WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

The Threat of Growing Cyber Crime in India: A Comparative Study

[1]Vanita Patil, [2]Suhani Kachare, [3]Pranali Jadhav.

[1]Prof, Department of Computer Application and Management
[2,3]Student, Department of Computer Application.
D.Y. Patil Institute of Computer Applications and Management, Akurdi, Pune.

ABSTRACT

This paper provides an analysis of the escalating threat of cybercrimes in India from 2018-2022 and online and social media crimes reported from 2020-2024, exploring the types, causes, and impacts of these crimes. It also highlights the preventive measures and technologies used to combat cybercrimes, providing insights into the role of data analysis. A comprehensive literature review is undertaken to examine prior research in the field, followed by an analysis of the proposed work, its outcomes, and a comparison with previous studies.

Keywords: Cyber security, cybercrime, cyber-attack, hacking, IT act, IPC, SLL, social media crime;

1. Introduction

Cybercrime has emerged as one of the most pressing threats to India's digital economy and social fabric. It happens in virtual world but causes real harm. With rapid digitization, the number of offences involving hacking, online fraud, identity theft, and social media exploitation has risen at an alarming rate. According to the NCRB, cybercrime cases increased steadily between 2018-2022, with notable spikes in states like Uttar Pradesh, Karnataka, Maharashtra, and Telangana. Simultaneously, the expansion of social media crimes from 2020 onwards created new channels for fraud, harassment, and misinformation.

This study provides a comparative analysis of cybercrime trends in India, examining state-wise patterns (2018-2022), offences under IT Act, IPC, SLL and online and social media crime (2020-2024).

2. Theoretical Background

2.1 Cybercrime:

As defined under the Information Technology (IT) Act 2000, encompasses unlawful acts where computers, networks, or digital platforms are either the tool or target. These include:

2.2 Crimes against individuals:

identity theft, cyber-stalking, defamation, online harassment.

2.3 Crimes against property:

hacking, data theft, credit card fraud.

2.4 Crimes against society/government:

cyber terrorism, denial-of-service attacks, online misinformation campaigns.

2.5 Phishing:

Phishing is a technique used to illicitly acquire sensitive personal details like passwords, usernames, credit-card information and digital signatures by exploiting internet, networks, websites, and online payment systems.[8]

2.6 Online Fraud:

This encompasses cybercrimes involving identity theft, phishing, and hacking activities aimed at defrauding individuals of their finances. Internet fraud suggests to crimes facilitated by internet services and software to deceive or exploit victims.[8]

2.7 Denial of Service (DoS) Attack:

A DoS attack involves disrupting the normal functioning of a device or network, preventing authorized users from accessing the system.[8]

2.8 Hacking:

Hacking refers to the unauthorized access of computer or network, often carried out by a skilled programmer, known as a hacker.[8]

2.9 Credit Card Fraud:

It involves unauthorized access and use of another person's credit card details to make purchases, carry out transactions, or open new accounts.[8]

2.10 Cyber-Stalking/Bullying:

This term refers to the act of stalking, harassing, or threatening an individual, group, or organization through the internet or other technological means.[8]

3. Literature Survey

Numerous studies have highlighted the alarming growth of cybercrime in India:

- Technological advancements have significantly contributed to cybercrime, posing serious risks not only to individual safety but also to national security.[9]
- Research shows that over 60% of cybercrime cases reported between 2018 and 2020 were related to fraud, with the IT Act being pivotal in legal proceedings.[8]
- Emerging threats like phishing, ransomware, and social engineering attacks are particularly detrimental to developing nations with limited digital awareness.[5]
- To reduce cybercrime, it is crucial to develop more secure and efficient technology and networks to safeguard individuals' vital data. Simultaneously, awareness programs targeting groups like women, children, and senior citizens are necessary to educate them about various cybercrimes and how to protect their data through cybersecurity practices.[6]
- Government and non-government organizations should focus on educating the public about the risks and threats of cybercrime and provide guidance on protecting personal data and systems from unauthorized access. Anti-crime agencies also need to enhance their efforts to raise awareness across communities, businesses, and enterprises.[21]
- Cybercrime is a global concern, and as it continues to grow, it presents opportunities for significant improvement and countermeasures.[7]
- Previous studies also highlight issues such as underreporting, jurisdictional challenges, and the lack of cyber-literacy, all of which hinder effective enforcement.

However, there is a gap in research when it comes to comparing cybercrime trends across different states and how they evolve with emerging digital platforms. The aim of this paper is to fill this gap by analysing data from both social media-related offenses and general IT Act violations, examining the growth patterns of these trends.

4. Proposed Work

The proposed study:

1. Comparative Analysis of State-wise Cybercrime (2018-2022): Using NCRB data, identify top and bottom states in cybercrime incidence.

2. Examination of Offences under IT Act, IPC, and SLL: Understand how legal frameworks categorize and evolve with changing crime patterns.

3. Online and Social Media Crimes (2020-2024): Study growth trends specifically in internet-enabled offences like fraud, defamation, and exploitation.

4. Comparative Approach: Evaluate overlaps and differences between traditional cybercrime (2018-2022) and newer social media-based crimes (2020-2024).

5. Methodology

Secondary data collection, analysis and comparative approach.

Data Sources: NCRB Crime in India reports (2018–2022).

Ministry of Home Affairs responses on cybercrime (2020–2024 NCRP data).

6. Results and Analysis

A. State-wise Analysis (2018-2022):

State/UT	2018	2019	2020	2021	2022
Andhra Pradesh	1207	1886	1899	1875	2341
Arunachal Pradesh	7	8	30	47	14
Assam	2022	2231	3530	4846	1733
Bihar	374	1050	1512	1413	1621
Chhattisgarh	139	175	297	352	439
Goa	29	15	40	36	90
Gujarat	702	784	1283	1536	1417
Haryana	418	564	656	622	681
Himachal Pradesh	69	76	98	70	77
Jharkhand	930	1095	1204	953	967
Karnataka	5839	12020	10741	8136	12556
Kerala	340	307	426	626	773
Madhya Pradesh	740	602	699	589	826
Maharashtra	3511	4967	5496	5562	8249
Manipur	29	4	79	67	18
Meghalaya	74	89	142	107	75
Mizoram	6	8	13	30	1
Nagaland	2	2	8	8	4
Odisha	843	1485	1931	2037	1983
Punjab	239	243	378	551	697
Rajasthan	1104	1762	1354	1504	1833
Sikkim	1	2	0	0	26
Tamil Nadu	295	385	782	1076	2082
Telangana	1205	2691	5024	10303	15297
Tripura	20	20	34	24	30
Uttar Pradesh	6280	11416	11097	8829	10117
Uttarakhand	171	100	243	718	559
West Bengal	335	524	712	513	401
A&N Islands	7	2	5	8	28

State/UT	2018	2019	2020	2021	2022
Chandigarh	30	23	17	15	27
D&N Haveli and Daman & Diu+	0	3	3	5	5
Delhi	189	115	168	356	685
Jammu & Kashmir	73	73	120	154	173
Ladakh	0	0	1	5	3
Lakshadweep	4	4	3	1	1
Puducherry	14	4	10	0	64
Total	**27248**	**44735**	**50035**	**52974**	**65893**

Table: Cybercrime cases in India from 2018-2022

Source: National Crime Records Bureau (NCRB)

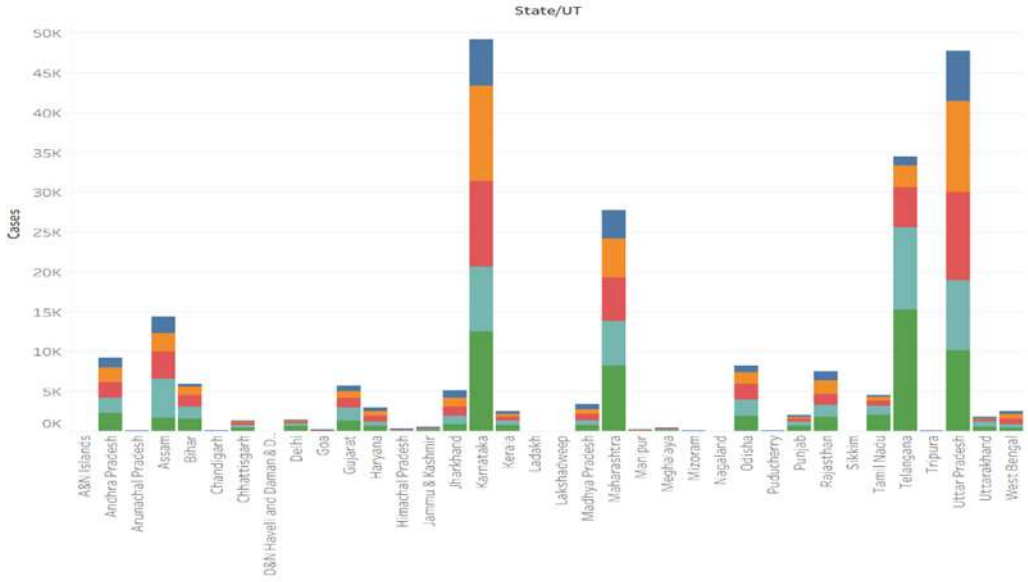

Fig: Bar graph of cybercrime in India from 2018-2022

Between 2018 and 2022, reported cybercrime cases in India rose sharply from 27,248 to 65,893. This reflects an absolute increase of 38,645 cases, amounting to an overall growth of approximately 142% over the 5-year period. Such a steep rise highlights not only the growing prevalence of cybercrimes but also the increasing challenges forced by law enforcement in addressing this evolving threat

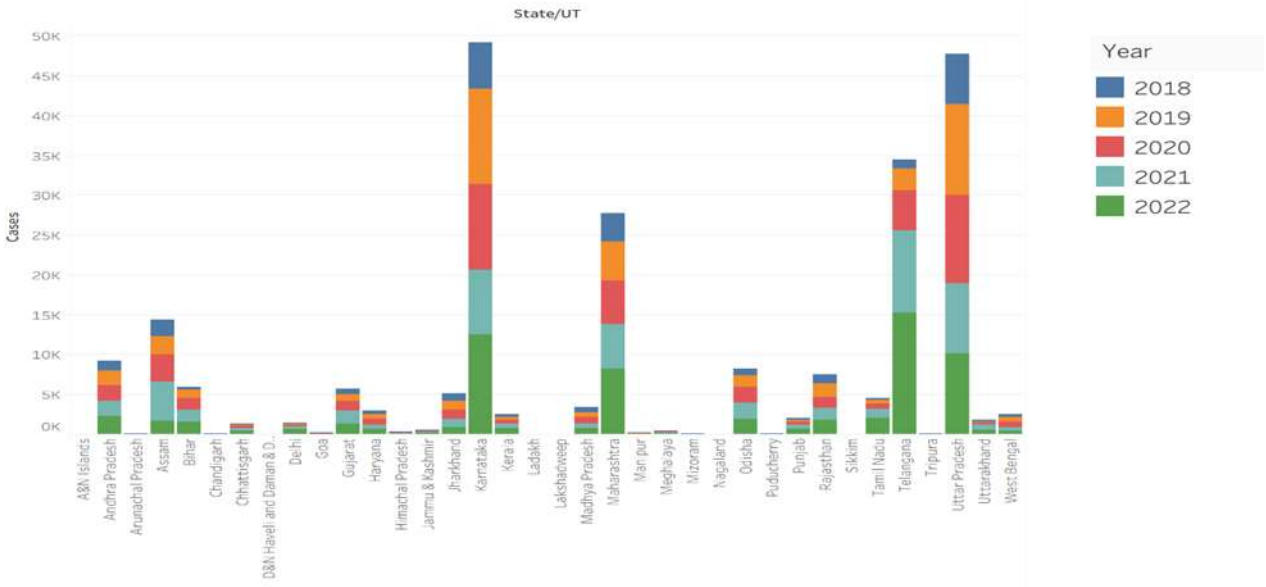

Fig: Stacked Bar graph of cybercrime in states of India throughout five years

Uttar Pradesh, Karnataka, Maharashtra, and Telangana consistently reported the highest number of cases.

Smaller states like Arunachal Pradesh and Goa reported negligible cases, possibly due to underreporting rather than absence of crime.

B. Offences by Law (2018-2022):

Offences	2018	2019	2020	2021	2022
IT Act	18495	30846	29643	27427	31908
IPC	8647	13800	20201	25384	33798
SLL	106	89	191	163	187

Table: Cases registered under cybercrimes during 2018-2022

Source: National Crime Records Bureau

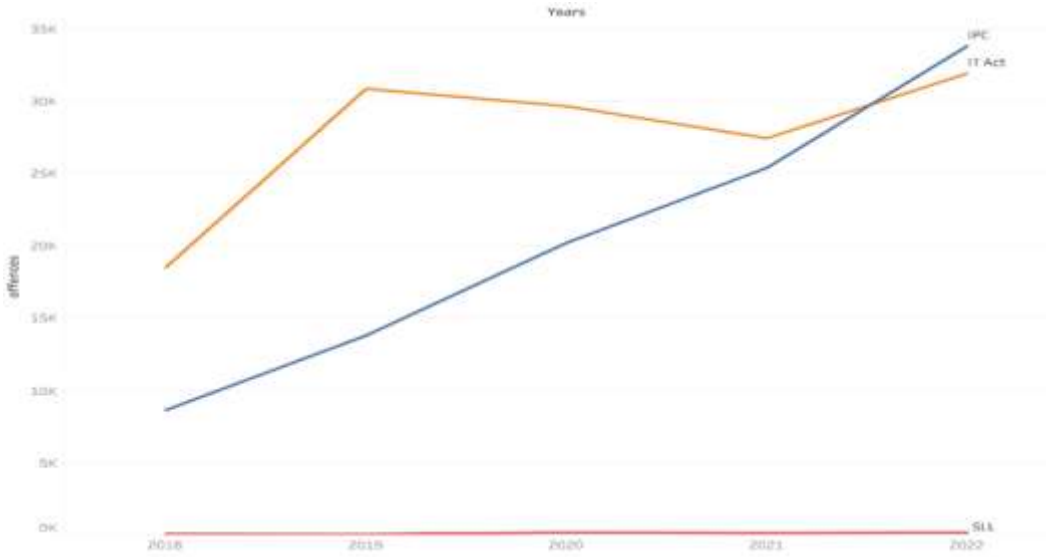

Fig: line graph of cybercrimes registered of different cybercrime act

IT Act offences rose from 18,495 in 2018 to 31,908 in 2022 which comprises of a massive 72.57% increase in just five years period. IPC-linked cyber offences grew faster with 8,647 cases registered in 2018 to 33,798 cases getting registered in 2022, reflecting criminal adaptation to broader penal provisions and a more crimes getting committed in this category as the number of increased cases is 290.9%. SLL offences remained relatively low, showing gaps in applicability.

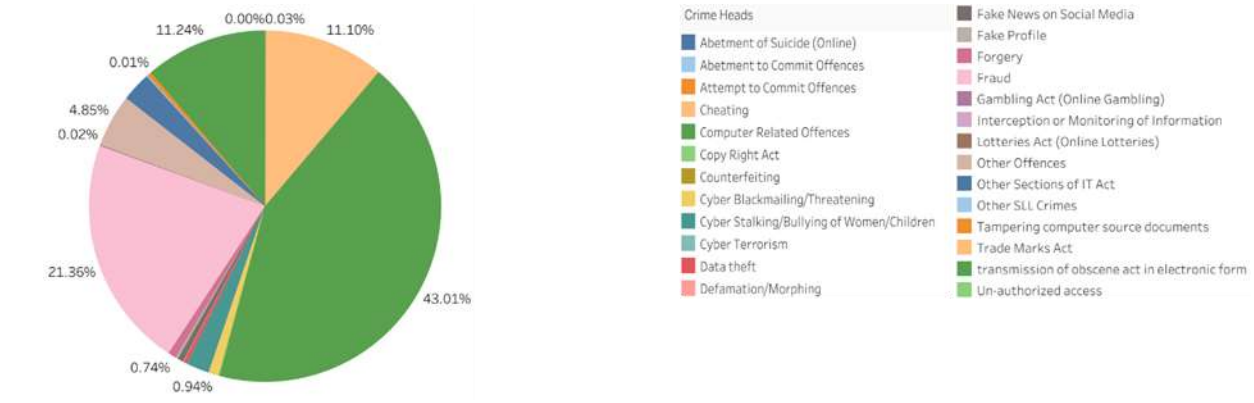

Fig: pie chart of types of cybercrimes registered from 2018-2022

Online and Social-Media Related Crime	**2020**	**2021**	**2022**	**2023**	**2024**
E-Mail Phishing	897	798	1364	1272	2009
Cheating by Impersonation	9808	12617	20041	18135	19989
Fake/Impersonating Profile	12310	15843	23626	30234	39846
Profile Hacking/Identity Theft	10419	10650	26288	33724	38295
Provocative Speech for unlawful acts	5237	2320	4092	3597	5250
Impersonating Email	225	208	285	304	586
Intimidating Email	245	149	227	228	571
Online Job Fraud	4973	7504	10292	13764	10461
Online Matrimonial Fraud	528	623	1149	926	854
Cyber Bullying /Stalking / Sexting	11641	21589	44270	39080	39077

C. Online & Social Media Crimes (2020-2024):

Table: Online and social media crimes from 2020-2024

Source: Ministry of Home Affairs, National Cyber Crime Reporting Portal

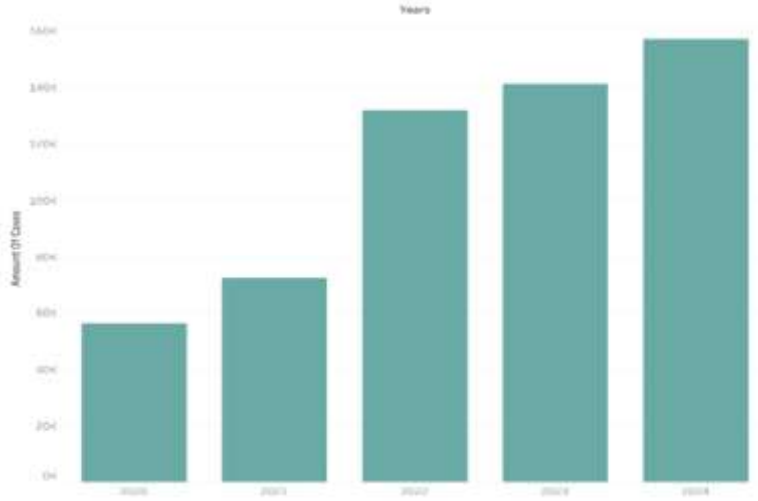

Fig: bar graph of the crimes committed in online and social media category.

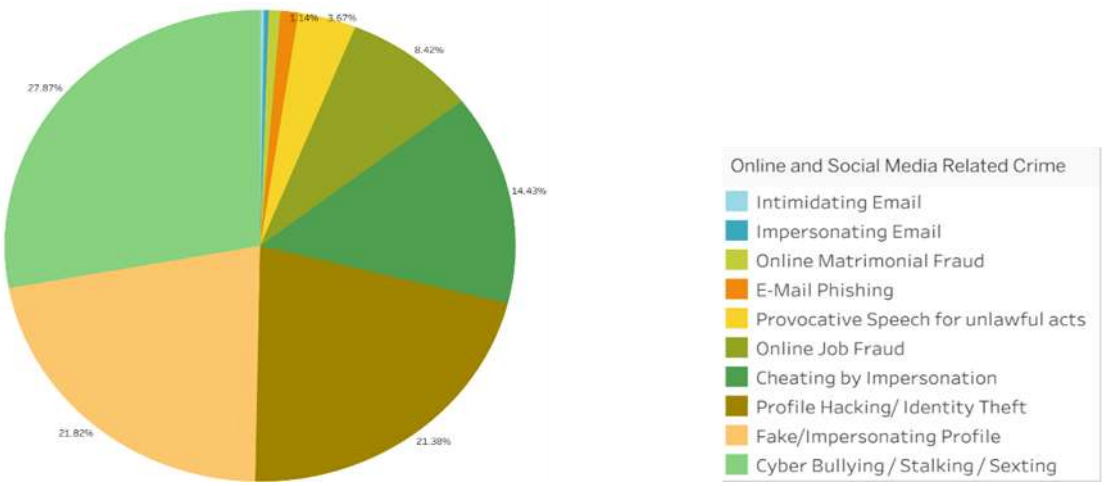

Fig: pie chart of the crimes committed in online and social media category by types.

Significant rise in crimes involving social media fraud, impersonation, and harassment, especially post 2020, with the top types of crime being cyber bullying, cyber stalking, impersonation, identity theft and online fraud comprising of more that half of the crimes. In mere 2 years span i.e. from 2020-2022 the number of cases increased from 11,641 to 32,629 which is again a huge increase of 280.1% but in the next 2 years saw a slow drop of cases from 44,270 to 39,077 a 11.7% decrease which establishes a hope that measures for control are somewhat working.

But this also suggests that in coming years, social platforms are becoming the primary battlefield of cybercrime.

D. Comparative Findings:

General cybercrime (2018-2022) shows steady quantitative growth, while social media crimes (2020-2024) show rapid qualitative shifts in nature suggesting the growing threat of cybercrimes.

State patterns remain consistent: high-reporting states for general crimes also report high social media-related crimes.

7. Discussion

The results highlight that cybercrime in India is both growing and diversifying. The analysis reveals two key dimensions:

1. Scale: Both datasets show rapid growth, confirming India's vulnerability to cybercrime.

2. Nature: The dominance of fake profiles, identity theft, and cyberbullying after 2020 marks a new phase in cyber threats, demanding tailored interventions.

7.1 Policy Response:

The Government of India has:

1. Launched the NCRP portal and 1930 helpline for faster reporting.
2. Established forensic labs and training programs under I4C.
3. Run nationwide cyber awareness campaigns via social media and radio.

7.2 Challenges:

1. Under-reporting due to stigma and lack of awareness.
2. Jurisdictional hurdles in investigating cross-border crimes.
3. Need for stricter social media regulation and identity verification systems.

States with higher internet penetration and urbanization tend to report more cases, indicating both higher vulnerability and stronger reporting mechanisms.

8. Comparison with Previous Work

Unlike earlier works that focused primarily on types of cybercrime, this study provides a temporal and comparative dimension by bridging general cyber offences with online/social media crimes.

Prior papers emphasize prevention strategies (e.g., strong passwords, legal awareness, firewalls). This paper adds value by quantifying regional and legislative trends and showing the transition from broad IT Act crimes to platform-specific offences.

9. Conclusion

India faces a dual challenge: managing the steady growth of conventional cybercrime and addressing the explosive rise of social media-enabled offences. Comparative analysis suggests that legal frameworks must evolve, cyber awareness needs strengthening, and state-level enforcement requires resource allocation proportional to internet penetration.

10 References

[1] National Crime Records Bureau (2018-2022). Crime in India Reports.

[2] Ministry of Home Affairs (2025). Parliamentary Replies on Cybercrime.

[3] "A Comprehensive Survey of Cybercrime and Cybersecurity," *IEEE Fifth International Conference on Advances in Electronics, Computers and Communications*, by K. S. Shindagi, K. V. Koppad, A. Jayakkanavar and S.V. Gorabal2023, Bengaluru, pp. 1-5, 2023.

[4] "A Review on Cyber Security and its Threats," *2022 11th International Conference on System Modeling & Advancement in Research Trends*, by B. J and B. N, Moradabad, pp. 1624-1627, 2022.

[5] "A Survey on Cyber Security Threats," *2021 International Conference on Technological Advancements and Innovations*, by Gulshan and S. S. Chauhan, Tashkent, pp. 218-223, 2021.

[6] "A Technical Review Report on Cyber Crimes in India", *2020 International Conference on Emerging Smart Computing and Informatics*, by P. Datta, S. N. Panda, S. Tanwar and R. K. Kaushal, Pune, pp. 269-275, 2020.

[7] "An Analysis on Scope of Cyber Security," *2019 6th International Conference on Computing for Sustainable Global Development*, by H. K. Thakar, R. A. Joshi and A. Dobariya, New Delhi, pp. 612-615, 2019.

[8] "An empirical analysis of Cyber Crimes, their prevention measures, and laws in India," *2022 Seventh International Conference on Parallel, Distributed and Grid Computing*, by N. Aggarwal, M. Sehgal and A. Arya, Solan, pp. 570-575, 2022.

[9] "An Empirical Study of Cybercrime and Its Preventions," *2020 Sixth International Conference on Parallel, Distributed and Grid Computing*, by S. Batra, M. Gupta, J. Singh, D. Srivastava and I. Aggarwal, Waknaghat, pp. 42-46, 2020.

[10] "Classification and Impact of Cyber Threats in India: A Review", *2020 8th International Conference on Reliability, Infocom Technologies and Optimization*, by S. Tanwar, T. Paul, K. Singh, M. Joshi and A. Rana, Noida, pp. 129-135, 2020.

[11] "Comprehensive Analysis of Various Cyber Attacks", *2021 IEEE Mysore Sub Section International Conference, by S. R. Kavya Rani, B. C. Soundarya*, H. L. Gururaj and V. Janhavi, Hassan, pp. 255-262, 2021.

[12] "Comprehensive Study on Cyber Security and Cyber Attacks", *2024 First International Conference on Electronics, Communication and Signal Processing*, by S. Almass and S. K. Chowdhary, New Delhi, pp. 1-6, 2024.

[13] "Cyber Security and Frameworks: A Study of Cyber Attacks and Methods of Prevention of Cyber Attacks", *2023 International Conference on Sustainable Computing and Data Communication Systems*, by S. Purkait and M. Damle, Erode, pp. 1310-1315, 2023.

[14] "Cyber Security Challenges and Trends on Recent Technologies", *2022 6th International Conference on Computing Methodologies and Communication*, by H. Arora, T. Manglani, G. Bakshi and S. Choudhary, Erode, pp. 115-118, 2022.

[15] "Cyber Security Goal's, Issue's, Categorization & Data Breaches," *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing*, by R. Adlakha, S. Sharma, A. Rawat and K. Sharma, Faridabad, pp. 397-402, 2019.

[16] "Analyzing University Students' Awareness of Cybersecurity," *2023 International Conference on Emerging Trends in Networks and Computer Communications*, by M. A. Haque, S. Ahmad, S. Haque, K. Kumar, K. Mishra and B. K. Mishra, Windhoek, pp. 250-257, 2023.

[17] "Data Breaches: Financial and Reputational Impacts of Vulnerabilities on Organizations to Enhance Cybersecurity Strategies," *2024 3rd International Conference on Automation, Computing and Renewable Systems*, by A. Gite et al., Pudukkottai, 2024.

[18] "Growing cyber crimes in India: A survey," *2016 International Conference on Data Mining and Advanced Computing*, by P. N. V. Kumar, Ernakulam, pp. 246-251, 2016.

[19] "Historical Consciousness of Cyber Security in India," *IEEE Annals of the History of Computing, vol. 42, no. 4*, by R. Subramanian, pp. 71-93, 2020.

[20] "India's Adoption of the Latest Development in Cyber Security Legislation and Practices," *2024 Parul International Conference on Engineering and Technology*, by Shikha and N. Sharma, Vadodara, 2024, pp. 1-4.

[21] "Internet Crimes-It's Analysis and Prevention Approaches," *2021 9th International Conference on Reliability, Infocom Technologies and Optimization*, by D. Gupta, S. K. Jha and S. Mann Maharaja Surajmal, Noida, pp. 1-4, 2021.

[22] "Present & Future Paradigms of Cyber Crime & Security Majors- Growth & Rising Trends," *2014 4th International Conference on Artificial Intelligence with Applications in Engineering and Technology*, by V. K. Gunjan, A. Kumar and A. A. Rao, Kota Kinabalu, pp. 89-94, 2014.

[23] ""Space in space": Cyber security capabilities in Indian context," *2016 Online International Conference on Green Engineering and Technologies*, by A. Thakral, N. Rakesh and A. Gupta, Coimbatore, pp. 1-6, 2016.

[24] "Understanding People's awareness towards social engineering with survey," *2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security*, by A. Raval, S. Chakrabarty, H. Jasoliya and D. Swain, Gunupur, pp. 1-5, 2022.