iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 Issue: VI Month of publication: June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53624

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Exploring the Evolving Landscape of Cybercrime in India and Strategies for Prevention

Kirti[1], Dr. Jyoti Singh[2]
[1]*BSc (H) Forensic Science, Student,* [2]*Assistant Professor (III), Amity Institute of Forensic Science, Amity University, Sector-125, Noida, U.P., Pin code-201301, India*

Abstract: Cybercrime refers to criminal activities that either target computers or networks such as hacking, phishing, and spamming, or involve the use of computer to commit offensive and illegal activities, such as hate crimes and child pornography. The research aims to explore the evolving landscape of cybercrime in India along with Indian cybercrime statistics, motives behind cybercrimes like fraud, extortion, sexual exploitation, terrorist activities, Inciting Hate against Country, Sale Purchase illegal drugs, etc. In addition, the paper will delve into specific types of cybercrime, unique challenges, and strategies for prevention of same. The paper investigates cybercrimes reported in India from 2016 to 2020 under the IT Act 2000 and Indian Penal Code (IPC), identifying both persistent and emerging types of cybercrimes, Police, and court Disposal of Cyber Crime Cases. The research design for this study will be a review type and will use both qualitative and quantitative data analysis techniques to present a bibliographic overview of the evolving landscape of cybercrime in India. The data analysis process will involve using statistical techniques to summarize the data and present it in a meaningful way. The findings of this research will be useful for policymakers, law enforcement agencies, and other stakeholders in the fight against cybercrime in India. This article will serve as the data set for various studies associated with the digital forensic investigations.

Keywords: Cybercrime, IT Act 2000, Indian cybercrime Statistics, Indian Penal Code(IPC), Cybercrime Trends

I. INTRODUCTION

Cybercrimes are modern offences committed through the use of electronic devices. Electronics are now a commonplace aspect of daily life and are regarded as the fourth fundamental element after oxygen, food, and shelter. Unfortunately, because of users' lack of awareness and education, behaviors like extortion, stalking, bullying, harassment, and even acts that result in suicide have become frequent. Due to the lack of the essential tools, technology, and cyber professionals, our ability to tackle cybercrimes is substantially behind. In the meantime, criminals constantly develop and create new types of cybercrimes, surpassing our capacity.[1] The escalating proliferation of abusive content on social media platforms is a troubling issue. Over the past five years (from 2016-2020), the number of reported cybercrime cases has shown a significant upward trajectory: 12,317 cases in 2016, 21,796 cases in 2017, 27,248 cases in 2018, 44,735 cases in 2019, and 50,035 cases in 2020. This trend raises serious concerns and calls for effective measures to address the problem. States like Karnataka, Uttar Pradesh, Maharashtra[2], and Telangana have shown rapid increase in cybercrime in years 2019-2020 as the crime rate has almost doubled due to increased use of online platform during Covid-19 and due to lowering of cyber defenses as major focus of authorities was on health crisis (as per figure-1). Union territories like A&N islands and D&N haveli and Daman and Diu, Ladakh and Lakshadweep have very less almost negligible cybercrime rates whereas Chandigarh, Delhi and Jammu and Kashmir are the top among cybercrime trends in Union Territories. Delhi and Chandigarh cover all the cybercrime under IT act, the IPC act and SLL (as per figure 2)

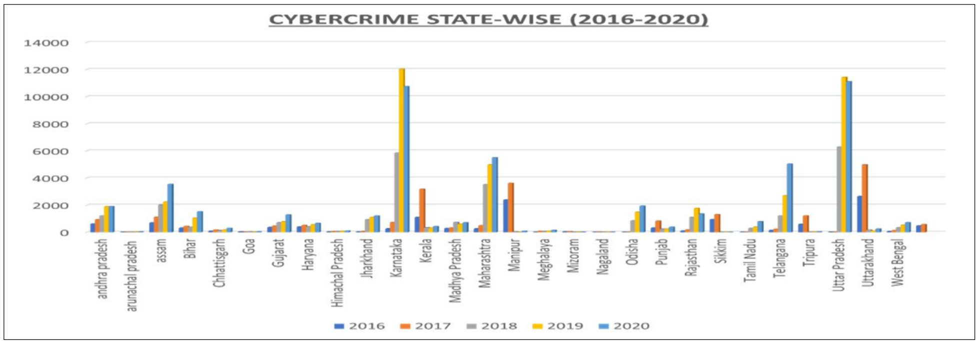


FIGURE 1 - Trends of cybercrimes from year 2016-2020 in different states

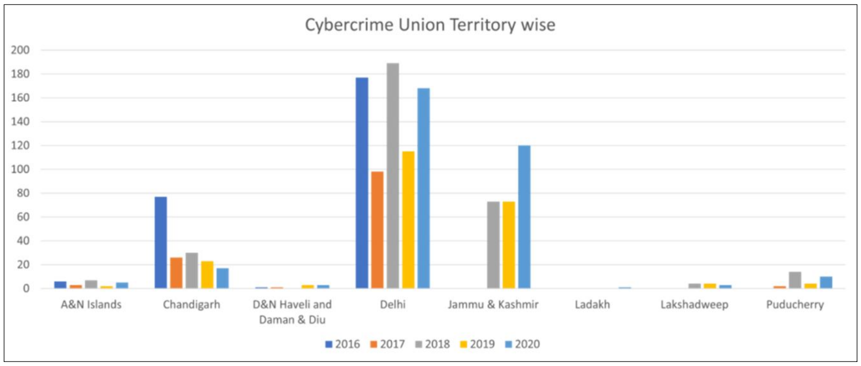


FIGURE 2 - trends of cybercrime among Union territories of India from year 2016-2020.

II. DATA COLLECTION METHOD -

To gather information on cyber-crimes recorded between the years 2016 and 2020 under the IT Act 2000 and the Indian Penal Code, secondary data was collected from the National Crime Records Bureau website[3]. Additionally, secondary data was obtained from the 'Cyber Security' article published by NITI Aayog to examine emerging crimes reported between 2016 and 2020. In order to capture the evolving internet usage in India, secondary data was sourced from various websites including internetlivestats, Statista, and iamai.

III. DATA ANALYSIS METHOD

A trend analysis was conducted to determine the proportion of internet users across India and study the growth of internet usage from 2016 to 2020. Furthermore, a trend analysis was performed on the number of cyber-crimes recorded under the IT Act 2000 and the Indian Penal Code[3]. The cybercrime trend was recorded and analyzed on the basis of motives, cybercrimes trends against women and children, police disposal of the cybercrime. To analyze the newly emerging cyber-crimes and illustrate the distribution of recent cyber-crimes in 2016-2020, 2D bar charts were utilized.

IV. RESULTS AND DISCUSSION

1) *Cybercrime Motive:* The primary motivation for cybercrime is monetary and financial gain without being present at the scene of crime using a virtual identity. Various types of cybercrime motives are personal revenge, anger, fraud, extortion, causing dispute, prank etc., with majorly being contributed by fraud as per the data provided by the states to NCRB. Computer fraud is a malicious attack with an intent to either steal data or to retain someone’s personal information for monetary or financial gain[4]. As per the data provided by the states and union territories to the NCRB, Uttar Pradesh constitutes the highest fraud rate, then Karnataka and then Maharashtra which almost doubled from year 2018 to year 2019 and rate keeps on increasing in 2020 also (as per figure 3).

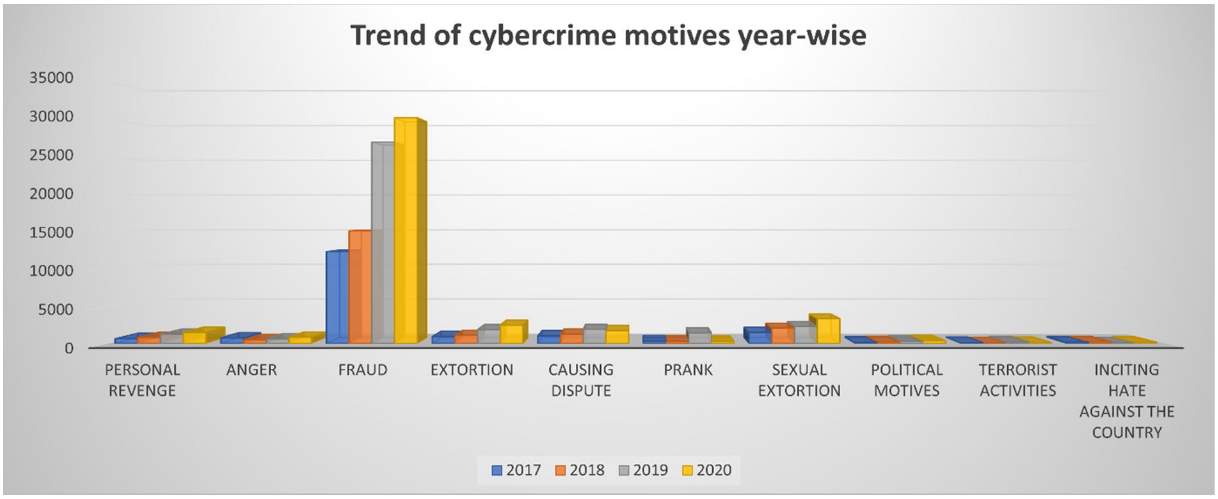


FIGURE 3 - Trend of cybercrime motives from year 2016-2020

2) *Cybercrime Against Women:* Crimes against women have persisted throughout history, encompassing various forms such as the Sati system, dowry-related offenses, cruelty, domestic violence, and rape. Despite 70 years of independence and numerous studies and reports, these crimes against women continue to rise. In the modern age, cybercrime targeting women has emerged as a new form of offense, involving acts committed through electronic medium. Different categories of cybercrimes committed against women are cyber blackmailing or threatening or fake profile etc., with majority of which contributed by cyber pornography or publishing obscene materials and cyber stalking and cyber bullying (as per figure 4). According to the most recent NCRB report, there were 4,242 cases of cybercrimes against women reported in 2017, 6,030 cases in 2018, 8,379 cases in 2019, and 10,405 cases in 2020. 7,184 of the incidents that were reported in 2020 were classified as "other crimes," which shows that India lacks specialized legislation to address cybercrimes against women[5]. With 1,655 recorded incidents, cyberpornography/hosting/publishing obscene sexual materials was the most common sort of cybercrime, followed by cyberstalking/bullying with 887 cases. The biggest number of cases against women were reported in Karnataka (2,859), followed by Maharashtra (1,632 instances) and Assam (1,071 cases), in that order. [5]

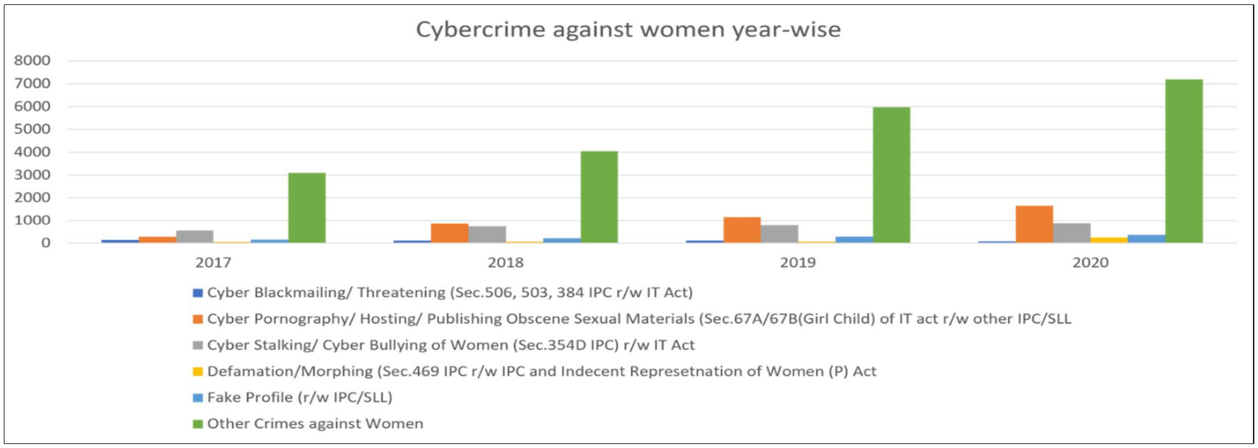


FIGURE 4 – cybercrime trend against women year-wise and types of cybercrime against women.

Year	Cybercrime statistics
2017	19.46%
2018	22.13%
2019	18.73%
2020	20.79%

TABLE 1 - Statistics of cybercrime against women from year 2017-2020

3) Cybercrime against children- Cybercrime against children has become a grave concern in today's digital age. With the rapid advancement of technology and the widespread use of the internet, children are increasingly vulnerable to various forms of online exploitation, abuse, and harassment. Cybercriminals target children with malicious intent, causing significant harm to their emotional, psychological, and physical well-being. It is crucial to understand the reasons behind these crimes, analyze the trends state wise, delve into the motives of offenders, and discuss effective prevention measures. Several factors contribute to the rise of cybercrime against children. The anonymity and accessibility of the internet make it easier for offenders to exploit unsuspecting children.[6] The lack of awareness and digital literacy among both children and parents adds to the vulnerability. Moreover, the rapid growth of social media platforms, online gaming, and messaging apps has created ample opportunities for perpetrators to groom and exploit children. In 2017 and 2018, 80% crimes still classified as other cybercrimes against children as no specified legislation for their classification, 8% of cybercrime constituted by cyber pornography or publishing obscene sexual materials depicting children and cyberstalking and cyberbullying also constitute 8%, cyber blackmailing constitutes 1% and fake profile constitute 3% (as per figure 5). In 2019, 50% crimes classified as other cybercrimes against children, 34% of cybercrime constituted by cyber pornography or publishing obscene sexual materials depicting children which is the second highest and cyberstalking and cyberbullying constituting 15%. The depiction of cybercrime against children in 2020 highlights a significant shift in trends. The majority of these crimes, accounting for 67%, were attributed to cyber pornography or the

distribution of explicit sexual material involving children. This represents a notable increase, making cyberpornography the most prevalent form of cybercrime against children. On the other hand, the category of "other" cybercrimes against children, which held the highest percentage in 2017-2019, now occupies the second position with a reduced rate of 20%. Cyberstalking and cyberbullying make up 13% of the reported cases, placing them as the third most common types of cybercrimes against children (as per figure 6).

Cybercrime Trends Against Children

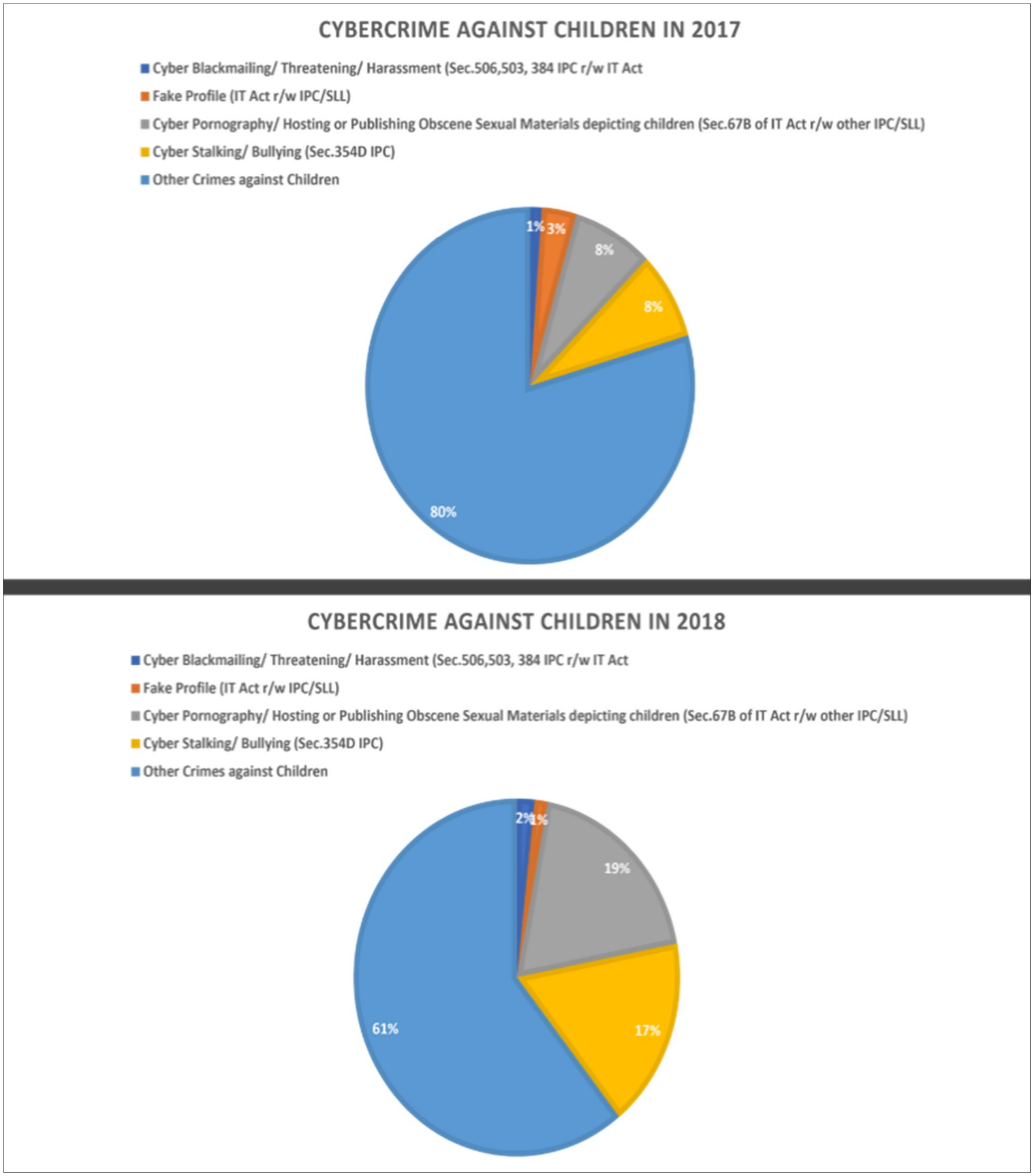


FIGURE 5 – CYBERCRIME TREND AGAINST CHILDREN IN 2017 AND 2018

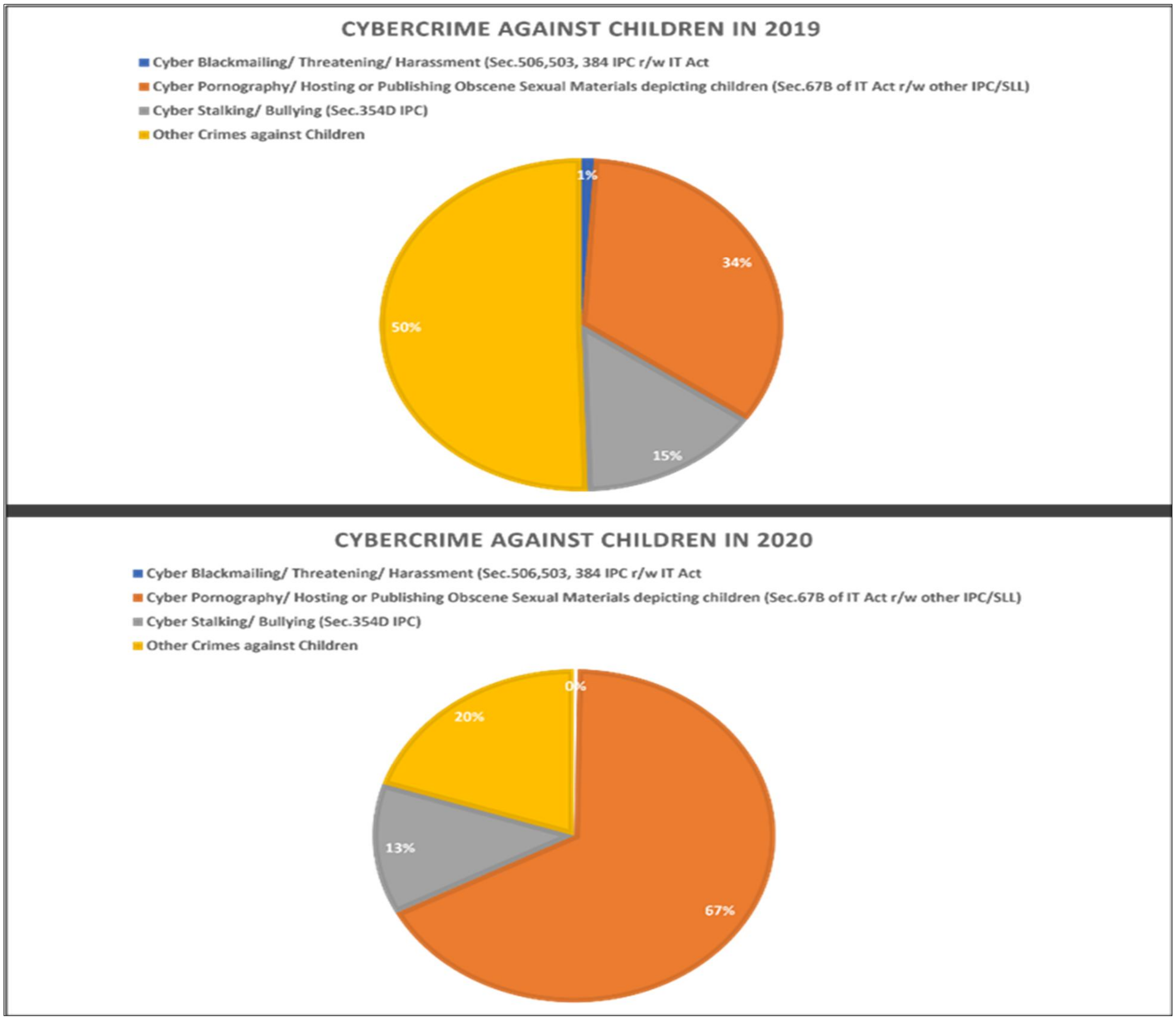


FIGURE 6 – CYBERCRIME TREND AGAINST CHILDREN IN 2019 AND 2020

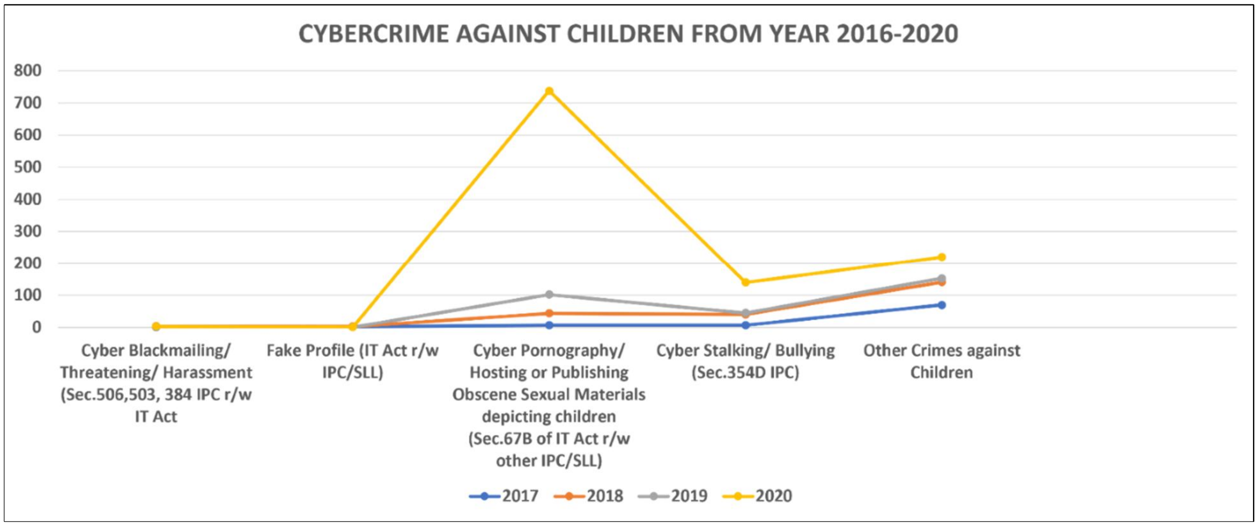


FIGURE 7 – COMPARATIVE CYBERCRIME TREND AGAINST CHILDREN FROM 2016-2020

4) *Police Disposal of Cybercrime:* Cases pending investigation from previous year is increasing tremendously as pending cases in 2017 were 14831, in 2018 it was 22610, in 2019 it increased to 32099, in 2020 it reached up to 53157 as per NCRB crime report. The number of cases reported in 2017 were 21796, in 2018- 27248, in 2019- 44546, in 2020- 50035. Number of Cases that were true but insufficient evidence in 2017 were 7333, in 2018 – 8604, in 2019 – 11517 and in 2020 it reached up to 13384 (as per figure 8).

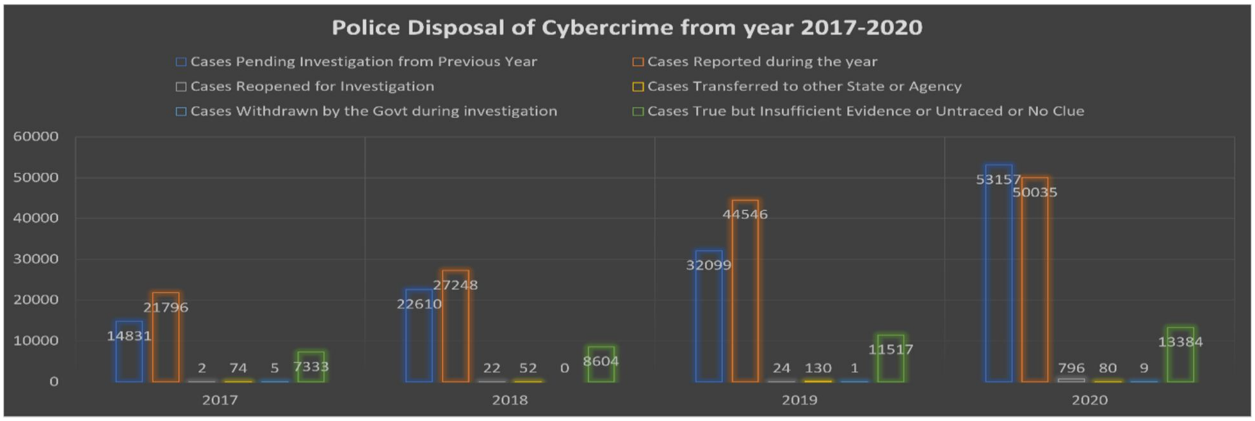
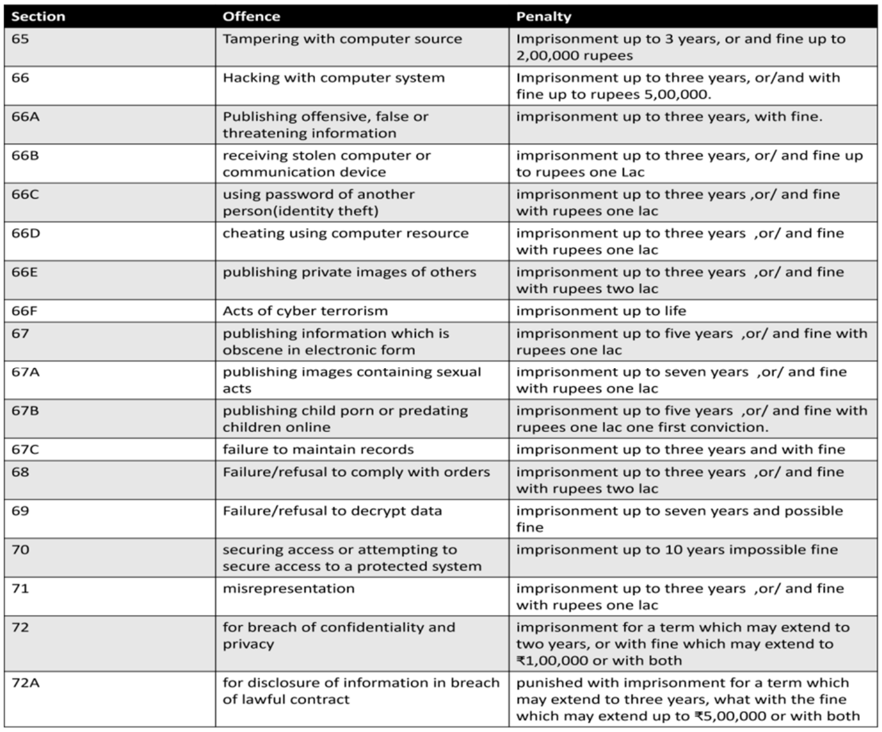


FIGURE 8 – police disposal of cybercrime from 2017 – 2020.

5) *Cybercrimes under IT Act 2000:* The "Information Technology Act, 2000" was approved by the Indian Parliament on October 17, 2000, to handle cybercrime in sectors including e-commerce, e-governance, and e-banking and to set penalties and punishments. The exact offences that have been punishable are listed in the Information Technology (IT) Act, 2000[7]. Certain cybercrimes under IT act are – tampering computer source document (under section-65), computer related offences, identity theft (section-66C) etc. The highest proportion of cybercrimes under IT act are contributed by computer related offences and identity theft. Cases of computer related offences were 10108 in 2017, in 2018 it reached 14141, in 2019 it increased to 23612 (which is approximately 1.5* cybercrimes in 2018) and in 2020 it reduced to 21926. The cases of identity theft were 3724 in 2017, 6688 in 2018 and 12255 in 2019 (almost double from year 2018) and reduced to 5148 in 2020 (reduced to almost half from year 2019). (as per figure 9)



Section	Offence	Penalty
65	Tampering with computer source	Imprisonment up to 3 years, or and fine up to 2,00,000 rupees
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to rupees 5,00,000.
66A	Publishing offensive, false or threatening information	imprisonment up to three years, with fine.
66B	receiving stolen computer or communication device	imprisonment up to three years, or/ and fine up to rupees one Lac
66C	using password of another person(identity theft)	imprisonment up to three years ,or/ and fine with rupees one lac
66D	cheating using computer resource	imprisonment up to three years ,or/ and fine with rupees one lac
66E	publishing private images of others	imprisonment up to three years ,or/ and fine with rupees two lac
66F	Acts of cyber terrorism	imprisonment up to life
67	publishing information which is obscene in electronic form	imprisonment up to five years ,or/ and fine with rupees one lac
67A	publishing images containing sexual acts	imprisonment up to seven years ,or/ and fine with rupees one lac
67B	publishing child porn or predating children online	imprisonment up to five years ,or/ and fine with rupees one lac one first conviction.
67C	failure to maintain records	imprisonment up to three years and with fine
68	Failure/refusal to comply with orders	imprisonment up to three years ,or/ and fine with rupees two lac
69	Failure/refusal to decrypt data	imprisonment up to seven years and possible fine
70	securing access or attempting to secure access to a protected system	imprisonment up to 10 years impossible fine
71	misrepresentation	imprisonment up to three years ,or/ and fine with rupees one lac
72	for breach of confidentiality and privacy	imprisonment for a term which may extend to two years, or with fine which may extend to ₹1,00,000 or with both
72A	for disclosure of information in breach of lawful contract	punished with imprisonment for a term which may extend to three years, what with the fine which may extend up to ₹5,00,000 or with both

TABLE 2 – offences under IT Act 2000 along with their penalties

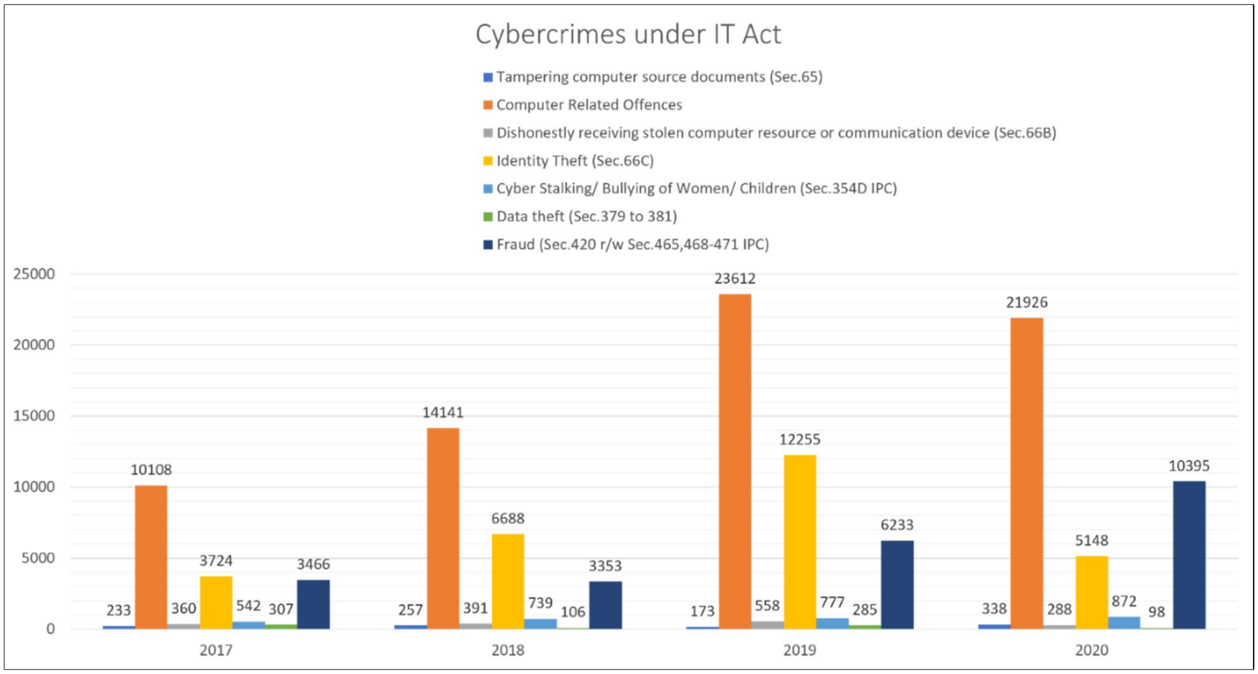


FIGURE 9 – Trend of cybercrime under IT act from 2017-2020.

6) *Cybercrimes under IPC:* In year 2016, 2.98 million cybercrime cases were registered under IPC, in 2017 cases increased to 3.06 million, in 2018- 3.13 million, in 2019 it increased to 3.23 million, in 2020 it reached up to 4.25 million cases and reduced to 3.66 in 2021 (as per figure 10)[7].

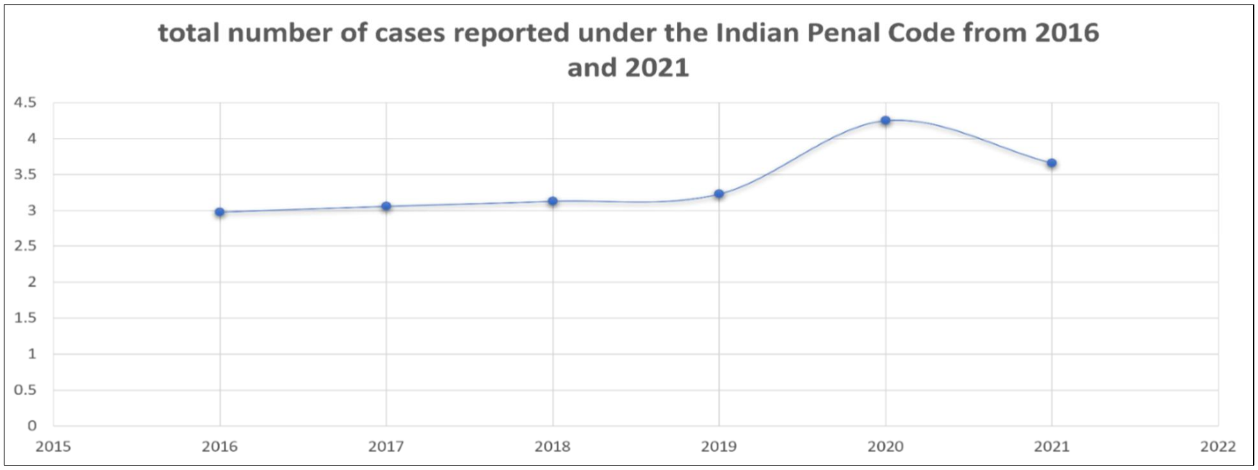


FIGURE 10 – Total number of cases reported under the Indian Penal Code from year 2016-2021 in millions.

V. STRATIGIES FOR PREVENTION OF CYBERCRIME

Preventing cybercrime involves following security guidelines and implementing best practices. The following recommendations can help minimize security risks:

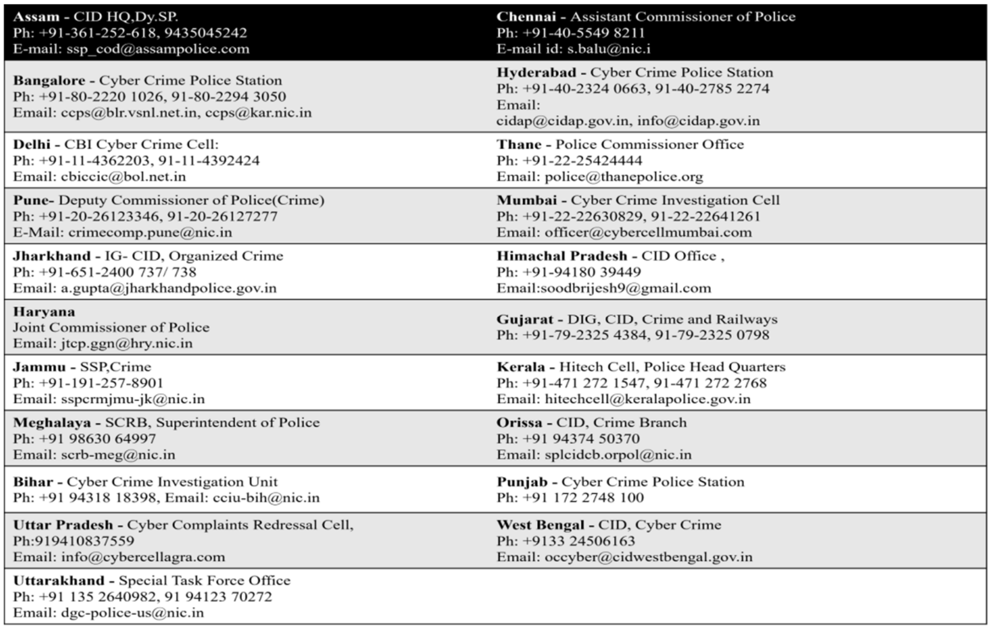
1) *Regularly Update Computer Systems:* Keep operating systems and antivirus software up to date. While this won't provide complete protection, it significantly reduces the chances of hackers gaining unauthorized access, blocks many basic attacks, and enhances overall security.[8]
2) *Utilize Secure Passwords:* Choose passwords with at least eight characters, a mix of letters, numbers, and symbols (for example, # $%!?), and at least one symbol. Instead, using information that may be easily guessed, such as names or city names, use non-dictionary words. Keep your passwords secure and avoid using the same password on several internet accounts. It is advisable to update passwords once every 90 days.

3) *Install Security Software:* Utilize security software such as firewalls and antivirus programs. Firewalls control online communication and determine who or what can access your computer. Antivirus software keeps track of internet actions and protects users from viruses, worms, Trojan horses, and other harmful software. Every time you connect to the Internet, set up your antivirus and antispyware software to update itself automatically.[8]
4) *Protecting Individual Information:* Take security measures to safeguard sensitive data while disclosing personal information online.

Follow these guidelines:

a) Be cautious of phishing messages that pressure you to act quickly or threaten negative consequences. Ignore and do not respond to such messages.
b) Legitimate companies do not request personal information via email, so avoid responding to email requests for personal data.
c) Instead of clicking on links within emails or instant messages, manually type the URL into your web browser when visiting websites.
d) Protect your email address from unsolicited emails and spam.

5) *Exercise Caution with Online Offers:* Beware of offers that seem too good to be true, as they may involve bundled advertising software that tracks your behavior or displays unwanted ads. Exercise caution when downloading free software or services.
6) *Regularly Review Bank and Credit Card Statements:* Identity theft and online crimes can be mitigated by promptly detecting any suspicious activity. Regularly monitor bank and credit card statements for any unauthorized transactions. Many financial institutions employ fraud prevention systems that alert you to unusual purchase patterns.
7) *Be Social Media Savvy:* Adjust the privacy settings of social networking profiles, such as Facebook or Twitter, to private. Regularly review and modify security settings. Exercise caution when sharing personal information online.
8) *Mobile Devices Should be Secured:* Be aware that viruses and hacking efforts might affect mobile devices. Only download software via reliable sources.
9) *Wireless Network Should be Secured:* Ensure that your home Wi-Fi network is properly secured. Review and modify default settings to prevent unauthorized access. Avoid using public Wi-Fi networks, as they can pose security risks.[8]
10) *Seek Assistance from Cybercrime Cells:* To address cybercrime incidents, law enforcement agencies in India have established cybercrime investigation cells nationwide. These specialized units focus on looking into a variety of cybercrimes, such as hacking, virus distribution, pornography, account manipulation, data alteration, software piracy, fraudulent websites, the creation of counterfeit money and visas, the theft of intellectual property, email spam, denial of access, password theft. The table below lists the contact information for numerous active cybercrime cells present in India, including contact details and email addresses:



Assam - CID HQ,Dy.SP. Ph: +91-361-252-618, 9435045242 E-mail: ssp_cod@assampolice.com	**Chennai -** Assistant Commissioner of Police Ph: +91-40-5549 8211 E-mail id: s.balu@nic.i
Bangalore - Cyber Crime Police Station Ph: +91-80-2220 1026, 91-80-2294 3050 Email: ccps@blr.vsnl.net.in, ccps@kar.nic.in	**Hyderabad -** Cyber Crime Police Station Ph: +91-40-2324 0663, 91-40-2785 2274 Email: cidap@cidap.gov.in, info@cidap.gov.in
Delhi - CBI Cyber Crime Cell: Ph: +91-11-4362203, 91-11-4392424 Email: cbiccic@bol.net.in	**Thane -** Police Commissioner Office Ph: +91-22-25424444 Email: police@thanepolice.org
Pune- Deputy Commissioner of Police(Crime) Ph: +91-20-26123346, 91-20-26127277 E-Mail: crimecomp.pune@nic.in	**Mumbai -** Cyber Crime Investigation Cell Ph: +91-22-22630829, 91-22-22641261 Email: officer@cybercellmumbai.com
Jharkhand - IG- CID, Organized Crime Ph: +91-651-2400 737/ 738 Email: a.gupta@jharkhandpolice.gov.in	**Himachal Pradesh -** CID Office , Ph: +91-94180 39449 Email:soodbrijesh9@gmail.com
Haryana Joint Commissioner of Police Email: jtcp.ggn@hry.nic.in	**Gujarat -** DIG, CID, Crime and Railways Ph: +91-79-2325 4384, 91-79-2325 0798
Jammu - SSP,Crime Ph: +91-191-257-8901 Email: sspcrmjmu-jk@nic.in	**Kerala -** Hitech Cell, Police Head Quarters Ph: +91-471 272 1547, 91-471 272 2768 Email: hitechcell@keralapolice.gov.in
Meghalaya - SCRB, Superintendent of Police Ph: +91 98630 64997 Email: scrb-meg@nic.in	**Orissa -** CID, Crime Branch Ph: +91 94374 50370 Email: splcidcb.orpol@nic.in
Bihar - Cyber Crime Investigation Unit Ph: +91 94318 18398, Email: cciu-bih@nic.in	**Punjab -** Cyber Crime Police Station Ph: +91 172 2748 100
Uttar Pradesh - Cyber Complaints Redressal Cell, Ph:919410837559 Email: info@cybercellagra.com	**West Bengal -** CID, Cyber Crime Ph: +9133 24506163 Email: occyber@cidwestbengal.gov.in
Uttarakhand - Special Task Force Office Ph: +91 135 2640982, 91 94123 70272 Email: dgc-police-us@nic.in	

FIGURE 11 - Indian cybercrime cells

VI. CONCLUSION

1) In conclusion, this research paper delves into the evolving landscape of cybercrime in India and proposes strategies to prevent and combat this growing threat. The findings emphasize the urgent need for proactive measures and increased awareness about cybercrime among individuals, organizations, and government bodies. Understanding the various forms of cybercrime prevalent in India is crucial for effectively identifying and mitigating potential risks. This necessitates targeted awareness campaigns, educational initiatives, and the dissemination of best practices for online safety and security.[1]
2) The research highlights the significance of investing in robust cybersecurity infrastructure, urging both public and private organizations to implement comprehensive security measures to safeguard critical systems and sensitive data. This includes the deployment of encryption technologies, firewalls, intrusion detection systems, and regular security audits. Fostering a cybersecurity culture within organizations promotes a proactive approach to risk management.
3) Addressing the shortage of skilled cybersecurity professionals is a critical concern, and bridging the expertise gap requires partnerships between educational institutions, industry associations, and government bodies. Specialized cybersecurity training programs, certifications, and internships can equip individuals with the necessary skills to detect, prevent, and respond to cyber threats effectively.[3]
4) Collaboration between the public and private sectors is essential for an effective prevention and response strategy. The research advocates for information sharing platforms, public-private partnerships, and joint efforts between law enforcement agencies, industry associations, and cybersecurity experts. Sharing intelligence, resources, and best practices enhances the collective ability to detect and disrupt cybercriminal activities.
5) Furthermore, the research emphasizes the need to strengthen legal frameworks and legislation to keep pace with evolving cyber threats and enable swift prosecution of cybercriminals. Regular review, amendment, and introduction of new laws are vital to address emerging challenges.
6) In conclusion, combatting cybercrime in India requires a multi-faceted approach encompassing awareness, technological advancements, skill development, collaboration, and robust legal measures. By adopting a proactive stance and implementing the strategies outlined in this research, India can enhance its cybersecurity posture, protect its citizens, businesses, and critical infrastructure, and create a safer digital environment for all.

VII. FUTURE CHALLENGES

1) *Evolving Technology:* Rapid technological advancements create new opportunities and challenges for cybercriminals. Emerging technologies like artificial intelligence, Internet of Things (IoT), and quantum computing introduce vulnerabilities that can be exploited. Developing effective security measures becomes crucial in combating cybercrime.
2) *Increasing Sophistication of Cyber Attacks:* Cybercriminals are becoming more sophisticated in their tactics, making it challenging to detect and prevent cyber-attacks. Advanced persistent threats (APTs), ransomware attacks, and zero-day exploits bypass traditional security measures. Proactive defense strategies and advanced cybersecurity solutions are necessary to counter evolving threats.[9]
3) *Insider Threats:* Individuals within organizations exploiting access privileges pose a significant challenge. Insiders may intentionally leak sensitive information, engage in financial fraud, or sabotage computer systems. Identifying and mitigating insider threats requires robust security protocols, employee training, and effective monitoring systems.
4) *Cybersecurity Skills Gap:* The shortage of skilled cybersecurity professionals globally hinders efforts to combat cybercrime effectively. Organizations struggle to find qualified professionals to fill cybersecurity roles. Addressing the skills gap requires increased investments in cybersecurity education, training programs, and industry collaboration.
5) *Cross-Border Jurisdictional Challenges:* Cybercrime transcends borders, creating challenges in terms of jurisdiction and international cooperation for law enforcement agencies. Coordinating efforts, sharing intelligence, and establishing effective legal frameworks for international cooperation are crucial in tackling cross-border cybercrime.
6) *Cloud Security:* As cloud computing adoption increases, securing cloud-based systems and data becomes critical. Cloud services introduce new security risks, such as data breaches, misconfigurations, and unauthorized access. Robust cloud security measures, including strong access controls, encryption, and regular security audits, are vital to protect sensitive data.
7) *Social Engineering Attacks:* Social engineering attacks, such as phishing and social media manipulation, remain prevalent and effective. Cybercriminals exploit human psychology to manipulate individuals into divulging sensitive information or performing certain actions. Raising awareness, implementing multi-factor authentication, and providing cybersecurity training can help mitigate the risks associated with social engineering attacks.

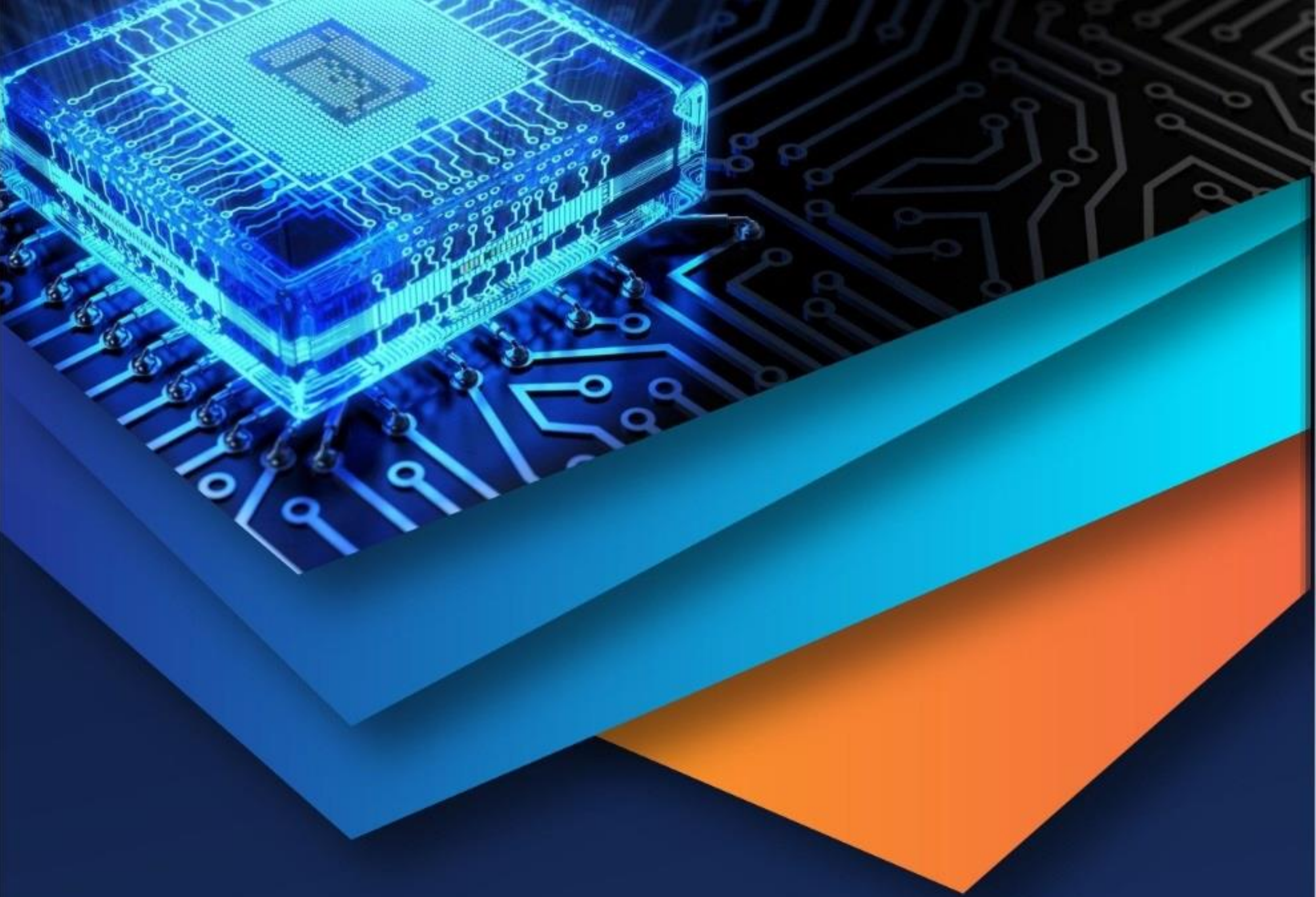
8) *Internet of Things (IoT) Security:* Securing interconnected IoT devices presents a significant challenge. IoT devices often lack adequate security measures and can serve as entry points for cyber-attacks. Strengthening IoT security standards, implementing robust authentication mechanisms, and regularly updating firmware and software patches are essential to mitigate IoT-related risks.
9) *Data Privacy and Compliance:* Data privacy regulations impose strict requirements on organizations to protect individuals' personal data. Ensuring compliance with regulations like GDPR and CCPA while safeguarding sensitive data poses complexity. Establishing comprehensive data privacy frameworks, implementing privacy-by-design principles, and conducting regular privacy audits are crucial.[9]
10) *Emerging Threats in Critical Infrastructure:* Critical infrastructure systems, such as power grids and transportation networks, are increasingly vulnerable to cyber-attacks. Disrupting critical infrastructure can have severe consequences for public safety and national security. Strengthening cybersecurity, conducting risk assessments, and developing incident response plans specific to critical systems are essential to mitigate these threats.

VIII. RECOMMENDATIONS

1) *Strengthen Legislation and International Cooperation [10]:* Governments should continuously update and strengthen cyber laws to keep pace with emerging threats. International cooperation and information sharing among law enforcement agencies are crucial for combating cross-border cybercrime.
2) *Enhance Cybersecurity Awareness and Education:* Promoting cybersecurity awareness among individuals, businesses, and organizations is vital. Educating users about best practices, such as using strong passwords, updating software, and recognizing phishing attempts, can significantly reduce the risk of falling victim to cybercrime.
3) *Invest in Cybersecurity Infrastructure:* Governments and organizations should allocate resources to develop robust cybersecurity infrastructure. This entails putting in place cutting-edge security measures like firewalls, antivirus software, and encryption as well as performing frequent security assessments.
4) *Foster Public-Private Partnerships:* Collaboration between governments, law enforcement agencies, and the private sector is essential for effectively combating cybercrime. Public-private partnerships can facilitate information sharing, joint investigations, and the development of innovative cybersecurity solutions.
5) *Strengthen Cybercrime Investigation and Forensics Capabilities:* Law enforcement agencies need to enhance their cybercrime investigation and digital forensics capabilities. This includes training personnel in cybercrime investigation techniques, establishing specialized cybercrime units, and investing in advanced forensic tools and technologies.
6) *Promote Ethical Hacking and Bug Bounty Programs:* Encouraging ethical hacking and bug bounty programs can help identify vulnerabilities in computer systems and networks. Offering rewards to individuals who responsibly disclose vulnerabilities can incentivize proactive cybersecurity measures.
7) *Raise Awareness on Cybercrime Impact:* Governments, NGOs, and educational institutions should raise awareness about the impact of cybercrime on individuals, businesses, and society. This includes highlighting the potential financial, emotional, and reputational consequences of cybercrime.

REFERENCES

[1] N. Jain, "'CYBER CRIME CHANGING EVERYTHING-AN EMPIRICAL STUDY,'" International Journal of Computer Application Issue 4, vol. 1, 2014
[2] Ieee and Ieee, 2013 International Conference on Intelligent Systems and Signal Processing (ISSP).
[3] M. R. Shah, "CYBER CRIMES IN INDIA: TRENDS AND PREVENTION," International Journal of Research and Analytical Reviews, 2019, [Online]. Available:
[4] Amity University, Amity University. Amity Institute of Information Technology, Institute of Electrical and Electronics Engineers. Uttar Pradesh Section, and Institute of Electrical and Electronics Engineers, ICRITO'2020 : IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) : conference date: 4-5 June 2020 : conference venue: Amity University, Noida, India.
[5] A. Kabi, A. Marisport, S. Gori, and A. Singh Tomar, "The Facets Of Cyber Crimes Against Women In India: Issues And Challenges." [Online]. Available:
[6] T. J. Holt and A. M. Bossler, "The Palgrave Handbook of International Cybercrime and Cyberdeviance.
[7] "Cyber Laws in India."
[8] V. Kandpal and R. K. Singh, "Latest Face of Cybercrime and Its Prevention In India," International Journal of Basic and Applied Sciences Kandpal & Singh, vol. 2, no. 4, pp. 150–156, 2013, [Online]. Available:
[9] J. Iqbal, "Cybercrime in India: Trends and Challenges," 2017. [Online]. Available: http://www.coe.int/cybercrime
[10] D. Gupta and N. Agrawal, "Global Journal of Enterprise Information System Empirical Study of Cyber Crimes in India using Data Analytics", doi: 10.18311/gjeis/2018/19960



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY