Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(3), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

DIGITAL CRIME INVESTIGATION AND EVIDENTIARY CHALLENGES IN THE CYBER ERA

Dr. Krishna Kanhaiya Bhardwaj
Assistant Professor* (Guest Faculty)
Govind Guru Tribal University, Banswara (Rajasthan)

Abstract

The rapid expansion of digital technologies has transformed human life and simultaneously given rise to new forms of criminal activity known as cybercrime. These crimes extend beyond individual harm and increasingly impact financial systems, governance structures, and national security frameworks. Unlike conventional offences, cybercrimes are technically complex, borderless in nature, and heavily dependent on digital evidence.

Investigating such offences requires specialized technical knowledge, forensic expertise, and international cooperation. However, challenges such as encryption, jurisdictional conflicts, data volatility, and lack of trained professionals often hinder effective investigation and prosecution.

This paper examines the nature and classification of cybercrimes, the investigative process, the significance of electronic evidence, and the evidentiary challenges faced during judicial proceedings. It further analyses India's legal framework under the Information Technology Act, 2000 and the Indian Evidence Act, 1872, along with judicial interpretations relating to electronic evidence. The study concludes with practical suggestions for strengthening cybercrime prevention and investigation mechanisms.

Keywords: Cybercrime, Digital Evidence, Cyber Forensics, Electronic Records, IT Act 2000, Cyber Investigation

1. Introduction

The twenty-first century is widely recognized as the era of digital transformation. Technologies such as the internet, smartphones, cloud computing, artificial intelligence, and digital payment systems have significantly enhanced convenience and efficiency across sectors including banking, education, healthcare, and governance.

However, this technological progress has also created a parallel rise in cyber-enabled criminal activities. Cybercrime has emerged as one of the fastest-growing forms of crime globally, affecting individuals, organizations, and even state institutions.

Unlike traditional crimes, cyber offences do not require physical presence. A perpetrator can operate from any part of the world while targeting victims located elsewhere. Criminals often use anonymizing tools such as VPNs, proxy servers, encryption, and dark web platforms to conceal their identity.

In such a scenario, digital evidence becomes the backbone of investigation. Yet, its fragile nature, easy manipulability, and dependence on technical systems make its handling highly challenging. Therefore, cybercrime investigation requires a blend of legal knowledge and advanced technical expertise.

2. Meaning and Concept of Cybercrime

Cybercrime refers to illegal activities committed using computers, digital devices, or communication networks. It also includes crimes where computer systems themselves are the target.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(3), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

In simple terms, any unlawful act involving digital technology or cyberspace falls under cybercrime.

Key Features of Cybercrime

- Conducted in digital or virtual environments
- Identity of offenders is often concealed
- Borderless and transnational in nature
- High speed of execution and spread
- Strong dependence on electronic evidence
- Technically complex and evolving in nature

3. Major Categories of Cybercrime

Cybercrimes can be classified into several categories based on their nature and impact.

3.1 Unauthorized Access (Hacking)

Hacking involves illegal access to computer systems or networks to steal, modify, or destroy data. It is often targeted at government databases, banking systems, and corporate servers.

3.2 Phishing and Online Fraud

Phishing refers to the use of fake emails, messages, or websites to deceive users into revealing sensitive information such as passwords or banking details. It is one of the most common forms of financial cyber fraud.

3.3 Identity Theft

Identity theft occurs when personal information such as Aadhaar numbers, bank details, or login credentials are misused for illegal financial gain or fraudulent activities.

3.4 Cyber Stalking

Cyber stalking involves repeated harassment or intimidation of individuals through social media, emails, or messaging platforms. It is a serious threat to privacy and mental well-being.

3.5 Cyber Terrorism

Cyber terrorism refers to attacks on critical infrastructure such as banking systems, power grids, or government networks with the intent to threaten national security.

3.6 Online Financial Crimes

With the rise of digital payment systems, fraud through UPI transactions, fake calls, OTP scams, and malicious applications has increased significantly.

4. Cybercrime Investigation Process

Cybercrime investigation is a structured technical-legal process aimed at identifying offenders and collecting admissible evidence. It requires coordination between law enforcement agencies, cyber forensic experts, and legal authorities to ensure accuracy and legality of digital evidence handling. The process also demands strict adherence to procedural safeguards so that evidence remains reliable in court proceedings.

4.1 Filing of Complaint

The process begins when a victim reports the incident to cyber police or through online reporting systems. Supporting materials such as screenshots, emails, and transaction records are collected initially.

In many cases, victims also provide mobile numbers, URLs, or suspicious links for preliminary verification. Early reporting significantly improves the chances of tracing the offender and preventing further damage.

4.2 Collection of Digital Evidence

Investigators seize electronic devices such as laptops, mobile phones, and storage devices. Server logs, chat records, and transaction histories are also preserved.

During this stage, proper documentation is maintained to ensure the chain of custody remains intact. Even minor negligence in handling can lead to loss of evidentiary value in court.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(3), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

4.3 Forensic Examination

Digital forensic experts analyze recovered data using specialized tools. Even deleted or hidden data can often be retrieved through forensic techniques.

This process helps in reconstructing the sequence of cyber activities and identifying malicious software or unauthorized access. Advanced forensic tools also assist in detecting data tampering or encryption-based concealment.

4.4 Network and IP Tracing

Investigators use IP addresses and network logs to trace the origin of cyber activities. However, tools like VPNs often complicate this process. To overcome such challenges, investigators also rely on ISP records, device fingerprints, and timestamp analysis. In cross-border cases, international cooperation may be required for accurate tracing.

4.5 Legal Action and Prosecution

After investigation, a charge sheet is prepared and submitted before the court along with supporting digital evidence for trial proceedings. Prosecutors must ensure that all electronic records comply with legal admissibility standards, particularly certification requirements. Strong documentation increases the likelihood of successful conviction.

5. Role and Nature of Digital Evidence

Digital evidence includes any information stored or transmitted in electronic form that is relevant to legal proceedings.

Examples

- Emails and chat logs
- Banking transaction data
- CCTV recordings
- Server logs
- Mobile phone data
- Social media activity

Characteristics

- Highly fragile and easily alterable
- Requires scientific handling
- Can be stored on remote servers or cloud systems
- Needs authentication for legal acceptance

6. Key Challenges in Cybercrime Investigation

Cybercrime investigation faces multiple technical and legal obstacles.

6.1 Technological Complexity: Rapidly evolving technologies make it difficult for law enforcement agencies to keep pace with cybercriminal methods. New hacking tools, malware, and anonymization techniques are constantly emerging, making detection more difficult.

6.2 Data Volatility: Digital evidence can be easily deleted, modified, or corrupted, making timely preservation critical. Even a small delay in action can result in permanent loss of important evidence.

6.3 Jurisdictional Issues: Cybercrimes often involve multiple countries, creating legal difficulties in investigation and prosecution.

Differences in international laws and lack of cooperation between nations further complicate the process.

6.4 Shortage of Experts: There is a significant lack of trained cyber forensic professionals and technically skilled investigators.

This shortage reduces the efficiency and speed of cybercrime investigations.

6.5 Encryption Barriers: End-to-end encryption prevents access to crucial communication data during investigations.

This makes it extremely difficult for authorities to trace or decode suspect communications.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(3), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

6.6 Cloud Data Accessibility: Data stored on foreign servers creates legal and procedural barriers for law enforcement agencies. Requests for cross-border data access often take a long time to process and approve.

6.7 Privacy Concerns: Investigations must balance security needs with individual privacy rights. Improper access to personal data can lead to legal and ethical violations.

7. Evidentiary Challenges in Court (Brief)

- **Establishing authenticity of electronic records:** Courts must verify that digital evidence is genuine and has not been tampered with.
- **Maintaining proper chain of custody:** It is necessary to document every step of evidence handling to ensure it remains reliable.
- **Compliance with Section 65B certification requirements:** Electronic evidence must be properly certified under legal rules to be admissible in court.
- **Recovery of deleted or hidden data:** Extracting lost or concealed digital data is technically difficult but often crucial for cases.
- **Identifying fake online identities:** Tracing and proving the real identity behind anonymous or fake accounts is a major challenge.

8. Legal Framework in India

8.1 Information Technology Act, 2000

This Act provides legal provisions to deal with cyber offences such as:

- Section 43: Covers damage caused to computer systems or networks.
- Section 66: Deals with computer-related criminal offences.
- Section 66C: Addresses identity theft cases.
- Section 66D: Covers cheating through online platforms.
- Section 67: Punishes publication or transmission of obscene content online.

8.2 Indian Evidence Act, 1872

Section 65B governs the admissibility of electronic records in court. It requires proper certification to ensure that digital evidence is valid and legally acceptable.

8.3 Penal Law Provisions

Relevant provisions under the Bharatiya Nyaya framework (previously IPC) are applied in cases involving fraud, forgery, and criminal intimidation to support cybercrime prosecution.

9. Cyber Forensics

Cyber forensics is the scientific process of identifying, preserving, analyzing, and presenting digital evidence.

Types

- Computer Forensics
- Mobile Forensics
- Network Forensics
- Cloud Forensics

Common Tools

- EnCase
- FTK (Forensic Toolkit)
- Wireshark
- Autopsy

10. Judicial Approach in India

Indian courts have consistently recognized the importance of electronic evidence in modern litigation. However, they emphasize strict compliance with procedural safeguards to ensure authenticity.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(3), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

The Supreme Court has clarified that Section 65B certification is essential for the admissibility of electronic records. Courts also stress maintaining a proper chain of custody and using forensic methods to prevent tampering or manipulation.
Thus, while electronic evidence is widely accepted, its reliability is strictly scrutinized in judicial proceedings.

11. Preventive and Reformative Measures

11.1 Strengthening Infrastructure: Establishment of advanced cyber police stations and forensic laboratories equipped with modern tools.
This helps in faster investigation and better handling of digital evidence.

11.2 Capacity Building: Regular training programs for police officers, judges, and legal professionals in cyber law and forensic science.
It improves their ability to understand and handle complex cybercrime cases.

11.3 Public Awareness: Campaigns to educate citizens about safe digital practices, phishing scams, and online fraud prevention.
Awareness reduces the chances of people becoming victims of cybercrime.

11.4 International Cooperation: Strengthening collaboration between countries for investigation and information sharing.
This is essential because many cybercrimes cross national borders.

11.5 Legal Reforms: Continuous updating of cyber laws to address emerging threats and technologies.
It ensures laws remain relevant in the fast-changing digital environment.

11.6 Data Protection Framework: Implementation of strong data protection laws to safeguard personal and financial information. This builds trust in digital systems and protects user privacy.

12. Conclusion

Cybercrime represents one of the most serious challenges of the digital age. Its borderless nature, technical complexity, and dependence on electronic systems make investigation and prosecution highly demanding.
While India has established a strong legal framework through the Information Technology Act and evidence laws, continuous improvement is necessary to keep pace with evolving technologies.

An effective cybercrime control strategy must integrate legal reforms, technical advancement, international cooperation, and public awareness to ensure a secure digital environment.

Additionally, coordination between government agencies and private sector organizations is essential for timely detection and response.
A proactive approach focusing on prevention rather than only punishment can significantly reduce cyber threats in the long run.

Strengthening digital literacy among citizens is also crucial to minimize cyber risks at the grassroots level.
Overall, a balanced combination of law, technology, and awareness is the key to effectively combating cybercrime in the modern era.

13. Recommendations

To effectively combat cybercrime, a multi-layered approach is required involving legal, technical, and social measures. The government should further strengthen cyber laws and ensure their timely updates to match emerging technologies and new types of cyber threats. Investment in advanced cyber forensic infrastructure and well-equipped cyber police stations should be increased to improve investigation efficiency. Regular training programs for law enforcement agencies, judiciary, and cybersecurity professionals should be made mandatory to enhance technical expertise. Public awareness campaigns should be expanded to educate citizens about safe internet usage, fraud prevention, and data protection practices. Additionally,

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :10.16(2026); IC VALUE:5.16; ISI VALUE:2.286
Peer-Peer Reviewed, Refereed & Open Access International Journal - As per UGC Norms
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:15, Issue:5(3), May 2026
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

stronger international cooperation mechanisms should be developed for faster information sharing and cross-border investigation of cyber offences.

Furthermore, private organizations and tech companies should also be encouraged to adopt stronger cybersecurity frameworks and reporting mechanisms. The use of artificial intelligence and machine learning tools should be promoted for early threat detection and prevention. A dedicated national cybercrime coordination center can also help in real-time monitoring and faster response to cyber incidents.

References

1. Information Technology Act, 2000
2. Indian Evidence Act, 1872
3. Cyber Law and Information Technology – Dr. Farhat Khan
4. Cyber Crime and Digital Forensics – V.D. Jadhav
5. Indian Penal Framework – Avtar Singh
6. Supreme Court Judgments on Electronic Evidence
7. NCRB Cyber Crime Reports
8. Government Reports on Cyber Security