INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 1 [2025] | Page 261 - 265

EVIDENTIARY CHALLENGES IN CYBER FRAUD: DIGITAL FORENSICS UNDER THE BHARATIYA SHAKSHYA ADHINAYAM

-Sreya Chakraborty[1]

ABSTRACT

The growing prevalence of cyber fraud presents significant challenges to traditional legal systems, particularly in the admissibility and evaluation of digital evidence. In India, the Bharatiya Shakshya Adhinayam (Indian Evidence Act) provides the legal framework for addressing these issues, but its application to cybercrimes remains fraught with complexities. This paper explores the evidentiary challenges associated with digital forensics in cyber fraud cases, focusing on critical aspects such as the authentication, preservation, and chain of custody of digital evidence. Through an analysis of key judicial precedents and procedural gaps, the study highlights limitations in the current legal framework and its ability to address evolving cyber threats. Additionally, the paper examines advancements in forensic methodologies and their role in enhancing evidence reliability.

To strengthen the evidentiary process, actionable recommendations are proposed, including legislative updates, enhanced training for legal and law enforcement personnel, and the adoption of international best practices. By bridging the gap between digital forensics and legal standards, this research aims to contribute to more effective cybercrime prosecutions and provide insights for policymakers, legal practitioners, and academics.

Keywords: Cyber Fraud, Digital Forensics, Bharatiya Shakshya Adhinayam, Digital Evidence, Cybercrime Laws

INTRODUCTION

Cyber fraud has emerged as a major issue in the digital age, impacting individuals, organizations, and governments globally. Data from the National Crime Records Bureau (NCRB) reveals that cybercrime in India rose by 15% in 2022 compared to the previous year, with financial fraud making up the majority of the reported incidents. The prosecution of digital crimes heavily relies on the admissibility of digital evidence, as defined by the Indian Evidence Act (Bharatiya Shakshya Adhinayam). First enacted in 1872, this law underwent significant revisions in 2023 to address the

[1] PhD Research Scholar, Department of Law, University of Calcutta, Hazra Campus

challenges presented by the digital era. This research delves into these updates, analyzing how they bridge the gap between traditional evidence rules and the realities of modern technology. It emphasizes the critical role of digital forensics in ensuring the reliability and legal acceptance of electronic evidence.

EVOLUTION OF THE INDIAN EVIDENCE ACT

The Indian Evidence Act of 1872 marked a significant milestone in codifying the rules of evidence admissibility. However, its provisions were not equipped to address digital evidence, as the concept of technology was non-existent at the time. The Information Technology Act of 2000 sought to bridge this gap by introducing Sections 65A and 65B, which specifically deal with the admissibility of electronic records. However, these sections were frequently criticized for being vague and lacking practical relevance in the fast-changing landscape of technology.

The 2023 amendments to the Bharatiya Shakshya Adhinayam represent a significant shift towards addressing these concerns. By incorporating advancements in digital forensics and aligning with international best practices, these amendments aim to make the evidentiary framework more robust and adaptable to cybercrime investigations.

KEY HIGHLIGHTS OF THE 2023 AMENDMENTS

1. **Enhanced Definitions:** The scope of "electronic record" was expanded to include metadata, blockchain records, and cloud-stored data.
2. **Chain of Custody Provisions:** Mandatory documentation was introduced for every stage of evidence handling to ensure integrity.
3. **Admissibility Standards:** Dual-authentication requirements were established to validate the reliability of electronic records.
4. **Judicial Discretion:** Courts were empowered to rely extensively on forensic expert testimony to determine evidence authenticity.

ROLE OF DIGITAL FORENSICS IN CYBER FRAUD CASES

Digital forensics plays a vital role in addressing the challenges of evidence collection in cases of cyber fraud. It involves the application of specialized methods and strategies to gather, examine, and present electronic evidence in a manner that is acceptable in legal proceedings. The key areas where digital forensics plays a pivotal role include:

AUTHENTICATION OF DIGITAL EVIDENCE

- Techniques such as hashing and metadata analysis ensure the integrity and authenticity of electronic records.
- The 2023 Act emphasizes the importance of Section 65B certificates, but practical difficulties persist, especially in obtaining certificates from international entities.

PRESERVATION AND CHAIN OF CUSTODY

- Digital forensics mandates the creation of tamper-proof copies of evidence using techniques like disk imaging and secure storage protocols.
- Implementation challenges, including inadequate infrastructure, continue to hinder the effectiveness of these provisions.

INCIDENT RECONSTRUCTION

- Analyzing network logs, email headers, and transaction records enables forensic experts to recreate fraudulent activities.
- Emerging technologies like blockchain analysis and AI-driven anomaly detection enhance accuracy.

EXPERT TESTIMONIES

- The 2023 amendments recognize the role of forensic experts in explaining technical details and verifying evidence authenticity.
- However, India faces a shortage of certified forensic professionals, causing delays and inaccuracies in trials.

JUDICIAL PERSPECTIVES AND CASE STUDIES

The Indian judiciary has been instrumental in defining the approach to digital evidence. In the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court highlighted the importance of Section 65B, stressing the mandatory requirement of certificates for electronic records to be considered admissible. The 2023 amendments resolve the ambiguities identified in such cases by incorporating clear provisions for dual-authentication and expert verification.

The case of *Shafhi Mohammad v. State of Himachal Pradesh* highlighted the difficulties in acquiring certificates under Section 65B when the electronic record originates outside the jurisdiction of Indian authorities. To address these issues, the proposed amendments introduce alternative methods for verifying evidence.

In the case of *State of Tamil Nadu v. Suhas Katti*, one of the earliest cybercrime convictions in India, the efficient handling and authentication of digital evidence resulted in the accused being convicted within a few months. This underscores the significance of promptly collecting and expertly analyzing electronic records. Similarly, In the case of Anvar P.V. v. P.K. Basheer, the Supreme Court ruled that electronic evidence can only be accepted if it is accompanied by a certificate as required under Section 65B, emphasizing the importance of following the proper procedures for electronic records.

In the case of Sonu @ Amar v. State of Haryana, the Supreme Court addressed whether electronic evidence presented in court could be deemed invalid due to the lack of a Section 65B certificate. The Court affirmed that the evidence could still hold value, considering the surrounding context. This case highlights the need for judicial discretion when dealing with digital evidence.

COMPARATIVE ANALYSIS: 1872 ACT VS. 2023 AMENDMENTS

The following table outlines the key differences between the Indian Evidence Act of 1872 and the Bharatiya Shakshya Adhinayam of 2023:

Aspect	**Indian Evidence Act, 1872**	**Bharatiya Shakshya Adhinayam, 2023**
Definition of Evidence	Limited to physical and documentary evidence	Includes digital data, metadata, and blockchain records
Admissibility	General rules for documents	Dual-authentication for electronic records
Chain of Custody	Implicit and underdeveloped	Explicit and detailed requirements
Role of Forensic Experts	Minimal	Central, with enhanced judicial discretion
International Alignment	Absent	Partial alignment with global best practices

RECOMMENDATIONS

LEGISLATIVE REFINEMENTS

- Address jurisdictional challenges in obtaining evidence from international platforms.
- Incorporate provisions for emerging technologies like AI and IoT.

CAPACITY BUILDING

- Establish a national network of accredited digital forensic labs with uniform standards.
- Offer targeted education and development programs for law enforcement personnel, judges, and prosecutors.

TECHNOLOGICAL INTEGRATION

- Utilize blockchain for maintaining an immutable chain of custody.
- Implement AI-powered tools for analyzing large volumes of digital data.

GLOBAL COLLABORATION

- Enhance the effectiveness of Mutual Legal Assistance Treaties (MLATs) to improve the exchange of evidence across borders.
- Actively participate in international cybersecurity initiatives to align domestic laws with global practices.

CONCLUSION

The Bharatiya Shakshya Adhinayam, 2023, represents a crucial step forward in updating India's legal system to tackle cyber fraud. Although the law introduces significant improvements, challenges remain in its implementation, international cooperation, and the availability of specialized expertise. Digital forensics provides powerful techniques to maintain the integrity and admissibility of evidence. By improving legislation, enhancing skills, and fostering global collaboration, India can better address cyber fraud. A flexible and evolving legal system that keeps pace with technological progress is vital for delivering justice in the digital age.