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

Trends and Patterns: Analysing Cybercrime Statistics in India

Deepak Kumar Parewa[1], Dr. Deepa Mordia[2]

[1]Research scholar, Department of Statistics, University of Rajasthan, Jaipur
[2]Assistant Professor, Department of Statistics, University of Rajasthan, Jaipur

Abstract
This research paper addresses the evolving landscape of cybercrime in India, focusing on the annual percentage change over the period 2020 to 2022. In response to the escalating threats in the digital realm, the study investigates the influence of population density (Per lakh Population) and temporal factors on the observed cybercrime trends. Leveraging a comprehensive dataset, the research aims to provide nuanced insights crucial for developing effective countermeasures and enhancing cybersecurity strategies in the Indian context.

Keywords: Cybercrime, Trends, India, Population Density, Temporal Factors.

1. Introduction:

In an era dominated by rapid technological advancements and an increasingly interconnected global society, the prevalence of cybercrime has emerged as a critical challenge for nations worldwide(Horgan et al., 2021). India, with its burgeoning digital landscape and escalating reliance on information technology, finds itself at the forefront of this digital revolution. As the country witnesses unprecedented growth in internet penetration, e-commerce, and digital communication, it concurrently grapples with the escalating menace of cyber threats and criminalactivities(Shah et al., 2022). Recognizing the imperative to comprehend, contextualize, and address this multifaceted issue, this research paper delves into a comprehensive statistical analysis of cybercrime trends and patterns in India. This study encapsulates the essence of our exploration into the dynamic landscape of cyber threats faced by the nation. Through rigorous statistical examination, we aim to unearth underlying trends, identify patterns, and draw insights that not only shed light on the current state of cybersecurity but also contribute to the formulation of effective preventive strategies and mitigation measures.The significance of this research lies in its potential to bridge the gap between theoretical understanding and practical application. By scrutinizing a wealth of cybercrime data, this study endeavours to provide a nuanced perspective on the nature and scope of cyber threats in India. In doing so, researchers hope to empower policymakers, law enforcement agencies, and cybersecurity professionals with evidence-based insights that can inform proactive measures to safeguard the nation's digital infrastructure. This paper begins with an exploration of the historical context of cybercrime in India, offering a backdrop against which contemporary trends can be assessed. This study then proceeds to delve into the statistical methodologies employed in this analysis, ensuring transparency and reproducibility in our findings. Subsequently, the paper unfolds into a detailed examination of key cybercrime categories, identifying prevalent attack vectors, and dissecting the evolving strategies employed by cybercriminals.As we navigate through the intricate web of cyber

threats, this research seeks not only to quantify the scale of the challenge but also to uncover the modus operandi behind cyber-attacks. By deciphering the statistical intricacies, we aspire to empower stakeholders with the knowledge required to fortify India's cybersecurity defences, thereby fostering a resilient digital ecosystem.

2. Review of Literature

In the ever-evolving landscape of cybersecurity, understanding the trends and patterns of cybercrime is imperative for devising effective strategies to safeguard digital ecosystems. This section, the "Review of Literature," serves as a compass for our study offering a comprehensive examination of existing scholarly works that have contributed to the understanding of cyber threats in the Indian context.

(Nag et al., 2022)stated that Technology's advancement has transformed crime-solving strategies, leveraging interdisciplinary research to understand crime origins, forms, intensity, and dynamics. Government agencies and police departments now utilize sophisticated tools for tracking criminal events, collecting specific data and spatial-temporal information. This paper introduces the Prophet model, employing an additive approach for forecasting time series data. With a focus on non-linear patterns, seasonality, and holiday effects, the model is applied to predict crimes.

(Subashka Ramesh & others, 2021)highlighted the dual nature of Big Data in criminal activity analysis—it poses a challenge, yet offers opportunities to enhance crime prevention and investigation. The system discussed addresses current challenges in Cybercrime Investigations, particularly those involving Big Data, and proposes approaches to combat cybercrime. The outcomes aim to provide law enforcement agencies with a better understanding of criminal issues, enabling effective resource allocation, operational tracking, incident forecasting, and policymaking optimization. The review advocates for the integration of cutting-edge data analytics, machine learning, and computer modeling in criminal inquiries, emphasizing the effectiveness of computational solutions in analyzing vast, unstructured datasets for crime prevention and detection.

(Rajput & Rajput, 2020)analysed trends and patterns in Cybercrimes and Cyber Economic Crimes, focusing on crime registration, criminal profiles, gender and age distribution, and types of cyber economic crimes. Using case studies from Maharashtra and Mumbai, which together account for a significant portion of cybercrime in India, the analysis reveals that a substantial majority of cases in these regions are Cyber Economic crimes. The findings, supported by statistics from 2002 to 2016, are compared with six other metro cities, offering insights into the regional variations of cybercrime in India.

(Farsi et al., 2018)explored the diverse dimensions of cyber-criminology, emphasizing the shift from corrective actions to predictive and preventive measures. It focuses on the application of quantitative techniques, such as machine learning, for providing strategic insights to law enforcement and police forces. The discussion extends to the analysis of cybercrime patterns, benefiting not only law enforcement but also businesses navigating the risks of the Internet. The study offers a concise overview of machine learning techniques for crime analysis and critically examines data mining and predictive analysis within the context of cyber-criminology.

(Sathyadevan et al., 2014)highlighted the significance of crime analysis and prevention as a systematic approach to identify patterns and trends in crime. The described system utilizes predictive capabilities to identify high-probability crime regions and visualize crime-prone areas. With the integration of computerized systems, crime data analysts can expedite the process of solving crimes. The approach

bridges computer science and criminal justice through data mining, extracting valuable information from unstructured data to enhance crime-solving procedures. Unlike traditional approaches, the emphasis is placed on daily crime factors rather than underlying causes such as criminal background or political enmity.

3. Research Methodology

The research methodology serves as the navigational framework that guides the systematic exploration of trends and patterns in cybercrime rates across Indian states from 2020 to 2022. Drawing exclusively from secondary data sources, this study delves into the computation of cybercrime rates per lakh population, motives as a percentage of the population, and the annual percentage change in cybercrime rates per capita. The methodology employs descriptive and trend analyses to unravel the dynamics of cybercrime, with a specific focus on geographical variations and temporal shifts. Furthermore, a regression model, incorporating predictors such as Per lakh Population and Time, is utilized to discern underlying patterns. Ethical considerations, data privacy, and methodological limitations are carefully addressed, ensuring the reliability and validity of the study's outcomes. The methodology encapsulates a comprehensive approach, amalgamating quantitative analyses, and regression modelling to offer valuable insights into the evolving landscape of cybercrime in India.

3.1 Objective:

- To analyze and identify trends in cybercrime rates across states and union territories in India from 2020 to 2022.
- To explore cybercrime motives as a percentage of population.
- To assess the annual percentage change in cybercrime rates per capita.

3.2 Data Collection:

- Source: Secondary data obtained from official government reports, crime databases, and relevant publications.
- Data Variables:Cybercrime rates per lakh population for each state/union territory in 2020, 2021, and 2022.Cybercrime motives expressed as a percentage of population.Annual percentage change in cybercrime rates per capita.
- Additional data for predictors in the regression model: Per lakh Population, Time.

3.3 Data Analysis:

Descriptive Analysis: Computation of cybercrime rates per lakh population for each state/union territory in 2020, 2021, and 2022 was done.Calculation of cybercrime motives as a percentage of population was done. The annual percentage change in cybercrime rates per capita was determined.

Trend Analysis: Trend charts illustrating the trends in cybercrime rates across states and union territories from 2020 to 2022 were developed.Trend charts for cybercrime motives as a percentage of population were constructed.Trend charts depicting the annual percentage change in cybercrime rates per capita were also presented.

Regression Analysis: Construction of a regression model with predictors including per lakh Population and Time.The dependent variable is the Annual % Change in cybercrime rates per capita.

3.4 Ethical Considerations:

Data Privacy: Ensuring confidentiality and anonymization of individual and state-level data.

Data Source Validity: Verification of the accuracy and reliability of secondary data sources.

3.5 Limitations:

Data Quality: Acknowledging potential limitations in the accuracy and consistency of official crime data.
External Validity: Recognizing that findings are specific to the timeframe and data available.

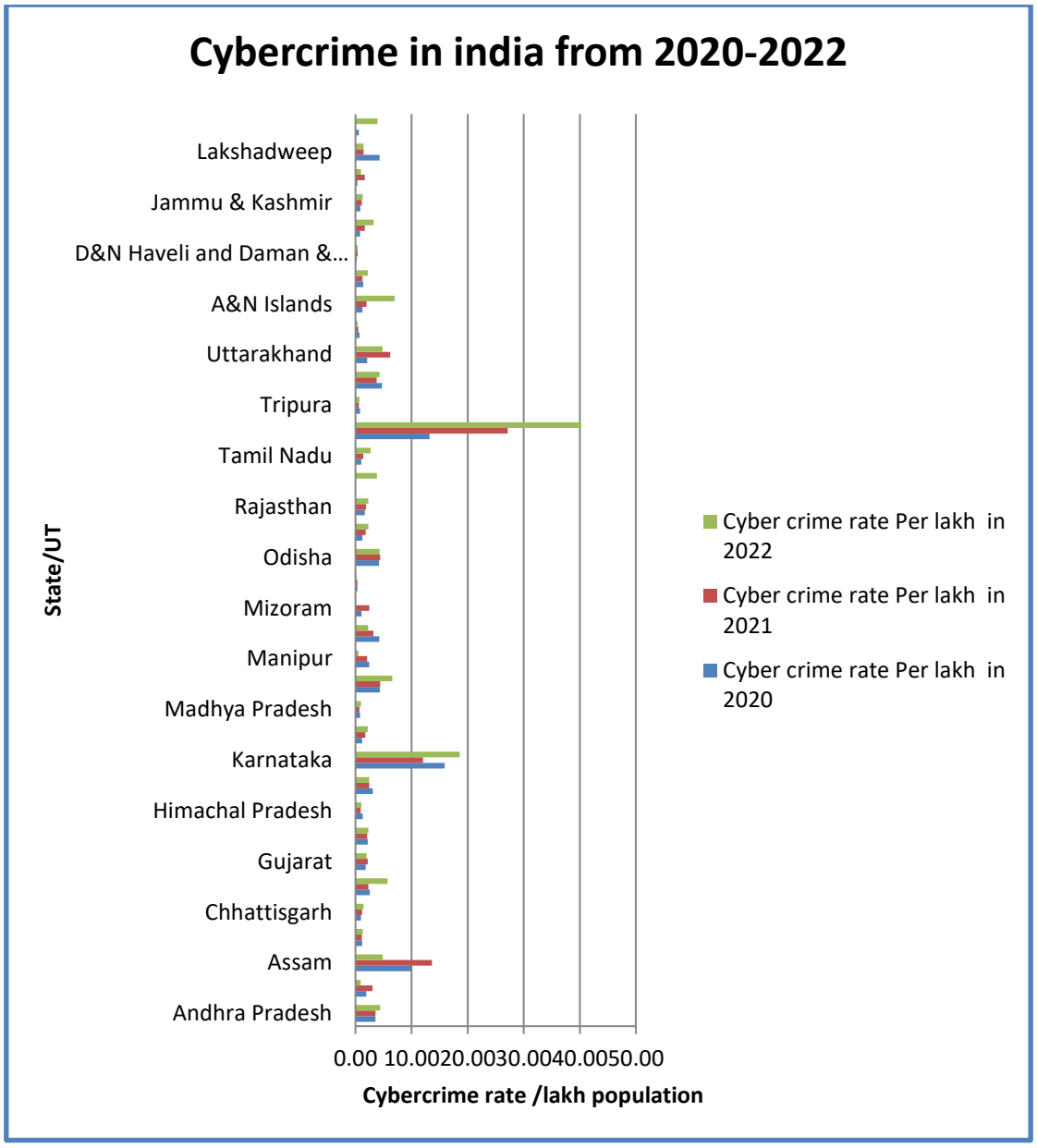
4. Results and Discussion

Cybercrime rate Per lakh

Following dataset provides a comprehensive overview of cybercrime rates per lakh population across Indian states and union territories for the years 2020, 2021, and 2022. The diverse figures present a mosaic of cybercrime occurrences, reflecting both inter-state variations and temporal trends. This information serves as the foundation for our study, enabling a focused analysis of trends and patterns in cybercrime across the country. By examining these rates and their fluctuations, our study aims to contribute valuable insights into the dynamics of cybercrime, offering a nuanced understanding of its prevalence and variations across different regions in India.

State/UT	Mid-Year Projected Population (in Lakhs)	Cybercrime rate Per lakh in 2020	Cybercrime rate Per lakh in 2021	Cybercrime rate Per lakh in 2022
Andhra Pradesh	530.3	3.58	3.54	4.41
Arunachal Pradesh	15.5	1.94	3.03	0.90
Assam	354.9	9.95	13.65	4.88
Bihar	1255.3	1.20	1.13	1.29
Chhattisgarh	299.5	0.99	1.18	1.47
Goa	15.7	2.55	2.29	5.73
Gujarat	709.3	1.81	2.17	2.00
Haryana	299.7	2.19	2.08	2.27
Himachal Pradesh	74.4	1.32	0.94	1.03
Jharkhand	391.4	3.08	2.43	2.47
Karnataka	674.1	15.93	12.07	18.63
Kerala	356.8	1.19	1.75	2.17
Madhya Pradesh	858.9	0.81	0.69	0.96
Maharashtra	1257.4	4.37	4.42	6.56
Manipur	32.0	2.47	2.09	0.56
Meghalaya	33.3	4.26	3.21	2.25
Mizoram	12.3	1.06	2.44	0.08
Nagaland	22.2	0.36	0.36	0.18
Odisha	460.8	4.19	4.42	4.30
Punjab	306.0	1.24	1.80	2.28
Rajasthan	804.4	1.68	1.87	2.28
Sikkim	6.8	0.00	0.00	3.82
Tamil Nadu	767.1	1.02	1.40	2.71
Telangana	379.5	13.24	27.15	40.31
Tripura	41.2	0.83	0.58	0.73

Uttar Pradesh	2340.9	4.74	3.77	4.32
Uttarakhand	115.6	2.10	6.21	4.84
West Bengal	987.6	0.72	0.52	0.41
A&N Islands	4.0	1.25	2.00	7.00
Chandigarh	12.2	1.39	1.23	2.21
D&N Haveli and Daman & Diu	12.0	0.25	0.42	0.42
Delhi	211.0	0.80	1.69	3.25
Jammu & Kashmir	135.4	0.89	1.14	1.28
Ladakh	3.0	0.33	1.67	1.00
Lakshadweep	0.7	4.29	1.43	1.43
Puducherry	16.2	0.62	0.00	3.95
TOTAL ALL INDIA	**13797.5**	3.63	3.84	4.78



The presented data offers a snapshot of cybercrime rates per lakh population across various states and union territories in India for the years 2020, 2021, and 2022. As we scrutinize the figures, several observations align with the study objectives:

- **Inter-State Variations:** There is a noticeable variability in cybercrime rates among states, with Telangana exhibiting a substantial increase from 13.24 in 2020 to 40.31 in 2022. Karnataka also shows a substantial rise from 15.93 in 2020 to 18.63 in 2022, highlighting inter-state disparities in cybercrime occurrences.
- **Temporal Trends:** The temporal trends, reflected in the increasing or decreasing cybercrime rates over the three years, provide valuable insights. States like Assam and Kerala experienced notable fluctuations, showcasing the dynamic nature of cybercrime patterns over the study period.
- **Small Territories with High Rates:** Smaller territories such as Lakshadweep and A&N Islands demonstrate relatively high cybercrime rates per lakh population, indicating potential vulnerabilities in these regions that merit further investigation.

- **Regional Dynamics:** The cybercrime rates in states like Maharashtra, Delhi, and Telangana, which are technology and commerce hubs, underscore the potential influence of economic and technological factors on cybercrime occurrences.

Hence, the presented data establishes a foundation for the subsequent analytical phase of the study, enabling a nuanced exploration of trends and patterns in cybercrime rates across diverse regions in India.

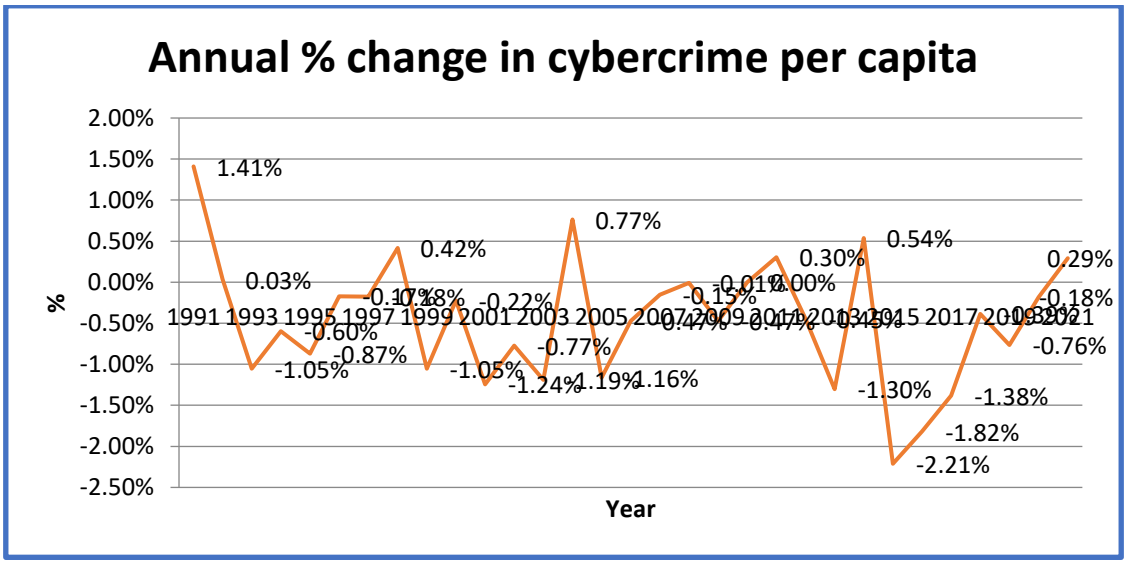
Cybercrime Motives % per lakh population- 2022

Following dataset on cybercrime motives as a percentage of the population in 2022 provides a panoramic view of the varied motivations driving cyber offenses across Indian states and union territories. Each percentage denotes the prevalence of specific motives, ranging from personal vendettas to financial fraud and sexual exploitation.

Cybercrime Motives % per lakh population- 2022										
State/UT	Personal Revenge	Emotional motives like Anger etc	Fraud	Extortion	Causing Disrepute	Prank	Sexual Exploitation	Political Motives	Others	Total
Andhra Pradesh	20.2%	1.9%	275.9%	8.9%	0.2%	0.6%	27.7%	2.3%	95.2%	441.4%
Arunachal Pradesh	0.0%	12.9%	25.8%	12.9%	0.0%	0.0%	6.5%	0.0%	32.3%	90.3%
Assam	72.4%	18.0%	52.1%	177.0%	9.3%	14.9%	13.0%	4.2%	126.0%	488.3%
Bihar	8.9%	7.6%	96.2%	6.1%	1.2%	0.9%	7.1%	0.1%	1.1%	129.1%
Chhattisgarh	0.0%	0.7%	19.7%	1.7%	18.0%	0.0%	11.7%	0.0%	94.8%	146.6%
Goa	6.4%	0.0%	414.0%	6.4%	101.9%	0.0%	31.8%	6.4%	6.4%	573.2%
Gujarat	1.1%	2.1%	112.1%	3.4%	52.3%	1.1%	10.2%	0.1%	16.1%	199.8%
Haryana	3.7%	1.0%	54.7%	11.7%	5.0%	0.7%	44.7%	0.7%	104.8%	227.2%
Himachal Pradesh	4.0%	1.3%	37.6%	18.8%	13.4%	0.0%	20.2%	0.0%	6.7%	103.5%
Jharkhand	0.3%	0.0%	228.4%	5.4%	0.0%	0.0%	4.9%	0.0%	7.7%	247.1%
Karnataka	4.7%	9.3%	1635.5%	56.2%	4.0%	0.1%	50.1%	1.3%	98.5%	1862.6%
Kerala	19.9%	6.2%	90.5%	7.0%	10.1%	0.6%	61.1%	0.0%	19.1%	216.6%
Madhya	0.5%	1.3%	39.9%	1.3%	29.2%	1.5	11.9%	0.0%	10.5	96.2%

Pradesh						%			%	
Maharashtra	5.2%	3.0%	438.6%	10.3%	2.5%	0.0%	62.6%	0.0%	132.7%	656.0%
Manipur	0.0%	0.0%	18.8%	0.0%	0.0%	0.0%	34.4%	3.1%	0.0%	56.3%
Meghalaya	3.0%	3.0%	102.1%	12.0%	12.0%	0.0%	45.0%	3.0%	36.0%	225.2%
Mizoram	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	8.1%	8.1%
Nagaland	0.0%	0.0%	9.0%	0.0%	0.0%	0.0%	4.5%	0.0%	0.0%	18.0%
Odisha	0.0%	15.4%	397.6%	0.0%	0.0%	0.0%	3.0%	0.0%	14.3%	430.3%
Punjab	6.2%	2.9%	106.5%	9.5%	6.9%	1.6%	32.0%	0.7%	57.2%	227.8%
Rajasthan	3.2%	1.7%	77.2%	12.2%	12.6%	0.2%	33.7%	0.2%	79.6%	227.9%
Sikkim	29.4%	0.0%	220.6%	29.4%	0.0%	0.0%	0.0%	29.4%	0.0%	382.4%
Tamil Nadu	6.4%	5.1%	215.1%	4.0%	2.2%	0.1%	24.6%	3.8%	7.4%	271.4%
Telangana	6.9%	57.2%	2896.2%	117.8%	0.0%	0.0%	40.1%	7.1%	620.3%	4030.8%
Tripura	7.3%	0.0%	29.1%	2.4%	12.1%	0.0%	4.9%	4.9%	2.4%	72.8%
Uttar Pradesh	1.6%	4.6%	192.5%	53.4%	37.7%	2.5%	23.2%	2.4%	110.4%	432.2%
Uttarakhand	0.0%	0.0%	134.1%	306.2%	1.7%	0.0%	31.1%	0.0%	0.9%	483.6%
West Bengal	1.6%	0.7%	9.6%	1.1%	0.3%	0.4%	0.9%	0.1%	25.7%	40.6%
A&N Islands	50.0%	0.0%	150.0%	0.0%	75.0%	0.0%	125.0%	0.0%	300.0%	700.0%
Chandigarh	0.0%	0.0%	32.8%	0.0%	8.2%	0.0%	73.8%	0.0%	90.2%	221.3%
D&N Haveli and Daman & Diu	8.3%	0.0%	0.0%	8.3%	0.0%	0.0%	25.0%	0.0%	0.0%	41.7%
Delhi	0.9%	0.0%	131.8%	3.8%	0.0%	3.8%	25.6%	0.0%	154.0%	324.6%

Jammu & Kashmir	0.0%	0.0%	78.3%	7.4%	1.5%	1.5 %	11.1%	0.0%	17.7 %	127.8 %
Ladakh	0.0%	0.0%	0.0%	0.0%	0.0%	0.0 %	0.0%	0.0%	100.0 %	100.0 %
Lakshadweep	0.0%	0.0%	142.9 %	0.0%	0.0%	0.0 %	0.0%	0.0%	0.0%	142.9 %
Puducherry	0.0%	0.0%	0.0%	24.7%	0.0%	0.0 %	0.0%	0.0%	370.4 %	395.1 %
TOTAL ALL INDIA	6.2%	5.7%	309.5 %	26.4%	13.8%	1.3 %	24.9%	1.2%	78.2 %	477.6 %



The data on cybercrime motives as a percentage of the population in 2022 reveals intriguing patterns across Indian states and union territories. Each motive category, expressed as a percentage, offers a nuanced understanding of the diverse motivations behind cybercrimes. Several key observations align with the study objectives:

Varied Motivations: Different states exhibit diverse motives for cybercrimes, ranging from personal revenge and emotional triggers to financial fraud, causing disrepute, and even sexual exploitation. The wide spectrum of motives underscores the multifaceted nature of cybercrime.

State-Specific Trends: States like Telangana and Karnataka show significant spikes in specific motive categories, such as emotional motives and financial fraud. Meanwhile, states like Goa and Maharashtra demonstrate a notable prevalence of sexual exploitation motives. These trends emphasize the importance of considering regional dynamics in understanding cybercrime motivations.

Dominant Motives: Across the entire dataset, the most prevalent cybercrime motives include financial fraud, causing disrepute, and sexual exploitation. These dominant motives collectively contribute to the intricate landscape of cybercrimes occurring throughout the country.

Territorial Disparities: Smaller territories like A&N Islands and Chandigarh exhibit strikingly high percentages for certain motives, showcasing potential vulnerabilities or distinctive patterns in these regions.

Understanding impact of population density and time on annual percentage change in cybercrime

The hypothesis tested in following regression model posits that the annual percentage change in cybercrime can be predicted by two factors: the population density (expressed as Per 100K Population) and time.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.475[a]	.225	.170	.028681	1.578

a. Predictors: (Constant), Per 100K Population, Time

b. Dependent Variable: Annual % Change in cybercrime

ANOVA

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	.007	2	.003	4.074	.028[b]
	Residual	.023	28	.001		
	Total	.030	30			

a. Dependent Variable: Annual % Change in cybercrime

b. Predictors: (Constant), Per 100K Population, Time

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	-.546	.195		-2.801	.009	-.946	-.147
	Time	.008	.003	2.250	2.562	.016	.002	.014
	Per 100K Population	.101	.037	2.419	2.754	.010	.026	.175

a. Dependent Variable: Annual % Change in cybercrime

Residuals Statistics

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	-.04589	.01925	-.01697	.014947	31

Residual	-.059256	.066545	.000000	.027708	31
Std. Predicted Value	-1.935	2.423	.000	1.000	31
Std. Residual	-2.066	2.320	.000	.966	31
a. Dependent Variable: Annual % Change in cybercrime					

The regression analysis aimed to investigate the predictors influencing the annual percentage change in cybercrime, considering population density (Per 100K Population) and time as key factors. The model demonstrated a moderate fit, explaining approximately 22.5% of the variance in the annual percentage change in cybercrime. The overall model was found to be statistically significant, indicating that at least one of the predictors significantly contributes to the observed variance. Both time and population density exhibited positive coefficients, with statistically significant p-values, suggesting that over time and with higher population density, there is a meaningful increase in the annual percentage change in cybercrime. The residuals analysis further affirmed the model's reliability, with mean residuals close to zero and standardized residuals within an acceptable range.

5. Conclusion

This study delves into the intricate dynamics of cybercrime trends and patterns in India, employing a comprehensive analysis encompassing statistical, temporal, and population-related dimensions. The study underscores the significance of considering both time and population density as influential factors in understanding the annual percentage change in cybercrime. The positive coefficients associated with these variables suggest a discernible upward trend over time and an increased vulnerability in regions with higher population density. The overall model's statistical significance and reliability, as indicated by the residuals analysis, affirm the robustness of the findings. As the digital landscape continues to evolve, these insights contribute to a nuanced comprehension of the cybercrime landscape in India, providing valuable information for policymakers, law enforcement agencies, and cybersecurity professionals. The implications extend beyond statistical correlations, emphasizing the need for proactive measures, strategic interventions, and continuous vigilance to effectively mitigate and counter the growing challenges posed by cybercrime in the country.

References

1. Farsi, M., Daneshkhah, A., Far, A. H., Chatrabgoun, O., & Montasari, R. (2018). Crime data mining, threat analysis and prediction. *Cyber Criminology*, 183–202.
2. Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology*, *11*(3), 222–239.
3. Nag, A., Ranjan, R., & Kumar, C. N. S. V. (2022). An Approach on Cyber Crime Prediction Using Prophet Time Series. *2022 IEEE 7th International Conference for Convergence in Technology (I2CT)*, 1–5.
4. Rajput, B., & Rajput, B. (2020). Emerging trends and patterns of cyber economic crimes. *Cyber*

Economic Crime in India: An Integrated Model for Prevention and Investigation, 97–142.

5. Sathyadevan, S., Devan, M. S., & Gangadharan, S. S. (2014). Crime analysis and prediction using data mining. *2014 First International Conference on Networks \& Soft Computing (ICNSC2014)*, 406–412.
6. Shah, N., Rajadhyaskha, A., & Hasan, N. (2022). *Overload, Creep, Excess--An Internet from India*.
7. Subashka Ramesh, S. S., & others. (2021). Using Big Data, An Extensible System for Forecasting and Analyzing Relations Among Crimes. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 7032–7040.