IMPORTANCE OF DIGITAL ELECTRONICS EVIDENCE IN COURT OF LAW

Shahar Tanjila Ansari[1]

Mohd. Shanib[2]

ABSTRACT

In the modern era, where technology permeates almost every aspect of life, the role of digital and electronic evidence in the judicial system has become more critical than ever before. Courts of law are increasingly confronted with data that is not tangible but stored in binary code such as emails, CCTV footage, digital voice recordings, social media posts, computer logs, and metadata. This form of evidence, known as electronic or digital evidence, has revolutionized the evidentiary process by offering more objective, traceable, and sometimes real-time insights into events relevant to legal disputes.

This research paper delves into the growing importance of digital evidence in the Indian legal context, tracing the evolution of legal recognition through legislative amendments and judicial pronouncements. The Indian Evidence Act, 1872 was amended by the Information Technology Act, 2000 to include provisions under Sections 65A and 65B, which specifically govern the admissibility of electronic records. A significant part of the analysis revolves around the interpretation of these provisions by the Indian judiciary in landmark cases such as *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, which clarified the mandatory nature of the Section 65B certificate and set the standard for admissibility.

Beyond the legal framework, the paper examines various categories of digital evidence, the technical procedures for collection and preservation, and the challenges in ensuring authenticity and integrity. Issues such as chain of custody, risk of tampering, manipulation, and jurisdictional hurdles in cross-border data access are also addressed. Additionally, the paper highlights the practical challenges faced by courts and law enforcement agencies in dealing with rapidly evolving technologies, particularly in the absence of adequate training and infrastructure. The research further adopts a comparative approach by briefly exploring how other common law jurisdictions like the United States and the United Kingdom handle digital evidence. Unlike the rigid requirements of certification in India, these jurisdictions often rely on principles of authenticity, reliability, and the discretion of the trial court, which may offer useful lessons for legal reform in India. The paper concludes by offering constructive suggestions to strengthen the use of digital evidence in Indian courts, such as judicial training, uniform procedures for certification, legislative clarity, and integration of modern forensic tools like blockchain and digital signatures. It emphasizes that while digital evidence enhances the ability to administer justice in a more accurate and transparent manner, it also necessitates a cautious approach to safeguard rights and prevent misuse.

[1] Author – Indore Institute of law

[2] Co-author - Aligarh Muslim University, Mallapuram

INTRODUCTION

The emergence of digital technology has transformed not only how people communicate, transact, and store information but also how justice is administered. In today's interconnected and technology-driven society, almost every individual leaves behind a digital footprint be it through social media, emails, messaging apps, surveillance footage, or cloud-based storage. As a result, courts of law are increasingly relying on digital and electronic records as essential components of evidence in both civil and criminal trials.

Electronic evidence, also known as digital evidence, refers to any probative information that is stored or transmitted in digital form and can be used in a court of law to support or refute an argument. Unlike traditional forms of evidence, digital records can be duplicated instantly, are vulnerable to tampering, and often require expert verification to establish authenticity. This makes their admissibility and legal reliability both technically complex and procedurally sensitive.

In India, the growing role of digital evidence led to significant legislative reforms with the introduction of the Information Technology Act, 2000, which amended the Indian Evidence Act, 1872, to incorporate Sections 65A and 65B provisions that specifically deal with the admissibility of electronic records. However, despite statutory recognition, the use of electronic evidence in Indian courts has often been mired in controversy due to inconsistent judicial interpretations, lack of technical expertise, and procedural lapses in handling and preserving such evidence.

Notably, the landmark decisions of the Supreme Court in Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) have played a decisive role in laying down the procedural framework for admitting electronic records, especially emphasizing the mandatory nature of the Section 65B certificate. These rulings have not only brought clarity but also raised important questions about the challenges in ensuring the integrity and admissibility of digital evidence.

Moreover, as courts increasingly encounter cases involving encrypted data, digital forgeries, blockchain records, and cross-border cybercrime, the need for a more robust and technologically sound evidentiary system has become urgent. The judicial system must evolve to handle the complexities of digital evidence without compromising on the principles of fairness, transparency, and due process.

This paper seeks to critically examine the legal landscape governing electronic evidence in Indian courts, analyse key judicial precedents, discuss procedural and technical challenges, and explore comparative insights from other jurisdictions such as the United States and the United Kingdom. Ultimately, it proposes recommendations for strengthening the digital evidentiary framework in India to ensure that justice is not only served but served in accordance with the needs of a digital age.

LEGAL RECOGNITION OF DIGITAL EVIDENCE

International Perspective (Brief Overview)

Across the globe, legal systems have gradually adapted to recognize the evidentiary value of digital or electronic records. Countries [3]such as the United States, United Kingdom, Singapore, and Australia have enacted specific laws and rules for the admissibility of electronic evidence.

In the United States, the Federal Rules of Evidence (FRE) lay down broad principles for evidence admissibility, including digital evidence. Rule 901 deals with the authentication requirement, where the proponent must present evidence sufficient to support a finding that the item is what it claims to be. Similarly, Rule 803(6) allows digital business records as hearsay exceptions, provided certain conditions are met.

In the United Kingdom, electronic evidence is governed primarily by the Police and Criminal Evidence Act (PACE), 1984, and supplemented by the Criminal Procedure Rules and common law principles. The UK courts focus on authenticity, reliability, and relevance, rather than requiring formal certificates for admissibility. Expert reports and audit trails are often used to support digital integrity.

Other countries, like Singapore (under the Evidence Act, Cap. 97), have created comprehensive provisions that allow digital records, including those stored in cloud platforms or received through mobile devices, to be admitted under certain presumptions.

Overall, the international trend leans toward functionality and reliability over strict procedural formalism, ensuring that digital evidence is not excluded purely due to technical defects if it is otherwise authentic and relevant.

Legal Framework in India: Sctions 65A & 65B of the Indian Evidence Act

In India, digital evidence gained formal recognition with the introduction of the Information Technology Act, 2000, which amended the Indian Evidence Act, 1872 to include Sections 65A and 65B. These provisions are crucial for the admissibility of electronic records in Indian courts.

- **Section 65A** lays down the special provisions as to the evidence relating to electronic records. It acts as a qualifying clause and refers to **Section 65B**, which provides the actual procedure.
- **Section 65B** outlines the conditions under which electronic records may be considered admissible in court. Subsection (1) states that any information stored in an electronic form that is printed, stored, or copied on optical or magnetic media is deemed a document, provided certain conditions are fulfilled.
- The **Section 65B(4) certificate** is mandatory. This certificate must include:

Identification of the electronic device;

  - Description of the manner in which the data was produced;
  - Details of the device involved;
  - Statement by a responsible person in control of the system, attesting to its accuracy.

[3] The Indian Evidence Act, 1872, §§ 65A, 65B (India).

This section essentially creates a self-contained code for the admissibility of electronic evidence, making traditional rules under Sections 63 and 65 inapplicable.

Judicial Interpretations: Key Case Laws

The Indian judiciary has played a vital role in interpreting these provisions and clarifying ambiguities.

- **Anvar P.V. v. P.K. Basheer**[4], (2014) 10 SCC 473
  This landmark case overruled earlier judgments like *Navjot Sandhu (Afsan Guru)* and held that oral evidence or secondary copies of electronic records are not admissible without a Section 65B certificate. The Supreme Court emphasized that the procedure under Sections 65A and 65B is mandatory and exclusive.
- **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**, [5](2020) 7 SCC 1
  This judgment reaffirmed and clarified *Anvar*. It held that production of the original electronic device is not required if the Section 65B certificate is furnished. However, if the party does not possess the device (e.g., a public authority does), it may apply to the court to direct the concerned authority to produce the certificate.

These decisions underscore a strict procedural approach in India towards digital evidence—unlike the functionalist approach seen in the UK and the US. This has made admissibility often dependent on technical compliance, which may lead to exclusion even of probative evidence if procedural steps aren't strictly followed.

TYPE OF DIGITAL EVIDENCE

Digital evidence, also known as electronic evidence, can originate from a variety of sources and formats. Unlike traditional forms of physical evidence such as documents or fingerprints, digital evidence is intangible, often exists in multiple copies, and can be stored, altered, or deleted remotely. The diversity and scope of digital evidence have expanded rapidly with the evolution of digital devices, cloud technology, and internet-based communication.

Below are the major types of digital evidence commonly encountered in courts of law:

Emails and Electronic Communication

Emails are one of the most widely accepted forms of digital evidence. They may contain critical information like conversations, timestamps, sender/receiver details, and attachments. Courts often rely on email evidence in matters involving fraud, defamation, contract disputes, and cybercrime. The authenticity of email headers and metadata plays a crucial role in proving their credibility.

Call Detail Records (CDRs) and Mobile Data

[4] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).
[5] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).

Call logs, tower location data, and text messages retrieved from telecom service providers are often used in criminal investigations to establish the movement or communication pattern of suspects. CDRs, when properly authenticated, are admissible under Section 65B of the Indian Evidence Act, provided the certification requirements are met.

CCTV and Surveillance Footage

Closed-Circuit Television (CCTV) footage is frequently used in both civil and criminal cases, especially in theft, assault, and property disputes. Such recordings are usually stored digitally and require careful preservation to avoid tampering. Courts consider timestamps, camera angles, and audio (if any) when assessing reliability.

Social Media Content

Posts, comments, messages, and images from platforms like Facebook, Instagram, X (formerly Twitter), and WhatsApp often serve as important digital evidence in cases of cyberbullying, harassment, defamation, or breach of trust. However, due to ease of editing or deletion, courts require proper chain of custody and certification to accept such data.

Computer Files and Hard Drive Data

Documents, spreadsheets, presentations, and logs stored on desktops or laptops may contain key evidence in corporate fraud, intellectual property disputes, or internal investigations. These files often include metadata such as creation/modification date, author information, and access logs which can be critical in legal analysis.

Internet and Browser History

Internet search history, cookies, downloaded files, and browsing patterns can help establish intent, preparation, or motive in criminal cases. Such data, when retrieved legally and authenticated properly, can support charges related to child pornography, terrorism, or illegal purchases.

Cloud Storage and Online Accounts

Files stored in cloud platforms such as Google Drive, Dropbox, or iCloud can also serve as digital evidence. Access to these accounts must follow proper legal process, and any content downloaded must be verified with a valid Section 65B certificate. Chain of custody and audit trails are especially important here.

Blockchain Records and Cryptographic Evidence

Emerging forms of evidence include blockchain transaction logs, crypto wallet data, and smart contract execution records. These are gaining recognition in cases involving cryptocurrency fraud or digital asset disputes. While their immutable nature makes them reliable, their technical complexity demands expert verification.

Audio/Video Recordings

Audio clips, voice recordings, and video files are commonly used in sting operations, interviews, and interrogation recordings. Courts usually require evidence to be unedited, clearly audible, and accompanied by certification as per law.

Logs and Metadata

System logs, server logs, and metadata generated by devices or networks (such as timestamps, geolocation, device IDs) are used to validate other digital evidence. These are often technical in nature and require forensic analysis to interpret properly.

COLLECTION AND PRESERVATION OF DIGITAL EVIDENCE[6]

The collection and preservation of digital evidence are crucial stages in ensuring its admissibility, authenticity, and integrity in courts of law. Unlike physical evidence, digital data is fragile, easily alterable, and often invisible to the naked eye. Any lapse in the procedure can compromise the evidence, rendering it inadmissible in court. Therefore, courts, law enforcement agencies, and forensic experts must adhere to stringent protocols while handling electronic records.

Importance of Proper Collection

The process of collecting digital evidence begins at the crime scene or point of discovery. This may involve confiscating devices such as mobile phones, laptops, external hard drives, CCTV recorders, or cloud access credentials. In certain cases, digital evidence may also be extracted from third-party service providers such as social media platforms or telecom companies.

Some key principles for proper collection include:

- **Avoiding modification**: Devices must not be operated or altered during seizure. Powering on a device without proper precautions may change metadata or erase volatile memory.
- **Documentation**: A clear inventory of all devices collected, their serial numbers, timestamps, and conditions must be prepared at the scene.
- **Use of forensic tools**: Collection must be conducted using certified tools like write blockers or forensic imaging software to ensure no data is modified during extraction.

Failure to adhere to these principles can cast doubt on the reliability of the evidence and lead to objections in court.

Chain of Custody

The chain of custody is a chronological record of who collected, handled, transferred, and stored the digital evidence. It is essential for demonstrating that the evidence presented in court is the same as what was originally collected, without any tampering or unauthorized access.

A valid chain of custody should include:

- Names and signatures of all handlers;

[6] R.V. Kelkar, *Lectures on Criminal Procedure*, 6th ed. (Eastern Book Company, 2018).

- Dates and times of transfer;
- Reasons for movement (e.g., forensic examination, court submission);
- Storage details (e.g., locker ID, server location).

Courts place heavy reliance on the continuity and transparency of the chain of custody while deciding on admissibility. Even highly probative digital evidence can be rejected if the custody trail is broken or inadequately recorded.

Preservation Techniques

Preserving digital evidence involves protecting it from alteration, degradation, or deletion throughout the legal process. Best practices include:

- **Forensic Imaging**: Creating an exact bit-by-bit copy of the storage media (called a mirror image) allows investigators to work on the duplicate without disturbing the original.
- **Hashing Algorithms**: Techniques such as MD5 or SHA-256 are used to generate a unique digital fingerprint (hash value) of the evidence. Any alteration in the data changes the hash, helping detect tampering.
- **Secure Storage**: Evidence must be stored in tamper-proof environments either encrypted digital lockers or sealed physical packaging for hardware devices.
- **Write Blockers**: Devices that prevent data from being written or changed on the source media during examination.[7]

Legal & Procedural Safeguards

Under Indian law, for digital evidence to be admissible, it must meet the conditions set out in Section 65B of the Indian Evidence Act. Preservation efforts must support the issuance of a valid 65B certificate, which should specify:

- The method used to collect and store the data;
- The identity of the device and the system used;
- A statement from a responsible person attesting to the accuracy of the process.

Courts have emphasized that procedural lapses in the handling or certification of digital evidence such as failure to maintain chain of custody or inability to explain how the data was retrieved can result in the evidence being rendered inadmissible, regardless of its relevance.

Role of Cyber Forensics

Cyber forensic experts play an indispensable role in:

- Extracting encrypted or deleted data;
- Preparing forensic reports;
- Testifying in court regarding the validity of collection and preservation methods;
- Assisting in identifying manipulated or fake data.

---

[7] Prashant Iyengar, "Data Privacy and the Indian Legal Framework", (2018) 31(3) *National Law School of India Review*.

Their technical inputs help bridge the gap between law and technology and provide courts with a scientifically sound basis for evaluating digital evidence.

Admissibility and Authenticity of Digital Evidence

The admissibility and authenticity of digital or electronic evidence remain the cornerstone of its utility in any judicial proceeding. Courts are bound by statutory and procedural rules to assess whether a particular piece of electronic evidence can be considered legally acceptable and whether it is sufficiently reliable and unaltered. In the context of Indian law, the Indian Evidence Act, 1872, particularly Sections 65A and 65B, provides the framework for determining the admissibility of such evidence.

Admissibility Under the Indian Evidence Act

Section 65A of the Indian Evidence Act acts as a special provision for the admissibility of electronic records and directs that the contents of electronic records may be proved in accordance with the provisions of Section 65B. Section 65B lays down a detailed procedure for the admissibility of electronic records and introduces the requirement of a "certificate" that confirms the authenticity of the digital record, the device from which it was produced, and the manner in which it was generated.

According to Section 65B(4), a certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities. This certificate must include particulars of the device involved in the production of the electronic record and describe how the record was produced.

This procedure was first emphasized in the landmark case of *Anvar P.V. v. P.K. Basheer*, [(2014) 10 SCC 473], wherein the Supreme Court held that secondary evidence of electronic records is not admissible unless accompanied by a certificate under Section 65B(4). The Court made it clear that oral evidence cannot be a substitute for the certificate and stressed the mandatory nature of compliance with the provision.

Clarification and Evolution: Arjun Panditrao Khotkar Case

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, [(2020) 7 SCC 1], a three-judge bench of the Supreme Court revisited the Anvar ruling to clarify its scope. The Court affirmed that the requirement of the certificate under Section 65B(4) is mandatory unless the original electronic record is produced before the court. The Court further clarified that the certificate is not needed if the owner of the device brings the original device to court and establishes its authenticity through primary evidence.

This clarification was particularly important in contexts where obtaining such certificates was impractical—such as when the source of the evidence was controlled by third parties like telecom companies or social media platforms. The judgment allowed for some flexibility in interpretation without diluting the evidentiary standard.

AUTHENTICITY AND INTEGRITY

Beyond admissibility, the authenticity of digital evidence is paramount. Authenticity refers to whether the evidence is what it purports to be. The chain of custody, metadata verification, and

digital forensic analysis are crucial in establishing authenticity. Any break in the chain of custody, alteration, or manipulation may render the evidence inadmissible or reduce its probative value.

Digital signatures, hash values, timestamps, and audit trails often serve as tools for proving that digital evidence has not been tampered with. Courts also consider expert testimony from digital forensic analysts to establish or refute claims regarding the integrity of such evidence.

Comparative Perspective

In jurisdictions like the United States, the Federal Rules of Evidence (especially Rule 902(14)) allow self-authentication of digital evidence using certified forensic processes. Similarly, the UK has developed robust guidance under the Police and Criminal Evidence Act (PACE), where emphasis is laid on reliability and continuity of evidence.

CHALLENGES AND ISSUE IN HANDLING DIGITAL EVIDENCE

The increasing reliance on digital evidence in legal proceedings has exposed several structural, procedural, and technological challenges. While electronic evidence offers unparalleled objectivity and efficiency, it also brings with it complex problems that directly impact the integrity of the judicial process. Some of the major challenges are discussed below:

Privacy Concerns

Digital evidence often involves access to private and sensitive information, such as emails, call logs, WhatsApp chats, GPS data, and search histories. The use of such information in court raises serious privacy concerns, especially when obtained without consent or proper legal sanction. In *K.S. Puttaswamy v. Union of India*, the Supreme Court of India recognized the right to privacy as a fundamental right under Article 21 of the Constitution. This decision has significant implications for digital evidence, emphasizing the need to balance the right to a fair trial with the right to privacy. Without strict data protection laws and clear judicial guidelines, there is a risk that digital evidence may be misused, violating personal liberties.

Technical Literacy of Judiciary and Legal Practitioners

One of the fundamental obstacles in the admissibility and appreciation of digital evidence is the lack of technical expertise among judges, lawyers, and even law enforcement agencies. The highly technical nature of digital records, encryption, metadata, and cyber forensics requires an understanding that goes beyond conventional legal training. As a result, courts may either over-rely on expert testimony or misinterpret the nature and significance of electronic data. This knowledge gap hampers effective cross-examination, delays trials, and sometimes leads to unjust outcomes.

Risk of Tampering, Fabrication, or Deepfakes

Unlike physical evidence, digital data can be easily edited, manipulated, or even fabricated using sophisticated tools. The rise of *deepfakes* AI-generated fake audio or video further adds to the concern, making it increasingly difficult to distinguish genuine evidence from fabricated material. Courts need reliable mechanisms to verify the authenticity of digital evidence. However, India's legal infrastructure currently lacks a standardized system of digital forensics

that can guarantee the genuineness of every piece of submitted evidence. This creates a serious threat to justice, especially in criminal matters.

Cross-Border Digital Evidence and Jurisdictional Challenges

In today's interconnected world, digital evidence often resides on servers located in foreign jurisdictions. This gives rise to complex issues of jurisdiction, mutual legal assistance treaties (MLATs), and sovereignty. For example, a crime committed in India may have key evidence stored on a U.S.-based cloud server. Gaining access to such data requires international cooperation, which is often slow and uncertain. Moreover, companies like Google, Meta, or Apple may refuse to comply without a local court order from their jurisdiction. This hinders timely investigation and prosecution, especially in cybercrime and terrorism cases

RECENT DEVLOPMENT & JUDICIAL TRENDS IN DIGITAL EVIDENCE

.The Indian legal system is undergoing a significant transformation in how it handles digital evidence. Courts are increasingly acknowledging the evolving nature of electronic records and adapting their interpretations to align with technological developments. Recent judicial pronouncements and innovative practices reflect a growing commitment toward ensuring that digital evidence remains reliable, admissible, and legally sound.

Newer Judgments and Evolving Jurisprudence

a. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1[8]

In this landmark case, a three-judge bench of the Supreme Court reaffirmed the mandatory requirement of a certificate under Section 65B(4) of the Indian Evidence Act for the admissibility of electronic records. The Court clarified that secondary electronic evidence (like printouts, CDs, pen drives, etc.) is not admissible without such certification, unless the original device is produced in court. This ruling resolved the confusion left by earlier conflicting decisions, particularly *Shafhi Mohammad v. State of Himachal Pradesh*.

Importantly, the Court emphasized that Section 65B is a "complete code" in itself for the admissibility of electronic records, and oral evidence cannot be a substitute for the certificate.

b. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473[9]

While not recent, *Anvar* continues to shape judicial understanding. It overruled *State (NCT of Delhi) v. Navjot Sandhu*, which had allowed admissibility based on Section 63 and 65, and established that only Section 65B governs digital evidence. This case marks the shift toward stricter standards of admissibility to avoid manipulation.

c. Jagjit Singh v. State of Punjab (2021 SCC Online SC 1007)

---

[8] • *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).

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

In this case related to farmer protests, the Court relied on video clips, social media posts, and WhatsApp messages as key digital evidence. The judgment acknowledged the growing role of social media content in establishing facts but also stressed the need for authenticity, source verification, and certification under Section 65B.

d. Rahul Gandhi Defamation Case (2023)

In the criminal defamation proceedings involving Rahul Gandhi, transcripts of public speeches and digital recordings were produced in court. This case illustrated how real-time digital records from YouTube, news portals, and social media are becoming increasingly accepted subject to certification.

EMERGING PRACTICES IN HANDLING DIGITAL

a. Use of Cloud-Based Evidence[10]

With most digital interactions now occurring on cloud platforms—Google Drive, iCloud, OneDrive—the law enforcement and judiciary have begun to acknowledge cloud-based data as valid evidence. However, challenges persist regarding data jurisdiction, authenticity verification, and access rights. Courts are increasingly directing investigating agencies to obtain metadata and access logs from cloud service providers through mutual legal assistance treaties (MLATs) or letters rogatory.

Example: In certain cybercrime cases from Maharashtra and Delhi (2021–2024), Gmail chats and cloud-stored documents were admitted after forensic labs confirmed timestamps and server logs.

b. Blockchain Logs and Crypto Evidence

The emergence of blockchain technology has opened new avenues for digital evidence. Blockchain logs, due to their immutable and time-stamped nature, are being explored in commercial disputes, financial frauds, and cryptocurrency-related litigation. While Indian courts are yet to deliver a precedent-setting judgment based entirely on blockchain evidence, startups and legal tech companies have started using blockchain for e-contract signing, digital notary, and document integrity verification.

For example, in arbitration proceedings involving smart contracts, certain tribunals have considered Ethereum-based transaction logs and hash-linked audit trails to determine the timeline and authenticity of contractual actions.

c. Metadata and Digital Forensics as Standard Practice

The use of metadata (timestamps, author ID, edit history) is gaining traction in courts to establish authorship and tampering. Courts now expect investigating agencies to submit forensic analysis reports generated by certified labs (such as CFSL or Truth Labs), which include hash values and system logs.

---

[10] https://www.interpol.int/en/Crimes/Cybercrime/Digital-forensics

d. Video Conferencing & Virtual Evidence Handling

Post-COVID, virtual hearings and e-filing of evidence have become normalized. The judiciary, especially the Delhi High Court and Supreme Court, has issued practice directions for electronic submissions, including the filing of 65B certificates and original digital media. Courts have also allowed cross-examination based on screen-shared content.

AUTHOIRS SUGGESTIONS

1. **Amending the Indian Evidence Act**
   The Indian Evidence Act, 1872 was never originally designed to deal with the intricacies of electronic records. Though Sections 65A and 65B were introduced via amendment, they now require further revision to adapt to modern technological realities. A more flexible and technology-neutral legal framework should be incorporated that doesn't rely solely on certificates under Section 65B for admissibility.
2. **Preservation Infrastructure**
   There is an urgent need for dedicated digital evidence preservation labs at state and district levels. These labs must maintain chain-of-custody protocols and be equipped with standard digital forensic tools to ensure evidence integrity from the moment of seizure to presentation in court.
3. **Training and Capacity Building**
   Judges, prosecutors, police, and lawyers should receive mandatory training in the handling, analysis, and implications of digital evidence. Without adequate understanding, even genuine digital evidence may be rejected due to procedural lapses or misinterpretation.
4. **Stronger Data Privacy and Security Norms**
   As digital evidence often comes from personal devices or cloud-based platforms, it is essential that Indian law strike a balance between privacy rights (as held in *Justice K.S. Puttaswamy v. Union of India*) and the needs of investigation. A clear standard for lawful seizure, handling, and use of such data is necessary.
5. **Use of Emerging Technologies in Evidence Validation**
   India must encourage use of blockchain-based logging mechanisms and tamper-proof audit trails to verify the authenticity of digital evidence. Forensic watermarking and AI-powered verification tools could be deployed to assess originality.
6. **Digital Evidence Bench Guidelines**
   The Supreme Court of India or the Ministry of Law & Justice can consider releasing a standardized "Digital Evidence Handbook" for trial courts, ensuring consistency and procedural uniformity across jurisdictions.
7. **Cross-border Cooperation for Cloud Evidence**
   With more data now residing in servers abroad (Google, Meta, Amazon Web Services), India should strengthen its Mutual Legal Assistance Treaties (MLATs) and adopt data-sharing protocols such as the CLOUD Act to speed up access to crucial evidence in transnational cases.

CONCLUSION

The exponential growth of technology has irreversibly transformed the way evidence is created, stored, transmitted, and presented in courts of law. From emails and mobile data to blockchain logs and cloud storage, digital evidence has emerged as a cornerstone of modern litigation. In India, while the legal system has made commendable strides with the introduction of Sections 65A and 65B of the Indian Evidence Act and key Supreme Court decisions like *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, challenges still persist in practice.

Issues such as the technical complexity of collecting and preserving digital data, the rigid procedural requirements for admissibility, and the lack of digital literacy among legal stakeholders have limited the full potential of electronic evidence. Furthermore, the increasing reliance on cloud-based services and international data servers has added jurisdictional and privacy complexities that demand urgent legal and infrastructural reforms.

Nevertheless, the future holds promise. With continuous judicial evolution, policy initiatives, and integration of forensic and technological tools, digital evidence can be made more reliable and accessible. It is imperative for lawmakers, law enforcement, and the judiciary to work collaboratively to build a more robust framework—one that upholds justice without compromising on privacy, due process, or the rule of law.

In essence, the importance of digital evidence in modern litigation is no longer a futuristic possibility but a present-day reality. To ensure that the legal system remains responsive, fair, and effective, adapting to this digital paradigm is not optional it is essential.