VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL
VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Security, Privacy & Ethics in Digital Era

Hemangi Tandel[1], Rudraksh Zodage [2]
[1](*Department of AI ML, VIVA Institute of Technology/ Mumbai University, India)*
[2](*Department of AI ML, VIVA Institute of Technology/ Mumbai University, India)*

Abstract: *The rapid growth of digital technologies has transformed the way we live, work, and interact, but has also raised significant concerns about security, privacy, and ethics. As we increasingly rely on digital systems, we are vulnerable to various types of threats, including phishing, ransomware, malware, social engineering, cyberstalking, online harassment, and identity theft. Furthermore, the rise of advanced persistent threats (APTs), zero-day exploits, and IoT-based attacks has exacerbated these concerns, posing significant risks to individual autonomy, privacy, and human rights. Additionally, the proliferation of fake news, deepfakes, and disinformation campaigns has created new challenges for online trust and credibility. To address these concerns, it is essential to develop and implement robust security measures, ensure transparency and accountability in data collection and use, and promote digital literacy and critical thinking, while establishing clear ethical guidelines and regulations that prioritize human values and well-being, balancing the benefits of technology with the need to protect individual rights, promote social justice, and ensure human well-being. Ultimately, this requires a multidisciplinary approach that involves policymakers, industry leaders, civil society organizations, and individual citizens working together to create a secure, private, and ethical digital future.*

Keywords – *Cybersecurity, Data Protection, Digital Ethics, Online Privacy, Surveillance Capitalism, Trust Management, Malware, Social Engineering.*

I. INTRODUCTION

The contemporary era of digitalization has undergone a metamorphosis in our lifestyle, profession, and interpersonal interactions. The pervasive adoption of digital innovations, such as the worldwide web, social networking platforms, and handheld devices, has revolutionized our communication methods, access to information, and business operations. However, this digital transformation has also raised substantial apprehensions about security, privacy, and ethics. In today's digital terrain, individuals, corporations, and governments are vulnerable to various types of cyber threats, including phishing, ransomware, and malware, social engineering, and identity theft. According to a report by Cybersecurity Ventures, the global cost of cybercrime is projected to reach $6 trillion by 2021, up from $3 trillion in 2015.

Furthermore, the collection and examination of vast amounts of personal data have raised questions about informed consent, monitoring, and bias. A survey by the Pew Research Center found that 72% of Americans believe that their personal data is less secure than it was five years ago. The use of artificial intelligence, machine learning, and data analysis has further aggravated these concerns, posing significant risks to individual autonomy, privacy, and human rights. For instance, a study by the MIT Technology Review found that AI-powered facial recognition systems can be biased against certain racial and ethnic groups. To address these concerns, it is essential to develop and implement effective security measures, ensure openness and responsibility in data collection and utilization, and promote digital awareness and analytical thinking. This requires a multidisciplinary approach that

involves policymakers, industry leaders, civil society organizations, and individual citizens working together to create a secure, private, and ethical digital future.

Common Types of Online Fraud:

- **Phishing**: Deceptive emails, messages, or websites designed to steal confidential information like passwords, credit card numbers, or bank account details.
- **Identity Theft:** The unauthorized use of someone's personal information (such as Social Security numbers or bank details) to commit fraud or other illicit activities.
- **Online Banking Fraud:** Dishonest activities involving unauthorized transactions, theft of online banking credentials, or fraudulent attacks targeting banking users.
- **Credit/Debit Card Fraud:** Deceptive use of a credit or debit card for unauthorized purchases, including card cloning or skimming.
- **Business Email Compromise (BEC):** Scams where attackers impersonate executives or employees within a company to manipulate employees into transferring funds or sharing confidential information.
- **Ransomware:** A type of malicious software that locks users out of their systems or encrypts their data, demanding payment for access to be restored.
- **Social Media Scams:** Fraudulent activities conducted on social media platforms, including fake profiles, impersonation, and scams that deceive users into sharing personal or financial details.
- **Online Auction Fraud:** Dishonest activities that occur in online auction sites, where sellers mislead buyers about product quality or fail to deliver the promised items.
- **Cryptocurrency Scams:** Fraudulent schemes that trick users into investing in bogus cryptocurrency opportunities or mining schemes, resulting in loss of funds.
- **Fake Online Stores:** E-commerce websites set up to scam users by offering nonexistent products or delivering counterfeit or low-quality goods.

II. METHODOLOGY

I. Research Design

We used a **mixed-methods approach**, combining both quantitative (numbers) and qualitative (stories) research to get a complete understanding of the topic, as shown in **Figure 2**.

II. Data Collection Methods

We used three main methods to gather data:

1. **Survey**: A set of questions to collect numerical data.
2. **Secondary Data Analysis**: Analyzing existing data to support our findings.
3. **Interviews**: Speaking with people to gather detailed, personal insights, as shown in **Figure 4**.

III. Data Analysis Methods

We applied **descriptive statistics** to summarize and interpret the data collected, as shown in **Figure 3**.

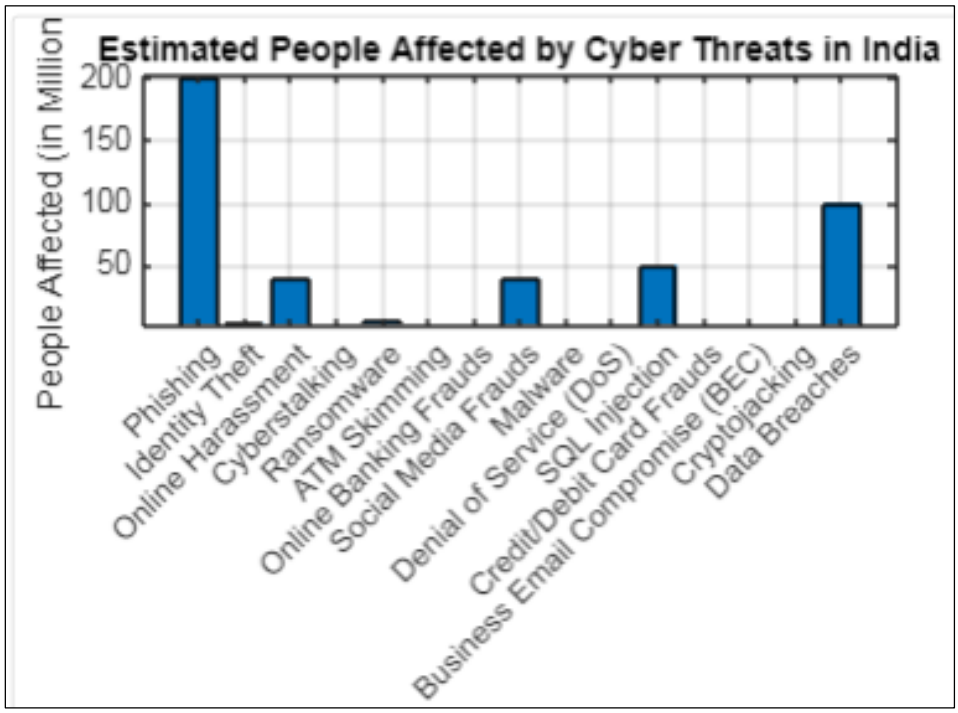
IV. Sampling Strategy

Two sampling methods were used:

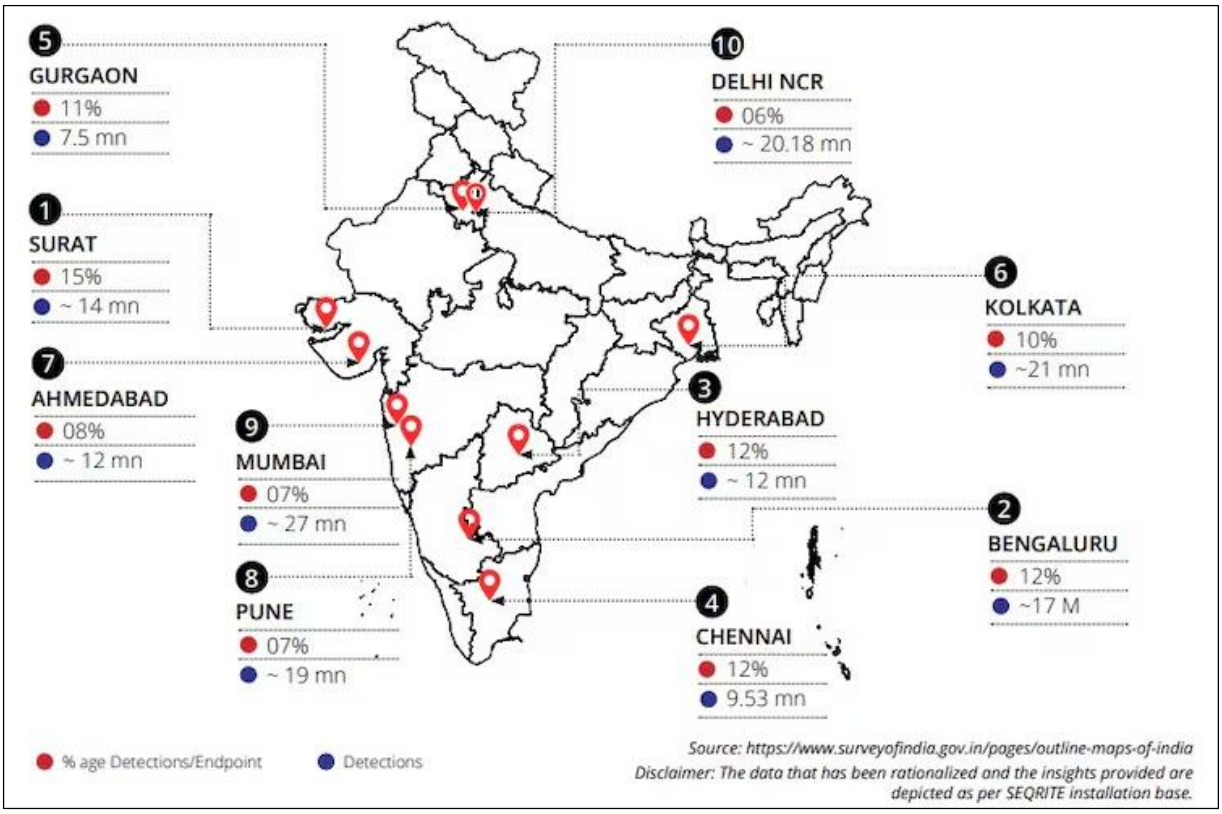
1. **Random Sampling**: Randomly selecting participants to ensure fairness.
2. **Purposive Sampling**: Selecting specific individuals who had relevant experiences to provide deeper insights into the topic.

III. CHART AMD TABLE

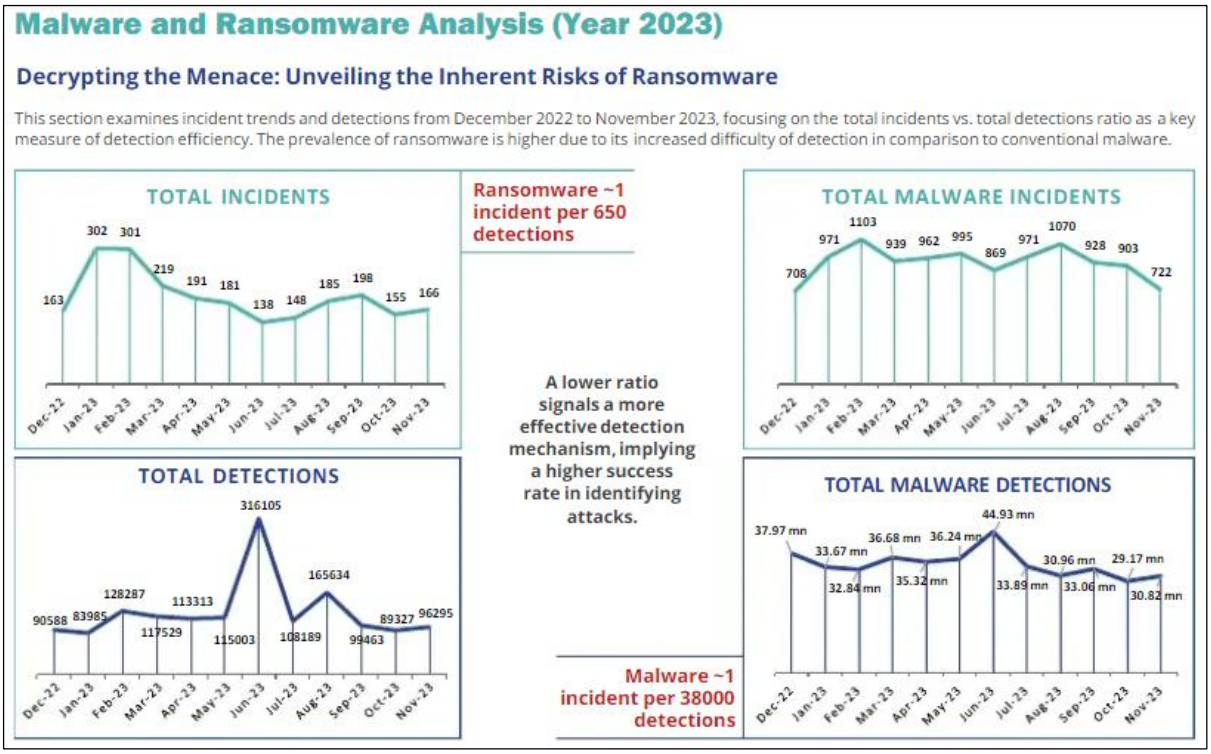
(FIG. 1) (ESTIMATED PEOPLE AFFECTED BY CYBER THREATS BY OUR RESEARCH)



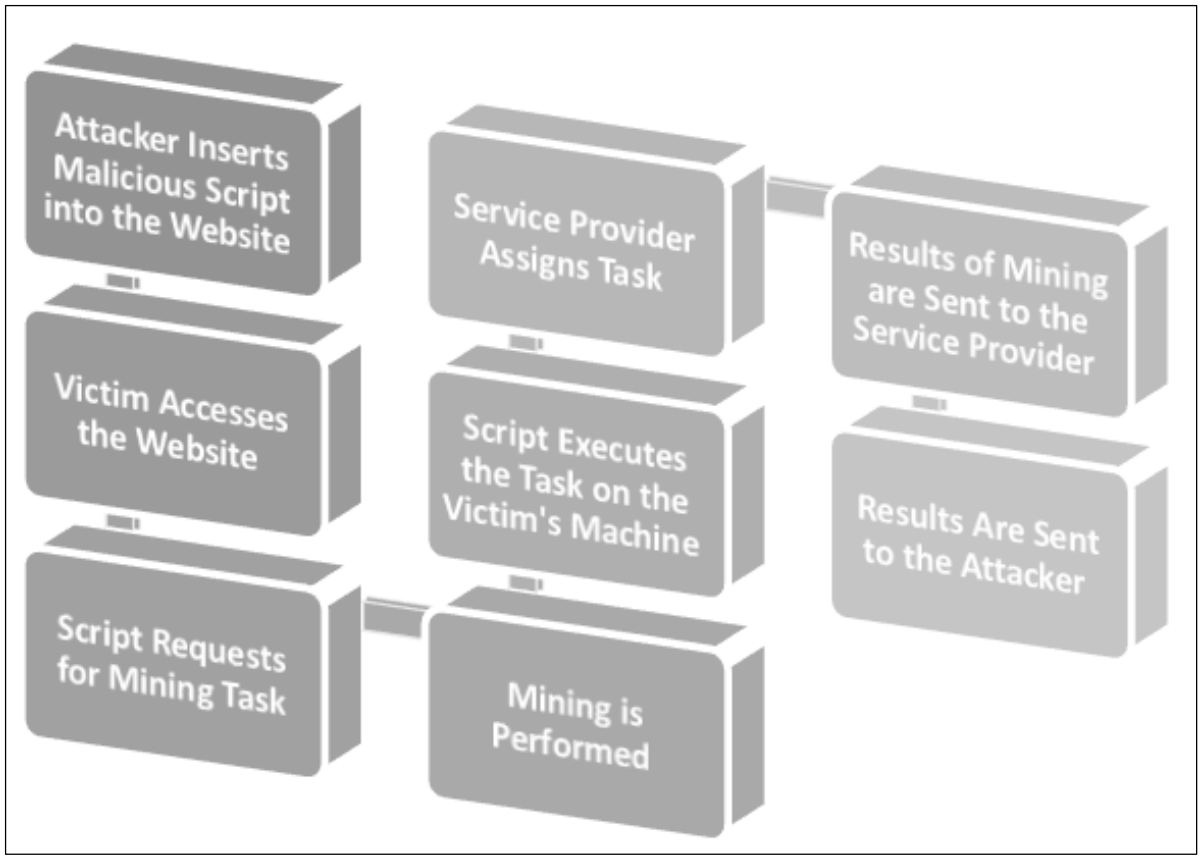
(FIG. 2) (STATES AFFECTED BY CYBER THREATS IN INDIA IN 2023)



(FIG. 3) (MALWARE AND RANSOMWARE ANALYSIS IN INDIA IN 2023)



(FIG. 4) (PROCESS OF WEB HACKING)



(Table. 1) (Past Record of Company's Data which was Breached)

Company Name	Year of Breach	Number of Records Compromised	Type of Data Compromised
Yahoo	2013-2014	3 billion	Email addresses, passwords, names
Equifax	2017	147 million	Social Security numbers, credit card info
Target	2013	40 million	Credit/debit card information
Facebook	2018	50 million	Usernames, passwords, security tokens
Adobe	2013	153 million	Email addresses, encrypted passwords
LinkedIn	2012	165 million	Email addresses, passwords
Marriott International	2018	500 million	Passport numbers, personal details
Sony PlayStation Network	2011	77 million	Names, passwords, payment info
Uber	2016	57 million	Names, email addresses, phone numbers
Capital One	2019	106 million	Credit card application data
SBI (State Bank of India)	2020	1 million+	Customer details, account info
BigBasket	2020	20 million+	Names, email addresses, addresses

Aadhaar	2018	1.1 billion	Personal details
Zomato	2017	17 million	Usernames, hashed passwords
Air India	2021	4.5 million	Personal details, passport info
JustDial	2017	100 million	Personal details, phone numbers
Flipkart	2020	1 million+	Customer details, payment info
Myntra	2018	2 million	Usernames, shipping addresses
IndusInd Bank	2020	1.4 million	Customer account details, card information
Paytm	2018	3.4 million	Mobile numbers, transaction details
ICICI Bank	2020	1 million+	Customer details, account info
Snapdeal	2017	6 million	Usernames, email addresses, phone numbers
HDFC Bank	2021	4 million	Account information, debit/credit card details
Bharat Sanchar Nigam Limited (BSNL)	2020	2 million	Customer names, phone numbers, addresses
Quikr	2017	1.5 million	Usernames, email addresses, phone numbers
Zoom	2020	500,000+	Email addresses, passwords, information
KYC (Know Your Customer) Database	2021	1 million+	Personal details, financial information
IRCTC (Indian Railways)	2018	20 million	Personal information, booking details, passwords
Cleartrip	2019	2 million	Customer details, flight booking info

III. Acknowledgment

I would like to express my sincere appreciation to everyone who supported and contributed to the successful completion of this research. I am especially thankful to my mentor for their invaluable direction, encouragement, and expertise, which were pivotal in shaping this work. My gratitude also extends to the faculty members, researchers, and experts whose contributions laid the foundation for my study. I am grateful to my peers and colleagues for their moral support, constructive discussions, and insightful suggestions that helped refine my approach. Additionally, I acknowledge my family and friends for their unwavering encouragement, understanding, and patience throughout this journey, which kept me focused and motivated. Finally, I express my gratitude to the organizations and resources that provided valuable data and research papers, as their contributions made this work possible. Thank you all for your constant support and encouragement.

IV. CONCLUSION

The analysis emphasizes the growing repercussions of cyber threats in India, with millions affected by phishing, identity theft, malware attacks, and data leaks. Notable occurrences involving companies such as Zomato and Air India expose deficiencies in data protection systems, while financial fraud and online bullying remain prevalent. To tackle these challenges, it is imperative to boost awareness, implement stringent cybersecurity protocols, embrace cutting-edge technologies, and reinforce enforcement frameworks. Cooperative efforts are essential to safeguarding India's digital ecosystem and ensuring the protection of its users. Given the dynamic nature of cyber threats, it is crucial to continuously evolve protective measures, keeping pace with emerging technologies and strategies. Educating users on safe digital practices and promoting a proactive stance against cybercrimes will also be pivotal in mitigating these risks. Furthermore, stronger partnerships between government bodies, private sectors, and the community will help build a more resilient cybersecurity infrastructure, ultimately fostering a safer digital environment for all in this world and make the feel safer than better.

V. REFERENCES

[1] Cybersecurity in India: Challenges, Threats, and Future Directions" by Ravi Kumar, Shweta Agarwal, and Deepak Mehta. (2020)
[2] Phishing Attacks and Detection Methods in India: A Review" by Anjali Sharma and Rakesh Singh. (2021)
[3] Impact of Ransomware in India: A Study on Cybercrime Trends and Prevention" by Amit Kumar and Neha Rani. (2022)
[4] Online Banking Fraud in India: Vulnerabilities and Preventive Measures" by Sudhir S. Patil and Shruti Deshmukh. (2019)
[5] N. Pandey and A. B. Sharma, "Cyberstalking and Online Harassment in India: Legal and Technological Challenges," *Journal of Cyber Law and Ethics*, vol. 10, no. 1, pp. 22-30, 2022.