INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

ISSUES IN CYBER FORENSICS IN INDIA

AUTHOR – MANSI SINGH, STUDENTS AT AMITY UNIVERSITY, LUCKNOW CAMPUS

BEST CITATION – MANSI SINGH**,** ISSUES IN CYBER FORENSICS IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (6) OF 2026, PG. 336-347, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Cyber forensics, also known as digital forensics, is a critical field in modern criminal investigations, especially in the context of rapidly increasing cybercrime. It involves the systematic process of identifying, collecting, preserving, examine and presenting digital evidence from electronic devices such as computers, mobile phones and networks. In India, the expansion of internet access, widespread use of smartphones and growth of digital payment systems have significantly increased the number and complexity of cybercrimes, including online fraud, identity theft, hacking and ransomware attacks.

Cyber forensics has become essential for law enforcement agencies to trace cybercriminals and ensure that digital evidence is admissible in courts. However, despite its importance, the field faces several serious challenges in India. The primary issues is the inadequacy of existing legal frameworks, which often struggle to keep pace with rapidly evolving technologies and sophisticated cyber threats. There is a shortage of trained cyber forensic professionals, which limits the efficiency and effectiveness of investigations.

Keywords: Cyber Forensics, Digital Evidence, Cybercrime, India, Legal Challenges, Data Privacy, Investigation

Introduction

The digital revolution in India has brought about a profound transformation in the way people communicate, conduct business and interact with government systems. With the widespread availability of the internet, smartphones and affordable data services, India has become of the largest digital economies in the world. Online platforms are now integral to daily life, enabling activities such as digital payments, e-governance services, online education and social networking. Initiatives like Digital India have further accelerated this transformation by promoting technology-driven development and improving accessibility. This rapid digitization has also created new vulnerabilities, exposing individuals, businesses and government institutions to various forms of cyber threats. As more sensitive data is stored and transmitted online, the risk of misuse & unauthorized access has significantly increased.[1]

Alongside these advancements, India has witnessed a sharp rise in cybercrimes, which have become more sophisticated and widespread. Cybercriminals exploit technological loopholes and human errors to carry out illegal activities such as hacking, identity theft, phishing attacks, financial fraud and even cyber terrorism. These crimes not only cause financial losses but also threaten national security and individual privacy. The anonymity provided by the internet and the ability to operate across borders make it difficult to identify and apprehend offenders. In this context, cyber forensics plays a crucial role in investigating cybercrimes by tracing digital footprints and uncovering evidence. It helps law enforcement agencies reconstruct events,

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

identify perpetrators and present reliable evidence in courts, thereby ensuring justice & accountability.

Cyber forensics also known as digital forensics, involves the application of scientific and systematic techniques to collect, preserve, examine & examine data from digital devices such as computers, mobile phones, servers and networks. The ultimate goal is to present this evidence in a manner that is legally admissible in court. Despite its growing importance, India faces several challenges in implementing effective cyber forensic practices. These include inadequate legal frameworks, shortage of skilled professionals, lack of advanced forensic infrastructure and difficulties in handling encrypted or cloud-based data. Maintaining the integrity of digital evidence and ensuring proper chain of custody remain critical concerns.

Addressing these challenges is essential for strengthening India's ability to combat cybercrime effectively and keep pace with the rapidly evolving digital landscape.

Growth of Cybercrime in India

India has experienced a significant surge in cybercrime over the past decade, largely driven by rapid digitalization and increased dependence on online platforms. The primary factors contributing to this growth is the widespread increase in internet penetration. With affordable smartphones and low-cost data plans, millions of people, including those in rural areas, have gained access to the internet. While this has promoted digital inclusion and economic growth, it has also expanded the target base for cybercriminals. Many new users lack basic cybersecurity knowledge, making them more vulnerable to online threats and scams.[2]

Another major factor is the rapid adoption of digital payment systems. Platforms such as UPI, mobile wallets and online banking have revolutionized financial transactions in India by making them fast and convenient. However, this convenience has also created opportunities for cybercriminals to exploit system vulnerabilities and user negligence. Fraudsters often use techniques like fake payment links, OTP scams and phishing messages to gain unauthorized

access to users' financial information. As a result, financial fraud has become one of the most

common forms of cybercrime in the country.[3]

The growing popularity of social media platforms has further contributed to the rise in cybercrime. Millions of users actively share personal information, photos and opinions online,

often without understanding the potential risks. Cybercriminals take advantage of this behavior to carry out identity theft, impersonation, cyberstalking and social engineering attacks. Fake profiles and malicious links are frequently used to deceive users & steal sensitive information. Misinformation and online harassment have become serious concerns, affecting individuals and society at large.[4]

A lack of cybersecurity awareness among the general population is another critical issue. Many users are unaware of basic safety practices such as using strong passwords, recognizing suspicious links or securing their devices. This lack of awareness makes it easier for attackers to exploit vulnerabilities. Small businesses and organizations often neglect cybersecurity measures due to limited resources or knowledge, making them easy targets for cyberattacks.

Common types of cybercrimes in India include phishing attacks, ransomware, online fraud, and data breaches. Phishing involves tricking users into revealing sensitive information through fake emails or websites. Ransomware attacks lock users' data and demand payment for its

release, causing significant financial and operational damage. Online fraud, especially in the form of financial scams, has become widespread, while data breaches expose

confidential information, leading to privacy violations and identity theft.

Issues in Cyber Forensics in India

The most significant challenges in cyber forensics in India is the inadequacy of the legal and regulatory framework. Although India has enacted laws such as the Information Technology Act- 2000 to address cyber-related offenses, these laws often struggle to keep pace with the rapidly evolving nature of cyber threats. When the Act was introduced, cybercrime was relatively limited in scope, but today it includes complex issues such as ransomware attacks, cryptocurrency fraud, dark web activities and cyber terrorism. As a result, many provisions of the law are either outdated or insufficient to deal with modern cybercriminal techniques.[5]

Another major issue is the lack of clear jurisdiction in cases involving cross-border cybercrimes. Cyber offenses often originate from outside India, with perpetrators using servers and networks located in multiple countries. This creates legal complications regarding which country has the authority to investigate and prosecute the crime. Mutual legal assistance treaties (MLATs) are often slow and inefficient, leading to delays in accessing critical digital evidence. Such jurisdictional ambiguity hampers timely investigation and weakens the effectiveness of cyber forensic processes.[6]

The admissibility of digital evidence in Indian courts remains a complex issue. For digital evidence to be accepted, it must comply with strict procedural requirements under the Indian Evidence Act- 1872, particularly Section 65B, which mandates certification for electronic records. In many cases, improper handling, lack of technical expertise, or failure to maintain the chain of custody results in evidence being rejected. This significantly affects the outcome of cybercrime cases, even when strong technical evidence exists.

A notable example highlighting these challenges is the ***Anvar P.V/S v/s P.K. Basheer case***.[7] In this landmark judgment, the Supreme Court of India emphasized that electronic evidence must be accompanied by a valid Section 65B certificate to be admissible in court. The ruling made it mandatory to follow strict procedural guidelines, which, although ensuring authenticity, also created practical difficulties for investigators who may not always be able to

obtain such certification, especially in complex cybercrime cases involving multiple devices or foreign servers.

Lack of Skilled Professionals

The major challenges affecting cyber forensics in India is the shortage of skilled professionals with expertise in digital investigation techniques. Cyber forensics is a highly specialized field that requires knowledge of computer systems, networks, data recovery, encryption and legal procedures. India faces a significant gap between the demand for trained cyber forensic experts and the available workforce. With the rapid increase in cybercrime cases, law enforcement agencies are often overwhelmed, and the limited number of experts leads to delays in investigation and analysis of digital evidence.

Another issue is the lack of adequate education and training programs in cyber forensics. Although some universities and institutions offer courses in cybersecurity, specialized training in cyber forensics is still limited and not uniformly available across the country. Many programs are theoretical and do not provide hands-on experience with real-world forensic tools and case scenarios. As a result, graduates may not be fully prepared to handle complex cyber investigations. There is a lack of continuous professional development programs for law enforcement personnel, which is essential to keep up with rapidly evolving technologies and cybercrime techniques.

Investigating officers at the ground level often lack the necessary technical expertise

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

to properly handle digital evidence. In many cases, police personnel are not trained in basic cyber forensic procedures such as securing devices, preserving evidence, or maintaining the chain of custody. This can lead to accidental data alteration or loss, ultimately weakening the case in court. The absence of technical understanding also makes it difficult for investigators to interpret digital evidence accurately or collaborate effectively with forensic experts.

A relevant example is the Cosmos Bank Cyber Attack Case, where hackers siphoned off large sums of money through malware and ATM withdrawals across multiple countries. The investigation faced initial hurdles due to the complexity of the attack and limited availability of highly trained cyber forensic experts. Authorities had to rely on external agencies and international cooperation to trace the attackers, highlighting the gap in domestic expertise.[8]

Another example is the Aadhaar Data Leak Controversy, where concerns were raised about unauthorized access to sensitive personal data. Investigating such cases required advanced forensic analysis and cybersecurity knowledge, but the lack of adequately trained professionals complicated the process and delayed clarity on the extent of the breach.

Inadequate Infrastructure

Inadequate infrastructure is a critical issue hindering the effectiveness of cyber forensics in India. Despite the rapid rise in cybercrime cases, the country still lacks a sufficient number of well-equipped cyber forensic laboratories. Most states have only a limited number of such facilities and many regions, especially rural & semi-urban areas, do not have easy access to them. As a result, digital evidence often has to be sent to centralized laboratories located in major cities, causing significant delays in investigation. This shortage creates a bottleneck in handling cybercrime cases efficiently and affects timely justice delivery.

Another major concern is the lack of advanced tools and technologies required for modern cyber forensic investigations. Cybercriminals today use sophisticated techniques such as encryption, anonymization, malware obfuscation and cloud-based attacks. To counter these, forensic labs need high-end software, hardware and regularly updated tools. However, many government laboratories in India still rely on outdated systems that are not capable of handling complex digital evidence. This technological gap reduces the accuracy and efficiency of forensic analysis and limits the ability of investigators to uncover crucial evidence.

The existing cyber forensic facilities are often overloaded with a large number of pending cases. Due to the increasing volume of cybercrime complaints and the limited number of labs and experts, there is a backlog in forensic analysis. This leads to delays in examining digital devices such as mobile phones, laptops and servers. In many cases, evidence analysis can take months or even years, which weakens the investigation and may result in loss of crucial data or reduced chances of conviction. Delayed reports also affect court proceedings and prolong the justice process.

Case Studies

The earliest significant cyber fraud incidents in India is the Union Bank of India v/s Unknown (Cyber Fraud Case). Although this case did not result in a reported AIR citation (as it was primarily an investigative and banking fraud matter rather than a fully reported Supreme Court judgment), it remains a landmark incident in Indian cybercrime history. In 2016, hackers attempted to transfer nearly $171 million through unauthorized SWIFT transactions by infiltrating the bank's internal systems. The attackers used phishing and malware techniques to gain access to credentials and manipulate international

transactions. From a cyber forensic perspective, investigators faced major challenges such as tracing the malware origin, examine compromised systems, and coordinating with foreign banks and agencies. The case exposed weaknesses in cyber forensic readiness and highlighted the lack of skilled personnel & advanced tools required for complex financial investigations.

Another important case is the ***K.S. Puttaswamy v/s Union of India,***[9] which is indirectly connected to the Aadhaar Data Leak Controversy. While the Puttaswamy case is a constitutional law case rather than a cybercrime prosecution, it established the fundamental right to privacy under Article-21 of the Indian Constitution. This judgment became highly relevant in the context of alleged Aadhaar data leaks, where concerns were raised regarding unauthorized access to personal data. Cyber forensic investigations into the Aadhaar controversy faced difficulties in tracing the exact source of the leak due to the massive scale of the database and involvement of multiple agencies. The absence of a direct AIR-reported criminal case on the leak itself reflects the complexity of cyber forensic evidence and challenges in prosecution.

A major recent cyber incident is the ***AIIMS Delhi v/s Unknown (Ransomware Attack Case)***[10]***.***

This case also does not yet have an AIR citation, as it is primarily an ongoing investigation involving national cybersecurity agencies. In 2022, the All India Institute of Medical Sciences (AIIMS), New Delhi, suffered a ransomware attack that disrupted hospital operations and compromised sensitive patient data. Systems remained down for several days, severely affecting healthcare services. From a cyber forensic standpoint, investigators faced difficulties in decrypting data, identifying attackers, and restoring systems. The case highlighted gaps in infrastructure and the urgent need for advanced forensic tools capable of handling ransomware and encrypted environments.

Another recent case is the Air India Data Breach Case, which involved the leakage of personal data of around 4.5 million passengers. Similar to many cyber incidents, this case does not have an AIR citation because it primarily involved corporate liability and international data security issues rather than a reported court judgment. The breach was linked to a third-party service provider, making forensic investigation more complex. Investigators faced challenges in tracing the source of the breach, especially since the data was stored on foreign servers. This case emphasized the importance of cybersecurity compliance and forensic readiness in corporate environments.

A more recent and widespread category of cybercrime includes UPI fraud and phishing scams,

often registered under various FIRs across India rather than a single reported case. Example is the ***State v/s Unknown (UPI Phishing Fraud Cases)***. These cases involve criminals using fake payment links, QR codes and impersonation tactics to deceive victims into transferring money. Due to the decentralized nature of these crimes, they rarely result in AIR-reported judgments but represent a significant portion of cybercrime in India. Cyber forensic challenges include tracing digital transactions, identifying anonymous perpetrators and collecting admissible electronic evidence under Section 65B of the Indian Evidence Act.

The ***UPI QR Code Fraud Case v/s Unknown (2025,)***[11] involves a growing number of incidents where cybercriminals trick victims into scanning fake QR codes under the pretext of receiving money. Instead of receiving funds, users unknowingly authorize payments from their own accounts. In this case, the victims are digital payment users, while the accused are unidentified

fraudsters using fake identities and mobile numbers. The matter is registered as State v/s Unknown, as the police investigate the

offense on behalf of the victim. From a cyber forensic perspective, tracing the transaction trail, identifying mule accounts and linking multiple frauds to a single network becomes a major challenge.

Other important example is the **Social Media Impersonation Fraud Case v/s Unknown (2025).** This case cybercriminals create fake profiles on platforms like Instagram or Facebook

by using photos and personal details of real individuals. They then contact the victim's friends

or followers to request money or sensitive information. The victims are both the impersonated individuals and those who are deceived financially. Since the offenders operate anonymously and often from different locations, the case is registered as State v/s Unknown. Cyber forensic investigators face difficulties in tracing IP addresses, identifying fake accounts and obtaining data from international social media servers.

A further case is the ***Job Portal Scam Case v/s Unknown (2025),*** where fraudsters post fake job opportunities on employment websites and social media platforms. Victims are asked to pay registration fees or provide personal and banking details under the promise of employment. In reality, these offers are fraudulent. The case involves job seekers as victims and unidentified cybercriminals as accused. It is ***handled as State v/s Unknown,*** with investigation focusing on tracking digital payment trails, fake websites and communication records. The lack of awareness among users and the use of temporary contact details by criminals make forensic investigation difficult.

Other emerging example is the ***Deepfake Video Fraud Case v/s Unknown (2025),*** where attackers use artificial intelligence to create realistic fake videos or voice recordings of individuals, especially company officials or family members, to manipulate victims into transferring money. In this case, the victims are individuals or organizations misled by the deepfake content, while the accused remain unidentified. The case is registered as State v/s Unknown and cyber forensic experts must analyze digital artifacts, metadata, and AI-generated inconsistencies to detect fraud. This represents a new and complex challenge for cyber forensics in India.

Government Initiatives

The Government of India has recognized the growing threat of cybercrime and the importance

of cyber forensics in ensuring effective investigation and prosecution. Over the years, several initiatives have been introduced to strengthen cybersecurity infrastructure, improve investigative capabilities and create awareness among citizens. These measures aim to build a robust system capable of addressing the complex and evolving nature of cyber threats. However, despite these efforts, there are still gaps that need to be addressed to make these initiatives more effective.[12]

The major steps taken by the government is the establishment of cyber forensic laboratories across the country. These laboratories are designed to assist law enforcement agencies in examine digital evidence collected from electronic devices such as computers, mobile phones and servers. Both central & state governments have set up such labs and efforts are ongoing to expand their reach. These facilities play a crucial role in recovering deleted data, examine malware and tracing digital footprints. However, many of these laboratories are concentrated in urban areas, leading to limited access in rural regions. Some labs lack advanced tools and technologies required to handle sophisticated cybercrimes, which reduces their effectiveness.

Other significant initiative is the launch of the National Cyber Crime Reporting Portal by the Ministry of Home Affairs. This online platform

allows citizens to report cybercrimes easily without visiting a police station. It is particularly useful for reporting financial frauds, online harassment and child exploitation cases. The portal has improved the reporting rate of cybercrimes and enabled faster response by authorities. However, challenges remain in terms

of timely action, coordination between states and proper follow-up of complaints. Many users are also unaware of the portal or do not fully understand how to use it effectively, which limits its potential impact.[13]

The government has also introduced various training programs for law enforcement agencies to enhance their cyber forensic capabilities. Police officers, investigators, and judicial officials are provided with training on handling digital evidence, understanding cyber laws and using forensic tools. Institutions such as the National Police Academy and other specialized training

centers conduct these programs. While these initiatives are important, the scale of training is still insufficient compared to the growing number of cybercrime cases. Many officers at the local level still lack basic technical knowledge, which affects the quality of investigations. Continuous skill development and practical training are essential to keep pace with rapidly evolving cyber threats.

India's cybersecurity framework is the CERT-In (Indian Computer Emergency Response Team). It functions as the national nodal agency for responding to cybersecurity incidents. CERT-In monitor's cyber threats, issues alerts and advisories & coordinates responses to major cyber incidents. It also collaborates with international organizations and provides guidance to government departments and private entities. CERT-In plays a vital role in incident response and threat intelligence. Its effectiveness depends on timely information sharing and coordination among various stakeholders, which can sometimes be challenging.

In addition to these measures, the government has launched awareness campaigns and initiatives under programs like Digital India to educate citizens about cybersecurity practices. Efforts are being made to promote safe online behavior, such as using strong passwords, avoiding suspicious links and reporting cyber incidents. Public awareness is crucial because many cybercrimes occur due to lack of knowledge and negligence. Despite these efforts, awareness levels in many parts of the country remain low, especially among new internet users.

The government has taken steps to improve international cooperation in tackling cybercrime, as many cyber offenses involve cross-border elements. Agreements and collaborations with

other countries help in sharing information and tracking cybercriminals operating from abroad. Legal and procedural delays often hinder quick access to digital evidence stored on foreign servers.

Recommendations

Legal reforms are essential for strengthening cyber forensics in India, as the existing legal framework often struggles to keep pace with rapidly evolving cyber threats. With the increasing complexity of cybercrimes such as ransomware attacks, data breaches and identity theft, it is necessary to regularly update cyber laws to ensure they remain relevant and effective. The Information Technology Act-2000, although a foundational legislation, was enacted at a time when digital technology was still developing. It lacks comprehensive provisions to address modern challenges like artificial intelligence-based crimes, cryptocurrency fraud and cyber warfare. Therefore, periodic amendments and introduction of new legislation are required to address emerging threats & ensure that cybercriminals can be effectively prosecuted.

Other important aspect of legal reform is the establishment of clear and standardized

guidelines for handling digital evidence. Digital evidence plays a crucial role in cybercrime investigations, but its admissibility in court depends on strict compliance with procedural requirements under the Indian Evidence Act-1872. In many cases, evidence is rejected due to improper collection, lack of certification, or failure to maintain the chain of custody. To overcome these issues, there is a need to develop uniform protocols for evidence collection, preservation, analysis and presentation. These guidelines should be simple, practical & adaptable to different levels of law enforcement. Training programs should be aligned with these standards to ensure that investigating officers follow correct procedures, thereby increasing the chances of successful prosecution.

Strengthening international cooperation is Other critical requirement in the context of cybercrime. Many cyber offenses originate outside national borders, with criminals using foreign servers, networks and financial systems to carry out illegal activities. This creates jurisdictional challenges and delays in accessing digital evidence. India must actively engage in international collaborations, treaties and information-sharing mechanisms to effectively combat cross-border cybercrime. Mutual Legal Assistance Treaties (MLATs) and partnerships with global cybersecurity organizations should be streamlined to ensure faster response and data exchange. India should work towards harmonizing its cyber laws with international standards to facilitate better cooperation and coordination.

In addition to these measures, the legal system must also focus on building capacity within the judiciary to handle cyber-related cases. Judges and legal professionals should be trained in understanding technical aspects of digital evidence and cybercrime. Fast-track courts for cyber

offenses can also be established to ensure timely resolution of cases. Delays in legal proceedings often reduce the effectiveness of cyber forensic investigations and may lead to loss

of evidence or reduced deterrence.

Public Awareness

Public awareness is a crucial element in strengthening cyber forensics and preventing cybercrime in India. A large number of cyber incidents occur not only due to technological vulnerabilities but also because of a lack of awareness among users. Many individuals are unaware of basic cybersecurity practices, making them easy targets for cybercriminals. Therefore, increasing public awareness is essential to reduce cybercrime and support effective forensic investigations.

The steps in this direction is conducting widespread awareness campaigns. The government, along with private organizations, should regularly organize campaigns to educate people about common cyber threats such as phishing, online fraud, identity theft, and malware attacks. These campaigns can be conducted through television, radio, social media, and community programs to reach a broader audience. Special attention should be given to rural areas and first-time internet users, who are often more vulnerable due to limited digital knowledge. Awareness campaigns should focus on practical tips such as identifying suspicious links, avoiding sharing sensitive information, and using secure passwords. By improving public understanding, the chances of falling victim to cybercrime can be significantly reduced.

Other important measure is promoting cybersecurity education at various levels. Cybersecurity should be introduced as a part of school and college curricula to ensure that individuals develop safe online habits from an early stage. Educational institutions should offer specialized courses and training programs in cybersecurity and cyber forensics to build a skilled workforce. Workshops and seminars can be conducted for employees in organizations to educate them about data protection and

safe digital practices. A well-informed population not only reduces cybercrime incidents but also supports cyber forensic investigations by preserving evidence and reporting incidents promptly.

Encouraging the reporting of cybercrimes is equally important. Many victims hesitate to report cyber incidents due to fear, lack of awareness, or belief that no action will be taken. This leads to underreporting, which allows cybercriminals to continue their activities without consequences. The government has introduced platforms like the National Cyber Crime Reporting Portal to make reporting easier and more accessible. However, more efforts are needed to promote these platforms and build trust among users. People should be encouraged to report cybercrimes immediately so that timely action can be taken and digital evidence can be preserved.

Collaboration between the government, private sector, and civil society is necessary to enhance awareness efforts. Technology companies, banks and social media platforms should actively participate in educating users about potential risks and safety measures. Regular alerts, notifications, and security updates can help users stay informed about emerging threats.

Future Scope

The field of cyber forensics is expected to undergo significant transformation in the coming years due to rapid advancements in emerging technologies such as Artificial Intelligence (AI), blockchain, and cloud computing. These technologies are not only reshaping the digital landscape but also influencing the methods used by cybercriminals, thereby requiring continuous evolution in forensic techniques. In India, the future of cyber forensics depends on how effectively these technologies are adopted and integrated into investigative processes.

Artificial Intelligence is likely to play a major role in enhancing cyber forensic capabilities. AI-based tools can help in automating the analysis of large volumes of digital data, identifying patterns and detecting anomalies that may indicate cybercrime. Machine learning algorithms can assist investigators in quickly processing evidence, recognizing malware signatures and predicting potential threats. This will significantly reduce investigation time and improve accuracy. Cybercriminals are also using AI to develop more sophisticated attacks, such as deep fakes and automated hacking tools, which creates new challenges for forensic experts.

Blockchain technology offers promising opportunities in ensuring the integrity and authenticity

of digital evidence. Since blockchain operates on a decentralized and tamper-proof system, it can be used to maintain secure records of digital transactions and forensic data. This can strengthen the chain of custody by providing a transparent and immutable record of evidence handling. In the future, blockchain-based systems may be widely adopted in cyber forensic investigations to enhance trust and reliability in legal proceedings.

Cloud computing is Other area that will shape the future of cyber forensics. As more data is stored and processed on cloud platforms, investigators must develop new techniques to collect and analyze evidence from distributed & virtual environments. Cloud forensics requires specialized tools and legal frameworks to handle issues such as data ownership, jurisdiction and access control. India needs to invest in developing expertise in cloud forensics to effectively investigate crimes involving cloud-based systems.

India must adopt global best practices and strengthen collaboration with international agencies. Cybercrime is often transnational and effective investigation requires cooperation across borders. Participation in global cybersecurity initiatives, information sharing & adoption of international standards will enhance India's cyber forensic capabilities.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Continuous training and skill development for law enforcement personnel are essential to keep up with technological advancements. Investment in research and development, establishment

of advanced forensic laboratories and integration of modern technologies will play a crucial role in shaping the future of cyber forensics in India.

Conclusion

Cyber forensics has emerged as a crucial tool in combating the rapidly increasing cybercrime landscape in India. With the country undergoing a massive digital transformation driven by internet penetration, digital payments, e-governance, and technological innovation, the dependency on digital platforms has grown significantly. While this transformation has brought numerous benefits, it has also exposed individuals, businesses and government systems to a wide range of cyber threats. In this context, cyber forensics plays a vital role in identifying cybercriminals, collecting and examine digital evidence and ensuring that justice is delivered through proper legal processes.

Over the years, India has made notable progress in strengthening its cyber forensic capabilities. The establishment of cyber forensic laboratories, the launch of cybercrime reporting platforms, and the creation of organizations like CERT-In have contributed to improving the country's response to cyber incidents. Training programs for law enforcement agencies and awareness initiatives have helped build a foundation for tackling cybercrime more effectively. These efforts indicate that the government recognizes the importance of cybersecurity and cyber forensics in maintaining national security and public trust in digital systems.

However, despite these advancements, several challenges continue to hinder the effectiveness

of cyber forensics in India. The primary issues is the gap in the legal framework, as existing laws often struggle to keep pace with rapidly evolving cyber technologies and crimes. The lack

of clear and updated legal provisions can lead to difficulties in prosecution & delays in justice delivery. Issues related to jurisdiction, especially in cross-border cybercrimes, complicate investigations and require stronger international cooperation.

Other major challenge is the lack of adequate infrastructure and technical resources. Many cyber forensic laboratories are either insufficient in number or lack advanced tools required to handle sophisticated cyber threats such as ransomware, encryption and cloud-based attacks.

This results in delays in evidence analysis and case resolution. In addition, the shortage of skilled professionals in cyber forensics significantly impacts the quality and speed of investigations. Many law enforcement officers lack specialized training, which leads to improper handling of digital evidence and reduces its admissibility in courts.

The increasing use of advanced technologies by cybercriminals further complicates the situation. Techniques such as anonymization, encryption, artificial intelligence and the use of the dark web make it difficult to trace offenders and collect reliable evidence. At the same time, issues related to data privacy and ethical considerations create a delicate balance between effective investigation and protection of individual rights.

To overcome these challenges, it is essential for India to adopt a comprehensive and forward-looking approach. Strengthening the legal framework through regular updates, establishing clear guidelines for digital evidence and enhancing international cooperation are critical steps. Investment in modern infrastructure, including advanced forensic laboratories and tools, is equally important. Capacity building through education, training and skill development programs must be prioritized to create a pool of qualified cyber forensic professionals.

Public awareness also plays a key role in preventing cybercrime and supporting forensic investigations. Educating citizens about safe online practices and encouraging timely reporting of cyber incidents can significantly reduce the impact of cyber threats. Collaboration between the government, private sector and international organizations will further strengthen India's ability to respond to cybercrime effectively.

References

- Information Technology Act- 2000 Indian Evidence Act- 1872
- CERT-In Reports (Annual Reports)
- National Crime Records Bureau (NCRB), *Cyber Crime in India Reports*
- Ministry of Home Affairs, Government of India, *National Cyber Crime Reporting Portal Data*
- Reserve Bank of India, *Annual Reports on Banking Frauds* NASSCOM, *Cybersecurity Reports*
- Data Security Council of India, *Cyber Threat Reports* Interpol, *Global Cybercrime Reports*
- United Nations Office on Drugs and Crime, *Cybercrime Studies*
- Casey, E. (2011). *Digital Evidence and Computer Crime*, Academic Press.
- Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to Computer Forensics and Investigations*, Cengage Learning.
- Volonino, L., & Anzaldua, E. (2018). *Computer Forensics for Dummies*, Wiley Kshetri, N. (2016). *Cybercrime and Cybersecurity in India*, Springer.
- International Journal of Cyber Criminology
- Journal of Digital Forensics, Security and Law
- International Telecommunication Union, *Global Cybersecurity Index Reports* World Economic Forum, *Global Risks Report (Cybersecurity Section)*
- Microsoft, *Digital Defense Reports* IBM, *Cost of a Data Breach Report*

Endnotes

1 Indian Evidence Act, 1872, §65B (as amended), relating to admissibility of electronic records.

2 National Crime Records Bureau (NCRB), Crime in India Report 2022; International Telecommunication Union, Global Cybersecurity Index Report 2023; Data Security Council of India, India Cyber Threat Report.

3 Reserve Bank of India, Annual Report on Banking Frauds; National Crime Records Bureau (NCRB), Crime in India Report; Ministry of Electronics and Information Technology, Digital Payments and Cybersecurity Reports.

4 Data Security Council of India, India Cyber Threat Report (DSCI, New Delhi); Microsoft, Digital Defense Report (Microsoft, 2023); United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (UNODC, Vienna).

5 Government of India, Information Technology Act, 2000; Ministry of Electronics and Information Technology, Report on Cyber Security Framework in India (MeitY, New Delhi); N.S. Kshetri, Cybercrime and Cybersecurity in India (Springer, 2016).

6 United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (UNODC, Vienna); Council of Europe, Convention on Cybercrime (Budapest Convention); Ministry of Home Affairs, Government of India, Guidelines on International Cooperation in Cybercrime Cases.

7 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473; Indian Evidence Act, 1872, §65B.

8 Reserve Bank of India, Report on Frauds in Banking Sector (RBI, Mumbai); Data Security Council of India, India Cyber Threat Report (DSCI, New Delhi); Ministry of Electronics and Information Technology, Cyber Security Incidents Reports (MeitY, New Delhi).

9 K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; Unique Identification Authority of India, Aadhaar Data Security and Privacy Reports (UIDAI, New Delhi); Ministry of Electronics & Information Technology, Reports on Data Protection and Cyber Security (MeitY, New Delhi).

10 Indian Computer Emergency Response Team, Cyber Incident Reports (CERT-In, New Delhi); Ministry of Health and Family Welfare, Government of India, Reports on AIIMS Cyber Incident; Data Security Council of India, India Cyber Threat Report (DSCI, New Delhi).

12 Ministry of Home Affairs, Government of India, CCPWC Scheme Reports: 2022 New Delhi Indian Computer Emergency Response Team, Annual Reports (2023, New Delhi).

13 Ministry of Home Affairs, Government of India, National Cyber Crime Reporting Portal Guidelines and Reports (2023, New Delhi); National Crime Records Bureau, Cyber Crime Statistics Report (2022, New Delhi).