

“AN ANALYSIS OF CYBER CRIME TRENDS IN RAJSTHAN (2021-2023)”

JITENDRA KUMAR KALBI
SCHOLAR

DEPARTEMENT OF GEOGRAPHY, MADHAV UNIVERSITY, PINDWARA(RAJASTHAN)
Jitendrakalbi0@gmail.com

DR. DEVENDRA MUZALDA
PROFESOR

DEPARTEMENT OF GEOGRAPHY, MADHAV UNIVERSITY, PINDWARA(RAJASTHAN)
Devendramuzalda@gmail.com

Abstract

Rajasthan's increasing number of cases illustrates how the digital era has created new challenges for cybercrime. According to the State Crime Records Bureau, the number of cybercrime cases has grown from 1,504 in 2021 to 2,435 in 2023, which is a 62% increase in two years. Jaipur, Jodhpur, Alwar, and the surrounding areas are hotspots for cybercrime activity, especially for identity theft, impersonation, phishing, financial fraud, and social media-related crimes. The primary statute regulating cybercrime is the Information Technology Act, 2000, which provides legal guidance for issues such as identity fraud, impersonation, and online harassment. Although various initiatives have been undertaken, such as creating police cybercrime units and conducting various public awareness campaigns about cybercrime, enforcement continues to be inadequate because of a lack of technical abilities, inadequate manpower, and a lack of general public knowledge about the existence of these units. Therefore, the objective of this research is to emphasize the urgent need for stronger institutional frameworks, enhanced capacity building, and citizen-focused public awareness programs to eradicate cybercrime effectively. It is worth noting that while there have been recent scholarly interests regarding cybercrime, there is a lack of regionally focused research in Rajasthan, and therefore this study represents a valuable addition to the body of regional cybercrime academic literature.

Keywords: Cyber Crime, Cyber Crime Trends, Cyberspace Crime, Cybercrime Rajasthan.

Literature Review

Brenner (2010) researched how cybercrime worldwide has expanded with the introduction of digital technology resulting in multiple types of criminal activities including online fraud, identity theft, and online harassment. Although her analysis is at the global level; Brenner's findings are relevant to the situation in India where many of these same types of threats are manifesting.

Nath, Singh and Gupta (2018) looked closely at cybercrime trends in India and found a correlation between an increase in electronic commerce and online banking and an increase in phishing and digital financial fraud cases. Their report notes that while India's rapid digital transformation is good for business, it has also created greater opportunities for exploitation through cybercrime.

Singh (2021) researched the rise in digital transactions during the post-COVID-19 period in Rajasthan, particularly via UPI transactions, and found a direct correlation between a rise in cyber fraud cases and the increased use of digital technology.

The Rajasthan Police (2022) report shows that cybercrime reports are still on the rise in many areas of Rajasthan, particularly in Jaipur, Alwar and Jodhpur. The report also details the systemic issues preventing law enforcement

agencies from responding to this increase including a lack of staff training and technological infrastructure at the grass roots level.

Identified Research Gaps

Even with all these positives, there is still a lack of data on the comparative district level in terms of cybercrime in Rajasthan. There have been no structured investigations into the number of cases reported from year to year or how well law enforcement agencies have responded or how effective awareness campaigns have been conducted or how many people are actually aware of their rights and responsibilities regarding cybercrime during the time period of 2021 through 2023.

The purpose of this study will be to provide a systematic and structured evaluation of cybercrime trends in Rajasthan through an analysis of categories of trends within Rajasthan during the time period of 2021 to 2023 as well as comparisons based on how many cases have been reported per district through the establishment of institutional mechanisms.

Methodology

The purpose of this research paper is to use a descriptive design to investigate the occurrence and geographic location of cybercrime in the State of Rajasthan from 2021-2023 through quantitative analysis using secondary data reports and statistical analysis.

Data Sources:

Data sources for this study were obtained through the State Crime Records Bureau (SCRB) of Rajasthan, which contains government statistics on reported cyber crimes. Additional sources have been consulted including literature from the National Crime Records Bureau (NCRB), reports from the Rajasthan Police and academic articles related to this topic.

Time Frame:

The analysis will include three consecutive years (2021, 2022 and 2023) of data that will be used to identify trends in terms of the level of increase from year to year and the type of increase from one year to another.

Analytical Tools:

1. Year-on-Year Trend Analysis:

A line chart illustrated the pattern of cybercrime case volume each year.

2. District-Level Analysis - Comparison of Districts:

District-wise information was analysed to identify areas of high incidence such as Jaipur, Jodhpur, Alwar, Udaipur, etc.

3. Qualitative Evaluation:

Police reports as well as literature were reviewed to determine the institutional response to the matter (e.g., the establishment of cyber police stations, awareness campaigns, and the judiciary response).

Scope and Limitations:

This study uses only officially documented instances in its evaluations and will likely not capture the full extent of the cyber-crime problem due to lack of reporting. Many of the socio-economic variables examined, including literacy rates, digital penetration, and levels of awareness were referenced only from previously reported data, making it impossible to conduct a meaningful cause and effect analysis on these factors.

Objectives of the Study

The aims of this research included:

1. Understanding how cyberspace crime has developed over time from 2021 through 2023
2. Looking closely at where crime has occurred at the county level, and identifying areas where there are large concentrations of these types of crimes
3. Providing recommendations to improve public awareness about ways to protect themselves from cyberspace crime throughout Rajasthan

Data Analysis

The dataset consists of 33 districts within the Indian state of Rajasthan, and shows all cases registered for cyber-crime in 2021, 2022, and 2023. There are also estimates of the 2021 population, with an approximate total of 80,133,242.

Source S.C.R.B. Rajasthan 2021,2022,2023

S. N O.	DISTRICT	CASE REGISTERED (2021)	CASE REGISTERED (2022)	CASE REGISTERED (2023)	POPULATION ESTIMATE (2021)
1.	AJMER	100	102	59	2921923
2.	BHILWARA	43	91	81	2736753
3.	TONK	19	16	22	1587857
4	JAIPUR	310	379	595	7977509
9	JHUNGHNU	25	24	35	2270991
6	SIKAR	165	79	61	2984512
7	DAUSA	58	51	64	2930450
8	ALWAR	134	157	186	4304608
9	CHURU	3	14	22	2320155
10	SRI GANGANAGAR	37	30	48	2098585
11	HANUMANGARH	6	38	48	1977592
12	BHARATPUR	82	72	135	2941869
13	SWAIMADHOPUR	37	49	65S	1525395
14	DHOLPUR	4	55	5	1415065
15	KARALI	34	53	10	1689407
16	JODHPUR	151	127	178	4467955
17	JALORE	6	11	0	2770188
18	JAISALMER	7	16	40	843963
19	BARMER	69	95	96	3244528
20	PALI	5	7	27	2177391
21	SIROHI	23	38	21	1205824
22	KOTA	59	50	119	2298521
23	BUNDI	2	2	7	1226389
24	JHALAWAR	12	31	21	1596920
25	BARAN	22	12	27	1393547
26	UDAIPUR	9	21	157	3589396
27	BANSWARA	9	14	22	2147629
28	CHITTORGARH	5	7	3	1694289
29	DUNGERPUR	1	1	0	1639193
30	RAJSAMAND	10	16	42	1282469
31	PRATAOGARH	6	34	8	1010912
32	NAGPUR	26	76	44	3782721
33	BIKANER	13	32	59	2828347
	TOTAL	1504	1833	2435	80133242

The data was processed to perform the calculations:

Year-wise state-level rates: Cases per year divided by total population, multiplied by 100,000 for standardization.

District-wise metrics: Total cases (sum across years), average annual cases (total / 3), and crime rate (average annual cases / population × 100,000).

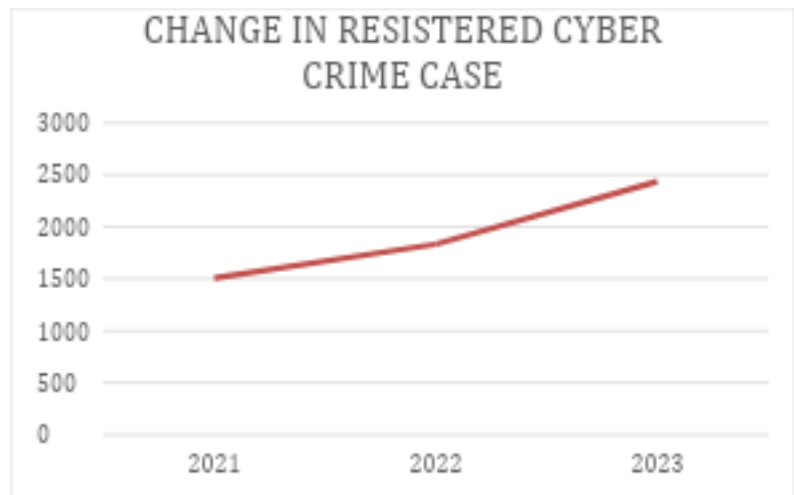
Categorization: Districts ranked by crime rate to identify top (high), low, and moderate levels.

Trends: Percentage change in cases year-over-year at state and district levels.

To arrive at these metrics: Sum the yearly cases for totals, divide by 3 for averages, then normalize by population (dividing average cases by population and multiplying by 100,000) to enable fair comparisons across districts of varying sizes.

Results

State-Level Trends: Cybercrime cases increased from 1,504 in 2021 to 1,833 in 2022 (21.9% rise) and 2,435 in 2023 (32.8% rise from 2022), representation of a 61.9% overall increase over the period. Crime rates per 100,000 population were 1.88 in 2021, 2.29 in 2022, and 3.04 in 2023, indicates a rapidly growing trend.



District-Wise Data: The full ranked list by crime rate is below (per 100,000 population, based on average annual cases):

District Crime Rate

Top (High) Districts (top 5 by rate): Jaipur City (5.37), Alwar (3.69), Sikar (3.41), Jodhpur (3.40), Kota (3.31). These account for near 45% of total cases.

Low Districts (bottom 5 by rate): Dungarpur (0.04), Jalore (0.20), Chittorgarh (0.30), Bundi (0.30), Churu (0.56).

Moderate Districts (middle 5 by rate): Pratapgarh (1.58), Hanumangarh (1.55), Dholpur (1.51), Baran (1.46), Jhalawar (1.34).

Discussion

The data indicate that upward trend in cybercrimes, with a 62% increase from 2021 to 2023, with references of national growth (e.g., India's cybercrimes rose 24% in 2022). Urban and semi-urban districts like Jaipur and Alwar dominate because that higher population density, internet penetration. For example, Reports have emerged of a rapid increase in cyber fraud in Bharatpur district (from 82 in 2021 to 135 in 2023), which a playing significant role in national cases and it also has a criminal history. Rural districts like Dungarpur show near-zero rates, this likely reflects underreporting rather than lack of crime as generalizing across population with limited digital access show that raw case numbers favour larger districts, but rates highlight hotspots like Swai Madhopur (3.30) even through it has only a moderately sized population. Factors such as economic disparities, nearness to urban centers (e.g., Alwar and Bharatpur is influence by NCR), and post-COVID digital shifts may contribute. Limitations include potential under reporting in the districts and lack of verification in the official district-wise 2023, which has done though state totals NCRB data for the various match.

Suggestions to Control Cyber Crime

1. Awareness & Education - Spread information of cyber safety knowledge through campaigns in schools, colleges, and village and use social media for awareness campaigns in local languages.
2. Police Strengthening - In every district open cyber police stations and give training to police on digital crimes.
3. Better Technology and Legal Support- In Rajasthan, build a modern cyber lab and use AI tools for detecting frauds, fake accounts, and phishing and introduce fast-track courts for cyber cases.
6. Rural Focus and Citizen Support - Train panchayat and rural police about cyber fraud and Launch a 24×7 cyber helpline in Rajasthan and promote easy complaint registration.

Reference

1. Brenner, S. (2010). *Cybercrime: Criminal threats from cyberspace*. Santa Barbara: Praeger.
2. Nath, V., Singh, A., & Gupta, R. (2018). Cybercrime in India: Emerging trends and challenges. *Journal of Information Security*, 12(3), 45–58.
3. Rajasthan Police. (2022). *Annual report on cybercrime in Rajasthan*. Jaipur: State Police Headquarters.
4. SCRB Rajasthan. (2023). *State Crime Records Bureau Report*. Jaipur: Government of Rajasthan.
5. Singh, R. (2021). Digital transactions and rising cyber frauds in Rajasthan post-COVID-19. *Indian Journal of Criminology*, 49(2), 112–128.
6. SCRB Rajasthan. (2021). *State Crime Records Bureau Report*. Jaipur: Government of Rajasthan.
7. SCRB Rajasthan. (2022). *State Crime Records Bureau Report*. Jaipur: Government of Rajasthan.
8. UNFPA India (2023). *District level population projection selected state in India 2021 and 2026*

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.