ISSN (Online): 3139-7689

Available online: www.ijsrmes.com

International Journal for Scientific Research in Modern Engineering and Science

Published in Conference Special Issue: Vol. 1, Special Issue 1, pp. 502–508, 2026

CRIMINAL LIABILITY IN CYBER ATTACKS AND DIGITAL EVIDENCE

M.M. Kumar[1]*, Sonakshi Sonwane[2]

[1]*Bachelor of Laws - Pt Kishori Lal Shukla Vidhi Mahavidhyalaya*
[2]*Assistant Professor, Bachelor of Laws - Pt Kishori Lal Shukla Vidhi Mahavidhyalaya*

Abstract

The rapid growth of digital technology and internet usage has significantly increased the risk of cyber-attacks and digital crimes. Cyber-attacks such as hacking, identity theft, phishing, and data breaches pose serious threats to individuals, organizations, and national security. In response to these challenges, legal systems have developed frameworks to impose criminal liability on offenders and regulate digital activities. In India, cyber offences are primarily governed by the Information Technology Act, 2000, which provides legal provisions for addressing cybercrimes and regulating electronic communication. [1]

In addition to substantive cybercrime laws, the role of digital evidence has become crucial in prosecuting cyber offenders. Electronic records such as emails, server logs, CCTV footage, and digital documents are frequently used in criminal investigations. The admissibility of such electronic evidence is governed by Indian Evidence Act, 1872, particularly Section 65B, which establishes the legal requirements for presenting electronic records before the court of law. It further understands provisions under the Indian Evidence Act, Information Technology Act, and Bharatiya Sakshya Adhamiya of both cybercrime and digital evidence. [2]

This paper examines the concept of criminal liability in cyber-attacks, analyses the role of digital evidence in cybercrime investigations, and highlights the legal challenges associated with proving cyber offences in courts.

Keywords: *Cyber Crime, Digital Evidence, Criminal Liability, Electronic Records, Cyber Law*

* *Corresponding author*

1. Introduction

The increasing dependence on digital technologies has transformed the way individuals, businesses, and governments operate. While technological advancements have brought convenience and efficiency, they have also created opportunities for cyber criminals to exploit digital systems. [3]

Cyber-attacks include unauthorized access to computer systems, online fraud, identity theft, malware attacks, and data breaches. These offences often involve complex technological methods and cross-border operations, making investigation and prosecution challenging for law enforcement agencies. [4]

To combat cybercrime, India enacted the Information Technology Act, 2000, which provides legal recognition to electronic records and prescribes penalties for various cyber offences. [5]

2. Concept of Cyber Attacks

Cybercrime refers to unlawful activity that involves computer or a networked device. The word Cyber is derived from Greek word 'kubernetikós' which means governing, piloting or skilled in steering. According to the Anderson and Gardener Cybercrime is "Criminal acts implemented through the use of a computer or other form of electronic communications" (2015). The Indian legislature had not mentioned a precise definition of cybercrime, even The Information Technology Act (2000) addressing cyber offences, does not explicitly define the term 'cybercrime'.

Cyber-attacks refer to malicious attempts to access, damage, disrupt, or steal information from computer systems and networks. These attacks may target individuals, corporations, or government institutions. [6]

Common forms of cyber-attacks include hacking, phishing, ransomware attacks, denial-of-service attacks, and online identity theft. Such offences can cause significant financial loss, reputational damage, and compromise of sensitive information. [7]

Due to the increasing number of cyber incidents worldwide, governments have strengthened cyber laws and enforcement mechanisms to hold offenders accountable. The International Organisation for Standardisation (ISO) defines cybercrime as 'the commission of criminal acts in cyberspace'. According to Ministry of electronics and Information Technology, cybercrimes have increased by 572% from 2018 to 2021.

Cybercrime is an uncontrolled evil that has no boundaries and operates cross jurisdictions easily.

2.2 Current Indian Scenario

- Increasing cybercrime incidents: Over the past few years, India has witnessed notable increase in cybercrime incidents. The increase in internet penetration and digital transactions has provided the cybercriminals more opportunities to take advantage of weakness. Common types of cybercrime in India include hacking, phishing, financial fraud and identity theft. Recently, Ministry of Home Affairs (MHA) answered the Rajya Sabha that the number of reported cybercrimes surpassed 2.2 lakh in 2024 in contrast 4.5 lakh in 2021, a jump over 40 percent.

Table 1. Judicial Decisions on Admissibility of Digital Evidence

Type of Case	Admitted Evidence (%)	Rejected Evidence (%)	Total Cases (N)
Cybercrime	72	28	50
Financial Fraud	65	35	40
Homicide/Violent Crime	58	42	30
Terrorism Cases	80	20	25

- Cyber terrorism: According to Pollitt "the premeditated, politically motivated attack against information, computer systems, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Cyber terrorism rising concern for India. Social media and internet are

being used more and more by terrorist groups for attack, recruitment, propaganda and planning attacks. The IT Act was amended to add provisions for cyberterrorism after the 2008 Mumbai attacks brought attention to the role that technology plays in enabling terrorism.

- Financial Frauds and Scams: Cybercriminals employ a range of tactics; Cybercriminals employ a range of tactics to mislead individuals and to extract financial information's. Rise of UPI, mobile wallets, and instant loan apps has highly further contributed to cyber fraud. The Ministry of Home Affairs (MHA) revealed a data to Rajya Sabha that digital financial frauds amounted to ₹4,245 crore in the first ten months (April–January) of the fiscal year 2024-25, involving 2.4 million.

3. Criminal Liability in Cyber Crimes

Criminal liability arises when an individual intentionally engages in unlawful activities that violate cyber laws. The Information Technology Act, 2000 provides several provisions for penalizing cyber offenders. [8]

For example, Section 43 and Section 66 of the Act deal with unauthorized access, data theft, and hacking activities. Section 66C addresses identity theft, while Section 66D punishes cheating by impersonation using computer resources. [9]

These provisions ensure that individuals who misuse digital technologies for illegal purposes can be prosecuted and punished according to law.

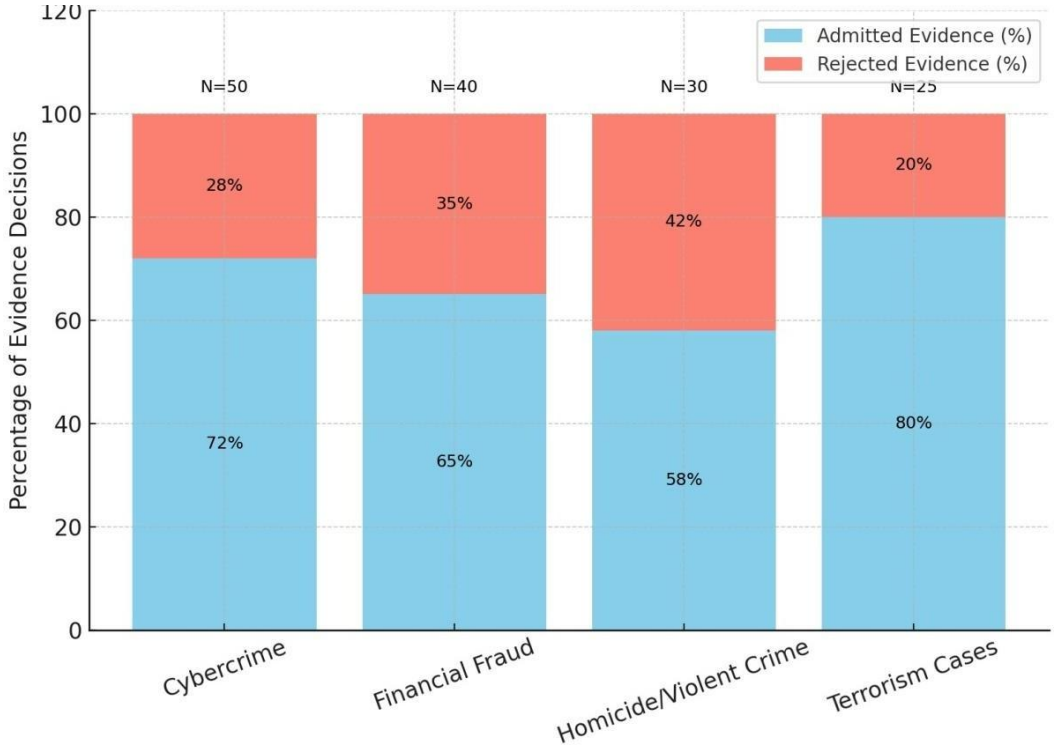

Figure 1. Judicial Decisions on Admissibility of Digital Evidence

4. Digital Evidence in Cybercrime Cases

Digital evidence plays a crucial role in the investigation and prosecution of cyber-attacks. Electronic records such as emails, online chats, system logs, and digital documents are often used to establish the involvement of accused persons in cyber offences. [10]

However, due to the easily alterable nature of digital information, courts require strict procedures for the admissibility of electronic evidence. Section 65B of the Indian Evidence Act provides the legal framework for admitting electronic records as evidence. [11]

The Supreme Court has emphasized the importance of compliance with Section 65B in several judgments, making the certificate requirement mandatory for electronic evidence in most situations.

5. Judicial Approach to Electronic Evidence

Indian courts have addressed the admissibility of digital evidence in various landmark cases. In Anvar P.V. v. P.K. Basheer, the Supreme Court held that electronic records must be accompanied by a valid Section 65B certificate to be admissible in court. [12]

Later, the Court reaffirmed this principle in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, clarifying that electronic evidence without a proper certificate cannot generally be relied upon by courts. [13]

In State of Tamil Nadu v. Suhas Katti (2004), the accused created a fake Yahoo account in Ms. Roselind's name and posted obscene and defamatory messages along with her phone number after she rejected his marriage proposal. As a result, she received abusive calls from strangers and filed a complaint in February 2004. The court found Suhas Katti guilty under Section 469 and 509 of the IPC and Section 67 of the Information Technology Act, 2000. He was sentenced to imprisonment and fines for posting obscene content online and harming the victim's reputation, making it one of the first cybercrime convictions in India.

These decisions have significantly influenced the legal standards for digital evidence in India.

6. Challenges in Proving Cyber Crimes

Despite legal provisions, several challenges exist in establishing criminal liability in cyber-attack cases. One major difficulty is identifying the actual offender, as cyber criminals often use anonymous identities and encrypted networks.

Table 2. Reported Challenges in Handling Digital Evidence

Challenge Category	Frequency Reported (%)
Lack of Standard Guidelines	65
Risk of Tampering	58
Technical Complexity	54
Cross-border Legal Issues	47

Another challenge is the preservation and authenticity of digital evidence. Improper handling of electronic records can lead to tampering or loss of crucial information, which may weaken the prosecution's case. [15]

Additionally, cybercrimes frequently involve cross-border elements, making jurisdiction and international cooperation important issues in cyber law enforcement. The sheer volume and velocity of digital data make manual analysis impractical. The ephemeral and volatile nature of some digital evidence (e.g., volatile memory, network logs) necessitates rapid incident response. Data encryption remains a persistent obstacle, requiring legal and technical decryption methods. Ensuring integrity and authenticity is paramount, demanding robust chain of custody procedures and cryptographic hashing. Legal and jurisdictional complexities arise from differing international laws on data privacy and cross-border transfers. The rapid pace of technological change constantly introduces new devices and formats, requiring continuous updates to forensic tools and skills. Finally, privacy implications of digital evidence collection must be carefully balanced with the need to investigate crimes, necessitating clear legal and ethical guidelines.

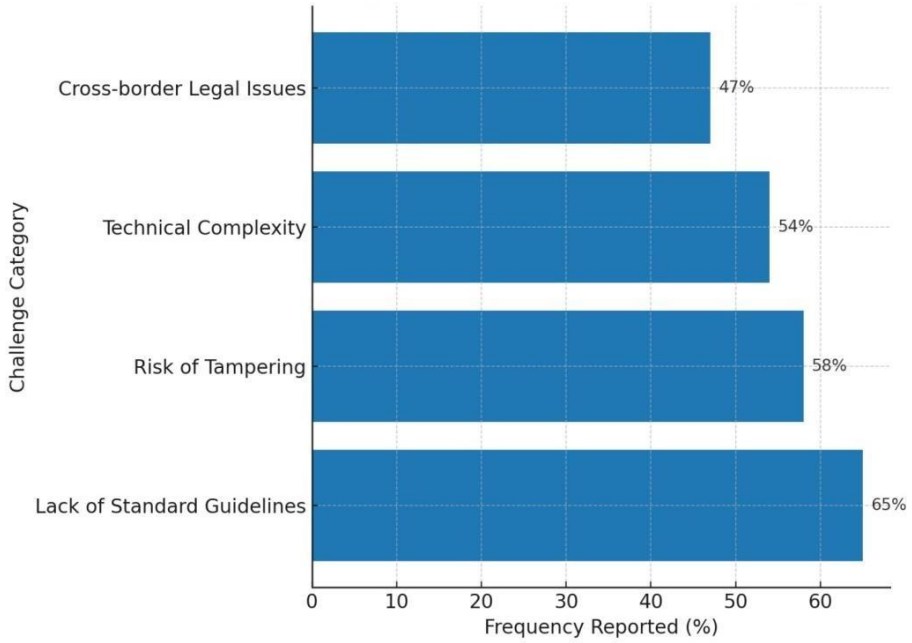

Figure 2. Reported Challenges in Handling Digital Evidence

7. Digital evidence and its legal frameworks

The IT Act, 2000, provides the primary legal framework for cybercrimes in India. Relevant sections, such as Section 43 (damage to computer systems) and Section 66 (computer hacking), can be invoked depending on the nature of the AI-related offense. The upcoming Digital Personal Data Protection Act, 2023, will further strengthen data protection measures relevant in cases where AI is used to compromise personal data. Section 39 of the Bharatiya Sakshya Adhiniyam, 2023, which allows the court to consult an Examiner of Electronic Evidence, is particularly significant in AI related cybercrimes. Expert opinions from AI and digital forensics specialists will be crucial in understanding the technical complexities of AI systems, the methods of manipulation, and the interpretation of AI-generated evidence.

"Digital evidence" or "Electronic Evidence" is any probative information stored or transmitted in digital form that may be used before the courts/ Income- tax authorities. Section 79A of the IT (Amendment) Act 2008 defines electric form evidences as "any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines".

7.1 Bharatiya Sakshya Adhiniyam, 2023

Section 2(1)(e) talks about electronic or digital records as documentary evidence. • Section 32 states that statements about the law found in law books or digital/legal texts are relevant and can be used as evidence.

Section 61 deals with recognition of electronic and digital record as evidence on the ground that it is an electronic or digital record and such record shall, subject to section 63.

Sections 65A and 65B of the Indian Evidence Act deal with the admissibility of electronic records in court. Section 65A states that electronic records must be proved according to Section 65B, which lays down the procedure for admitting such records as evidence. Section 65B allows electronic records (like emails, videos, or computer files) to be used in court if they were produced by a regularly used computer and are accompanied by a certificate under Section 65B (4).

The digital devices that can potentially include like desktop computer, Pen drives, hard drives, Mobile Phones, iPad, Personnel Digital Assistance, Electronic Organizer, Smartcards, Dongles, Biometric Scanners, Digital Cameras, Modems, Routers, Hubs and Switches etc.…

7.2 Admissibility of digital evidence

- Relevance: The Digital evidence must be directly related to the issues of the case.
- Authenticity: The Digital evidence must be genuine and not altered or made up.
- Reliability: The process by which the data obtained must be trustworthy and well documented.
- Hearsay: Digital records containing out-of-court statements may be excluded unless they meet exceptions.
- Expert Testimony: In some cases, digital evidence is complex or technical in certain aspects, experts may be required to explain about its authenticity, reliability and interpretation of the evidence.

8. Conclusion

Cyber-attacks represent one of the most serious challenges in the modern digital world. The growing reliance on technology has increased the vulnerability of individuals and organizations to cyber threats. Legal frameworks such as the Information Technology Act, 2000 and the provisions governing electronic evidence play an important role in addressing these challenges.

However, effective enforcement requires strong investigative mechanisms, technological expertise, and proper handling of digital evidence. Strengthening cyber security laws and improving digital forensic capabilities are essential for ensuring accountability and justice in cyber-crime cases.

References

[1] Information Technology Act, 2000.

[2] Indian Evidence Act, 1872, Section 65B.

[3] Jonathan Clough, Principles of Cybercrime, Cambridge University Press.

[4] Debarati Halder & K. Jaishankar, Cyber Crime and the Victimization of Women, Sage Publications.

[5] Ministry of Electronics and Information Technology, Government of India.

[6] Peter Grabosky, Electronic Crime, Pearson Education.

[7] OECD Report on Cyber Security and Digital Risk Management.

[8] Information Technology Act, 2000, Sections 43 and 66.

[9] Information Technology Act, 2000, Sections 66C and 66D.

[10] Eoghan Casey, Digital Evidence and Computer Crime, Academic Press.

[11] Indian Evidence Act, 1872, Section 65B.

[12] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

[13] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

[14] Brenner Susan W., Cybercrime: Criminal Threats from Cyberspace, Praeger.

[15] Stephen Mason, Electronic Evidence, LexisNexis.