Bridging the Digital Divide: A Study on the Adequacy of Technical Expertise and Infrastructure for Digital Evidence Management in Indian Law Enforcement and Judiciary

Ms. Razia Syed

Dr. Vibha Srivastav

Abstract

This report looks at how well India's law enforcement and courts are set up to handle digital evidence. Even with government efforts and new laws, there is still a "digital divide." This means not just a lack of technology, but also a shortage of special skills, standard tools, and proper systems for digital evidence. Key problems include complex rules for using evidence in court, not enough skilled people, and big differences in technology across different areas. The report shows that while new laws like the Bhartiya Sakshya Adhiniyam (BSA) 2023 try to make handling digital evidence easier, new unclear areas and existing problems still slow down justice. We suggest better training, fair technology distribution, clearer rules, and ways to keep skilled people to build a stronger and fairer digital justice system in India.

1. Introduction: The Digital Transformation of Justice in India

1.1. The Growing Importance of Digital Evidence in Modern Investigations

As digital technology becomes a part of everyday life, digital evidence is now crucial for solving crimes and in court cases. India, with many digital users, has seen a big rise in cybercrime. In 2022, there were 65,893 cybercrime cases, a 24.4% increase from the year before.[1] This shows how important it is to manage digital evidence well for quick and fair justice.

Digital evidence includes many types of data, from emails and server logs to social media posts, call records, and location data from devices.[2] Unlike physical evidence, digital evidence can change easily, be tampered with, and often comes from complex online networks, making it hard to collect, keep safe, analyse, and show in court.[3] Keeping this evidence accurate and making sure it can be used in court is vital for fair legal outcomes.

1.2. Defining the "Digital Divide" in India's Justice System

[1] ORF Expert Speak, India's Cyber Forensics Push Since 2020: Building National Capacity for Digital Investigations, ORF (June 24, 2025), https://www.orfonline.org/expert-speak/india-s-cyber-forensics-push-since-2020-building-national-capacity-for-digital-investigations (last visited Mar. 6, 2025).

[2] Virtual Hearings and Digital Evidence: Challenges in Ensuring Fair Trial, NFSU EJournal (Jan.–June 2024), https://jfj.nfsu.ac.in/Uploads/EJournal/3/4/(1-14)%20VIRTUAL%20HEARINGS%20AND%20DIGITAL%20EVIDENCE%20CHALLENGES%20IN%20ENSURING%20FAIR%20TRIAL.pdf (last visited Mar 21, 2025)

[3] Evolution of Electronic Evidence: Navigating the Admissibility of the New Criminal Laws in India, IJIRL (Feb. 26, 2025), https://ijirl.com/wp-content/uploads/2025/02/EVOLUTION-OF-ELECTRONIC-EVIDENCE-NAVIGATING-THE-ADMISSIBILITY-OF-THE-NEW-CRIMINAL-LAWS-IN-INDIA.pdf (last visited Apr. 15, 2025)

In this study, the "digital divide" means the major differences in India's justice system regarding the availability, access, and skill in using digital tools and systems for managing digital evidence.[4] This divide is not just about having basic technology; it also includes big gaps in advanced technical skills, standard forensic equipment, and smooth digital evidence management systems across police and courts. The real challenge is being fully ready for the digital age.

This digital divide is complex. It includes not only a lack of physical technology in some areas, especially rural ones, but also important differences in specialized technical skills, access to modern forensic tools, and the ability to follow the complex legal rules for digital evidence.[5] This means that even if basic digital tools are there, a lack of skilled people and standard ways of working still creates a digital divide, making it hard to manage digital evidence effectively. The issue is not just providing computers or internet, but making sure specialized digital forensic tools and the people who can use them are widely available and skilled. Without both, digital evidence cannot fully help in seeking justice.

1.3. Scope and Objectives of the Study

This report looks closely at the current state of technical skills and digital tools for managing digital evidence in Indian law enforcement and the judiciary. Its main goals are to find existing problems, check how well government programs and training work, and suggest practical solutions. Ultimately, this study aims to help close the digital divide, making India's justice system more efficient, fair, and trustworthy in the digital era.

2. Legal Framework for Digital Evidence Management in India

2.1. Evolution of Digital Evidence Admissibility: From IEA (Indian Evidence Act) 1872 to BSA 2023

Indian law has changed over time to include electronic evidence. The Indian Evidence Act, 1872 (IEA), was updated in 2000 with Sections 65A and 65B, which officially recognized electronic records in court.[6] Under the IEA, electronic evidence was mostly seen as secondary evidence, meaning it needed certain conditions to be accepted.[7] This first step in law showed that digital information was becoming important, but it was treated carefully because its nature was not fully understood.

A major change happened with the Bhartiya Sakshya Adhiniyam (BSA) 2023, which replaced the IEA 1872. The BSA greatly updates the approach by clearly including electronic records in the definition of "documents" and, importantly, calling them *primary evidence* unless there's a doubt about their truthfulness.[8] This change is meant to make it easier to show digital evidence in court, recognizing that digital information is often the original form of data today. The BSA also broadens what counts as electronic records to include information on semiconductor

[4] NextIAS, Integrating AI in India Judiciary and Law Enforcement, NextIAS (Feb. 27, 2025), https://www.nextias.com/ca/current-affairs/27-02-2025/integrating-ai-in-india-judiciary-and-law-enforcement (last visited Apr. 21, 2025)
[5] *Supra note1*
[6] Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473 (India).
[7] Shafhi Mohammad v. The State of Himachal Pradesh, (2018) 2 SCC 130 (India).
[8] PRS Legislative Research, The Bharatiya Sakshya Bill, 2023, PRSIndia, https://prsindia.org/billtrack/the-bharatiya-sakshya-bill-2023 (last visited 12 Mar, 2025)

memory or devices like smartphones and laptops, such as emails, location data, and voicemails. This big legal update aims to simplify how evidence is handled and speed up court cases, bringing laws up to date with new technology.[9]

2.2. Critical Supreme Court Pronouncements on Section 65B

How electronic evidence could be used, especially how Section 65B(4) of the IEA (which required a certificate for secondary electronic records) was understood, was often debated in court. This led to several important, sometimes conflicting, decisions by the Supreme Court.[10]

Navjot Sandhu (2005)[11]: At first, in *State (NCT of Delhi) v. Navjot Sandhu*, the Supreme Court was more flexible. It said that not having a Section 65B certificate would not always stop electronic evidence from being used. This allowed parties to use general rules for secondary evidence. This approach was more lenient when digital evidence was new to the legal system.

Anvar P.V. v. P.K. Basheer (2014)[12]: This important ruling by a three-judge bench completely changed things. It clearly overturned *Navjot Sandhu*, stating that Sections 65A and 65B were the only rules for electronic records. The Court firmly said that the 65B(4) certificate was *required* for secondary electronic evidence, and spoken evidence couldn't replace it. This decision showed the court's growing concern about the truthfulness and reliability of digital evidence.

Shafhi Mohammad v. The State of Himachal Pradesh (2018)[13]: This judgment offered some practical flexibility, suggesting that the certificate might not be needed if it served justice, especially when the person showing the evidence did not control the device that made the record.[14] The Court saw Section 65B as a rule about procedure, aiming to prevent unfair outcomes due to technicalities.

Arjun Panditrao Khotkar v. Kailash Kishanrao (2020)[15]: This major judgment by a larger bench firmly restated that Section 65B(4) must be strictly followed, effectively overturning *Shafhi Mohammad* and other differing rulings. The Court stressed that the certificate ensures the origin and truthfulness of electronic records, which can be easily changed or tampered with. It also provided a key solution: if a party tries hard but can't get the certificate, the court can order the person who has the device to produce it during the trial. This ruling aimed to make the use of digital evidence consistent and strict.

The changing court interpretations of Section 65B, ending with a strong confirmation that it is required, clearly show how much the judiciary struggles to balance fast-moving digital technology with the basic rules of evidence integrity and fair trials. The constant focus on mandatory certificates, especially in *Anvar P.V.* and *Arjun Panditrao Khotkar*, highlights a deep concern that digital evidence can be easily manipulated, which could lead

[9] *Supra note 2*
[10] Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473 (India).
[11] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 797
[12] Anvar P.V v. P.K. Basheer & Ors (2014 10 SCC 473)
[13] Shafhi Mohammad v. The State of Himachal Pradesh MANU/SC/0058/2018
[14] Lawful Legal, Digital Evidence and Its Admissibility in Indian Courts, Lawful Legal (June 1, 2025), https://lawfullegal.in/digital-evidence-and-its-admissibility-in-indian-courts/ (last visited Jun. 8 2025)
[15] Arjun Panditrao Khotkar v. Kailash Kishanrao AIR 2020 SC 4908

to unfair justice if strong safety checks aren't in place. Courts, as protectors of justice, have realized that because digital data can be altered so easily, strong rules are needed to ensure its reliability. This judicial caution shows that while technology offers speed, it also brings new challenges for evidence that need strong legal and procedural responses to keep public trust in the legal system.

2.3. Implications of the Bharatiya Sakshya Adhiniyam (BSA) 2023 on Electronic Records

The BSA 2023 is a major new law designed to make it easier to use digital evidence in court. It officially includes electronic records as "documents" and, importantly, calls them *primary evidence* unless their authenticity is questioned.[16] This change is meant to simplify how they are presented in court, reflecting that digital records are often the original form of information today.

However, when electronic records are used as secondary evidence, the BSA 2023 adds a new, stricter rule: it now requires *two* certificates. One must come from the owner or person in charge of the device that created the record, and another from an "expert". Also, the BSA says this expert certificate must clearly state the hash value (a unique digital fingerprint) of the electronic record and how it was obtained.[17]

While the BSA 2023 aims to simplify digital evidence by making it primary evidence, the new need for an "expert" certificate for secondary evidence, without clearly defining who this "expert" is (though Section 79A of the IT Act offers some guidance), could accidentally create new complex steps and confusion. This lack of clarity might continue, rather than solve, the very problems with evidence admissibility that have historically troubled Indian courts. The judiciary's past difficulties with Section 65B of the IEA, where interpretations swung between flexible and strict, suggest that any new undefined requirement could lead to similar long court battles and delays. The specific demand for hash values and algorithms in the expert certificate implies a high technical standard. Yet, without a clear definition of the certifying expert, the practical use and legal review of this rule might become a new source of disagreement, possibly hindering the efficiency the BSA aims for.

2.4. Challenges in Legal Interpretation and Procedural Compliance

Even with changing laws and court decisions, major problems in understanding and following rules for digital evidence still exist. The ease with which digital data can be changed, modified, or manipulated remains a main concern, directly affecting how real and reliable the evidence is, and thus, how fair trials are.

It's often hard to get the required certificates under Section 65B (or the new BSA rules), especially when the evidence comes from the accused, which raises questions about violating the right against self-incrimination under Article 20(3) of the Indian Constitution. Also, if the original creator or keeper of the data cannot be found or refuses to give the certificate, it creates big obstacles. Such complex procedures often lead to people being found not guilty in criminal cases due to technicalities rather than the actual facts, which lowers public trust in the justice system.

[16] PRS Legislative Research, The Bharatiya Sakshya Bill, 2023, PRSIndia, https://prsindia.org/billtrack/the-bharatiya-sakshya-bill-2023 (last visited Mar. 6, 2025)

[17] S3waas, Electronic Evidence, S3waas (Dec. 27, 2024), https://cdnbbsr.s3waas.gov.in/s3ec01a0ba2648acd23dc7a5829968ce53/uploads/2024/12/2024122766.pdf. (last visited Mar. 31, 2025)

Keeping a clear record of who handled digital evidence (chain of custody) is extremely important but remains tough because computer technology is always changing and vulnerable at every step. Digital data, often stored on many different servers (like phone records or WhatsApp messages), makes it hard to get and figure out where it came from, which hurts investigations. Following privacy and data protection laws when collecting evidence is also key, as illegally obtained evidence can't be used in court. This requires a careful balance between investigation needs and constitutional rights. Criminals increasingly use methods to hide their tracks and encrypt data, making it even harder for investigators to find and use evidence. The fact that forensic labs and cyber cells are not evenly spread across Indian states and territories, with some states having none, directly affects the quality of investigations and the ability to handle digital evidence well.

The legal system, despite constantly changing through new laws and court decisions, still struggles greatly with the real-world problems and weaknesses of digital evidence. This suggests that legal changes alone are not enough to close the digital divide; they must be matched by improvements in technical ability, standard ways of working, and clear ethical rules for handling digital evidence to ensure it is both admissible and follows constitutional rights. The ongoing issues of data manipulation, difficulty in getting certificates, and challenges in keeping a strong chain of custody show that the legal system's ability to manage digital evidence effectively is closely tied to its technological and operational readiness. Without a full approach that strengthens laws, technical skills, and ethical conduct at the same time, the risk of digital evidence leading to unfair justice or procedural failures remains a big worry.

3. Assessment of Technical Expertise in Digital Forensics

3.1. Current Capabilities of Law Enforcement in Digital Investigations

India has shown a strong commitment to improving its cyber forensics system since 2020, mainly because cybercrime rates are rising. The Indian Cyber Crime Coordination Centre (I4C), which started in January 2020 under the Ministry of Home Affairs, is the main national agency for preventing and responding to cybercrime.[18] This central body helps coordinate efforts against cybercrime across the country.

A key part of this system is the National Cyber Forensic Laboratory (NCFL), which has two main parts: NCFL (Investigation) in New Delhi, which has helped with over 11,800 cases by giving real-time support to police during early forensic checks, and NCFL (Evidence) in Hyderabad, opened in 2022, which offers advanced digital forensic services. The NCFL (Evidence) has significantly cut down forensic processing times by almost 50% by using advanced tools for imaging, malware analysis, and decryption.

Also, Central Forensic Science Laboratories (CFSLs) across the country have been updated to handle mobile forensics, cryptocurrency tracking, and secure cloud data analysis. These labs are connected through a national e-Forensics IT platform, which links over 117 state and central forensic labs. This allows for secure data transfer and real-time teamwork, reducing delays in evidence handling. To support these labs, over 550 mobile forensic

[18] *Supra note 1*

vans are used in districts across India. These mobile units can extract data, copy devices, and do quick digital checks on-site. This is very important for solving delays in evidence transfer, especially in remote or rural areas where full labs might not be available. The central government has also helped states through programs like the Cyber Crime Prevention against Women and Children (CCPWC), funding cyber forensic and training labs in 33 States and Union Territories and helping them get advanced tools and hire digital forensic experts.

3.2. Training Programs and Capacity Building Initiatives (ITEC, NCRB CyTrain)

India has set up various training programs for law enforcement to build specialized skills in digital forensics. The National Forensic Sciences University, through the Indian Technical and Economic Cooperation (ITEC) program, offers courses like "Digital Forensics and Cyber Security" and "Computer and Mobile Forensics".[19] These programs teach about digital investigation techniques, focusing on the basics of cybersecurity forensics, and cover key steps like preserving, analysing, and getting digital information from various devices, while also showing participants different forensic tools.[20]

The National Crime Records Bureau (NCRB) plays a big role with its CyTrain portal, which has a detailed "Forensic Track" with Basic, Intermediate, and Advanced courses for Digital Forensics Specialists.[21] These courses go into detail on topics like live data forensics, memory analysis, forensics for different computer systems (Windows, Linux, Mac), mobile forensics (including SIM card data and live mobile capture), network forensics (analysing network traffic), malware analysis, cloud forensics, and Internet of Things (IoT) forensics (including smartwatches and small computers). The advanced courses cover very specialized techniques like VOIP, JTAG & Chip-off (ways to get data from chips), advanced malware analysis, Dark Web investigations, and Cryptocurrency forensics. The CyTrain platform also stresses following standard procedures specific to India and provides practical knowledge of both commercial and free forensic tools like EnCase and FTK Imager through demonstrations.

While structured and thorough training programs like those from ITEC and NCRB CyTrain show a strong government commitment to building technical skills in law enforcement, whether this training is truly *enough* depends not just on the quality of the courses, but also on how *widely available* they are, how *often* they are given, and the *number of people trained* compared to the rising cybercrime rates and the high need for skilled professionals. The information given describes the course content but does not provide numbers on how many people are trained, which is key to knowing if it is truly enough. The fast growth of cybercrime, shown by the 24.4% increase in 2022, suggests that even good training programs might not produce enough qualified people to meet the growing demand, leading to a continued shortage of skilled workers.

3.3. Digital Literacy and Training for the Indian Judiciary and Prosecution

[19] Indian Technical and Economic Cooperation (ITEC), ITEC Courses List, ITEC (June 12, 2025), https://www.itecgoi.in/courses_listinst?salt6=5dboz/kOjM9vxy2SMZxp3w==&salt9=La40++gz6rpbHhcG50CjjQ== (last visited Apr. 04, 2025)

[20] *ibdi*

[21] National Crime Records Bureau (NCRB), Forensic Track Courses, CyTrain, https://cytrain.ncrb.gov.in/course/index.php?categoryid=4 (last visited Mar. 31, 2025)

Efforts to improve digital skills within the Indian judiciary are clear through projects like the e-Courts initiative, which has trained judicial officers. Over 14,000 judicial officers have learned to use the UBUNTU-Linux Operating System, and more than 3,900 court staff were trained as System Administrators for the Case Information System (CIS).[22] These trainings mainly focus on how to operate digital court systems and general computer use.

The NCRB CyTrain portal also has a special "Judiciary / Prosecution Track".[23] The basic course for this track, which takes about 8 hours and 48 minutes, aims to give judges and prosecutors an

understanding of how technology can be used in crime and what digital evidence is and how it can be used in a case.[24] It covers basics like Internet fundamentals, email investigations, social media basics, Open Source Intelligence (OSINT), and the basic steps of digital forensics.

Additionally, State Judicial Academies, like the Kerala Judicial Academy, offer specialized programs such as a "Refresher Programme on 'Cyber Laws & Appreciation & Handling of Digital Evidence'" for civil judges.[25] Internationally, groups like the IACP Cyber Center offer courses such as the 5-day "Digital Evidence for Judges (DEJ)" program, which covers topics including computer forensics, searching and seizing digital evidence, the forensic process, and importantly, how to evaluate expert testimony.[26] Private academies also offer digital forensics training that includes cybercrime law and digital evidence preservation.[27]

While there are programs to train judges and prosecutors in digital skills, the main focus seems to be on basic "awareness" and general digital literacy, rather than deep, practical technical skills in digital forensics. This creates a big "knowledge gap" in the judiciary. This difference in technical understanding, especially compared to the detailed, multi-level forensic training given to law enforcement, could make it harder for judges to properly evaluate complex forensic expert statements and the technical details of digital evidence, especially with the new, stricter "expert" certificate rules in the BSA 2023. The relatively short length and "awareness" goal of the courses for judges, contrasted with the intense, multi-stage forensic training for police, show an imbalance in the system. This means that judges, even though they handle cases heavily relying on digital evidence, might not have the deep technical knowledge needed to thoroughly check how digital evidence is collected, analysed, and proven authentic, which could affect the fairness and accuracy of their decisions.

3.4. Gaps in Skilled Manpower and Continuous Professional Development

[22] Press Information Bureau (PIB), Government of India, E-Courts Project Phase III Approved by Union Cabinet, PIB, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2085127 (last visited Mar. 12, 2025)
[23] National Cybercrime Training Centre (CyTrain), Judiciary / Prosecution Track (Basic Level Course), CyTrain, https://cytrain.ncrb.gov.in/course/view.php?id=36 (last visited Mar. 31, 2025)
[24] Kerala Judicial Academy, Kerala Judicial Academy, KJA, https://kja.gov.in/. (last visited Jun. 12, 2025)
[25] IACP Cyber Center, Digital Evidence for Judges (DEJ), IACP Cyber Center, https://www.iacpcybercenter.org/training_conferences/digital-evidence-judges-dej/. (last visited Mar. 18, 2025)
[26] The Knowledge Academy, Digital Forensics Training - India, The Knowledge Academy, https://www.theknowledgeacademy.com/in/courses/cyber-security-training/digital-forensics-training/ (last visited Mar. 18, 2025)
[27] SIFS India, Certificate Course in Digital Forensics, SIFS India, https://www.sifs.in/course-details/certificate-course-digital-forensics (last visited Jun 08, 2025)

Despite training programs and major infrastructure improvements, India still has a serious shortage of skilled forensic experts, which causes big delays in the criminal justice system. The fast and huge increase in cybercrime cases has clearly grown faster than the number of qualified forensic professionals available, leading to an imbalance between what is needed and what is supplied.

This shortage is made worse by many trained people leaving for the private sector, where they can get better pay and career opportunities. The appeal of higher salaries in private companies means the government struggles to keep its most skilled digital forensic specialists, leading to a constant loss of expertise. Also, many states forensic labs still lack enough resources and have old equipment, which not only slows down analysis but also makes it hard to attract and keep skilled staff.[28] A lack of consistent standards for lab equipment and software licenses across states further increases these differences.

The nature of cybercrime is always changing, with new methods, advanced techniques (like blockchain fraud or AI-powered cybercrimes), and clever ways to hide evidence appearing quickly. This means that skills and training programs need to be constantly updated.[29] This need for ongoing professional development is a constant challenge in making sure expertise stays current and useful. The continuous evolution of digital threats means that training and expert knowledge can quickly become outdated if not regularly refreshed.

The ongoing shortage of skilled workers in digital forensics, made worse by people leaving for private jobs and the constant evolution of cybercrime techniques, creates a serious and widespread weakness in India's digital evidence management system. This suggests that while current training efforts are good in content, they are either not big enough or lack effective ways to keep people, leading to a constant gap between the huge demand for experts and the available supply. The result directly affects the quality and speed of investigations, which in turn impacts how efficient the justice system is and contributes to low conviction rates in cybercrime cases. The inability to properly staff forensic labs and investigative units with highly specialized personnel means that digital evidence might not be collected, preserved, or analysed with the necessary care, ultimately harming the pursuit of justice.

4. Analysis of Digital Infrastructure for Evidence Management

4.1. National-Level Infrastructure and Laboratory Networks

At the heart of India's cyber forensic plan is the Indian Cyber Crime Coordination Centre (I4C), which started in January 2020 under the Ministry of Home Affairs (MHA). It acts as the main national agency for preventing and responding to cybercrime.[1] This central body coordinates national efforts and provides overall direction.

A key project under I4C is the National Cyber Forensic Laboratory (NCFL), which has two main parts: NCFL (Investigation) in New Delhi, and NCFL (Evidence) in Hyderabad.[1] Since it began, the NCFL (Investigation) unit has helped with over 11,800 cases, giving real-time support to law enforcement during initial forensic checks.

[28] Forensic Evidence in India: Bridging the Gap Between Law Enforcement and Judiciary, Law J., https://www.lawjournal.info/article/152/4-2-44-721.pdf. (last visited Mar. 31, 2025)
[29] NextIAS, Integrating AI in India Judiciary and Law Enforcement, NextIAS (Feb. 27, 2025), https://www.nextias.com/ca/current-affairs/27-02-2025/integrating-ai-in-india-judiciary-and-law-enforcement (last visited Jun 02, 2025)

The NCFL (Evidence) lab, opened in 2022, offers advanced digital forensic services and has greatly reduced forensic processing times by almost 50% using advanced imaging, malware analysis, and decryption tools.

At the same time, Central Forensic Science Laboratories (CFSLs) have been updated to include mobile forensics, cryptocurrency tracking, and secure cloud data analysis capabilities. These labs are now connected through a national e-Forensics IT platform, which links over 117 state and central forensic labs. This allows for secure data transfer, real-time teamwork, and fewer delays in evidence handling. This connected network shows a big effort to centralize and standardize forensic capabilities across the country.

4.2. Bridging the Federal Gap: State and District Level Initiatives

While national institutions are very important, cybercrime affects local areas deeply. To deal with this effectively, the central government has helped states build their capabilities through the Cyber Crime Prevention against Women and Children (CCPWC) scheme. Since 2020, this program has funded the creation of cyber forensic and training labs in 33 States and Union Territories, greatly increasing the reach of forensic services across the country.

Furthermore, over 550 mobile forensic vans are used in districts across India. These vans are equipped to extract data, copy devices, and do quick digital checks on-site. These mobile units are crucial for solving delays often linked to transferring evidence to central labs, especially in rural or remote areas. They ensure quicker initial forensic examination and preservation of digital evidence that can easily disappear. Under the Nirbhaya Fund and the MHA's modernization plans, states have received help to buy advanced tools, hire digital forensic experts, and get specialized training, further spreading and strengthening forensic capabilities.

4.3. E-Courts Project and Digital Evidence Management in Judiciary

The e-Courts Mission Mode Project is a major government initiative that aims to use Information and Communication Technology (ICT) to modernize and develop the Indian Judiciary.[30] Started in 2005, the project has gone through several stages, with the goal of transforming the Indian Judiciary by making courts technology-enabled.[31]

Phase-I (2007-2015) focused on computerizing over 14,000 district and lower courts, installing hardware, local area networks (LAN), and Case Information Software (CIS). Phase-II (2015-2023) further improved court services with better ICT infrastructure, more video conferencing facilities (connecting 1272 jails and 3240 court complexes), and the creation of the National Judicial Data Grid (NJDG) to store case and judgment data. The government has approved e-Courts Project Phase III (2023 onwards) as a Central Sector Scheme with a large budget of ₹7210 crore.

Phase III aims to make justice as easy as possible by moving towards digital, online, and paperless courts. This involves fully digitizing all court records, including old files, and making e-filing and e-payments common

[30] Press Information Bureau (PIB), Government of India, E-Courts Project Phase III Approved by Union Cabinet, PIB, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2085127 (last visited Mar. 31, 2025)
[31] e-Courts Project, E-Courts: About Us, e-Courts Project, https://ecourts.gov.in/ecourts_home/static/about-us.php (last visited Mar. 21, 2025)

through e-Sewa Kendras. It also plans to use smart systems that help judges and court staff make data-based decisions for scheduling and prioritizing cases, and to use software for live streaming and handling electronic evidence. New technologies like Artificial Intelligence (AI) and its parts like Optical Character Recognition (OCR) are being used to analyse pending cases and predict future legal trends. The WAN Project, part of e-Courts, has connected 99.5% of all court complexes, ensuring a strong network. To help people who might not have digital access, 1394 e-Sewa Kendras have been set up in District Courts and 36 in High Courts, providing access to e-Courts services, e-filing, and virtual hearings.

For showing digital evidence in court, the e-Courts project imagines paperless courts where all legal arguments, evidence, orders, and judgments are stored digitally.[32] This includes digitizing past and ongoing cases, organizing them for easy finding, and verifying digitized records. A large, interactive touch screen monitor is placed on the judge's desk, allowing access to all digital case documents, organized into different folders.[33] While the information does not detail specific digital exhibit management systems in Indian courts, international examples, like Indiana's Digital Evidence Portal, show how secure systems can upload, store, review, manage, and present multimedia exhibits with controlled access and full searchability.

4.4. Persistent Infrastructural Disparities and Operational Challenges

Despite major national investments and efforts, ongoing differences in technology, especially at state and district levels, along with the natural difficulties of digital data (like encryption and cross-border issues), mean that a truly unified and effective system for managing digital evidence is still a goal, not a reality. A 2024 review shows uneven development across states, with some areas lacking basic equipment or access to updated forensic tools and software, especially in local or rural facilities.[1] This leads to delays in reports, case backlogs, and too few technical staff.

Investigators often struggle to get encrypted or cross-border data, usually because of long bureaucratic delays in international legal agreements (MLATs) and requests to remove content. The growing use of cloud computing for data storage by governments and companies adds more complexity, as getting data from these systems can be harder. If any part of the connected e-court, e-prison, e-prosecution, or e-forensics systems fails, the whole system can be affected, possibly harming fair trials.

Furthermore, investigators face big challenges in recovering data when it is lost, deleted, or hidden on computer systems, networks, and large servers. Criminals increasingly use anti-forensic techniques and encryption to hide their actions and data, making it harder for law enforcement to collect and use evidence in court. The fact that forensic labs and cyber cells are not evenly spread across Indian states and union territories, with some states

[32] Indiana Judicial Branch, Digital Evidence Portal, Indiana Courts, https://www.in.gov/courts/evidence/ (last visited Apr. 13, 2025)
[33] *ibid*

having no such facilities, directly affects the quality of investigations and the ability to handle digital evidence effectively.[34]

The unequal distribution of resources and the ease with which data can be manipulated or lost continue to hurt the efficiency and reliability of the justice system, especially affecting conviction rates. For example, in 2022, despite many cybercrime incidents in big cities like Bengaluru, Mumbai, and Hyderabad, only a small percentage led to a chargesheet (22.6%, 16.6%, and 25.4% respectively). This shows that while technology exists, its uneven quality, combined with the complex nature of digital evidence and procedural hurdles, prevents effective prosecution and leads to low conviction rates in cybercrime cases. The challenges go beyond just providing technology; they include the operational strength and fair access to the entire digital evidence management process.

5. Conclusions and Recommendations

5.1. Synthesized Conclusions

This study shows that India has made good progress in using technology in its justice system, especially for managing digital evidence. Important new laws, like the Bhartiya Sakshya Adhiniyam (BSA) 2023, aim to make it easier to use electronic records in court by calling them primary evidence. At the same time, a lot of money has been put into national digital forensic tools, including the I4C, NCFLs, updated CFSLs, and mobile forensic vans, along with big e-Courts projects that have digitized court processes and improved connections.

However, a persistent and complex digital divide still challenges whether technical skills and technology are good enough. Legally, while the BSA 2023 tries to be clear, the new rule for an "expert" certificate for secondary digital evidence, without a clear definition of who this "expert" is, creates potential confusion that could continue the problems with evidence admissibility seen before. The judiciary's past struggles with understanding digital evidence show a basic concern for its authenticity and integrity, given how easily digital data can be changed.

In practice, despite thorough training programs for law enforcement, there is a serious lack of skilled workers, made worse by many leaving for private jobs and the fast changes in cybercrime methods. For the judiciary, training mostly focuses on "awareness" rather than deep technical skills, creating a knowledge gap that makes it hard to properly evaluate complex digital forensic evidence. In terms of technology, while national facilities are strong, there are big differences at state and district levels, with uneven access to modern tools and software. These gaps, along with problems in accessing data (encryption, cross-border issues) and keeping a clear chain of custody, all together reduce the efficiency, reliability, and fairness of justice, leading to low conviction rates in cybercrime cases.

[34] Evolution of Electronic Evidence: Navigating the Admissibility of the New Criminal Laws in India, IJIRL (Feb. 26, 2025), https://ijirl.com/wp-content/uploads/2025/02/EVOLUTION-OF-ELECTRONIC-EVIDENCE-NAVIGATING-THE-ADMISSIBILITY-OF-THE-NEW-CRIMINAL-LAWS-IN-INDIA.pdf. (last visited Apr. 13, 2025)

5.2. Strategic Recommendations

To effectively close the digital divide and build a stronger, more efficient, and fairer digital justice system in India, a multi-part strategic approach is essential:

5.2.1. Enhanced and Targeted Training

1. **For Law Enforcement:** The number and frequency of advanced training programs from places like ITEC and NCRB CyTrain must be greatly increased to meet the growing need for digital forensic experts. Training materials should be constantly updated to include new technologies like Artificial Intelligence (AI) and blockchain forensics, reflecting how cybercrime is changing. Also, national standard training and certification, possibly following international standards like ISO 17025 for forensic labs, should be put in place to ensure consistent expertise across all agencies.[35]
2. **For Judiciary & Prosecution:** Training for judges and prosecutors needs to go beyond basic "awareness" to build a deeper, more detailed technical understanding of digital forensics. Special courses should be created to give judges the skills to carefully evaluate complex digital forensic reports, understand what hash values mean, and grasp the effects of anti-forensic techniques. It should be considered to make regular advanced training mandatory for judges handling cases with digital evidence.

5.2.2. Robust and Equitable Infrastructure Development

1. **Address Regional Differences:** It is crucial to give priority funding and resources to states and districts that do not have enough, so they can set up and improve forensic labs, buy necessary tools, and get software licenses. This will ensure everyone across the country has fair access to modern forensic capabilities.
2. **Strengthen Mobile Forensic Units:** More mobile forensic vans should be deployed, and they should be equipped with even more advanced tools for on-site data extraction, copying, and quick checks to speed up initial evidence handling, especially in remote areas.
3. **Secure Centralized Digital Evidence Infrastructure:** Investing in secure, central cloud-based storage for digital evidence is essential. Such systems must ensure data integrity, allow authorized people to access it, and follow strict privacy rules, reducing the risks of tampering or loss.
4. **Use AI and New Technologies Responsibly:** Continue to use AI for things like predicting crime, advanced forensic analysis, and automating office tasks in the justice system. However, this must come with strong ethical rules and ways to reduce bias to ensure fairness and impartiality in legal decisions.

5.2.3. Legal and Procedural Clarity

1. **Clarify "Expert" Definition under BSA 2023:** The government must issue clear guidelines or change laws to precisely define the qualifications, official recognition, and responsibilities of the "expert" needed

[35] Interpol, Interpol guidelines for best practices for search and seizure of electronic and digital evidence., Forensic Resources (Oct. 5, 2021), https://forensicresources.org/resources/guidelines-for-digital-forensics-first-responders/ (last visited Apr. 13, 2025)

to provide certificates for secondary electronic evidence under the BSA 2023. This could involve formally linking the role to agencies or departments officially recognized under Section 79A of the Information Technology Act, 2000, which are allowed to give expert opinions on electronic evidence.

2. **Standardize Chain of Custody Protocols:** National, legally binding Standard Operating Procedures (SOPs) must be developed and strictly followed for collecting, preserving, analysing, and presenting digital evidence. This standardization is vital to reduce technical objections and problems with evidence being used in court.
3. **Address Privacy Concerns:** Develop clear rules that follow the constitution for seizing and analysing electronic data. These rules must carefully balance the needs of investigations with basic constitutional rights to privacy (Article 21) and protection against self-incrimination (Article 20(3)), ensuring that illegally obtained evidence is not used.

5.2.4. Human Capital Development and Retention

1. **Attract and Retain Talent:** To stop skilled digital forensic professionals from leaving for private companies, the government must offer competitive salaries, good benefits, and clear career paths within law enforcement and forensic agencies. Creating special groups for digital forensic experts could also improve their professional recognition and encourage them to stay.
2. **Foster Inter-Agency Collaboration:** Improve cooperation and sharing of knowledge between law enforcement agencies, forensic laboratories, and the judiciary. This can be done through joint training, workshops, and shared research projects to build a connected digital evidence management system.

5.2.5. International Best Practices and Collaboration

1. **Adopt International Standards:** India should continue to align its digital evidence handling practices with recognized international standards, such as Interpol guidelines for searching and seizing electronic evidence [36] and ISO/IEC 17025 accreditation for forensic laboratories.[37] This ensures global compatibility, improves the credibility of Indian forensic reports, and helps with investigations across borders.
2. **Streamline MLAT Processes:** Efforts to simplify and speed up Mutual Legal Assistance Treaty (MLAT) processes are crucial for quick access to digital data across borders, which is increasingly important in fighting international cybercrime.

By putting these strategic recommendations into action, India can significantly close its digital divide, making sure its law enforcement and judiciary are well-equipped with the technical skills and technology needed for effective, fair, and timely digital evidence management in the changing digital world.

[36] ANAB, ISO/IEC 17025 Forensic Documents Resources, ANAB, https://anab.ansi.org/resource/iso-iec-17025-forensic-documents-resources/ (last visited Apr. 30, 2025)
[37] Interpol, Interpol guidelines for best practices for search and seizure of electronic and digital evidence., Forensic Resources (Oct. 5, 2021), https://forensicresources.org/resources/guidelines-for-digital-forensics-first-responders/ (last visited Apr. 30, 2025)