introduced to the internet. Opportunistic cybercriminals exploited the increased digital activity and users' lack of awareness, resulting in a dramatic increase in cybercrime incidents. According to reports, cybercrime surged by nearly 86% during the early stages of the pandemic [18].

This study aims to examine the nature and dynamics of cybercrime in Tripura, focusing specifically on the periods before and during the COVID-19 pandemic. By analyzing cybercrime trends between 2017 and 2022, this research seeks to identify the key factors responsible for the rise in cybercrime and suggest viable strategies for mitigating these threats in the future. For this study, the pre-COVID period is defined as 2017–2019, while the COVID-19 period encompasses the years 2020–2022.

2. Literature Review

Cybercrime can broadly be defined as a wrongful act or criminal activity where a computer, network, or related device is used either as a tool or a target to perpetrate the crime. The definition itself has evolved over time, reflecting the increasing complexity and technological advancement of cyber-based offenses.

Phillips et al. [17] provide a comprehensive overview of the conceptual framework surrounding cybercrime. Their study delves into the various terminologies, protocols, and taxonomies used for categorizing cybercrime. Notably, they propose a new integrative classification system that bridges the concepts of cybercrime and cyberdeviance. The authors also emphasize the importance of adopting a multidimensional framework for effectively defining and classifying cybercrime in today's digital age.

In a separate but closely related study, Feldmann et al. [7] analyze how Internet traffic patterns changed during the COVID-19 pandemic. Using data from a central European Internet Service Provider (ISP), multiple Internet Exchange Points (IXPs), and an academic network, they report a 15–20% spike in traffic within the first week of lockdowns. This increase was driven by the heightened usage of remote work applications, digital entertainment platforms, and online learning tools. Interestingly, traffic from non-hypergiant sources, such as Virtual Private Networks (VPNs), video conferencing platforms, and online gaming, exhibited higher growth than that from hypergiants like Netflix or YouTube. The study also highlights a shift in daily usage patterns, where weekdays began to resemble weekends in terms of internet consumption behavior.

The increase in internet usage during the pandemic also corresponded with a surge in cyberattacks. Lallie et al. [11] examined the global rise in cybercrime during the COVID-19 crisis, noting that cyberattacks significantly increased following a brief delay after the virus outbreak in China. Their analysis, which uses the UK as a case study, demonstrates how cybercriminals strategically exploited major public events and official announcements to launch targeted cyberattacks.

Saleous et al. [19] conducted a thorough review of the cybersecurity landscape throughout the pandemic. Their research identifies critical threats such as phishing schemes, ransomware attacks, misinformation campaigns, and vulnerabilities in remote work infrastructure. The authors highlight that sectors such as finance, education, healthcare, military, and e-commerce became prime targets due to their digital dependency and societal importance. Furthermore, the study outlines challenges in threat detection, legal responses, and mitigation strategies, advocating for robust and innovative cybersecurity frameworks to combat the evolving nature of cyber threats in crisis situations.

Kashif et al. [10] focus specifically on the increased dependency on digital platforms during the COVID-19 pandemic and the resulting vulnerabilities. Their study finds a sharp increase in cybercrimes targeting sectors like education, banking, and social media. They stress the growing concerns over the security of widely-used platforms, underlining the urgent need for enhanced digital security protocols.

Nguyen et al. [14] present an analysis of digital communication transformation during the lockdown period. Surveying over 1,300 American adults, the study reveals increased engagement with text messaging, social media platforms, video conferencing, and online games, primarily for maintaining social connections. The study also brings attention to widening digital inequalities, showing that older individuals, those with limited internet proficiency, or those lacking stable internet access were disproportionately affected, thus exacerbating the existing digital divide.

A study by Buil-Gil et al. [5] conducted a time series analysis in Northern Ireland to examine the impact of multiple COVID-19 lockdowns on crime patterns. Their findings reveal that offline crimes initially declined due to restricted mobility, but eventually returned to pre-pandemic levels. Simultaneously, the increase in online activities, such as remote work and digital commerce, created more opportunities for cybercriminals to exploit vulnerabilities.

MunaAhmead et al. [1] performed a cross-sectional analysis focusing on students aged 18 to 22. Their research highlights risky online behaviors, such as excessive social media use and lack of awareness about cyber threats. The study identifies a concerning gap in knowledge and preparedness among young internet users, stressing the importance of comprehensive digital safety education and cybercrime awareness initiatives in academic institutions.

Similarly, Karagiannopoulos et al. [8] explore cybercrime awareness among older adults. Through qualitative interviews with individuals over the age of 60, the study uncovers significant knowledge gaps regarding online safety. The findings suggest the urgent need for demographic-specific awareness campaigns and educational initiatives to equip older populations with the necessary skills to navigate the digital world safely.

Collectively, these studies paint a nuanced picture of the multifaceted nature of cybercrime, particularly in the context of the COVID-19 pandemic. They underscore the importance of tailored, adaptive cybersecurity strategies that consider demographic, sectoral, and technological factors to address the increasing threats in the digital domain.

According to Meena *et al.* (2024) [12], cybercrime can be broadly classified into four major categories:

1. **Crimes against individuals** — including spoofing, hacking, cyber defamation, and cyberstalking.
2. **Crimes against the government** — encompassing cyber warfare and cyber terrorism.
3. **Crimes against society** — such as online gambling and cyber trafficking.
4. **Crimes against property** — including identity theft, pharming, and phishing.

Spoofing refers to the unlawful act of assuming a false identity to obtain something valuable or advantageous. **Hacking** involves exploiting vulnerabilities in a system to gain unauthorized access. **Cyber defamation** is the act of disseminating false information about an individual in electronic form using a computer or digital device. **Cyberstalking** is the persistent monitoring, harassment, or following of someone via electronic means, despite clear indications of disinterest by the victim.

Cyber warfare refers to the use of digital tactics in conflicts between two or more governments to compromise each other's systems. **Cyber terrorism** involves illegal online activities that threaten lives or cause intimidation, often as a political tool.

Online gambling refers to wagering on sports, games, or lotteries via websites or applications, typically requiring a monetary deposit. **Cyber trafficking** involves the exploitation of individuals, especially children, through internet platforms.

Identity theft entails the unlawful acquisition of personal information such as names, photographs, certificates, or sensitive banking details, which are then used to create forged documents or commit crimes. **Pharming** involves inserting malicious code into a target computer to redirect it to deceptive websites, allowing hackers to steal sensitive data. **Phishing** is the practice of creating fake but convincing identities or websites to deceive individuals into revealing confidential information, such as banking or insurance details.

The **Information Technology Act (IT Act)**, enacted in India in 2000 and amended in 2008, provides the primary legal framework for addressing cybercrime in the country. It facilitates electronic commerce, validates digital signatures, and covers offences such as hacking, data theft, impersonation, privacy violations, and the publication of obscene or sexually explicit content.

According to the *World Cybercrime Index* (WCI) 2024, published on April 11, 2024, India ranks among the top ten countries most affected by cybercrime globally [4].

This study is organized into the following sections: Section 3 presents the Statistical Analysis of Crime across India, the North Eastern (NE) Region, and the State of Tripura during the Pre-COVID and COVID-19 periods (2017–2022). Section 4 provides the Analysis and Discussion of Cybercrime Trends. Section 5 outlines Future Recommendations for Cybercrime Precautions in Tripura, followed by Section 6, which presents the Conclusion and future research directions.

3. Statistical Analysis of Crime across India, the North East(NE) Region and the state of Tripura during Pre-COVID and COVID 19(2017–2022)

3.1. Crime statistics in India(2017–2022)

Total FIR(Overall) registered in India during Pre-COVID and COVID 19(2017–2022) According to the *Crime in India* statistics published by the National Crime Records Bureau (NCRB) [13], the total number of First Information Reports (FIRs) registered across all police stations in India during the pre-COVID-19 period (2017–2019) was **15,237,851** (one crore fifty-two lakhs thirty-seven thousand eight hundred fifty-one) as shown in Table 1 . In comparison, during the COVID-19 period (2020–2022), the number of registered FIRs rose to **18,522,541** (one crore eighty-five lakhs twenty-two thousand five hundred forty-one). This indicates an overall increase of **21.56%** in the number of FIRs during the COVID-19 period compared to the pre-COVID-19 period in India.

Table 1: Total FIR(Overall) registered in India during Pre-COVID and COVID 19 period
Source: National Crime Record Bureau [13]

Year	Number of FIR (Overall)	Year wise change	Total	Relation with COVID
2017	50,07,044	-	1,52,37,851	Pre-COVID
2018	50,74,635	1.3%		
2019	51,56,172	2%		
2020	66,01,285	28%	1,85,22,541	COVID-19
2021	60,96,310	-8%		
2022	58,24,946	-4%		

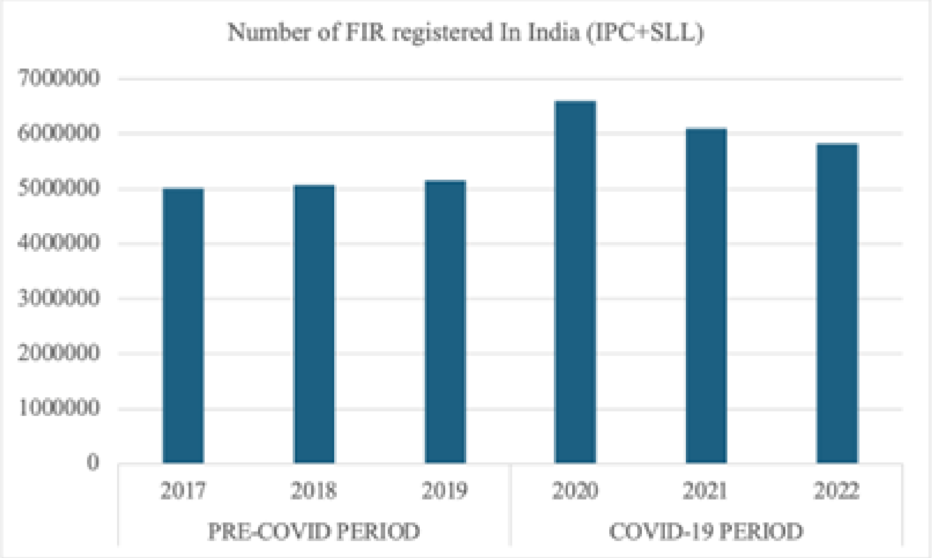

Figure 1: Total FIR registered in India during Pre-COVID and COVID-19 period.

Figure 1 presents the year-wise number of First Information Reports (FIRs) registered in India under the Indian Penal Code (IPC) and Special and Local Laws (SLL) during the period 2017–2022. The data are classified into two distinct phases: the **pre-COVID period** (2017–2019) and the **COVID-19 period** (2020–2022). The graph indicates a relatively stable trend in FIR registration during the pre-COVID years, followed by a substantial spike of approximately 28% in 2020, coinciding with the onset of the COVID-19 pandemic. Although the numbers slightly declined in 2021 and 2022, they remained higher than pre-COVID levels. This trend suggests that the pandemic period was associated with an overall increase in reported offences, possibly due to heightened cybercrime, domestic conflicts, and pandemic-related socio-economic stressors.

Total Cyber Crime cases registered in India during pre-COVID and COVID-19 period Table 2 depicted a total of 93,590 cybercrime cases were registered across India during the pre-COVID-19 period (2017–2019). Whereas, the number of cybercrime cases reported during the COVID-19 period (2020–2022) rose sharply to 168,902, reflecting an overall increase of 80.38 %. This trend shows that the COVID-19 pandemic and more use of digital platforms led to a sharp rise in cybercrime in India, as shown in Figure 2.

Table 2: Total Cyber Crime cases registered in India during pre-COVID and COVID-19 period
Source: National Crime Record Bureau [13]

Year	Number of FIR (Cyber)	Year wise change	Total	Relation with COVID
2017	21796	-	93590	Pre-COVID
2018	27248	25%		
2019	44546	63%		
2020	50035	12%	168902	COVID-19
2021	52974	6%		
2022	65893	24%		

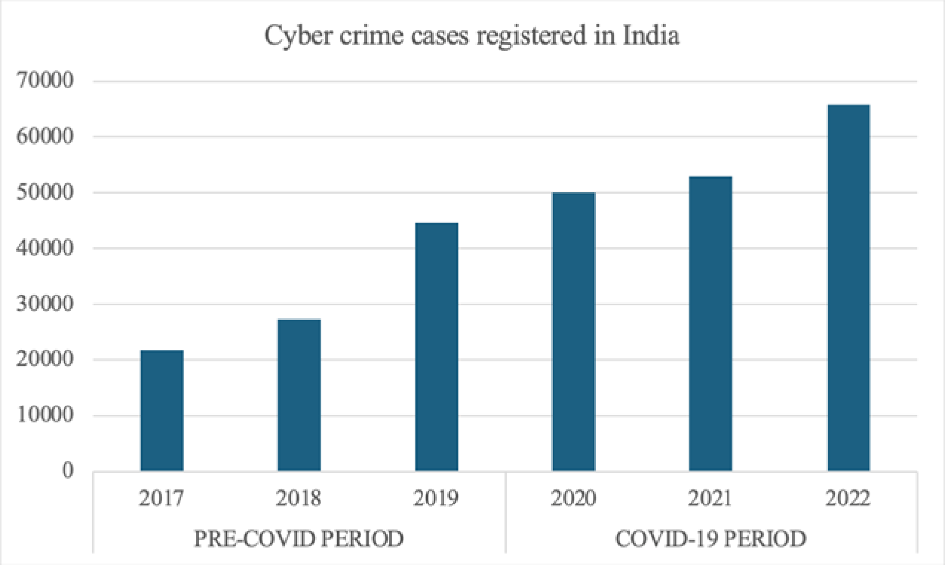

Figure 2: Total Cyber Crime cases registered in India during pre-COVID and COVID-19 period

Types of cyber-crime cases registered in India during Pre-COVID and COVID 19(2017-2022) The types of cybercrimes registered in India during the pre-COVID-19 and COVID-19 periods primarily fell into three categories: (1) Cyber Fraud, (2) Sexual Exploitation, and (3) Causing Disrepute,(4) personal revenge, (5) anger, (6) extortion, (7) prank, (8) political motives, (9) terrorist activities, (10) inciting hatred against country, (11) disrupt public service, (12) sale/purchase illegal drugs, (13) developing own business, (14) spreading piracy, (15) psycho or pervert, (16) steal information, (17) abetment to suicide and (18) others as shown in Table 3.

During the pre-COVID-19 period (2017–2019), the total number of cyber fraud cases was 54,155 (12,213 in 2017; 15,051 in 2018; and 26,891 in 2019). In the COVID-19 period (2020–2022), the reported number of cyber fraud cases rose to 105,082 (30,142 in 2020; 32,230 in 2021; and 42,710 in 2022), reflecting an increase of 94.03 %.

In the category of sexual exploitation, the total reported cases during the pre-COVID-19 period amounted to 5,756 (1,460 in 2017; 2,030 in 2018; and 2,266 in 2019). This figure increased to 11,282 during the COVID-19 period (3,293 in 2020; 4,555 in 2021; and 3,434 in 2022), representing a 96% rise.

For the category of causing disrepute, the total number of cases during the pre-COVID-19 period was 4,088 (1,002 in 2017; 1,212 in 2018; and 1,874 in 2019). In the COVID-19 period, this number increased to 8,971 (2,440 in 2020; 2,883 in 2021; and 3,648 in 2022), marking a 119.44% increase. This significant growth is illustrated in Figure 3.

Table 3: Types of Cyber Crime reported in India during Pre-COVID and COVID-19 period
Source: National Crime Record Bureau [13]

Year	Total Cyber Crime	Cyber Fraud	Sexual Exploitation	Causing disrepute	Personal Revenge	Anger	Extortion	Prank	Political Motives	Terrorist Activities
2017	21796	12213	1460	1002	628	714	906	321	149	110
2018	27248	15051	2030	1212	794	461	1050	296	218	44
2019	44546	26891	2266	1874	1207	581	1842	1385	316	199
2020	50035	30142	3293	2440	1470	822	2440	254	356	113
2021	52974	32230	4555	2883	1724	883	2883	240	311	11
2022	65893	42710	3434	3648	857	792	3648	173	165	6

(a) Major cybercrime categories

Year	Total Cyber Crime	Inciting Hate against Country	Disrupt Public Service	Sale/Purchase Illegal Drugs	Developing Own Business	Spreading Piracy	Psycho or Pervert	Steal Information	Abetment to Suicide	Others
2017	21796	206	55	8	156	90	17	10	5	3756
2018	27248	218	21	6	198	671	4	16	2	4956
2019	44546	49	28	10	181	45	1	93	0	7578
2020	50035	165	92	21	210	75	0	62	0	8814
2021	52974	31	40	14	117	74	3	40	0	8043
2022	65893	34	70	11	1068	89	2	137	4	10791

(b) Other specific motives and activities

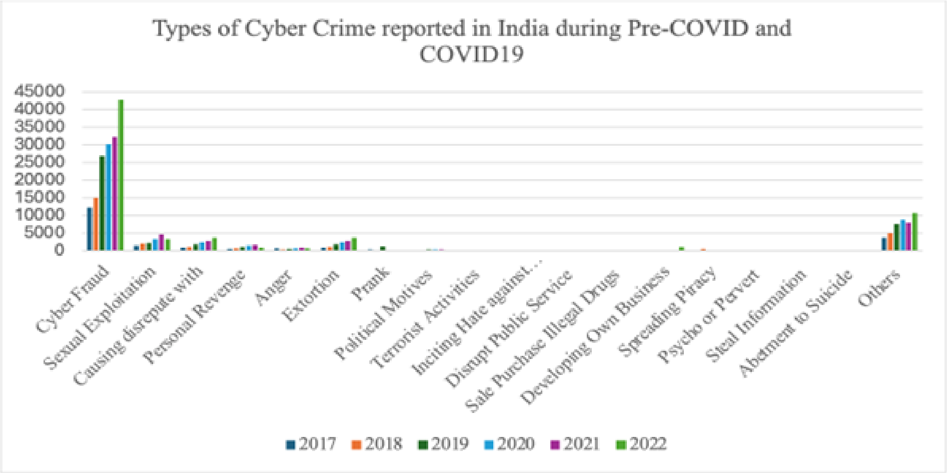

Figure 3: Types of Cyber Crime reported in India during Pre-COVID and COVID 19 period

3.2. Crime statistics in the North East(NE) region of India (2017-2022)

Total FIR (IPC+SLL) registered in the NE region of India during Pre-COVID and COVID 19(2017-2022) Tripura is situated in the North-Eastern (NE) region of the country consisting of total 08 (eight) states namely Assam, Arunachal Pradesh, Meghalaya, Manipur, Mizoram, Nagaland, Tripura and Sikkim.

As presented in Table 4 the total number of FIR reported was 432646 (four lakh thirty-two thousand six hundred forty-six) in the North-Eastern region, during pre-COVID19 period and during COVID-19, it was 389446 (three lakh eighty-nine thousand four hundred forty six), thus reduced by 11.09 % , as visualized in Figure 4.

Table 4: Total FIR(overall)registered in the NE region during Pre-COVID and COVID 19 period Source: National Crime Record Bureau [13]

STATE	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Tripura	4238	6038	5988	4653	4788	4532
Mizoram	2738	2351	2880	2289	3196	4133
Nagaland	1553	1775	1661	1511	1478	1592
Manipur	4250	3781	3661	2986	3204	3914
Sikkim	979	869	821	675	728	819
AP	2746	2817	2877	2503	3039	2761
Meghalaya	3952	3412	3897	3744	3428	3625
Assam	109952	120573	132783	121609	133239	68937
Total	**132425**	**143634**	**156587**	**141990**	**155121**	**92335**
Total in 3 years (2017–2019)			**432646**	**Total in 3 years (2020–2022)**		**389446**

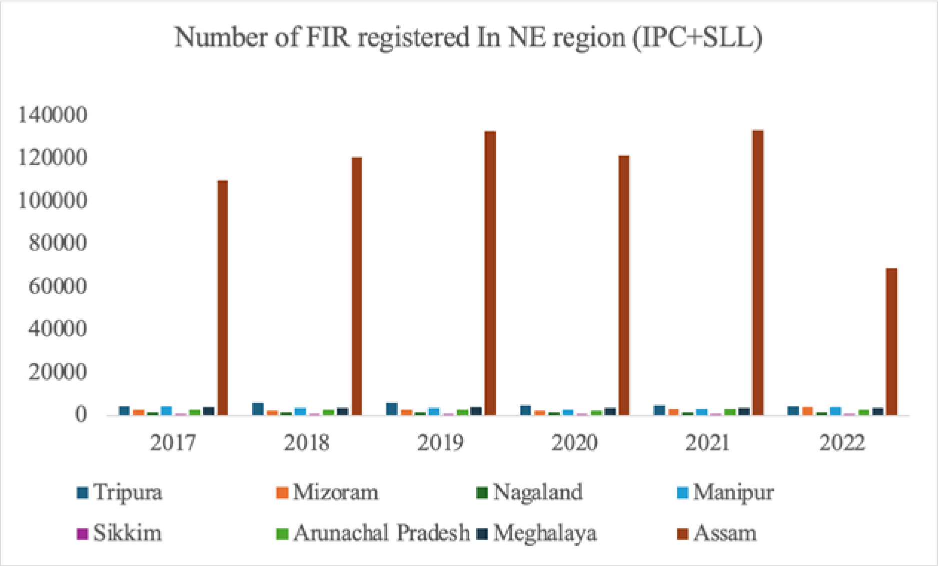

Figure 4: Total FIR (overall) registered in the NE region during Pre-COVID and COVID 19 period

Cyber Crime Cases registered in the NE region of India during Pre-COVID and COVID 19(2017-2022) An overview of Table 5 reveals that the total number of cyber-crimes reported in the North-Eastern region increased from 5,777(five thousand seven hundred seventy-seven) in the pre-COVID-19 period to 10,866(ten thousand eight hundred sixty-six) during the COVID-19 period, representing a rise of 88 %.This trend is further illustrated in Figure 5.

Table 5: Total Cyber Crime Cases registered in the North-Eastern states during Pre-COVID and COVID 19 period
Source: National Crime Record Bureau [13]

STATE	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**
Tripura	7	20	20	34	24	30
Mizoram	10	6	8	13	30	1
Nagaland	0	2	2	8	8	4
Manipur	74	29	4	79	67	18
Sikkim	1	1	2	0	0	26
AP	1	7	8	30	47	14
Meghalaya	39	74	89	142	107	75
Assam	1120	2022	2231	3530	4846	1733
Total	**1252**	**2161**	**2364**	**3836**	**5129**	**1901**
Total in 3 years (2017–2019)			**5777**	**Total in 3 years (2020–2022)**		**10866**

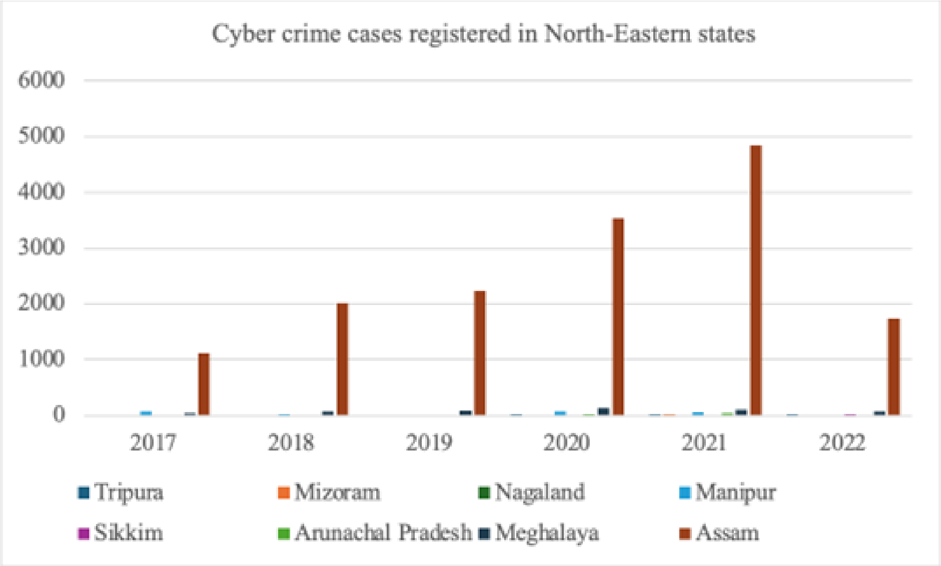

Figure 5: Total Cyber Crime Cases registered in the North-Eastern states during Pre-COVID and COVID 19 period

Types of Cyber-Crime cases registered in the North Eastern Region during Pre-COVID and COVID 19 (2017-2022) Table 6 shows the categories of cybercrimes registered across the eight North-Eastern states of India (Assam, Arunachal Pradesh, Mizoram, Meghalaya, Nagaland, Tripura, Arunachal Pradesh, and Sikkim) during the periods 2017–2019 (Pre-COVID) and 2020–2022 (COVID).The data, further illustrated in Figure 6, clearly demonstrates the sharp rise in cases and the growing diversity of cyber offences across the region

Table 6: Types of cyber-crime cases registered in the North Eastern Region during Pre-COVID and COVID 19 period
Source: National Crime Record Bureau [13]

Year	Total Cyber Crime	Cyber Fraud	Sexual Exploitation	Causing disrepute	Personal Revenge	Anger	Extortion	Prank	Political Motives	Terrorist Activities
2017	1252	108	233	40	265	87	108	40	12	45
2018	2161	448	128	238	245	50	156	0	16	5
2019	2364	295	300	42	563	276	530	19	19	54
2020	3836	405	506	100	675	177	454	39	37	4
2021	5129	794	1211	180	831	151	517	39	112	3
2022	1901	1280	76	42	263	67	637	53	21	2

(a) Major cybercrime categories in NE region

Year	Total Cyber Crime	Inciting Hate against Country	Disrupt Public Service	Sale/Purchase Illegal Drugs	Developing Own Business	Spreading Piracy	Psycho or Pervert	Steal Information	Abetment to Suicide	Others
2017	1252	2	0	0	1	5	0	1	0	353
2018	2161	15	1	2	0	6	1	0	0	850
2019	2364	3	4	0	0	1	0	0	0	258
2020	3836	58	12	0	3	1	0	3	0	1357
2021	5129	14	5	11	28	6	0	10	0	1217
2022	1901	1	5	0	7	3	0	0	0	466

(b) Other specific motives and activities in NE region

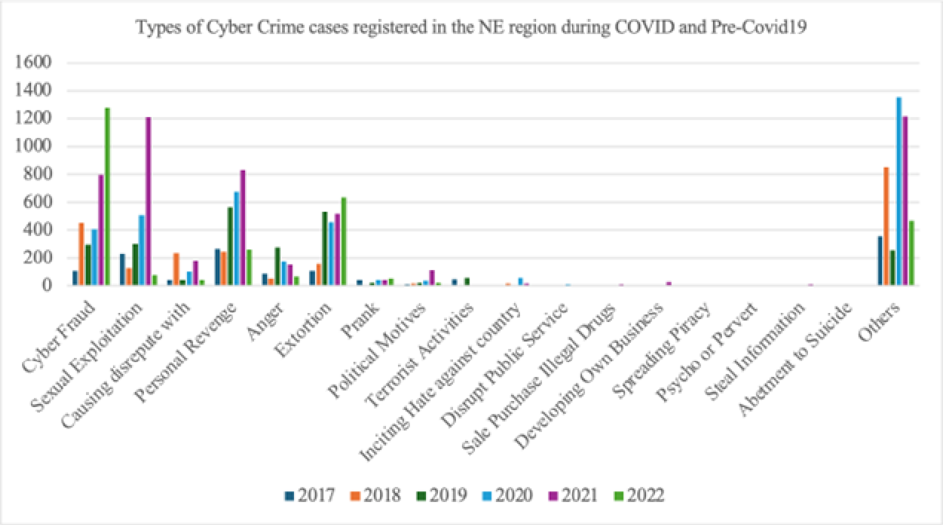

Figure 6: Types of cyber-crime cases registered in the North Eastern Region during Pre-COVID and COVID 19 period

3.3. Crime statistics in the state of Tripura(2017-2022)

Total FIR registered in the state of Tripura during Pre-COVID and COVID 19 (2017-2022) In Tripura, total FIR registered during pre-COVID 19 was 16264 (4,238 in 2017, 6,038 in 2018, and 5,988 in 2019) while during the COVID period it decreased to 13,973 (4,653 in 2020, 4,788 in 2021, and 4,532 in 2022), reflecting a decline of 14.08 % as shown in Table 7 and Figure 7.

Table 7: Total FIR registered in the state of Tripura during Pre-COVID and COVID 19 period Source: National Crime Record Bureau [13]

Year	**Number of FIR (Overall)**	**Year wise change**	**Total**	**Relation with COVID**
2017	4238	-	16264	Pre-COVID
2018	6038	42%		
2019	5988	-1%		
2020	4653	-22%	13973	COVID-19
2021	4788	3%		
2022	4532	-5%		

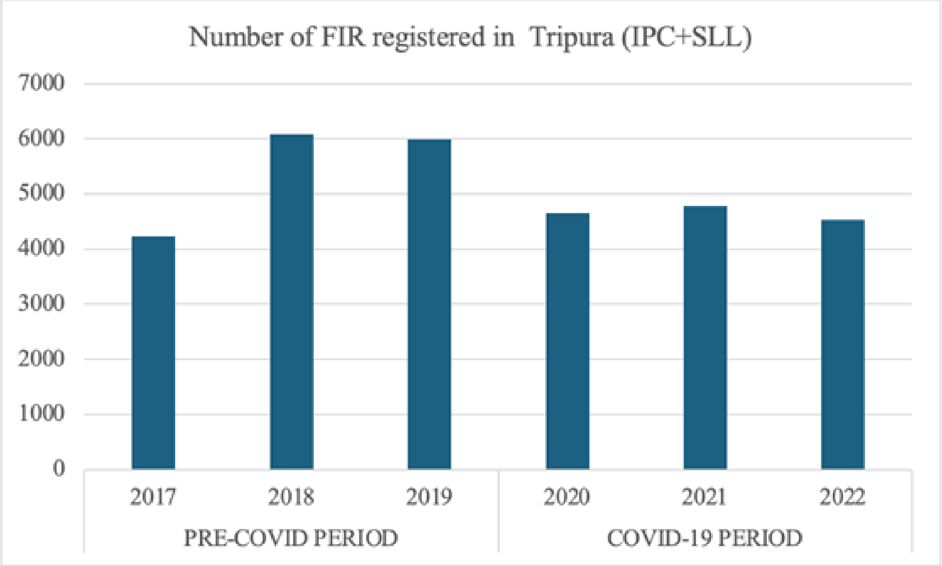

Figure 7: Total FIR registered in the state of Tripura during Pre-COVID and COVID 19 period

Cyber Crime Cases registered in the state of Tripura during Pre-COVID and COVID 19(2017-2022) In Tripura, the total number of cyber crime cases registered during the pre-COVID-19 period was 47 (7 in 2017, 20 in 2018, and 20 in 2019), whereas during the COVID-19 period it increased to 88 (34 in 2020, 24 in 2021, and 30 in 2022), as shown in Table 8.This indicates an overall increase of 87.23 %, as illustrated in Figure 8.

Table 8: Total Cyber Crime Cases registered in the state of Tripura during Pre-COVID and COVID 19 period Source: National Crime Record Bureau [13]

Year	**Number of FIR (Cyber)**	**Year wise change**	**Total**	**Relation with COVID**
2017	7	-	47	Pre-COVID
2018	20	186%		
2019	20	0%		
2020	34	70%	88	COVID-19
2021	24	-29%		
2022	30	25%		

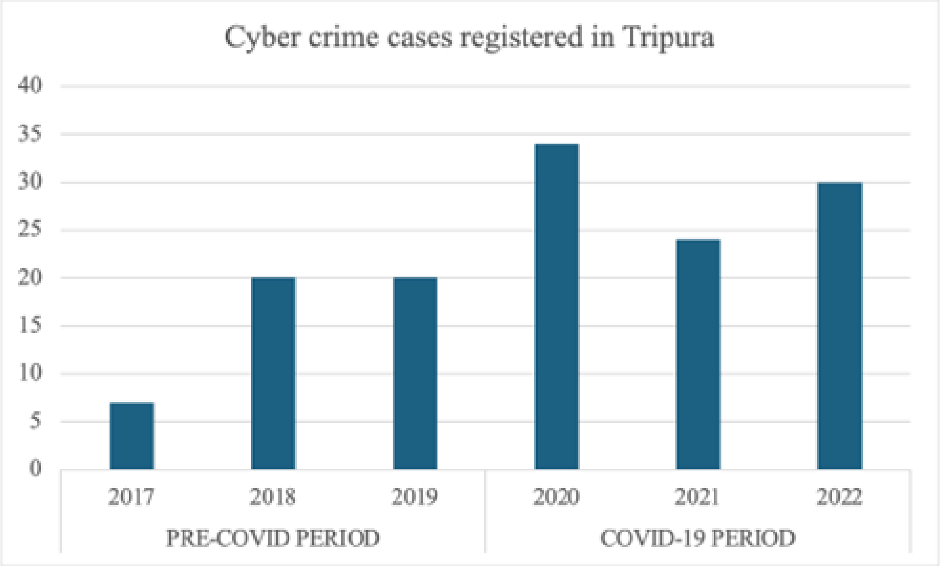

Figure 8: Total Cyber Crime Cases registered in the state of Tripura during Pre-COVID and COVID 19 period

Types of Cyber Crime reported in Tripura during Pre-COVID and COVID 19(2017–2022) In Tripura, cyber crime cases increased notably during the COVID-19 period compared to the pre-COVID years, with cyber fraud emerging as the major category. The categories of sexual exploitation and causing disrepute also recorded spikes, particularly during 2019–2020. Additionally, a limited number of cases related to personal revenge, anger, extortion, pranks, and political motives were reported. As presented in Table 9 and Figure 9, although the overall number of cases in Tripura remained relatively small compared to India and NE region, the rise in cyber fraud and digital dependency underscores the state's increasing vulnerability to digital threats during the pandemic.

Table 9: Types of Cyber Crime reported in Tripura during Pre-COVID and COVID 19 period
Source: National Crime Record Bureau [13]

Year	Total Cyber Crime	Cyber Fraud	Sexual Exploitation	Causing disrepute	Personal Revenge	Anger	Extortion	Prank	Political Motives	Terrorist Activities
2017	7	3	1	0	0	2	0	0	0	0
2018	20	8	3	0	5	0	0	0	4	0
2019	20	2	2	6	1	1	3	0	1	0
2020	34	11	3	2	14	1	0	0	1	0
2021	24	5	1	0	13	0	5	0	0	0
2022	30	12	2	5	3	0	1	0	2	0

(a) Major cyber crime categories in Tripura

Year	Total Cyber Crime	Inciting Hate against Country	Disrupt Public Service	Sale/Purchase Illegal Drugs	Developing Own Business	Spreading Piracy	Psycho or Pervert	Steal Information	Abetment to Suicide	Others
2017	7	0	0	0	0	0	0	0	0	1
2018	20	0	0	0	0	0	0	0	0	0
2019	20	0	0	0	0	0	0	0	0	4
2020	34	0	0	0	0	1	0	0	0	1
2021	24	0	0	0	0	0	0	0	0	0
2022	30	0	2	0	0	2	0	0	0	1

(b) Other specific motives and activities in Tripura

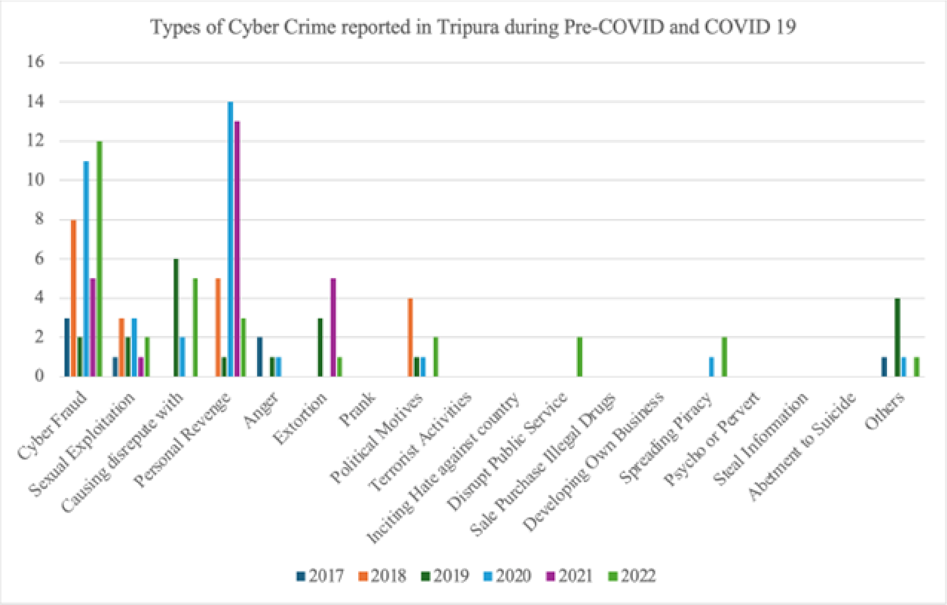

Figure 9: Types of Cyber Crime reported in Tripura during Pre-COVID and COVID 19 period

Table 10: Year-wise Cybercrime Statistics in India

Year	Total Cyber Crime	Cyber Fraud	Sexual Exploitation	Causing Disrepute With	Personal Revenge	Anger	Extortion	Prank	Political Motives	Terrorist Activities
2017	21796	12213	1460	1002	628	714	906	321	149	110
2018	27248	15051	2030	1212	794	461	1050	296	218	44
2019	44546	26891	2266	1874	1207	581	1842	1385	316	199
2020	50035	30142	3293	2440	1470	822	2440	254	356	113
2021	52974	32230	4555	2883	1724	883	2883	240	311	11
2022	65893	42710	3434	3648	857	792	3648	173	165	6

4. Analysis and Discussion of Cyber Crime Trends

In this section the data were tested and analyzed by finding mean, variance and standard deviation for comparing into different year on year like 2017-2018, 2018-19 for the pre Covid-19 and during the pic of the period. In addition regression analysis also carried out for different years for examining the trends.

4.1. Statistical Analysis Results

From Table 3(a) it is observed that Unstandardized Coefficients (B): This is the most crucial part for direct analysis.The value for "Year" (0.25) means that for every one-year increase, the number of cybercrimes is predicted to increase by 0.25 units (e.g., cases, in millions of rupees, etc.), holding all other variables constant. The "Constant" (1.50) is the baseline number of cybercrimes when all other variables are zero.

Standardized Coefficients (Beta): These values allow you to compare the relative strength of the different independent variables. In the example, the Beta value for "Internet Penetration" (0.92) is higher than that for "Year" (0.85), suggesting that internet penetration is a stronger predictor of cybercrime than the passage of time.

Sig. (p-value): This column indicates whether the relationship is statistically significant. A p-value less than 0.05 confirms that the relationship is unlikely to be due to random chance and is highly significant.

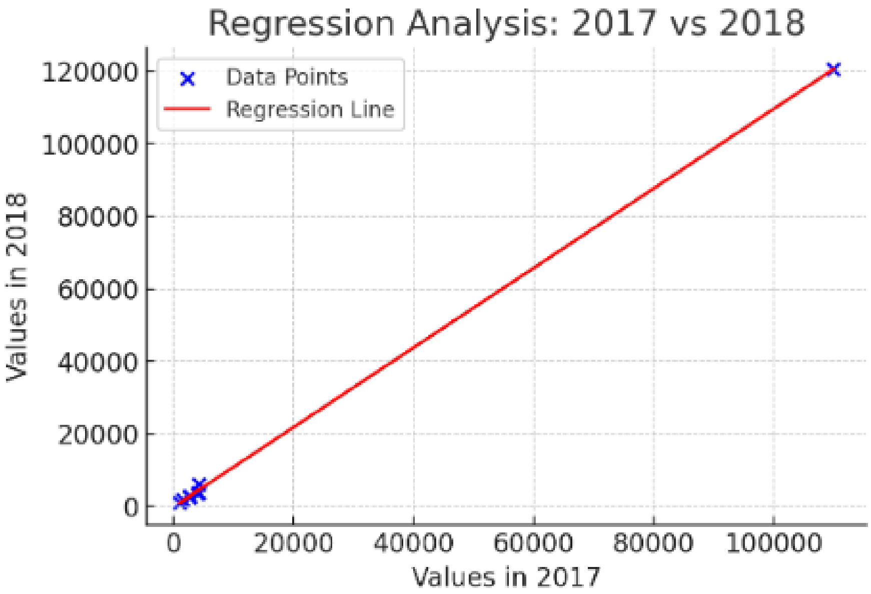

Figure 10: Regression Line-1

The graph analysis in Table 4 shows a linear regression line that is ordered in monotonically increasing ways in different Indian states (red) comparing the 2017 vs. 2018 values. Data points (blue crosses) lie almost perfectly along the line, suggesting a very strong positive correlation. The regression line is close to the line $y = x$, indicating that the values for 2018 are almost proportional to the values for 2017. From statistical measures, we have seen that the mean is 17,001.5, the variance is 1,476,819,138.67, and the standard deviation (S.D) is 38,429.40.
Variance is very high, which implies that the data values are spread over a wide range. Since the regression line passes through clustered points near the origin and some high values, this mean reflects the central tendency of the distribution. This is visible in the graph; some values are very close to zero, while others exceed 100,000. A high standard deviation confirms the presence of large fluctuations between smaller and larger data points. which is very risky. for the cases of such a crime. It means that individual yearly values deviate significantly from the mean of 17,001.5. Now, the regression line shows a consistent growth trend: Higher 2017 values are directly linked with higher 2018 values.

Clustering near the origin indicates that most values are relatively small, while a few extreme values (outliers) push the variance and standard deviation very high. Despite the large spread, the linear fit is excellent, which means that the 2017 values strongly predict the 2018 values.

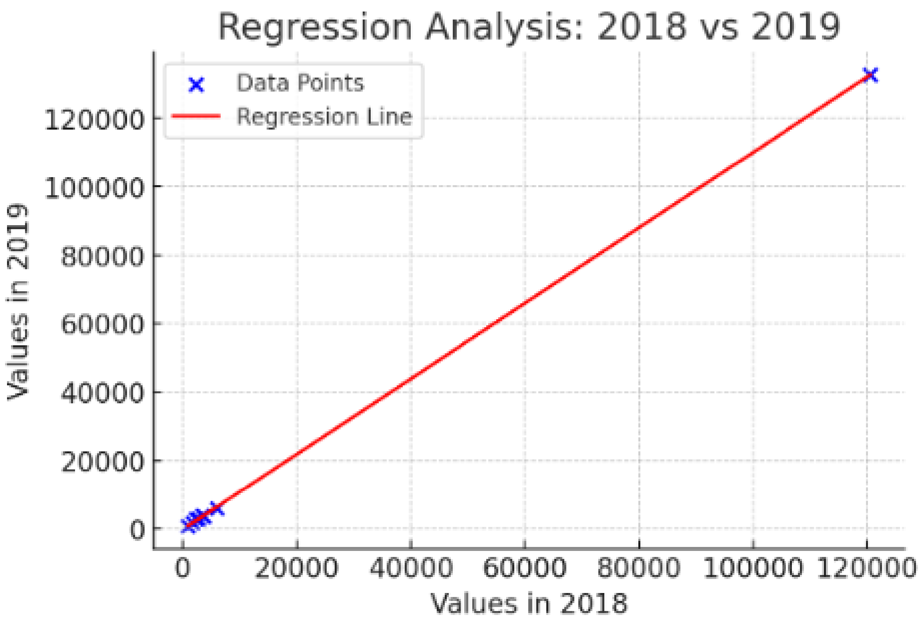

Figure 11: Regression Line-2

The graph plots the 2018 values vs. the 2019 values with a regression line (red). The data points (blue crosses) again lie very close to the line, showing a strong positive correlation. The regression line almost overlapsdiagonal, meanimeaning that the values in 2019 strongly mirror those in 2018 with proportional growth.

Statistical Measures: Here, Mean = 18,511.5 implies that the average value is slightly higher than in the 2017–2018 case (17,001.5). This indicates a general upward shift in values from 2018 to 2019.

Also the Variance is 1,790,038,472.80 The variance has increased compared to 2017–2018, suggesting that data points in 2019 are spread even more widely than the mean. Large deviations arise because of the presence of very high values (over 120,000) alongside many small ones. Standard Deviation (S.D) = 42,308.85. This large value indicates substantial variation in the dataset. Since the standard deviation is higher than in the previous case (38,429.40), confirming that the 2018–2019 data set is slightly more dispersed. The regression line demonstrates near-perfect linearity, confirming a predictable trend: higher 2018 values lead to proportionally higher 2019 values. The increase in both mean and standard deviation compared to the 2017–2018 analysis suggests growth in average values but also greater inequality (spread) among them. The clustering near the origin remains, meaning most values are still small, but a few outliers with very large values drive the variance upward.

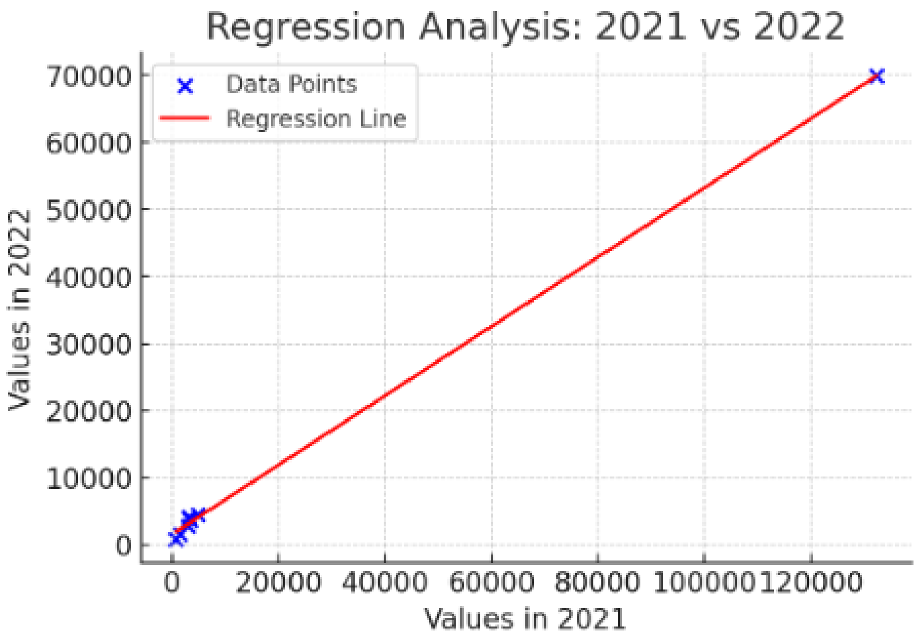

Figure 12: Regression Line-3

The regression line (red) fits the data points (blue) almost perfectly, showing a strong positive correlation between 2021 and 2022 values. Most of the points are concentrated near the lower values, while one or two extreme values extend far to the right, heavily influencing the regression line. Unlike earlier cases (2017–2018, 2018–2019), here the growth in 2022 values appears somewhat smaller compared to the very large 2021 values (e.g., a 120,000+ value in 2021 corresponds to 70,000 in 2022).

Here the Statistical Measures, Mean = 15,212.69 and Variance = 1,255,291,484.23. Clearly the average value is lower compared to the earlier periods (17,001.5 for 2017–2018 and 18,511.5 for 2018–2019). This suggests a decline in central tendency of the dataset in 2022 relative to previous years. The variance is still very high, but lower than the previous comparisons (1.47B and 1.79B). This indicates that while the data set still has extreme variations, the spread is slightly reduced compared to earlier years.

We have Standard Deviation (S.D) = 35,430.09, The standard deviation confirms this reduced spread. Compared to 2017–2018 (38,429.40) and 2018–2019 (42,308.85), the 2021–2022 dataset is less dispersed, even though outliers are still present.

The regression confirms strong linearity between 2021 and 2022, but the slope suggests that 2022 values did not grow as strongly as in previous years relative to 2021. The lower mean and reduced standard deviation indicate that the dataset has shifted toward smaller values, with fewer extreme increases compared to past years. Outliers are still present, but their impact on variance is weaker than in earlier datasets.

4.2. Comparative Insights

From the three regression analyses, we observe that: The regression lines consistently indicate a strong positive linear relationship across all years. The highest spread occurred in the 2018–2019 data, with both variance and standard deviation reaching maximum values. The 2021–2022 data shows stabilization, with lower mean and reduced variability compared to earlier years. Outliers consistently influence the variance and standard deviation, though their impact is weaker in 2021–2022.

Statistical Analysis Using mean, variance, and standard deviation for selected year pairs (from overall FIR totals):

This variation highlights **instability in reported cases** during COVID, with larger fluctuations compared to pre-COVID stability.

Year Pair	Mean	Variance	Standard Deviation
2017–2018	17,001.5	1.47×10^9	38,429.40
2018–2019	18,511.5	1.79×10^9	42,308.85
2021–2022	15,212.69	1.25×10^9	35,430.09

Table 11: Comparative statistical analysis of FIR data across year pairs

4.3. Analysis of Cyber Crime Satistics:Tripura

The cybercrime data from Tripura between **2017 and 2022** reveals notable statistical and trend-based characteristics. We analyze the FIR (First Information Report) registrations and cybercrime-specific cases in both **pre-COVID (2017–2019)** and **COVID (2020–2022)** periods.

Overall FIR Trends in Tripura From Table 7 of the dataset: Pre-COVID total (2017–2019): **16,264 FIRs** COVID total (2020–2022): **13,973 FIRs**

This shows a **14% decline in overall FIR registration during COVID**, which may reflect lockdown-induced restrictions on physical crimes.

Cybercrime FIRs (IT Act cases in Tripura) From Table 8: Pre-COVID total (2017–2019): **47 cases** COVID total (2020–2022): **88 cases**

This indicates an **87.2% increase in cybercrime cases during COVID**, consistent with the national trend of rising digital fraud.

Types of Cybercrime in Tripura From Table 9: **Cyber Fraud** consistently emerged as the leading category, with reported cases increasing from 3 (2017) to 12 (2022). **Sexual Exploitation** and **Causing Disrepute** also showed noticeable spikes, particularly in 2019 and 2020. Other motives such as **personal revenge** and **anger** had episodic peaks, reflecting socio-psychological stress during the pandemic.

4.4. Regression Analysis

From the dataset and various analyses, it is evident that the proportion of cybercrime within total crime has shown a consistent rise during the Covid-19 period. The regression lines constructed for paired years further validate this trend, highlighting a strong linear relationship in the reported FIR numbers.
2019–2020: $y \approx 2700 + 0.90x$
and 2020–2021: $y \approx 850 + 1.03x$
Interpretation: The slope less than 1 for 2019–2020 indicates a **drop in overall FIRs** during 2020. The slope greater than 1 for 2020–2021 indicates a **slight recovery** in FIRs during 2021.

4.5. Conclusion for Tripura

While overall FIRs decreased during COVID, cybercrime FIRs sharply increased, almost doubling in the period 2020–2022. Cyber fraud was the dominant category, followed by sexual exploitation and defamation-related offences. Mathematical indicators (variance, regression slope) confirm that COVID introduced **greater fluctuations and instability** in reported cases. Thus, Tripura's case study illustrates a **shift from conventional crime to digital crime** during the pandemic, highlighting the urgency for targeted cybersecurity measures.

5. Future Recommendations for Cybercrime Precautions in Tripura

The analysis of cybercrime trends in Tripura, based on both pre-COVID-19 (2017–2019) and COVID-19 (2020–2022) data, clearly indicates a significant escalation in reported cases, particularly in categories such as cyber fraud, sexual exploitation, and causing disrepute. These trends underscore the urgent need for multi-faceted precautionary strategies that are tailored to the socio-economic, technological, and cultural realities of the state. While the above analysis provides a comprehensive overview of cybercrime trends in Tripura during the pre- and post-COVID-19 periods, the absence of separate demographic data limits the ability to identify victims specific or offender specific patterns. Future research may include age, gender, socio-economical and educational variables to better in-depth analysis of sociological dimensions of cybercrime. This would enhance predictive trend analysis and devise targeted awareness strategies to the vulnerable groups of people.

The following recommendations aim to provide a robust framework for mitigating the impact of cybercrime in Tripura. We have also followed the following observation and suggestion:

Strengthening Cyber Awareness and Digital Literacy: Given Tripura's high literacy rate but comparatively low digital literacy, the first line of defense must be a sustained and inclusive awareness program. Conduct state-wide cyber safety awareness campaigns in Bengali, Kokborok, and other local languages to ensure inclusivity. Integrate cyber hygiene modules into school and college curricula, covering topics such as phishing detection, safe password management, and responsible social media usage. Partner with local community organizations, NGOs, and self-help groups to deliver door-to-door educational outreach, especially in rural and border areas where cyber awareness is minimal.

Capacity Building for Law Enforcement: The rising sophistication of cybercriminals demands that Tripura's police force and cyber cells be equipped with advanced tools and skills.

Provide specialized training in digital forensics, blockchain investigation, and AI-driven cyber threat detection. Develop a dedicated *Cybercrime Task Force* that can respond to incidents in real-time. Facilitate interstate and international collaboration to track cross-border cybercrime operations, especially given Tripura's proximity to international borders.

Enhancing Cybersecurity Infrastructure: Strengthening digital infrastructure is essential for timely detection, reporting, and mitigation of cybercrime incidents. Establish 24×7 toll-free cyber helplines with multilingual support. Set up district-level cybercrime reporting and assistance centers to decentralize response mechanisms. Implement AI-based early warning systems to detect large-scale phishing or ransomware campaigns. Strengthening cybersecurity infrastructure in Tripura requires not only institutional capacity-building but also the adoption of emerging digital technologies like Artificial Intelligence and Machine Learning (AI & ML) in critical analysis for prevention and detection of such crimes. AI-based early warning systems can be developed to detect large-scale phishing or ransomware attacks through pattern recognition. Advanced machine learning algorithms can assist law enforcement agencies in identifying cybercrime hotspots and predicting threat vectors. These technological interventions, combined with human intelligence, can substantially improve the state's capacity and preparedness for real-time response against cyber threats or incidents.

Securing the Financial Ecosystem: Financial fraud emerged as the most reported cybercrime category in Tripura during both study periods, making it imperative to reinforce security in banking and financial transactions.

Mandate multi-factor authentication for all online financial services and mobile banking applications. Organize cyber fraud prevention workshops for small traders, local entrepreneurs, and digital payment users. Establish fast-response fund-freezing protocols in collaboration with banks and payment gateways.

Regulating and Monitoring Social Media Platforms: With social media being a common medium for fraud, exploitation, and misinformation, targeted regulation is essential.

Create a state-specific *Social Media Monitoring Cell* to track and take down malicious accounts targeting Tripura residents. Collaborate with social media companies for quicker redressal and takedown of harmful content.

Rural Internet Safety Initiatives: Rural areas are often more vulnerable due to low cyber literacy despite increasing internet penetration. Provide free, periodic cybersecurity workshops at panchayat and village levels. Partner with telecom companies to send cyber safety SMS alerts in local languages.

Youth and Student Engagement: The younger population is both a frequent target and an important resource for combating cybercrime. Establish cybersecurity clubs in schools, colleges, and universities to promote ethical hacking and problem-solving skills. Introduce competitions, hackathons, and scholarships for innovative cybercrime prevention solutions.

Policy and Legal Measures: Finally, effective legislation and judicial processes are crucial for deterring cybercriminals. Draft state-specific cybercrime regulations aligned with the Information Technology Act, but adapted to local challenges. Set up fast-track courts for cybercrime to ensure timely justice and deterrence. Introduce mandatory cyber risk assessments for all government and public service portals.

6. Conclusion

In this article, we have undertaken a comprehensive study titled “Analysis of Cybercrime Trends in India with a Special Focus on Tripura (Pre- and During COVID-19)”. The primary objective of this work is to examine the variations in cybercrime cases over different years, especially highlighting the changes observed before and during the COVID-19 pandemic. To achieve this, we employed rigorous statistical methods for year-on-year comparison, which allowed us to identify patterns and fluctuations in the prevalence of cybercrime. Our findings indicate that cybercrime has shown a consistent upward trajectory, increasing steadily on a day-to-day basis, and this rise is comparatively higher than that of several other categories of crime.

Furthermore, regression analysis was applied to evaluate the strength of the relationship between datasets from successive years. The results suggest that cybercrime incidents are strongly correlated with previous year data, thereby reflecting a predictable pattern of growth. In addition to the statistical insights, we have also proposed certain policy recommendations aimed at curbing the alarming rise of cybercrime in India. These recommendations focus on preventive strategies, awareness programs, technological safeguards, and stronger law enforcement mechanisms. Overall, the analysis, grounded in statistical measurements, not only provides a clearer picture of the current scenario but also establishes meaningful relationships with historical datasets. This enables us to better understand the dynamics of cybercrime and offers a foundation for framing effective countermeasures.

Future research directions: the present study relies on data publicly available up to the year 2022 as published by the National Crime Records Bureau (NCRB). The availability of datasets for thr year 2023 and 2024 will give more clarity on pattern analyses and for developing a deeper understanding of the subject matter. In this study, cases registered under the Information Technology (IT) Act, 2000 were classified as cybercrime. However, in practice, certain offences with clear cyber elements were registered under provisions of the Indian Penal Code (IPC) without invoking sections of the IT Act, while in other instances, both the IPC and IT Act were simultaneously applied. These cases were often classified under non-cyber categories in official records. For instance, a rape case under the IPC, when accompanied by the online circulation of obscene video material, may also attract provisions of the IT Act. Nevertheless, because rape is treated as a major offence, the case is statistically categorized as “Crime Against Women” rather than as a cybercrime. Such overlaps and discrepancies suggest the need for separate analysis of these cases in order to obtain a more comprehensive and accurate picture of cybercrime trends during the study period.

Cybercrimes are borderless and committing crime from one country targeting other countries are very common and as such does not require border proximity. Sometimes, the turmoil situation of one country percolates to the other country through social media and other digital platforms. In future research, studies on the dynamics of the border with the bordering states and neighboring countries and its impact on the cybercrime pattern can be conducted to perform in-depth analysis and take corrective measures.

References

1. Muna Ahmead, Nuha El Sharif, and Issa Abuiram. Risky online behaviors and cybercrime awareness among undergraduate students at al quds university: a cross sectional study. *Crime Science*, 13(1):29, Oct 2024.

2. M. A. Andrews, Binu Areekal, K. R. Rajesh, Jijith Krishnan, R. Suryakala, Biju Krishnan, C. P. Muraly, and P. V. Santhosh. First confirmed case of covid-19 infection in india: A case report. *Indian Journal of Medical Research*, 151(5):490–492, May 2020.

3. Sewa Singh Bajwa. Need and necessity of digital media literacy in north-east india, July 2023.

4. M. Bruce, J. Lusthaus, R. Kashyap, N. Phair, and F. Varese. Mapping the global geography of cybercrime with the world cybercrime index. *PLOS ONE*, 19(4):e0297312, Apr 2024.

5. David Buil-Gil, Yi Zeng, and Steven Kemp. Offline crime bounces back to pre-covid levels, cyber stays high: Interrupted time-series analysis in northern ireland. *Crime Science*, 10(1):1–16, 2021.

6. Charlette Donalds and Kweku-Muata Osei-Bryson. Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, 92:403–418, 2019.

7. Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, and Georgios Smaragdakis. The lockdown effect: Implications of the covid-19 pandemic on internet traffic. *ACM Internet Measurement Conference(IMC'20)*, pages 1–18, Oct 2020.

8. Vasileios Karagiannopoulos, Annie Louise Kirby, Shakiba Oftadeh Moghadam, and Lisa Sugiura. Cybercrime awareness and victimisation in individuals over 60 years: a portsmouth case study. *Computer Law & Security Review*, 43:Article 105615, 2021.

9. Sumir Karmakar. Tripura reports first covid-19 positive case, April 6 2020. Last Updated April 6, 2020, 20:06 IST.

10. M. Kashif, A.-U. Rehman, M. K. Javed, and D. Pandey. A surge in cyber-crime during covid-19. *Indonesian Journal of Social and Environmental Issues (IJSEI)*, 1(2):48–52, 2020.

11. Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R. C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105:102248, 2021.

12. Deepti Meena, Sarita Dehariya Mehra, and Priyansh Samadhiya. Cyber crimes in india. page 229, 2024. Paperback.

13. National Crime Records Bureau. Crime in india – year-wise statistics. https://www.ncrb.gov.in/crime-in-india-year-wise.html.

14. Minh Hao Nguyen, Jonathan Gruber, Julia Fuchs, William Marler, Amanda Hunsaker, and Eszter Hargittai. Changes in digital communication during the covid-19 global pandemic: Implications for digital inequality and future research. *Social Media + Society*, 6(3):1–6, 2020.

15. Ministry of Electronics, Government of India Information Technology, and Better Than Cash Alliance. Catalyzing responsible digital payments in the north east region of india. https://www.rfilc.org/wp-content/uploads/2021/09/Catalyzing-Responsible-Digital-Payments-in-the-North-East-Region-of-India.pdf, 2021.

16. Press Trust of India. Tripura beats kerala in literacy, 2013.

17. Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, and Mary P. Aiken. Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences*, 2(2):379–398, 2022.

18. Reuters. Scammers try selling world's tallest statue as pandemic boosts india's cyber crime. https://www.reuters.com/article/us-health-coronavirus-india-fraud/scammers-try-selling-worlds-tallest-statue-as-pandemic-boosts-indias-cyber-crime-idUSKBN21P0KH/, 2020.

19. Heba Saleous, Muhusina Ismail, Saleh H. AlDaajeh, Nisha Madathil, Saed Alrabaee, Kim-Kwang Raymond Choo, and Nabeel Al-Qirim. Covid-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, 9(1):211–222, 2023.

20. Times of India. Complete lockdown in tripura on july 5 — cm biplab kumar deb. https://timesofindia.indiatimes.com/city/agartala/complete-lockdown-in-tripura-on-july-5-cm-biplab-kumar-deb/articleshow/76727364.cms, 2020.

21. Wikipedia contributors. Covid-19 lockdown in india. https://en.wikipedia.org/wiki/COVID-19_lockdown_in_India. Accessed: 2025-08-06.

Nirdesh Deb
Department of Government and Public Administration,
School of Social Sciences and Languages, Lovely Professional University,
Phagwara, Punjab, 144411, India
E-mail address: debnirdesh@gmail.com

and

Sharad Shekhawat,
Department of Government and Public Administration,
School of Social Sciences and Languages, Lovely Professional University,
Phagwara, Punjab, 144411, India
E-mail address: sharad.26827@lpu.co.in

and

Sanjib Debnath,
Department of Computer Science and Engineering,
ICFAI University Tripura, 799210, India.
E-mail address: sanjib.cst@gmail.com

and

Rakhal Das,
Department of Mathematics,
ICFAI University Tripura, 799210, India.
E-mail address: rakhaldas95@gmail.com, dasrakhaal@gmail.com