Pragati Jain, **International Journal of Advanced Trends in Computer Applications (IJATCA)**
Volume 10, Number 1, July - 2024, pp. 9-17
ISSN: 2395-3519

Perceptions of Cybercrime and Cybersecurity Measures Among the General Population of India

Pragati Jain[1*], Leoson Heisnam[2], Ashish Kumar[3], Shefali Chaudhary[4], Sonali Balouria[5], Abhishek Sapkal[6]

[1,3,4,5]MSc Forensic science, University Institute of Applied Health Science,
Chandigarh University, Ludhiana, Punjab
[2]Visiting Faculty, Institute of Forensic Science for Training and Skilling,
National Forensic Sciences University (NFSU)
[6]Bachelors of Computer Application, Amravati University,
Akola, Maharashtra
[1]pragatijain980@gmail.com, [2]leosonfs@yahoo.com, [3]ashishpal6898@gmail.com [4]schaudhary3993@gmail.com, [5]Sonalibalouria280@gmail.com, [6]agsofficial2003@gmail.com

Abstract: *Cybercrime, a term introduced by Sussman and Heuston in 1995, encompasses a wide range of criminal activities involving computers, computer networks, and the internet. With the increasing prevalence of internet usage, cybercrimes have emerged as a modern category of offenses. To combat these internet-related crimes, the Information Technology Act of 2000 was enacted, aiming to facilitate a conducive environment for commercial IT use. This study, conducted through both online Google Forms and offline questionnaires, seeks to examine perceptions of cybercrime and cybersecurity practices across various age groups in India, spanning from individuals under 18 to those aged 60 and above. The findings of the study are supported by existing research studies that signifies various aspects of cybercrime within the Indian context, highlighting the need for comprehensive cybersecurity strategies with respect to specific demographics. The importance of government cybersecurity efforts becomes apparent, with perceptions varying among age groups, reflecting the complexities of public trust and confidence in cybersecurity initiatives. Public awareness campaigns and interventions play a vital role in promoting mental well-being and safe internet practices, addressing both technical and psychological aspects of cybersecurity. By integrating survey findings with existing research studies, a comprehensive understanding of the cybersecurity landscape in India is achieved, highlighting the multifaceted challenges and opportunities in fostering digital resilience across different age groups.*

Keywords: Cybercrime, Cyber Security Practices, Government cybersecurity efforts, Safe internet practices

I. Introduction

Cybercrime is a broad term that encompasses criminal activities involving computers, computer networks, and the internet. Sussman and Heuston was the first to propose the term "Cyber Crime" in the year 1995 [1]. Cybercrime has no single definition it is considered as a collection of acts or conduct- these acts are based on the material offence object and modus operandi that affect computer data or systems. India, with over 560 million internet users, ranks second globally in terms of online market size, trailing only China. In 2023, India has over 650 million internet users. In 2018, a total of 27,248 cybercrime cases were registered in India, with 1,205 cases in Telangana. According to the FBI, India ranks third among the top 20 cybercrime victims. The national cybercrime reporting portal (available at cybercrime.gov.in) initiated by the central government has received 33,152 complaints so far, resulting in 790 FIRs being filed [2].

Table-1: Classification of different types of cybercrimes commonly victimizes Indian and worldwide Population.

Category	Type of Cybercrime	Description
A. Crimes against persons	Cyber-Stalking	Creating physical threats via computer technology like internet, email, etc., inducing fear [3], [4].
	Dissemination of Obscene Material	Includes indecent exposure/pornography, hosting prohibited materials causing harm, especially to adolescents [5].
	Defamation	Imputing false information to lower a person's dignity, often by hacking and sending vulgar emails [6].
	Hacking	Unauthorized control/access over a computer system, often leading to data destruction [2].

	Cracking	Intrusion into a computer system without consent, tampering with confidential data [1].
	E-Mail Spoofing	Misrepresenting the origin of an email, often to deceive the recipient [7].
	SMS Spoofing	Sending SMS from a victim's mobile number via the internet, a serious crime [2].
	Carding	Unauthorized use of ATM/debit/credit cards for monetary gain [2].
	Financial Fraud	Stealing passwords, data storage, leading to fraud and various accounts related white collared crime [8]
	Child Pornography	Creating, distributing, accessing materials sexually exploiting underage children [9].
	Assault by Threat	Threatening a person's life or their family's using computer networks [2].
	Illegal activities Via Dark web	Dark web is utilized as a platform for online trading of various illegal goods like drugs, human organs, ammunitions etc. These transactions leave no digital foot printing by the usage of cryptocurrency like bitcoins, monero [10], [11], [12].
B. Crimes against Property	Intellectual Property Crimes	Violating intellectual property rights, including software piracy, copyright infringement, etc [13].
	Cyber Squatting	Claiming a domain name like another, causing confusion [14].
	Cyber Vandalism	Deliberate destruction or damage to data or systems, disrupting network services [15].
	Hacking Computer System	Unauthorized access/control over computer systems, causing data loss [2].
	Transmitting Virus	Circulating viruses affecting data and computer systems [2].
	Cyber Trespass	Unauthorized access to a computer without disturbing or altering data [2].
	Internet Time Thefts	Unauthorized use of someone else's internet hours [2].
C. Cyber crimes against Government	Cyber Terrorism	Using the internet for terrorist activities like DDoS attacks, hate websites, endangering national sovereignty [16].
	Cyber Warfare	Politically motivated hacking for damage and spying, a form of information warfare [17].
	Distribution of pirated software	Distributing pirated software to damage government data and records [2].
	Possession of Unauthorized Information	Unauthorized access to and possession of sensitive information for political, religious, or ideological motives [2].

The Information Technology Act, 2000 was enacted with the primary goal of fostering a conducive environment for commercial IT use. This legislation outlines punishable acts related to technology. Additionally, amendments have been made to the Indian Penal Code, 1860, extending its scope to cover cybercrimes [2].

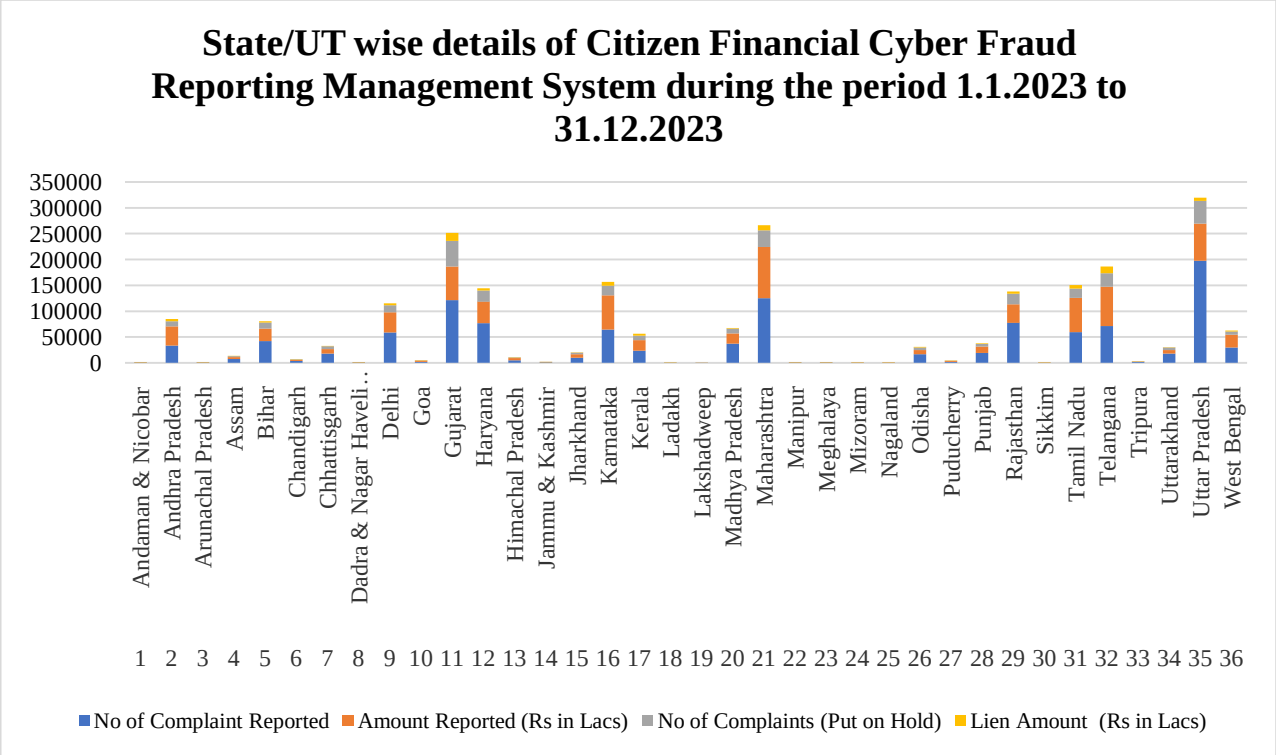

Figure 1: Depicts the State/UT wise details of Citizen Financial Cyber Fraud Reporting Management System during the period 1.1.2023 to 31.12.2023 [18]

In figure-1, The data depicts significant disparities across regions in terms of the frequency and financial implications of cybercrime incidents. For instance, states like Uttar Pradesh, Maharashtra, and Karnataka exhibit notably high numbers of reported complaints, with Uttar Pradesh topping the list at 197,547 complaints. Conversely, smaller regions such as Lakshadweep and Ladakh report relatively fewer incidents, with 29 and 162 complaints respectively. In terms of the financial impact, states like Maharashtra, Karnataka, and Gujarat stand out, reporting substantial amounts in crores of rupees. Maharashtra leads in both the number of complaints and the reported amount, with 125,153 complaints and Rs. 99,069.22 crores. Similarly, Karnataka reports 64,301 complaints with an amount of Rs. 66,210.02 crores, while Gujarat reports 1,21,701 complaints amounting to Rs. 65,053.35 crores. On the other end of the spectrum, regions like Lakshadweep and Sikkim report relatively minor financial implications of cybercrime, with amounts in lakhs of rupees. Additionally, the data highlights the number of complaints that have been put on hold, indicating ongoing investigations or unresolved issues. For instance, Uttar Pradesh, Maharashtra, and Karnataka exhibit a high number of complaints put on hold, suggesting the complexity and challenges involved in addressing cybercrime effectively [18].

II. Objective

Previously, several survey studies have explored the perceptions of cybercrime and cybersecurity measures among the general population in India [19], [20], [21], [22]. The primary objective of this study, conducted via Google Form and offline questionnaires, is to examine these perceptions across different age groups—from individuals below 18 years to those aged 60 and above—across various states in India. The survey comprises 10 straightforward queries related to cybercrime and everyday cybersecurity practices.

III. Material and Methods

3.1. Study Design

A cross-sectional design was utilized in the survey to investigate the perceptions of cybercrime and cybersecurity measures among the general population of India. The study employed a structured questionnaire to collect data from participants both online and offline.

3.2. Participants

The study targeted individuals from diverse age groups and geographical regions across India. A total of 1000 responses were collected to ensure adequate representation of the population.

3.3. Questionnaire

The survey questionnaire consists of 10 questions aimed at understanding the perceptions and behaviors of respondents regarding cybercrime and cybersecurity measures. Firstly, participants were asked to specify their age group, providing options ranging from below

18 years to above 60 years. Following this, respondents were queried about their level of concern regarding the possibility of falling victim to cybercrime, with response options ranging from "Not concerned at all" to "Extremely concerned."

The third question assessed participants' frequency of updating passwords for online accounts, offering response options of "Never," "Rarely," "Occasionally," "Often," and "Always." Subsequently, respondents were prompted to identify the most concerning cybercrime threat from a list including phishing attacks, identity theft, ransomware attacks, online scams, and data breaches.

Participants were then asked to rate their confidence in their ability to identify potential cyber threats on a scale from "Not confident at all" to "Extremely confident." The survey also inquired about respondents' perceptions of the adequacy of cybersecurity measures in India, providing options such as "Yes, completely adequate," "Somewhat adequate," "No, inadequate," and "Not sure."

A question regarding personal experiences with cybercrime asked whether respondents or individuals they knew had ever been victims of cybercrime, with response options of "Yes" or "No." Additionally, participants were queried about the frequency of backing up important data, with response options ranging from "Never" to "Always."

The survey then explored measures taken by respondents to protect their personal information online, including using strong, unique passwords, enabling two-factor authentication, avoiding suspicious links and emails, regularly updating security software, and encrypting sensitive data.

Further, participants were asked about their habits regarding reading privacy policies and terms of service before using online services, providing response options of "Never," "Rarely," "Occasionally," "Often," and "Always." Finally, the questionnaire concluded by assessing respondents' beliefs regarding the role of the government in enforcing cybersecurity measures, offering response options ranging from "Yes, strongly agree" to "No, strongly disagree."

This comprehensive questionnaire aimed to gather insights into the perceptions, concerns, behaviors, and beliefs of respondents regarding cybercrime and cybersecurity measures, contributing to a deeper understanding of the topic among the general population of India.

3.4. Data Collection

3.4.1. Online Survey: A Google Form questionnaire was created and distributed via various online platforms, including social media, email, and online forums. Participants were invited to complete the survey voluntarily.

3.4.2. Offline Survey: Printed copies of the questionnaire were distributed to individuals in public spaces, such as community centers, shopping malls, and educational institutions, allowing for participation from those with limited internet access.

3.5. Data Analysis

Quantitative data analysis was conducted using Microsoft Excel to summarize and analyze the survey responses. After analysis through Microsoft excel bar graphs generated by plotting age group of the population under examination in x-axis as constant for all 10 bar graphs. Y axis is plotted by segregating the responses gathered from 10 questions with respect to x-axis as age group in the bar graph.

Findings will be interpreted to identify prevalent perceptions, concerns, and behaviors related to cybercrime and cybersecurity among the general population of India.

3.6. Ethical Considerations

The study adhered to ethical guidelines for research involving human participants. Informed consent was obtained from all participants before they completed the questionnaire. Participation was voluntary, and participants were assured of confidentiality and anonymity.

3.7. Limitations

- The study's findings may be subject to response bias due to self-reporting.
- The sample may not be fully representative of the entire Indian population, particularly those without access to the internet.

IV. Result

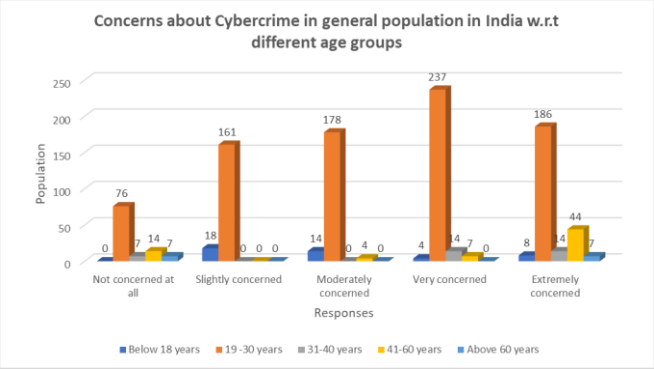

Figure 1: Concerns About Cybercrime in India According to Various Age Groups

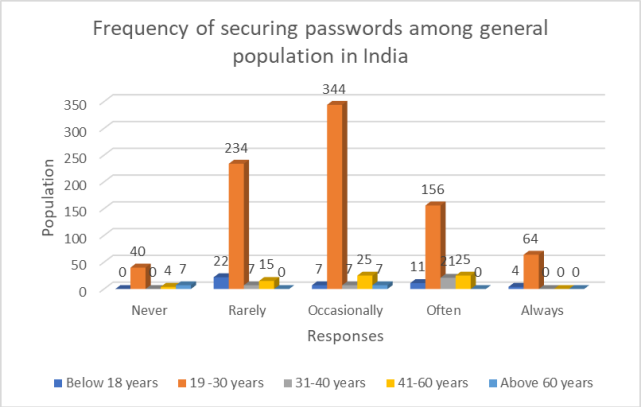

Figure 2: Frequency of Securing Passwords

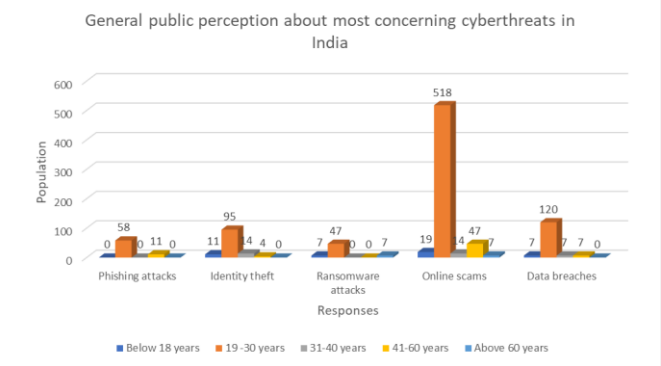

Figure 3: Public Perception about most concerning cyberthreats in India

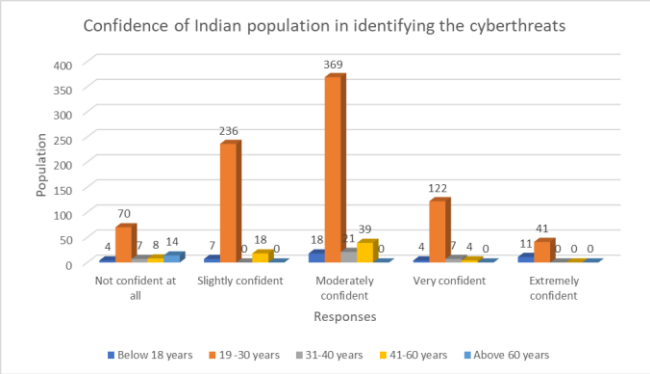

Figure 4: Confidence of Indian Population in Identifying Cyberthreats

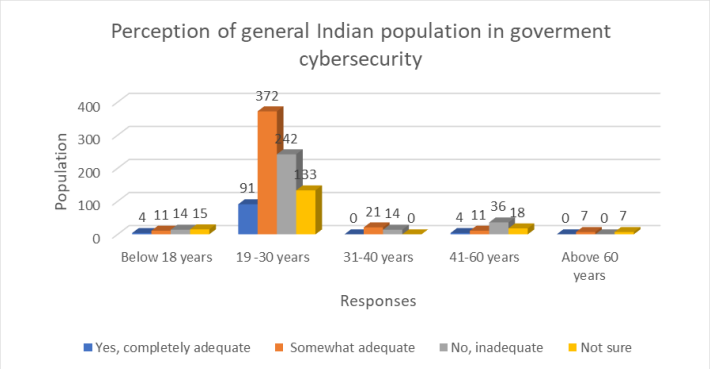

Figure 5: Perception Of Population Related to Government Cybersecurity

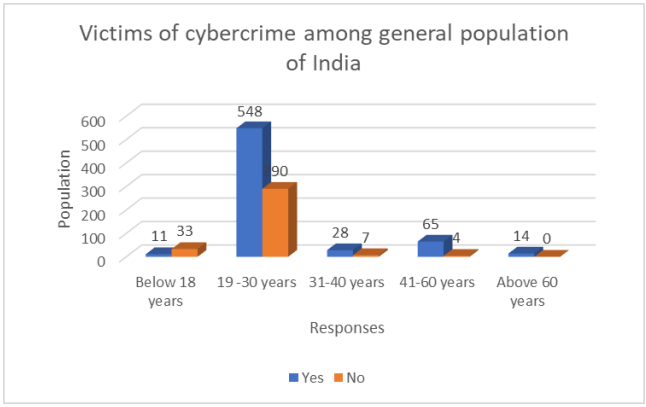

Figure 6: Victims Of Cybercrime Among General Population

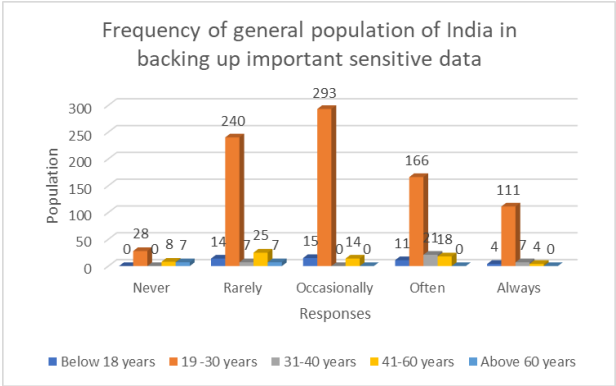

Figure 7: Frequency of population backing up sensitive data

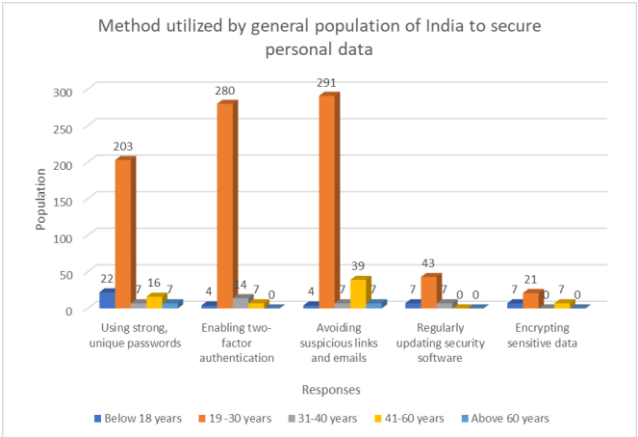

Figure 8: Method utilized by population to secure personal data.

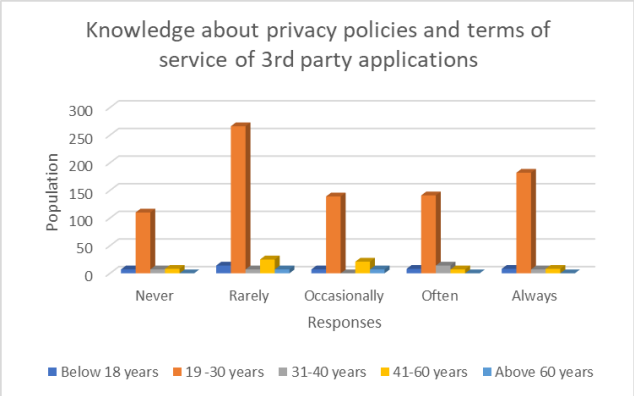

Figure 9: Knowledge about privacy policies and terms of service of 3rd party applications

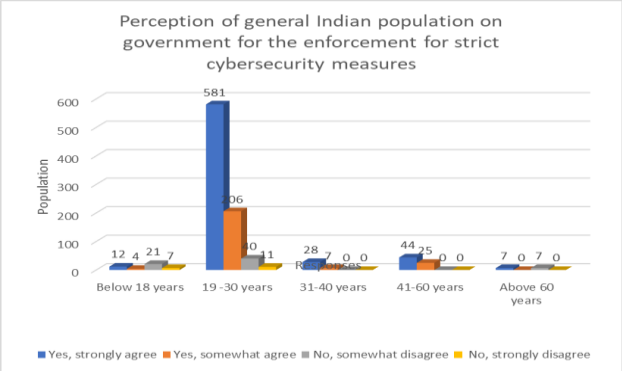

Figure 10: Perception of population about enforcement of strict anti-cybercrime measures

In figure 1, the data illustrates varying levels of concern about cybercrime across different age groups in India. Among individuals below 18 years, 44% are slightly concerned, 31% are moderately concerned, 9% are very concerned, and 18% are extremely concerned. In the age group of 19 to 30 years, the concern levels are higher, with 19% slightly concerned, 21% moderately concerned, 28% very concerned, and 22% extremely concerned. Individuals aged 31 to 40 years show minimal concern, with 40% extremely concerned. The age bracket of 41 to 60 years indicates varied levels of concern, with 20% not concerned at all, 5% moderately concerned, 10% very concerned, and 63% extremely concerned. Lastly, among individuals above 60 years, 50% are not concerned at all, 50% are extremely concerned.

In figure 2, the data from the table highlights the varied patterns of password security practices across different age groups in India. Among individuals below 18 years, about a 50% rarely secure their passwords, while roughly 9% consistently implement strong security measures. Notably, the age cohort of 19 - 30 years demonstrates a higher commitment to password security, with over half consistently securing their passwords, although a significant portion still exhibit irregular security practices. Individuals aged 31 - 40 years show a notable variability in password security behaviors, with 60% often securing their passwords, while none consistently maintain high-security standards. The age group of 41 - 60 years exhibits a mixed pattern, with around 36% often securing passwords but none consistently maintaining high-security practices. Among individuals above 60 years, approximately 50% never secure their passwords, indicating a significant gap in security awareness.

In figure 3, the data illustrates the public perception of the most concerning cyberthreats in India across various age groups. Among individuals below 18 years old, online scams are particularly worrying at 43% and identity theft at 25%. In the age group of 19 - 30 years, online scams emerge as the most concerning cyberthreat, with a striking 518 individuals expressing worry, followed by data breach at 120, identity theft at 95 and phishing attacks at 58. Individuals aged 31 - 40 years and 41 - 60 years exhibit relatively lower levels of concern across all categories, with online scams being the most worrying cyberthreat. For those above 60 years, ransomware attacks and online scams are the primary concerns, with 50% expressing worry in each category.

In figure 4, the data reflects the confidence levels of the Indian population across various age groups in identifying cyberthreats. Among individuals below 18 years old, 40% express moderate confidence. In the age bracket of 19 - 30 years, a substantial proportion (44%) feel moderately confident, while 4% feel extremely confident. Conversely, 8% in this age group admit to not feeling confident at all. Individuals aged 31 - 40 years show varied confidence levels, with 60% feeling moderately confident and 20% feeling very confident. Meanwhile, among those between 41 - 60 years, 56% feel moderately confident. For individuals above 60 years, 100% acknowledge feeling not confident at all. These findings highlight the need for targeted efforts to enhance cybersecurity awareness and education.

In figure 5, the data presents perceptions regarding the adequacy of government cybersecurity among various age groups. Among individuals below 18 years, 25% consider government cybersecurity to be somewhat adequate, while 31% find it inadequate. For the age group of 19 - 30 years, a significant majority (48%) perceive government cybersecurity as somewhat adequate, while 15% express uncertainty about its adequacy. Conversely, 31 - 40 years old, 60% believe

government cybersecurity is somewhat adequate, while 40% find it inadequate. Meanwhile, among those between 41 - 60 years, 15% view government cybersecurity as somewhat adequate, while 52% deem it inadequate. These findings suggest potential gaps in public confidence.

In figure 6, among individuals below 18 years old, 25% have reported being victims of cybercrime, while 75% have not experienced it. In the age group of 19 - 30 years, a significant majority (65%) have experienced cybercrime, while 34% have not. Among those aged 31 - 40 years, 80% have been victims of cybercrime. In the 41 - 60 age group, 100% have experienced cybercrime.

In figure 7, the data outlines the frequency with which individuals across various age groups back up important sensitive data. Among those below 18 years old, 31% rarely back up their data, while 34% do so occasionally, and 25% do it often. Conversely, 19 - 30-year-olds display a wider range of behaviors, with 28% rarely backing up data, 34% doing so occasionally, and 19% doing it often. Individuals aged 31 - 40 years and 41 - 60 years primarily back up data occasionally, with 60% and 20% respectively, while some do so rarely or often. Among those above 60 years, 50% back up data rarely and 50% do it occasionally, with none doing it often or always. These findings highlight potential areas for enhanced data management education and awareness initiatives.

In figure 8, the data showcases the methods employed by various age groups to secure their personal data. Among individuals below 18 years, a significant portion (50%) rely on using strong, unique passwords, while smaller percentages utilize other methods such as enabling two-factor authentication (9%), avoiding suspicious links and emails (9%), and regularly updating security software (15%). Similarly, in the 19 - 30 age group, substantial percentages prioritize using strong, unique passwords (24%) and enabling two-factor authentication (33%), while fewer individuals focus on other security measures. In the 31 - 40 age bracket, the emphasis on security methods is relatively lower, with only a small percentage opting for two-factor authentication (40%) and regular software updates (20%). Individuals aged 41 - 60 years demonstrate a mixed approach, with notable attention given to avoiding suspicious links and emails (56%) and using strong, unique passwords (23%). Among those above 60 years, the reliance on security measures is relatively lower, with minimal engagement in two-factor authentication and software updates.

In figure 9, the data reveals the frequency at which individuals of varying age groups engage with the privacy policies and terms of service of third-party applications. Among those below 18 years old, 31% admit to rarely or never reading these policies, while 15% occasionally do so, and 18% often or always review them. In the 19 - 30 age group, a significant proportion (67%) rarely or never delve into these documents, while 16% occasionally do, and 36% often or always do. Individuals aged 31 - 40 years exhibit relatively consistent patterns, with 50% indicating regular engagement. Similarly, individuals aged 41 - 60 years show comparable levels of involvement, with 40% indicating occasional or regular review. Among those above 60 years, 50% rarely read these policies.

In figure 10, the data presents the agreeability of individuals across various age groups regarding the enforcement of stricter anti-cybercrime measures by the government. Among those below 18 years old, 27% strongly agree, while 9% somewhat agree, with 47% indicating some level of disagreement. In the 19 - 30 age group, a significant majority (69%) strongly agree, while 25% somewhat agree, and only 4% express disagreement to some extent. Individuals aged 31 - 40 years and 41 - 60 years generally support the notion, with 80% and 63% expressing agreement respectively. Among those above 60 years, 50% strongly agree, while 50% indicate some level of disagreement.

V. Discussion

The survey results provide valuable insights into the cybersecurity landscape across different age groups in India, shedding light on perceptions, practices, and concerns regarding cyber threats and security measures. These findings are complemented by existing research studies that have delved into various aspects of cybercrime in the Indian context. [23] study emphasizes the imperative for a holistic approach in addressing cyber challenges, considering economic development, governance structures, and global dynamics. This resonates with the survey findings, which highlight varying levels of concern about cybercrime across different age groups, underscoring the need for comprehensive cybersecurity strategies. [24] advocate for regulatory compliance in data protection and international cooperation in combating cybercrime, aligning with the survey's emphasis on the importance of government cybersecurity efforts. The survey reveals varying perceptions of government cybersecurity measures among different age groups, reflecting the complexities of public trust and confidence in

cybersecurity initiatives. [25] stresses the importance of legal harmonization, international cooperation, and multifaceted approaches to combat cybercrime. This is echoed in the survey findings, which underscore the need for targeted cybersecurity education and awareness initiatives tailored to different age demographics. [26] advocate for raising awareness about cybersecurity and proactive measures to mitigate risks and protect data privacy. Similarly, the survey highlights disparities in confidence levels among different age groups in identifying cyber threats, suggesting opportunities for enhancing cybersecurity literacy and education. [27] and [28] explore public perceptions towards cybercrimes and the impact of cybersecurity threats on e-banking adoption, emphasizing the importance of strengthening security measures and raising awareness among the public. These findings underscore the urgency of addressing cybersecurity concerns and promoting safe online practices. [29] investigates the escalating cybercrime landscape in India and stresses the need for robust cybersecurity measures and legislative actions. This aligns with the survey's findings on the prevalence of cybercrime victimization and the importance of government intervention in combating cyber threats effectively. [30] discusses the impact of technological advancements on global communication and the rise of cybercrimes, highlighting the challenges in cybercrime investigations and proposing safety measures to combat cyber threats. These insights further inform the discussion on the evolving nature of cyber threats and the importance of adaptive cybersecurity strategies. [8] highlight the emergence of forensic accounting in combating financial frauds worldwide, emphasizing its significance in addressing economic crimes. This underscores the interconnectedness of cybercrime with financial fraud and the need for interdisciplinary approaches to combat cyber threats effectively. Kaur et al.'s study (2024) examines the psychological implications of accessing the dark web, emphasizing the need for public awareness campaigns and interventions to promote mental well-being and safe internet practices. This aligns with the broader discussion on the societal impacts of cybercrime and the importance of addressing both technical and psychological aspects of cybersecurity. In conclusion, the integration of survey findings with existing research studies provides a comprehensive understanding of the cybersecurity landscape in India and underscores the multifaceted challenges and opportunities in combating cyber threats and promoting digital resilience across different age groups.

VI. Conclusion

The rise of cybercrimes in India poses a significant threat, particularly for residents of Smart Cities (SCI), necessitating effective prevention measures. Addressing it, particularly in Smart Cities, demands a multi-faceted approach. This includes enhancing awareness among citizens through government-led initiatives like workshops, conferences, and awareness programs such as the National Information Security Awareness Program. The National Cyber Security Policy, 2013, serves as a cornerstone for establishing a secure cyberspace [31]. The survey findings provide valuable insights into the cybersecurity landscape across different age groups in India, highlighting varying levels of concern, practices, and perceptions regarding cyber threats and security measures. Effective cybersecurity measures, encompassing both technical and psychological aspects, are essential to combat cyber threats and promote digital resilience.

VII. Authors Contribution

Pragati Jain: Conceptualization, Survey Questionnaire Formation, Drafting of the article.
Leoson Heisnam: Survey questionnaire designing, questionnaire distribution offline, response collection, data handling, drafting of the original article, Editing etc.
Ashish Kumar: Online survey circulation, Data collection, drafting of the original article, proof reading etc.
Shefali Chaudhury: Literature review, Data Circulation online and offline, Data collection offline and online, drafting original article etc.
Sonali Balouria: Conceptualization, Survey Questionnaire Formation, Ammeding corrections instructed from the journal, proof reading, drafting of the original article etc.
Abhishek Sapkal: Statistical analysis of the data, Bar graph formation, data sorting, data handling, drafting of the original article etc.

References:

[1] P. Kapila, “Cyber crimes and cyber laws in India: an overview,” *Contemporary Issues and Challenges in the Society*, pp. 36–48.
[2] Nidhi Narnolia, “Cyber Crime In India: An Overview,” https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html.
[3] D. Halder, “Cyber stalking victimisation of women: Evaluating the effectiveness of current laws in India from restorative justice and therapeutic jurisprudential perspectives,” *Halder Debarati (2015)" Cyber Stalking Victimisation of Women: Evaluating the Effectiveness of Current Laws in India from Restorative Justice and*

Therapeutic, in Jurisprudential Perspectives," published in TEMIDA Decembar, pp. 103–130, 2015.
[4] A. Miftha, M. Conrad, and M. Gibson, "Cyber stalking is a social evil: from the Indian women's perspective," 2019.
[5] V. D. Sharma and F. Wooldridge, "The law relating to obscene publications in India," *International & Comparative Law Quarterly*, vol. 22, no. 4, pp. 632–647, 1973.
[6] N. Khan, A. Shaikh, and M. V. P. Singh, "Understanding of cyber defamation and its impact: a critical analysis," *Dogo Rangsang Res J*, vol. 13, pp. 168–173, 2023.
[7] K. Pandove, A. Jindal, and R. Kumar, "Email spoofing," *Int J Comput Appl*, vol. 5, no. 1, pp. 27–30, 2010.
[8] G. Kaur and D. Mukherjee, "An Insight into Forensic Accounting," *Indian Journal of Forensic Medicine and Toxicology*, vol. 17, Jan. 2023, doi: 10.37506/ijfmt.v17i1.18887.
[9] S. Bhadury, "Child pornography in India: issues and challenges," *Journal of Positive School Psychology*, pp. 6524–6529, 2022.
[10] G. Kaur, D. Mukherjee, B. Moza, V. Pahwa, K. Kaur, and K. Kaur, "The dark web: A hidden menace or a tool for privacy protection," *IP International Journal of Forensic Medicine and Toxicological Sciences*, vol. 8, pp. 160–167, Jan. 2024, doi: 10.18231/j.ijfmts.2023.034.
[11] I. Mahmood, M. A. Rahman, M. A. Kabir, and M. Shahriar, "A Survey on Dark Web Monitoring and Corresponding Threat Detection".
[12] D. M. B. M. Priyanka Verma, "Decentralized Money: A Comprehensive Review on Cryptocurrencies," *International Journal of Advanced Trends in Computer Applications*, vol. 9, no. 2, pp. 35–41, Aug. 2023.
[13] J. J. Román, A. Q. Al Obaidli, A. H. Almuaini, and C. A. Cancino, "Evolution and trends of intellectual property crime research between 1991 and 2020," *International Journal of Business Environment*, vol. 14, no. 3, pp. 370–394, 2023.
[14] C. Piyush, "A survey of the prominent effects of cybersquatting in india," *Int'l J. Info. Sec. & Cybercrime*, vol. 4, p. 47, 2015.
[15] J. K. Malik and S. Choudhury, "Policy Considerations In India Against Cyber Crime," *Int J Recent Sci Res*, vol. 9, no. 12, pp. 29811–29814, 2018.
[16] D. Halder, "Information Technology Act and cyber terrorism: A critical review," *Available at SSRN 1964261*, 2011.
[17] C. Billo and W. Chang, "Cyber warfare," *An Analysis of the means and motivations of selected nation states. Dartmouth, ISTS*, 2004.
[18] Ministry of Home Affairs, "Cases of Cyber Frauds," https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158.
[19] A. Sharma, A. Tyagi, and M. Bhardwaj, "Analysis of techniques and attacking pattern in cyber security approach: A survey," *Int J Health Sci (Qassim)*, no. II, p. 431188, 2022.
[20] V. K. Gunjan, A. Kumar, and S. Avdhanam, "A survey of cyber-crime in India," in *2013 15th international conference on advanced computing technologies (ICACT)*, IEEE, 2013, pp. 1–6.
[21] P. N. V. Kumar, "Growing cyber-crimes in India: A survey," in *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*, IEEE, 2016, pp. 246–251.
[22] A. C. Narahari and V. Shah, "Cyber Crime and Security–A Study on Awareness among Young Netizens of Anand, Gujarat State, India," *IJARIIE*, vol. 6, no. 2, pp. 1164–1172, 2016.
[23] N. Kshetri, "Cybercrime and cybersecurity in India: causes, consequences and implications for the future," *Crime Law Soc Change*, vol. 66, pp. 313–338, 2016.
[24] R. Sabillon, V. Cavaller, J. Cano, and J. Serra-Ruiz, "Cybercriminals, cyberattacks and cybercrime," in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, IEEE, 2016, pp. 1–9.
[25] X. Li, "Cybersecurity and Cybercrime in the 21st Century," *Helsinki, Finland: Informyth*, 2016.
[26] R. Buch, D. Ganda, P. Kalola, and N. Borad, "World of cyber security and cybercrime," 2017.
[27] Y. Chauhan, "Cybercrime: A Survey for Perception of Adults," *Supremo Amicus*, vol. 19, p. 672, 2020.
[28] A. B. Jibril, M. A. Kwarteng, M. Chovancova, and R. Denanyoh, "Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study," in *ICCWS 2020 15th International Conference on Cyber Warfare and Security*, Academic Conferences and publishing limited, 2020.
[29] V. P. S. Ponniah, "Cyber Security in India: Law and Practice," *NeuroQuantology*, vol. 20, no. 17, p. 1479, 2022.
[30] T. Gupta, "EMERGING TRENDS OF CYBER CRIME IN INDIA: A CONTEMPORARY REVIEW," *Journal of Law and Policy Transformation*, vol. 8, no. 1, pp. 57–65, 2023.
[31] S. Chatterjee, A. K. Kar, Y. K. Dwivedi, and H. Kizgin, "Prevention of cybercrimes in smart cities of India: from a citizen's perspective," *Information Technology & People*, vol. 32, no. 5, pp. 1153–1183, 2019.

Author's Profile

Pragati Jain
Post Graduate, University Institute of Applied Health
Science, Chandigarh University, Ludhiana, Punjab

Leoson Heisnam
Visiting Faculty, Institute of Forensic Science for Training and Skilling, National Forensic Sciences University (NFSU)

Ashish Kumar
Post Graduate, University Institute of Applied Health
Science, Chandigarh University,
Ludhiana, Punjab

Shefali Chaudhary
Post Graduate, University Institute of Applied Health
Science, Chandigarh University,
Ludhiana, Punjab

Sonali Balouria
Post Graduate, University Institute of Applied Health
Science, Chandigarh University,
Ludhiana, Punjab

Abhishek Sapkal
Bachelors of computer application,
Amravati University,
Akola, Maharashtra