IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Ethical Hacking And Cybersecurity Policies: Exploring Security Issues And Ethical Hacking Methods In India

Priyanka.M,
Dept of MCA, K.S Group of Institutions
Bengaluru, India

Abstract

This study highlights the importance of cybersecurity and ethical hacking in India by examining the various policies, tools, and methods. The focus revolves around the efficacy of legal structures and policies regarding the cybercrimes that are surfacing in India. Cybersecurity is essential in today's digital world, as it shields private information, sensitive data, and vital infrastructure from online attacks. The swift development of digital technologies in India has resulted in a rise in cybersecurity risks, jeopardizing the availability, confidentiality, and integrity of critical data. Ethical hacking has emerged as a crucial tool in identifying and mitigating these threats. Strong cybersecurity measures aid in preventing monetary, reputational, and even loss of life due to the increase in cyberattacks such as ransomware, malware, and phishing. This report highlights the security concerns and difficulties by examining the present status of cybersecurity regulations and ethical hacking techniques in India. Strong cybersecurity regulations, practical ethical hacking techniques, and awareness campaigns are necessary to counteract cyber threats, according to a thorough review of the literature and professional viewpoints.

Keywords: cybersecurity, cybercrime, ethical hacking, cybercrime in India, government policies on cybersecurity in India, data protection laws in India, cybercrimes in India

Introduction

As digital technology continues to evolve, cybersecurity has emerged as a crucial concern for national security, businesses, and individuals. To combat the growing threats in cyberspace, India has introduced various policies and regulations aimed at securing its digital infrastructure. Ethical hacking plays a significant role in this process by identifying vulnerabilities and strengthening security systems before cybercriminals can exploit them. Ethical hackers, also known as "white-hat" hackers, use their skills to detect security flaws and assist organizations in mitigating cyber risks.

This paper examines India's cybersecurity landscape by addressing key challenges such as data breaches, ransomware attacks, and privacy risks. It also highlights the role of ethical hacking in mitigating these threats while evaluating the legal and policy frameworks, including the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and directives from key agencies such as CERT-In and NCIIPC. Furthermore, this study explores various ethical hacking techniques, including penetration testing, vulnerability assessments, and red teaming, emphasizing the need for proactive security strategies to safeguard India's rapidly expanding digital ecosystem.

Cybercrimes in India

Prevalent Cybercrimes in India Today

As a result of India's rapid digital transition and growing reliance on online transactions, cybercrimes have increased dramatically. Businesses, people, and national security are all seriously threatened by these crimes. Some of the most common categories of cybercrimes in India include the following:

i) AI-Based Cybercrimes and Deepfake: As artificial intelligence advances, fraudsters use altered photos and videos to propagate misleading information. Additionally, consumers are being tricked by AI-powered scam calls that mimic human voices.

ii) Digital Arrest Scam: In order to extract money from gullible victims, scammers pose as government agencies, law enforcement officers, or financial regulators in the complex cyber fraud known as the "Digital Arrest Scam." Fraudsters employ intimidation and scare tactics, accusing the victim of engaging in illicit activities such as tax fraud, money laundering, or cybercrimes, and demanding quick payment to "avoid arrest" or legal action.

Recent Digital Arrest Cases in India:

Delhi-Based Digital Arrest Scam, 2024: A scam operation was discovered in which scammers posed as Interpol and CBI officials and tricked victims into sending lakhs of rupees to "secure" their release from false criminal charges.

Kolkata Cyber Fraud Case, 2024: Scammers in police uniforms used video calls to trick victims into visiting fictitious police stations where they demanded money. (Ghosh, 2024)

West Bengal Scam, 2025: A 70-year-old man from West Bengal lost ₹6.5 lakh after scammers morphed his images and threatened to leak them. They later impersonated police, falsely claiming a suicide case and demanding money. (Bhati, 2025)

iii) Financial Frauds: Cybercriminals use UPI platforms, digital wallets, and online banking systems to carry out illegal transactions. Frauds involving credit and debit cards, such as phishing and card skimming, are also frequent and cause large losses.

iv) Cyber Terrorism & Espionage: Attackers target government and defence systems, attempting to hack into critical infrastructure or disrupt national security operations. State-sponsored cyber-attacks from foreign entities pose significant risks to India’s digital sovereignty.

v) Call Center Scams: In India, call center scams have become a major cybercrime, with scammers posing as trustworthy organizations to trick victims. These scams pose major risks to people and businesses because they frequently incorporate identity theft, financial fraud, and social engineering techniques.

vi) Online Harassment & Cyberbullying: As social media has grown in popularity, so too have online harassment, cyberbullying, and cyberstalking. Defamation and hate speech are used to distribute false information and harm reputations. Criminals also engage in releasing sexual content without consent as an act of revenge, defamation or to bully targeted individuals.

vii) Ransomware & Malware Attacks: Cybercriminals use ransomware to encrypt files and demand a ransom to unlock them. Spyware and trojans are examples of malware that is used to compromise computers, steal information, and track user activity without authorization.

Cyber Crime on the Headlines

With the swift advancement of digital technologies across various sectors, cybercrimes in India have surged, presenting serious risks to individuals, businesses, and national security. Cybercriminals take advantage of weaknesses in digital systems to carry out crimes such as financial fraud, identity theft, phishing, ransomware attacks, and data breaches. As India transitions into a digital economy, driven by initiatives like Digital India and the growing reliance on online transactions, the threat of cyberattacks has intensified.

Recent data from the Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs (MHA), highlights the increasing prevalence of cyber fraud in India. In just the first nine months of 2024, cyber fraud led to financial losses exceeding ₹11,333 crore. Among the major categories, stock trading scams accounted for ₹4,636 crore across 2,28,094 complaints, while investment frauds resulted in ₹3,216 crore in losses across 1,00,360 cases. Additionally, digital arrest frauds caused damages worth ₹1,616 crore, with 63,481 complaints filed. A notable portion—nearly 45%—of these cybercrimes

originated from countries in Southeast Asia, including Cambodia, Myanmar, and Laos, demonstrating the cross-border nature of modern cyber threats (Manral, 2024)

According to the news report by NDTV, an investigation into transnational cyber-enabled financial fraud amounts to ₹117 crore. The Central Bureau of Investigation (CBI) conducted searches at 10 locations across Delhi and its surrounding areas. This operation was initiated following a complaint from the Indian Cyber Crime Coordination Centre (I4C) under the Union Ministry of Home Affairs, highlighting the increasing prevalence of cyber financial crimes in India. The case underscores the growing challenges in tackling cyber-enabled fraud and reinforces the need for stringent cybersecurity measures and enforcement mechanisms. (Press Trust of India, 2024)

India became the second most targeted country in the world after the United States in 2024 due to a spike in cyberattacks. 95 Indian companies experienced data breaches, according to CloudSEK's ThreatLandscape Report 2024, underscoring the nation's rising cybersecurity issues. (CloudSEK Annual Threat Landscape Report 2024 | CloudSEK, n.d.)

A startling 369.01 million unique malware detections were also disclosed in the Data Security Council of India's India Cyber Threat Report 2025, highlighting the hazards brought on by India's quick digitalization. (India Cyber Threat Report 2025, n.d.)

Furthermore, from 2019 to 2023, the number of cyberattacks against government institutions increased by 138%, from 85,797 in 2019 to 204,844 in 2023, according to the Indian Ministry of Electronics and IT. (Desk, 2024)

Statistics of Cyber Crime in India

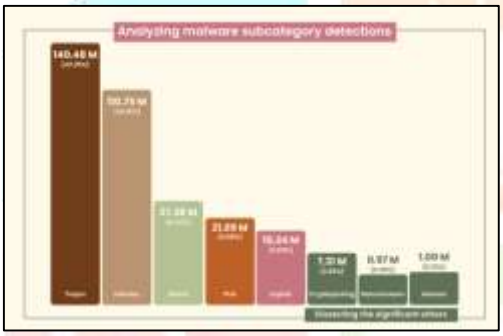

Figure 1
Source: (Data Security Council of India (DSCI) et al., 2025)

According to the India Cyber Threat report, 2025, India's cybersecurity environment has undergone an unprecedented transformation, characterized by major advancements in detection capabilities as well as an increase in attacks.

Malware remains a major problem in 2024, affecting millions of devices with different kinds of harmful software. By identifying the most common types of malwares and the efficacy of existing detection techniques, a closer examination of the malware subcategories and their detection rates offers important insights into the nature of cyber threats. (Data Security Council of India (DSCI) et al., 2025)

Analysis of Malware Subcategory Detections

The malware detection data highlights the dominance of Trojans, accounting for 43.25% (140.48 million) of total detections. This signifies that Trojans remain the most prevalent cyber threat, often serving as a gateway for further infections and unauthorized access.

Following closely, Infectors contribute to 34.10% (110.75 million) of detections. These are file-infecting malware that spread by embedding malicious code into legitimate files, making them a persistent challenge for security solutions.

Worms represent 8.43% (27.38 million) of detections, indicating their continued presence in self-replicating cyberattacks. Similarly, Potentially Unwanted Applications (PUAs) account for 6.68% (21.69 million) of detections, suggesting an increased need for awareness regarding software that may not be overtly malicious but can compromise system performance and security.

Meanwhile, Exploits, which take advantage of software vulnerabilities, contribute to 4.69% (15.24 million) of detections. This highlights the importance of timely patching and vulnerability management in cybersecurity strategies.

Among the less common but significant threats, Cryptojacking stands at 2.25% (7.31 million), showcasing the rise of unauthorized cryptocurrency mining attacks. Ransomware, though lower in percentage (0.30% or 0.97 million detections), remains a critical concern due to its potential for financial and operational damage. Similarly, Adware detections, at 0.31% (1 million), indicate the ongoing nuisance of intrusive advertisements and potential spyware risks. (Barik et al., 2022)

According to the report, most malware detections are caused by Trojan horses and infectors, underscoring the critical need for strong endpoint security measures to stop illegal access and data breaches. Furthermore, the constant threat posed by worms and potentially unwanted applications (PUAs) emphasizes the need for improved detection methods and raised user knowledge in order to reduce risks. Unpatched vulnerabilities continue to be a significant cybersecurity risk, as seen by the existence of exploits in the data. This highlights the need for frequent software upgrades and security patches to stop exploitation. Even though they happen less frequently, ransomware and cryptojacking assaults are still quite dangerous and require specific mitigating techniques to avoid operational and financial harm.

Government Policies to Mitigate Cybercrimes

The government has implemented several programs and laws to prevent and combat cybercrimes.

Cybersecurity And Cybercrime Response Agencies

CERT-In: The Indian Computer Emergency Response Team (CERT-In), functioning under MeitY, was created as the country's incident response agency under Section 70B of the Information Technology Act of 2000, is essential to protecting India's online environment. CERT-In guarantees prompt responses to reported cybersecurity incidents by running a 24-hour incident response help desk. (Safeguarding India's Digital Landscape, n.d.)

Indian Cyber Crime Coordination Centre: The Indian Cyber Crime Coordination Centre (I4C) is a government initiative set up under the Ministry of Home Affairs to deal with cybercrime in India. (Wikipedia contributors, 2025)

National Critical Information Infrastructure Protection Centre (NCIIPC):
The National Technical Research Organization (NTRO), which is a specialized institution under the Prime Minister's Office (PMO), houses the National Critical Information Infrastructure Protection Centre (NCIIPC). It was founded in 2014 with the goal of protecting India's Critical Information Infrastructure (CII) from online attacks.

Laws on Cybersecurity and Cybercrime in India

The Digital Personal Data Protection Act, 2023:
The Digital Personal Data Protection Act, 2023, incorporates established data protection principles and protects people's right to secure their personal data. Furthermore, the Reserve Bank of India's regulation under Section 10(2) and Section 18 of the Payment and Settlement Systems Act, 2007 requiring the storage of payment system data within India is an example of how the Act enforces strict restrictions on transfers of personal data. (Safeguarding India's Digital Landscape, n.d.-b)

Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021: India put into effect what are known as the Intermediary Rules in 2021. These rules create a legislative framework that regulates digital news sources, over-the-top (OTT) platforms, and social networking sites. Furthermore, they include provisions concerning data protection and complaint handling.

The DPDPA is a law that allows for the processing of digital personal data in a way that acknowledges both people's right to privacy and the necessity of processing such data for legitimate purposes. It contains explicit guidelines for reporting events and sanctions for noncompliance. (Singh & Banerjee, 2024)

Information Technology Act, 2000: Notified on October 17, 2000, the Information Technology Act, 2000 (ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000). It is India's primary law pertaining to electronic commerce and cybercrime. (Wikipedia contributors, 2025)

Some of the important Sections under the IT Act are:

Section 65 of the IT Act: Section 65 of the IT Act states that anyone who wilfully or knowingly tampers with computer source documents, conceals, destroys, alters, or causes another to conceal, destroy, or change any computer source code faces a maximum sentence of three years in prison, a fine of up to Rs two lakh, or both. According to Section 65, tampering computer source materials is a crime that carries a maximum sentence of three years in prison, a fine of Rs 200,000, or both. The Indian Penal Code (IPC) has been replaced by a new law known as the Bhartiya Nyaya Sanhita (BNS). (Singh & Banerjee, 2024)

Section 66 addresses hacking into computer systems, carrying a punishment of up to three years of imprisonment and/or a fine of up to ₹5,00,000. **Section 66B** pertains to receiving stolen computer devices or communication equipment, punishable by up to three years in prison and/or a fine of ₹1,00,000. **Section 66C** deals with unauthorized use of another person's password, leading to a similar penalty of up to three years of imprisonment and/or a fine of ₹1,00,000. **Section 66D** covers fraudulent activities using computer resources, imposing the same maximum punishment. **Section 66E** penalizes the unauthorized publication of private images of individuals, which can result in imprisonment for up to three years and/or a fine of ₹2,00,000. **Section 66F** specifically targets cyberterrorism, carrying the harshest penalty of life imprisonment. (Wikipedia contributors, 2025)

Further, **Section 67** criminalizes the publication of obscene material in electronic form, with penalties extending to five years of imprisonment and/or a fine of up to ₹10,00,000. **Section 67A** imposes even stricter penalties for sharing images containing sexual acts, leading to imprisonment for up to seven years and/or a fine of ₹10,00,000. Lastly, **Section 67C** mandates the proper maintenance of electronic records, with non-compliance resulting in imprisonment for up to three years and/or a monetary penalty. These provisions collectively aim to strengthen cybersecurity and uphold digital safety in India. (Wikipedia contributors, 2025)

Ethical Hacking

The act of intentionally searching computer systems, networks, or applications for security flaws, both legally and with consent, in order to find and address possible security threats before malicious hackers may take advantage of them is known as ethical hacking. Ethical hackers, sometimes referred to as penetration testers or white-hat hackers, employ the same strategies as cybercriminals for defensive objectives.

The Fundamentals of Ethical Hacking:

a) Authorized & Legal: Ethical hackers have the system owner's express consent.
b) Security testing: involves checking systems for flaws such software vulnerabilities, incorrect setups, or weak passwords.
c) Prevention: By locating and addressing security flaws, they assist companies in preventing cyberattacks.
d) Reporting & Suggestions: Following hacking efforts, ethical hackers record their discoveries and provide fixes.
e) Constant Learning: Since cyberthreats are constantly changing, ethical hackers need to keep up with the latest techniques and defences.

In India, ethical hacking is regulated under the Information Technology Act, 2000. The act criminalizes unauthorized access, making it essential for ethical hackers to obtain explicit permission from system owners before conducting security assessments.

To legally conduct ethical hacking in India, one must first get the system owner's written approval before performing any security assessments. A Non-Disclosure Agreement (NDA) must be signed, in order to maintain confidentiality when sensitive data is involved. As cybersecurity experts, ethical hackers are also required to follow the internal security guidelines of their organization. Additionally, participating in official bug bounty programs offered by companies provides a legal and structured way to identify vulnerabilities. Sections 43 and 66 of the Information Technology Act, 2000, make unauthorized hacking a crime that carries fines of up to ₹5 lakh and a maximum sentence of three years of imprisonment, even if done with good intentions.

Common Ethical Hacking Tools Used in India:

Ethical hacking in India involves using a variety of tools to assess and enhance the security of computer systems and networks.

These tools help cybersecurity professionals identify vulnerabilities, perform penetration testing, and strengthen digital defences.

Positive Outcomes of Cybercrime Legislation in India

Figure 2: Positive Outcomes

While cybercrime cases have surged due to increased digital adoption, some measures have shown success in mitigating losses, preventative behaviour and improving detection.

Increase in Public Awareness:

Growing Concern for Cybersecurity: According to a 2024 TechGig poll, 74% of Indian users expressed a high level of concern about cybersecurity, which is an increase over prior years. (Kumari, 2024)

Greater Responsibility Awareness: Over 84% believe individuals should take personal responsibility for their own digital safety—an encouraging cultural shift.

Increased Reporting of Cybercrime: More people are now aware of how and where to report cybercrimes, leading to greater use of platforms like the NCRP portal (cybercrime.gov.in). (Joshi & Ganapatye, 2023b)

Growth in Educational Initiatives:

Digital Literacy Campaigns: Government programs like Cyber Surakshit Bharat and Information Security Education and Awareness (ISEA) have helped improve public understanding, especially in urban and semi-urban areas. (Central Institute of Educational Technology, n.d.)

Workplace Training: Around 73% of Indian organizations now conduct regular cybersecurity training, as per 2023 industry reports.

Better Preventive Behaviour:

Two-Factor Authentication (2FA): Strong passwords and 2FA are being used more frequently, particularly by young, tech-savvy people. (Choudhary et al., 2025)

Secure App Selections: Even among non-technical users, there has been a noticeable shift toward the usage of antivirus software and privacy-focused apps.

Government and Institutional Efforts

Public Helplines: The launch of helpline 1930 has enabled quick responses and partial recovery of defrauded money, helping over 4.3 lakh victims as of late 2023.

School and College Involvement: Cybersecurity is increasingly being introduced in academic settings via workshops and awareness days, especially during Cyber Jaagrookta Diwas (Cyber Awareness Day) every month.

Conclusion

With the increasing sophistication of cyber threats, traditional security measures are no longer sufficient. The surge in AI-driven cyberattacks, state-sponsored hacking, quantum-based threats, and deepfake-enabled deception highlights the urgent need for advanced cybersecurity strategies. Enhancing ethical hacking practices, leveraging AI-powered threat detection, and preparing for post-quantum security measures are crucial for protecting digital systems. Looking ahead, a proactive and adaptive cybersecurity framework will be essential in mitigating these evolving risks.

The existing laws and strategies governing ethical hacking have significantly contributed to strengthening cybersecurity. The Information Technology Act, 2000, along with various cybersecurity policies and frameworks, has helped regulate ethical hacking, ensuring that security professionals can identify and resolve vulnerabilities while deterring cybercrime. Organizations are increasingly adopting penetration testing, bug bounty programs, and security audits to reinforce their defences. However, gaps remain, including vague legal definitions of ethical hacking, the absence of clear regulations on AI-driven cyber threats, and difficulties in enforcing cybersecurity laws across jurisdictions. To effectively address these challenges, stronger legislative measures, enhanced collaboration between government and private sectors, and continuous updates to cybersecurity policies are necessary to combat future cyber threats.

Acknowledgment

I sincerely express my gratitude to KSIT for providing me with the opportunity to conduct this research. I am especially thankful to Department of MCA, for their valuable guidance and encouragement throughout this process.

References

[1]Rafee, B. M., & Shariff, S. A. (2020). GOOD AND BAD ABOUT ETHICAL HACKING IN INDIAN PERSPECTIVE. International Journal of Technical Research & Science, 05(02), 12–18. https://doi.org/10.30780/ijtrs.v05.i02.002

[2]Savant, V. B., Kasar, R. D., & Savant, P. B. (2021). A REVIEW ON OVERVIEW OF ETHICAL HACKING. In Government Residential Women's Polytechnic Latur & SBSPM'S B Pharmacy College, International Journal of Engineering Applied Sciences and Technology (Vols. 4–4, pp. 379–383). http://www.ijeast.com

[3]Kumar, J. (2024). Legal Protection To Ethical Hacking In India (Current Scenario and Way Ahead). Legal Protection to Ethical Hacking in India (Current Scenario and Way Ahead). https://doi.org/10.2139/ssrn.4912640

[4]Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., & Koyuncu, M. (2022). Cybersecurity Deep: Approaches, attacks dataset, and comparative study. Applied Artificial Intelligence, 36(1). https://doi.org/10.1080/08839514.2022.2055399

[5]Safeguarding India's digital landscape. (n.d.). https://pib.gov.in/PressReleasePage.aspx?PRID=2037115#:~:text=The%20Indian%20Government%20has%20established,for%20addressing%20digital%20threats%20comprehensively.

[6]Wikipedia contributors. (2025, January 19). Indian Cyber Crime Coordination Centre. Wikipedia. https://en.wikipedia.org/wiki/Indian_Cyber_Crime_Coordination_Centre

[7]Manral, M. S. (2024, November 27). Rs 11,333 crore lost in just 9 months: A look at the cyber scams that have hit India the worst. The Indian Express. https://indianexpress.com/article/india/cyber-scams-india-pm-modi-9692771/

[8]Ghosh, D. (2024, September 26). 48-hr trauma for Sinthi man under 'digital arrest.' The Times of India. https://timesofindia.indiatimes.com/city/kolkata/kolkata-man-duped-of-rs-515-lakh-in-shocking-digital-arrest-scam/articleshow/113717999.cms

[9]Bhati, D. (2025, February 25). Scammers threaten West Bengal man with morphed image, dupe him of Rs 6.5 lakh in new cyber scam. India Today. https://www.indiatoday.in/technology/news/story/scammers-threaten-west-bengal-man-with-morphed-image-dupe-him-of-rs-65-lakh-in-new-cyber-scam-2685131-2025-02-25

[10]India Cyber Threat Report 2025. (n.d.). Data Security Council of India. https://www.dsci.in/resource/content/india-cyber-threat-report-2025

[11]Desk, T. T. (2024, December 5). 369 million malware threats and counting: Report reveals 'dangerous' scale of hacking in India. The Times of India. https://timesofindia.indiatimes.com/technology/tech-news/369-million-malware-threats-and-counting-report-reveals-dangerous-scale-of-hacking-in-india/articleshow/116016490.cms
Singh, M., & Banerjee, S. (2024, November 6). Cybersecurity Laws and Regulations India 2025. International Comparative Legal Guides International Business Reports. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
[12]Wikipedia contributors. (2025, January 6). Information Technology Act, 2000. Wikipedia. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
[13]Data Security Council of India (DSCI), Seqrite, & Godse, V. (2025). India Cyber Threat Report 2025. https://www.dsci.in/files/content/knowledge-centre/2024/India-Cyber-Threat-Report-2025.pdf
[14]Kumari, R. (2024, November 8). TechGig survey reveals 74 of users fear cyber threats, yet few take action. TechGig. https://content.techgig.com/TechGig-survey-reveals-74-of-users-fear-cyber-threats-yet-few-take-action/articleshow_b2b/115063242.cms?
[15]Joshi, M., & Ganapatye, M. (2023b, June 27). 22 lakh cybercrime complaints on national portal, but states' FIR count at 2%: RTI Response- News18. News18. https://www.news18.com/india/only-2-firs-filed-in-22-lakh-cybercrime-complaints-filed-on-national-portal-rti-response-reveals-8184589.html
[16]Central Institute of Educational Technology. (n.d.). Cyber Jaagrookta Diwas : Cyber Threats |. https://ciet.ncert.gov.in/activity/cjdct?
[17]Choudhary, P., Das, S., Potta, M. P., Das, P., & Bichhawat, A. (2025, January 24). Online authentication habits of Indian users. arXiv.org. https://arxiv.org/abs/2501.14330?