



Research Article

Comparative Analysis of Registered Cyber-Crimes among Rajasthan and Its Neighbouring States

Deepak Kumar Parewa^{1*}, Deepa Mordia²

^{1,2}Dept. of Statistics, University of Rajasthan, Jaipur, India

*Corresponding Author: deepakparewa30@gmail.com

Received: 10/Oct/2024; Accepted: 08/Nov/2024; Published: 31/Dec/2024

Abstract— This research paper examines the trends and comparative analysis of registered cyber-crimes across Rajasthan and its neighbouring states—Gujarat, Haryana, Madhya Pradesh, Punjab, and Uttar Pradesh—from 2012 to 2021. Rajasthan, a prominent state in India, has witnessed rapid digital growth alongside its traditional socio-economic development. However, this growth has also brought an increase in cyber-crimes. The study utilizes secondary data analysis to explore the annual variations in both the absolute numbers and percentages of cyber-crimes reported. Descriptive statistics, ANOVA, and Tukey's HSD tests are employed to analyze the differences in cyber-crime prevalence among the states. Findings reveal significant disparities in cyber-crime rates, with Rajasthan consistently showing a higher prevalence compared to most neighbouring states. Uttar Pradesh emerges as particularly vulnerable, reporting the highest percentage of cyber-crimes. These results underscore the need for tailored regional strategies to enhance cyber security measures and mitigate the growing threat of cyber-crimes across the studied states.

Keywords— Cyber Crimes, Rajasthan and Neighbouring States, Comparative Analysis, Cyber Security

1. Introduction

The digital revolution has transformed the socio-economic landscape globally, and India is no exception. As internet penetration deepens and digital platforms become integral to daily life, cyber-crimes have emerged as a significant challenge. Cyber-crimes include fraud, identity theft, hacking, and cyber bullying (Kshetri, 2010). These crimes not only threaten individual privacy and security but also have broader implications for national security and economic stability (Singh, 2013).

Rajasthan, a prominent state in India, has witnessed rapid digital growth alongside its traditional socio-economic development. However, this growth has also brought an increase in cyber-crimes. Understanding the dynamics of cyber-crimes in Rajasthan and comparing them with those in its neighbouring states—Punjab, Haryana, Uttar Pradesh, Madhya Pradesh, and Gujarat—provides valuable insights into the regional variations and commonalities in cyber-crime patterns (NCRB, 2021).

This research paper aims to conduct a comparative analysis of registered cyber-crimes in Rajasthan and its neighbouring states. By examining the types, frequency, and trends of these crimes, the study seeks to identify underlying factors contributing to regional differences. Additionally, the paper

explores the effectiveness of existing legal frameworks and enforcement mechanisms in addressing cyber-crimes, offering recommendations for policy enhancements to improve cyber security in the region (Gupta & Bajaj, 2017).

The analysis is based on data collected from official crime reports, government publications, and interviews with law enforcement officials and cyber security experts. This comprehensive approach will enable a nuanced understanding of the cyber-crime landscape, highlighting both the challenges and opportunities for strengthening cyber resilience in Rajasthan and its neighbouring states.

2. Review of Literature

Whelan, C. et. al (2024) argued about von Lampe's primary domains of organized crime, the paper emphasizes the relevance of crime in both physical and digital realms. It advocates for moving beyond debates about the existence of organized cybercrime to exploring new research questions proposing a reconceptualization of organized cybercrime.

Syahril, M. A. F. (2023) explored the regulatory efforts related to Law in Indonesia, emphasizing its role in recognizing and protecting human rights. The research specifically examines the extent of cybercrime handling in the City of Parepare, employing both normative and empirical

methods. The findings reveal that cybercrime remains a significant issue in Parepare, reflecting broader human rights violations. Despite the regulatory framework, the handling of cybercrime cases is ineffective. The existing regulations fail to provide a sufficient deterrent effect for perpetrators, leading to the continued prevalence of cybercrimes in the region.

Khan, S. et. al (2022) addressed the gap between rapidly advancing technology and the lagging cybercrime legislation. It emphasizes the critical role of legislation in combating cybercrime, highlighting the importance of efficient and up-to-date legal responses. The study systematically reviews literature across seven academic databases, ultimately analyzing 72 relevant studies out of 548 initial articles. The results emphasize the necessity of comprehensive and current cybercrime legislation to effectively counter cybercrime. The findings suggest that enhancing and updating legal frameworks is crucial to address the growing number of cybercrime incidents. The paper also identifies future research directions and practical implications for policymakers to strengthen legislative measures against cybercrime.

Horan, C., & Saiedian, H. (2021) focused on digital forensics and open-source intelligence as the main categories of cyber investigations, comparing various tools and methods used by investigators. It establishes criteria for evaluating the effectiveness and applicability of these tools. The findings reveal that no single tool can gather all necessary evidence, requiring a combination of tools for effective investigations. In open-source technologies, natural language processing is highlighted as the most versatile and useful tool. This comparison underscores the importance of using a multifaceted approach in cyber investigations.

Ch, R., Gadekallu et. al (2020) stated that internet usage has surged in the past decade, leading to a concurrent rise in cybercrime, projected to cost \$6 trillion annually by 2021. Cybercriminals exploit system vulnerabilities for financial gain and other benefits, with traditional manual and technical methods often failing to curb these attacks. This study addresses the gap by proposing a tool to predict and classify cybercrimes based on both structured and unstructured data. The tool, tested on India-based data, achieves 99% accuracy in classifying offenses, highlighting the potential of security analytics combined with data analytic approaches in combating cybercrime.

3. Research Gap

Despite the growing concern over cybercrime in India across different states, particularly Rajasthan and its neighbouring states. Existing literature often focuses on national-level data or individual state reports, failing to provide a detailed comparative analysis that could reveal regional patterns and discrepancies. Additionally, there is limited research examining the effectiveness of current legal frameworks and enforcement mechanisms in addressing cybercrime within

these states. This gap highlights the need for an in-depth comparative analysis that not only quantifies and categorizes cybercrimes but also evaluates the regional effectiveness of legal and enforcement responses. Such a study could inform more targeted and effective policy interventions, ultimately enhancing cyber security across the region.

4. Objectives

- i. To analyze the trend of cyber-crimes registered and the percentage of cyber-crimes relative to the
- ii. total reported in Rajasthan and its neighboring states (Gujarat, Haryana, Madhya Pradesh, Punjab, and Uttar Pradesh) from 2012 to 2021.
- iii. To identify significant differences in the percentage of cyber-crimes registered among Rajasthan and its neighboring states.

5. Research Methodology

For the comparative analysis of registered cyber-crimes among Rajasthan and its neighboring states, the research methodology involved gathering annual data on the number and percentage of cyber-crimes registered in study states from 2012 to 2021. Descriptive statistics, including mean, standard deviation, and ANOVA, were employed to analyze the data and compare the mean percentages of cyber-crimes across these states. Tukey's HSD test is used to identify significant differences in the mean percentages of cyber-crimes between pairs of states. The research methodology aimed to provide insights into the trends and variations in cyber-crime rates among these states, drawing implications for policy interventions to address cyber security challenges effectively

6. Results with Discussion

The comparison of annual registered cybercrimes between Rajasthan and its neighbouring states from 2012 to 2021 reveals several insights. Rajasthan consistently reports substantial numbers of cyber-crimes throughout the decade, with notable peaks in 2018, 2019, and 2020. In 2019, Rajasthan registered the highest number of cyber-crimes among all states, reaching 17,762 cases, significantly surpassing its neighbours. Uttar Pradesh consistently ranks high each year, reflecting its status as a frequent target for cyber-crimes within the region. Gujarat and Punjab generally report lower numbers compared to Rajasthan and Madhya Pradesh, which exhibit varying trends over the years. These variations highlight the dynamic nature of cyber security challenges across the states, suggesting the need for tailored strategies and collaborative efforts to address cyber-crime effectively.

Table 1. Trend Analysis for Rajasthan and neighbour states: Number of cyber-crimes registered

Rajasthan and neighbour states - Number of cyber-crimes registered						
Year	GUJARAT	HARYANA	MADHYA PRADESH	PUNJAB	RAJASTHAN	UTTAR PRADESH
2012	68	66	142	72	147	205
2013	61	112	282	146	239	372
2014	227	151	289	226	697	1737
2015	242	224	231	149	949	2208
2016	362	401	258	102	941	2639
2017	458	504	490	176	1304	4971
2018	702	418	740	239	1104	6280
2019	784	564	602	243	1762	11416
2020	1283	656	699	378	1354	11097
2021	1536	622	589	551	1504	8829

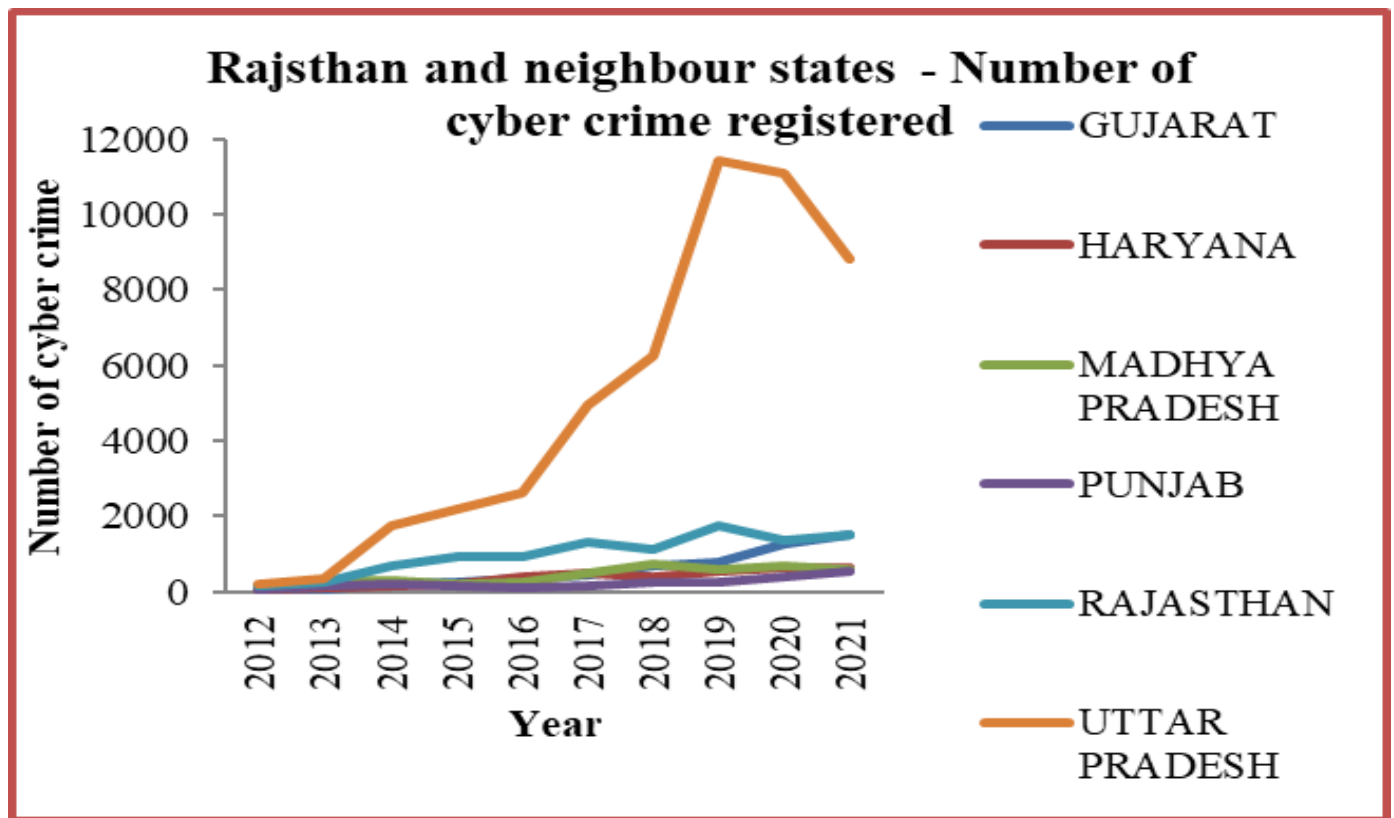


Figure 1 Rajasthan and neighbour states: Number of cyber-crimes registered

Table 2. Trend Analysis for Rajasthan and neighbour states (% of cyber-crimes registered)

Rajasthan and neighbour states - % of cyber-crimes registered						
Year	GUJARAT	HARYANA	MADHYA PRADESH	PUNJAB	RAJASTHAN	UTTAR PRADESH
2012	2.36	2.29	4.94	2.50	5.11	7.13
2013	1.40	2.57	6.47	3.35	5.49	8.54
2014	2.36	1.57	3.00	2.35	7.24	18.05
2015	2.09	1.93	1.99	1.29	8.19	19.05
2016	2.94	3.26	2.09	0.83	7.64	21.43
2017	2.10	2.31	2.25	0.81	5.98	22.81
2018	2.58	1.53	2.72	0.88	4.05	23.05
2019	1.75	1.26	1.35	0.54	3.94	25.52
2020	2.56	1.31	1.40	0.76	2.71	22.18
2021	2.90	1.17	1.11	1.04	2.84	16.67

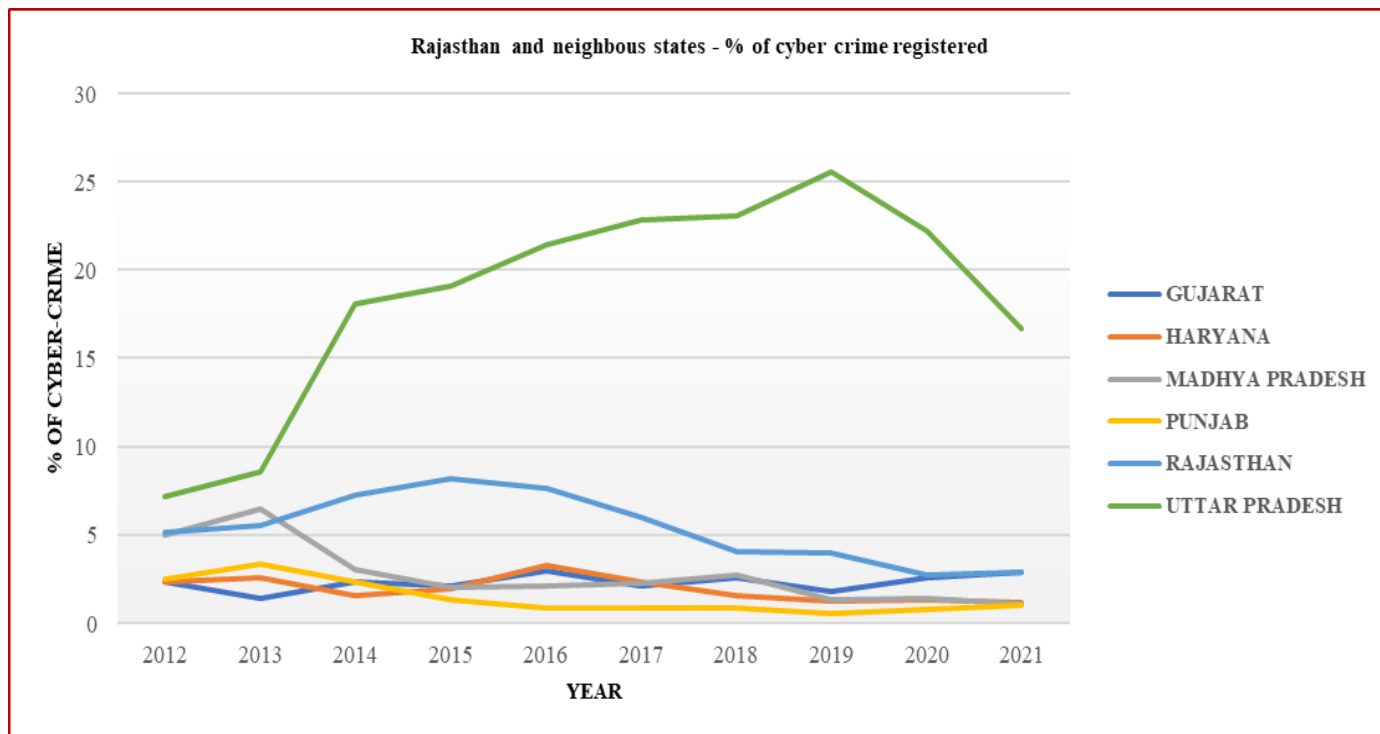


Figure 2. Rajasthan and neighbour states: % of cyber-crimes registered

The data illustrates the percentage of cyber-crimes relative to the total crimes registered in each state annually. Rajasthan consistently maintains a relatively higher percentage compared to its neighbours for most years, indicating a significant share of cyber-crimes within the region. Uttar Pradesh, while also showing a notable percentage, exhibits fluctuations across the years, reaching peaks in 2017 and gradually declining thereafter. Gujarat and Haryana generally report lower percentages, suggesting a comparatively lower incidence of cyber-crimes relative to their total crime rates. Madhya Pradesh and Punjab show varying percentages over the years, with Madhya Pradesh registering a higher

percentage in earlier years but stabilizing in recent years. Overall, the data highlights Rajasthan's notable presence in cyber-crime statistics among its neighbouring states, emphasizing the need for targeted interventions and collaborative efforts to address cyber security challenges effectively across the region.

Null Hypothesis (H₀): There is no significant difference in the mean percentage of cyber-crimes registered among Rajasthan and its neighbouring states.

Alternative Hypothesis (H₁): There is a significant difference in the mean percentage of cyber-crimes registered among Rajasthan and its neighbouring states.

Table 3. Rajasthan and neighbour states: Descriptives - % of cyber-crimes registered

State	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
				Lower Bound	Upper Bound		
				Rajasthan	5.32		
Gujarat	2.30	0.485	0.153	1.957	2.651	1.40	2.94
Haryana	1.92	0.679	0.215	1.434	2.406	1.17	3.26
Madhya Pradesh	2.73	1.714	0.542	1.506	3.958	1.11	6.47
Punjab	1.44	0.951	0.301	0.755	2.115	0.54	3.35
Uttar Pradesh	18.44	6.173	1.952	14.027	22.859	7.13	25.52
Total	5.36	6.593	0.851	3.656	7.062	0.54	25.52

Table 4. ANOVA

ANOVA						
	Sum of Squares	df	Mean Square	F	Sig.	
Between Groups	2146.513	5	429.303	55.444	0.000	
Within Groups	418.119	54	7.743			
Total	2564.632	59				

Table 5. Multiple Comparisons

Multiple Comparisons							
(I) State		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval		
					Lower Bound	Upper Bound	
Tukey HSD	Rajasthan	Gujarat	3.015	1.244	0.167	-0.662	6.692
		Haryana	3.399	1.244	0.085	-0.278	7.076
		Madhya Pradesh	2.587	1.244	0.314	-1.090	6.264
		Punjab	3.88400*	1.244	0.033	0.207	7.561
		Uttar Pradesh	-13.12400*	1.244	0.000	-16.801	-9.447
	Gujarat	Haryana	0.384	1.244	1.000	-3.293	4.061
		Madhya Pradesh	-0.428	1.244	0.999	-4.105	3.249
		Punjab	0.869	1.244	0.981	-2.808	4.546
		Uttar Pradesh	-16.13900*	1.244	0.000	-19.816	-12.462
	Haryana	Madhya Pradesh	-0.812	1.244	0.986	-4.489	2.865
		Punjab	0.485	1.244	0.999	-3.192	4.162
		Uttar Pradesh	-16.52300*	1.244	0.000	-20.200	-12.846
	Madhya Pradesh	Punjab	1.297	1.244	0.901	-2.380	4.974
		Uttar Pradesh	-15.71100*	1.244	0.000	-19.388	-12.034
Punjab	Uttar Pradesh	-17.00800*	1.244	0.000	-20.685	-13.331	

*. The mean difference is significant at the 0.05 level.

Table 6. % of cyber-crimes registered

% of cyber-crimes registered				
State		Subset for alpha = 0.05		
		1	2	
Tukey HSD ^a	Punjab	1.435		
	Haryana	1.920	1.920	
	Gujarat	2.304	2.304	
	Madhya Pradesh	2.732	2.732	
	Rajasthan		5.319	
	Uttar Pradesh			18.443
	Sig.	0.901	0.085	1.000
Tukey B ^a	Punjab	1.435		
	Haryana	1.920	1.920	
	Gujarat	2.304	2.304	
	Madhya Pradesh	2.732	2.732	
	Rajasthan		5.319	
Uttar Pradesh			18.443	

Means for groups in homogeneous subsets are displayed.

a. Uses Harmonic Mean Sample Size = 10.000.

Discussion: The analysis of the percentage of cyber-crimes registered across Rajasthan and its neighbouring states i.e., Gujarat, Haryana, Madhya Pradesh, Punjab, and Uttar Pradesh reveals significant variations and trends. An ANOVA test shows a statistically significant difference among the states ($F(5, 54) = 55.444, p < 0.001$), indicating that at least one state significantly differs from the others in terms of the percentage of cyber-crimes registered. Tukey's HSD post-hoc tests further elucidate these differences. Rajasthan (Mean = 5.32%) consistently shows a significantly higher proportion of cyber-crimes compared to Gujarat (Mean = 2.30%), Haryana (Mean = 1.92%), Madhya Pradesh (Mean = 2.73%), Punjab (Mean = 1.44%), and Uttar Pradesh (Mean = 18.44%). Uttar Pradesh, with the highest mean percentage, significantly differs from all other states, highlighting its unique position in cyber-crime prevalence.

7. Conclusion

Rajasthan stands out with a mean percentage of 5.32% of registered cyber-crimes, reflecting a notable presence within the region despite variability across the years. This suggests a relatively higher vulnerability to cyber security threats compared to its neighbouring states. Conversely, Uttar Pradesh significantly higher mean percentage underscores its elevated exposure to cyber-crimes, indicating a critical area for targeted cyber security measures and policy interventions. These findings underscore the importance of tailored strategies to address cyber security challenges effectively across different states in India.

References

- [1] Kshetri, N., *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Springer, **2010**.
- [2] Singh, A., "Cyber Crime in the Digital Age: Challenges and Solutions," *Indian Journal of Criminology*, Vol.41, Issue.1, pp.15-29, **2013**.
- [3] Gupta, M., & Bajaj, S., "Cyber Crime and Security: A Study of Select States in India," *Journal of Cybersecurity Studies*, Vol.4, Issue.2, pp.75-89, **2017**.
- [4] Ch, R., Gadekallu, T. R., Abidi, M. H., & Al-Ahmari, A., "Computational system to classify cyber-crime offenses using machine learning," *Sustainability*, Vol.12, Issue.10, pp.4087, **2020**.
- [5] National Crime Records Bureau (NCRB), *Crime in India 2020: Statistics*, Ministry of Home Affairs, Government of India, **2021**.
- [6] Horan, C., & Saiedian, H., "Cybercrime investigation: Landscape, challenges, and future research directions," *Journal of Cybersecurity and Privacy*, Vol.1, Issue.4, pp.580-596, **2021**.
- [7] Khan, S., Saleh, T., Dorasamy, M., Khan, N., Tan Swee Leng, O., & Gale Vergara, R., "A systematic literature review on cybercrime legislation," *F1000Research*, Vol.11, pp.971, **2022**.
- [8] Shah, N., Rajadhyaskha, A., & Hasan, N., "Overload, Creep, Excess--An Internet from India," *In the Proceedings of the 2022 International Conference on Internet Studies*, India, pp.542-545, **2022**.
- [9] Syahril, M. A. F., "Cyber Crime in terms of the Human Rights Perspective," *International Journal of Multicultural and Multireligious Understanding*, Vol.10, Issue.5, pp.119-130, **2023**.
- [10] Whelan, C., Bright, D., & Martin, J., "Reconceptualising organised (cyber) crime: The case of ransomware," *Journal of Criminology*, Vol.57, Issue.1, pp.45-61, **2024**.

AUTHORS PROFILE

Deepak Kumar Parewa earned a B.Sc. And M.Sc. from University of Rajasthan Jaipur in 2017 and 2019. Currently pursuing a Ph.D. with a specialization in Statistics, Department of Statistics from University of Rajasthan, Jaipur. He is a member of ISROSET since 2024. He has published more than two research paper in reputed international journals and conferences.



Dr Deepa Mordia earned a B.Sc., M.Sc. and Ph.D. from University of Rajasthan, Jaipur in 2001, 2003 and 2018. She is a currently working as Assistant professor in Department of Statics since from University of Rajasthan Jaipur since 2018. She has 18 years of teaching experience and 12 years of research experience. The earlier job involved teaching the Under Graduate and Post Graduate student of the Management branch (MBA, BBA), Computer Science, Electronics Mechanical, Civil, Computer Application and Post Graduate student of Bio-informatics and M.Tech She has published more than 50 resources paper in reputed International General and Conference.

