AUTHENTICITY OF DIGITAL EVIDENCE IN INDIAN CRIMINAL TRIALS

Gokul S, Vinayaka Missions Law School

Gayathri S, Vinayaka Missions Law School

ABSTRACT

Criminal trials in India now rest heavily on material that did not exist in a courtroom a generation ago: call detail records, CCTV footage, whatsapp Chats, location data and audio-video recordings. The difficulty is not whether such material can be received by a court, but whether it can be trusted. This paper examines how Indian Law has tried to answer that question, moving from section 65B of Indian Evidence Act, 1872to Bharatiya Sakshya Adhiniyam, 2023. It traces the supreme court's shifting position from Navjot Sandhu to Arjun Panditrao Khotakar, looks at the 2026 decision uploading the new hash value and expert certificate, and then turns to the practical weak points in investigation, seizure and chain of custody. The paper argues that the law has become more demanding on paper, but that authenticity will still depend on how carefully investigators and courts handle the record before it ever reaches the certificate stage.

Keywords: Digital evidence, Authenticity, Electronic records, bharathya shakshya adhiniyam, Chain of custody, criminal trails.

1. Introduction

A decade ago, a prosecutor who wanted to rely on a mobile phone record had to worry mostly about whether a witness would turn hostile. Today the worry is just as often about a pen drive. Electronic material now features in cases ranging from murder and terrorism to financial fraud, stalking and sexual offences and in many of them it is the only link between the accused and the crime.

The law of evidence was built for paper and for people. Its basic tools such as primary and secondary evidence, proof by witnesses and presumptions about documents, assumed that a document could be seen, handled and compared. A digital record is different. It can be copied without any visible change, edited without leaving an obvious trace, and stored in a form that no human can read without a machine. The Bharathiya Sakshya Adhiniyam, 2023 (BSA), which replaced the Indian Evidence Act, 1872 (IEA) from 1 July 2024, was drafted with this in mind.[1]

This paper is concerned with a narrow but important question. When a court says! That a piece of digital evidence is "authentic", what is it actually satisfied about and how does Indian law get it there? The Supreme Court itself has acknowledged that electronic records are open to tampering and interpolation, and that the rules governing them must be read with that risk in mind.[2] The paper first sets out what authenticity means in this setting, then examines the statutory scheme, the case law, the investigative practices that sit behind the courtroom, and finally some reforms that seem worth considering.

2. Research Methodology:

This research adopts a doctrinal method of legal research. It examines statutory provisions, judicial decisions, legal books and relevant reports to understand the authenticity of digital evidence in indian criminal trails.

The study primarily focus on (BSA) Bharathya Shakshya Adhiniyam 2023, and the judicial interpretation of electronic evidence. It also examines practical challenges relating to digital

[1] Bharatiya Sakshya Adhiniyam 2023 (Act 47 of 2023), brought into force on 1 July 2024, repealing the Indian Evidence Act 1872.
[2] Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.

forensic examination, chain of custody and emerging technologies.

3. What "Authenticity" Means for a Digital record:

Lawyers often use admissibility and authenticity as if they were the same thing. They are not. Admissibility is a legal threshold: is this item of proof allowed to go before the court at all? Authenticity is a factual and technical question: is the record what the party producing it says it is, and has it remained unaltered since it was created or seized? A record can clear the admissibility threshold on a technicality and still be unreliable, and the reverse is also possible.

Writers on electronic evidence generally break authenticity into few parts.[3] The first is origin, meaning which device or system created the record and who operated it. The second is integrity, meaning whether the content has changed. The third is continuity, meaning whether the record has been kept in a way that rules out interference between creation and trial. Each of these can fail independently. A genuine CCTV system may have its footage overwritten and replaced; a genuine phone may be handled by an officer who browses through it before sealing it.

The technical tool that has come to symbolise integrity is the hash value. A hash function produces a fixed length string from a file, and even a one-bit change in the file produces a completely different string. If the hash taken at the time of seizure matches the hash taken before trial, the court has good reason to believe the file is unchanged. The Supreme court has described the hash value as something like a digital fingerprint of the record.[4] That description is a helpful shorthand, though it should be remembered that a hash proves only that a file has not changed since the hash was computed. It says nothing about whether the file was genuine when the hash was taken.

4.The Statutory Framework:

4.1 Section 65B of the Indian Evidence Act

When the Information Technology Act, 2000 was passed, it amended the IEA by inserting Section 65A and 65b.[5] Section 65A declared that the contents of electronic records could be

[3] Stephen Mason and Daniel Seng (eds), Electronic Evidence and Electronic Signatures (5th edn, University of London Press 2021).
[4] Pune Bar Association v Union of India, Writ Petition (Civil) No 599 of 2026 (SC, decided 22 May 2026).
[5] Information Technology Act 2000, Second Schedule, inserting ss 65A and 65B into the Indian Evidence Act

proved only in accordance with section 65B. Section 65B then treated computer output as a document admissible without production of the original, provided certain condition about the computers regular use and proper functioning were met, Sub-section (4) required a certificate identifying the record, describing how it was produced and signed by a person in a responsible official position in relation to the device.

The drafting was awkward, and much of the litigation of the next twenty years was about what exactly the certificate was for, whether it could be dispended with and who could be made to sign it.

4.2 The Bharathiya Sakshya Adhiniyam, 2023

The BSA carries the same idea forward but change the machinery. Section 61 provides that an electronic records is not to be denied legal effect, validity or enforceability merely because it is in electronic form, and section 62 says the content of electronic records may be proved in accordance with section 63. [6]Section 63 then deals with the condition for treating an electronic records as a document, the position where several computers or devices are involved, and the certificate that must accompany the record.[7]

The most visible change lies in the certificate. Under section 63(4) it must be in the form given in the schedule to the act. The schedule is split into two parts. Part A is filled in by the person in charge of the device and the party producing the record, and it must state the hash value. Part B is to be completed by an expert. The old certificate had one signatory; the new one has two, and it has a technical statement of integrity built into it.

There is also change in how original are treated. The explanations to section 57, which defines primary evidence, now recognise that a digital record kept in proper custody, or stored simultaneously in several files, may itself count as primary evidence. [8] In principle this widens what can be proved without going through the certificate route, although courts have not yet explored how far that goes.

1872.
[6] Bharatiya Sakshya Adhiniyam 2023, ss 61 and 62.
[7] Bharatiya Sakshya Adhiniyam 2023, s 63 and the Schedule.
[8] Bharatiya Sakshya Adhiniyam 2023, s 57 (primary evidence), Explanations.

5. The Judicial Journey: from Navjot Shandhu to Khotkar:

5.1 State (NCT of Delhi) v Navjot Sandhu

In the case of parliament, the prosecution used the call logs from cellular operators. However, there was no section 65B certificate. The Supreme cout held that they could be used as a secondary evidence under the provisions of section 63 and 65 of IEA. For about a decade it became an accepted practice that the certificate would not be necessary.[9] It Would merely be beneficial during the trail.

5.2 Anvar P.V v P.K. Basheer

This position changed sharply in election dispute, video compact discs were produced without certificate. A three - judge bench held that section 65A and 65B from a complete code, that the general law on secondary evidence gives way to this special provision, and that the certificate is a condition for admissibility. *Navjot Sandhu* was overruled on this point.[10] The reasoning was explicitly tied to risk of manipulation: if electronic records were accepted without any safeguard, the court would have no assurance about their source or accuracy.

5.3 Shafhi Mohammad v. State of Himachal Pradesh

The strictness of *Anvar* created a practical problem. A victim or private litigant who has a recording but not own or control the device on which it was made cannot easily get a requirement was procedural and could be relaxed where the party was not in possession of the device.[11] Critics pointed out with some justice, that a bench of two had effectively diluted what three judges had decided.

5.4 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

The conflict was resolved by a three - judge bench in 2020. The court overruled *Shafhni Mohammad* and restored *Anvar*, holding that the certificate under the section 65B is mandatory precondition when secondary electronic evidence is produced.[12] It added two important qualification. The first is that the certificate need not to be produced at the very first moment

[9] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600.
[10] Anvar P.V. v P.K. Basheer (n 2).
[11] Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801.
[12] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

; where it is the missing, the court may allow it to be supplied at a large stage, and in appropriate cases can direct the concerned person to produce it. The second is that where the device is in the hands of the opposite party or the third party who refuse to corporate, the law does not demand the impossible, and the party seeking to rely on the record may ask court to summon the device or the certificate.

Khotkar also confirmed that a person who owns or operates the device can prove the original by entering the witness box and identifying it, in which case no certificate is needed because the evidence is primary.

5.5 Objection at the right time

A related line of the cases concerns when an objection must be taken. In the *sonu v. State of Haryana* the supreme court said that if an objection to the mode of proof of call records is not raised when the document is marked as an exhibit, it cannot be taken for the first time on the appeal.[13] The reasoning is that a defect in the mode of proof, as opposed to inadmissibility in law, can be cured if pointed out in time. In practicde this make the conduct of the defense counsel at the trail stage far more important than is often realised.

5.6 Failure to produce available recordings

The court have also been willing to draw an adverse inference where the prosecution has withheld electronic material that was clearly available.In *Tomaso Bruno v. State of Uttar Pradesh*, the prosecution did not produce CCTV footage from the place of occurrence even through it was available, and the Supreme Court treated this as a serious gap and a reason to doubt the case.[14] The decision is a reminder that authenticity cuts both ways: it is not only the accused who may be hurt by a doubtful record, but also the prosecution when it fails to place the best record before the court.

6. The 2026 Decision on Section 63(4):

The new certificate was challenged almost as soon as it come into force. In *Pune Bar Association v. Union of India,* decided on 22 May 2026, the petitioner argued that the schedule imposed an unreasonable burden on ordinary litigants, particularly because Part B required an

[13] Sonu @ Amar v State of Haryana (2017) 8 SCC 570.
[14] Tomaso Bruno v State of Uttar Pradesh (2015) 7 SCC 178.

expert's signature and Part A required a high value that most people could not generate.[15] A related argument, drawn from a Madras High Court ruling, was that only an Examiner of Electronic Evidence notified under section 79A of the Information Technology Act could sign Part B.

The Supreme Court upheld the validity of section 63 (4) and schedule. As reported, it emphasized that electronic records are a distinct species of evidence which is easy to manipulate, and that disclosing the hash value is a reasonable way of protecting integrity. On the second point, the court did not accept that the expert certificate was limited to notified examiners. It read section 39(1) of the BSA, which admits the opinion of person with special skill, together with section 39(2) and section 79A of the IT Act, and treated the two as operating side by side rather than one cutting down the other.[16]

Two observation may be made first, the judgement brings some certainty to a provision that had begun to produce conflicting High Court views within two years of its commencement. Second, by leaving the question of who qualifies as an expert to be worked out case by case, the court has left trail judges within a fair amount of discretion. This will likely affect how effective the new certificate is as to how the discretion is used and whether defense lawyers can really challenge and expert's credentials.

7. Authenticity Before the Courtroom: Investigation and Chain of Custody

It is tempting to think of the certificate as the point at which authenticity is established. In reality most of the damage to a digital record is done much earlier, in the hours and days after it is first found.

7.1 search, Seizure and recording

The Bharatiya Nagarik Suraksha sanhita, 2023 (BNSS) has tried to bring some discipline into this stage. Section 105 requires that the process of search and seizure be recorded by audio-video means, and section 176(3) requires, for offenses punishable with seven years or more, that forensic experts visit the scene and that the collection of evidence be videographed.[17] section 94 allows a court or police officer to require production of documents or things, and

[15] Pune Bar Association (n 4).
[16] Pune Bar Association (n 4); see also Bharatiya Sakshya Adhiniyam 2023, s 39.
[17] Bharatiya Nagarik Suraksha Sanhita 2023, ss 105 and 176(3).

the language is wide enough to cover electronic device and their contents.[18] These provisions are useful, but they depend on a police force that has the equipment, the training and the willingness to follow them. Anyone who has read the evidence of investigating officers in sessions trails will know that seizure memos are often prepared hurriedly and that device are sometimes not sealed in front of independent witnesses.

7.2 Imaging and hashing

Good practice in digital forensics is to make a bit -for-bit image of the device, compute a hash value for the image, and work only on the copy. The original is sealed and stored where this is not done, and the original device is switched on, browsed or connected to a network, files can be changed without anyone intending it. A defense lawyer who asks the Investigating Officer simply whether the phone was in flight mode when it was seized will often learn more about the quality of the investigation than from many page of cross-examination.

7.3 Chain of Custody

Indian law has no single statute dealing with chain of custody for electronic evidence, so courts rely on the general principle that the prosecution must account for the exhibit from seizure to production. A break in the chain, such as an unexplained gap between seizure and deposit in the malkhana, or between the malkhana and the forensic laboratory, does not by itself make the evidence inadmissible, but it weakens its value. The more technical the evidence, the less a court can afford to ignore such gaps, because the possibility of alteration cannot be checked by looking at the item.

7.4 Forensic laboratories

Section 79A of the IT Act allows the central Government to notify agencies as examiners of Electronic Evidence, and their opinion is treated as expert opinion under the evidence law.[19] The capacity of these laboratories is limited compared with the number of devices seized each year. Delay in examination is a common complaint and delay itself becomes an authenticity problem, because the longer a device remains in storage the more room there is for argument about what happened to it.

[18] Bharatiya Nagarik Suraksha Sanhita 2023, s 94.
[19] Information Technology Act 2000, s 79A.

8. Particular Problems with Common Forms of Digital Evidence

8.1 Messaging applications

Whatsapp and similar applications creates a special difficulty because the same conversation exists on the least two devices, and a screenshot is only an image of what appeared on at some moment. A screenshot without no certificate and no examination of the phone is a weak form of proof, since it can be assembled using a chat-simulation tool. End-to-end encryption also mean that the service provider cannot ordinarily vouch for the content, so the party relying on the chat generally has to produce the device itself and prove it through the section 63 route.

8.2 CCTV Footage

CCTV systems are often privately owned shop or residential systems with no maintenance records. Footage is frequently copied to a pen drive by a technician who is not an official of the system, and the certificate is signed by a person who has no real knowledge of how the system works. A court that is satisfied only by the presence of a signed form may be accepting a formality in place of proof. The better approach is to ask who extracted the footage, with what software, and whether the time stamp on the system was ever checked against actual time.

8.3 Call detail records and location data

Call detail records are in many way the most routine form of electronic evidence, and also the easiest to take for granted. They are generated by the service provider and are usually proved by a nodal officer's certificate. The practical issue is cell-tower location, which gives only an approximate area. Court have to be careful not to treat tower data as proof of exact presence, and defence counsel should insist that the technical limits be explained by a witness who can actually be cross examined.

8.4 Manipulated and synthetic media

The most serious emerging challenge is audio and video generated or altered by software. A convincing fake can now be produced cheaply, and the traditional method of authenticating a recording, which was to have a witness say that the voice or face was familiar, is not as reliable as it once was. Neither the BSA nor the BNSS has a specific provision on synthetic media. The existing framework, which depends on the certificate, the hash and experts opinion, may be

able to deal with it, but only if experts are able to detect alteration and courts are willing to ask whether they have done so.

9. Unlawfully obtaining digital Evidence and privacy:

A different aspects of authenticity concern the manner in which a record was obtained. Indian courts have historically held that evidence is not excluded merely because it was obtained through an illegal search or seizure, so long as it is relevant and its genuineness is proved.[20] This approach was followed in the 1970s in case such as *R.K.Malkani v. State of Maharashtra* for tape-recorded conversations, and in *Pooran Mal v. director of Inspection.*[21]

The recognition of privacy as a fundamental right in K.S.Puttaswamy v. Union of India has raised the question of whether this older approach can continue unchanged in the case of digital material such as phone data and location history, where the intrusion can be far greater.[22] The courts have not yet laid down a clear rule. Closely related is the question of compelling an accused to unlock a phone or give a password, which touches the protection against self-incrimination in Article 20(3) of the constitution. The reasoning in Selvi v. State of Karnataka on compelled testimonial acts offers some guidance, but its application to biometric and password based access remains unsettled.[23]

10.Suggestions:

The law has been strengthened in form, but several things might improve it in practice.

First, a standard operating procedure for seizure, imaging and storage of digital devices should be issues with binding force, preferably through rules under the BNSS, so that investigators across states follows the same method. At present practice varies widely from one police unit to another.

Second, defence counsel and judges need better access to technical training. A certificate has value only if the person reading it can ask intelligent question about it. Judicial academies could

[20] See generally the discussion in Ratanlal Ranchhoddas and Dhirajlal Keshavlal Thakore, The Law of Evidence (LexisNexis, latest edn).
[21] R.M. Malkani v State of Maharashtra (1973) 1 SCC 471; Pooran Mal v Director of Inspection (Investigation) (1974) 1 SCC 345.
[22] Justice K.S. Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[23] Selvi v State of Karnataka (2010) 7 SCC 263.

include short practical modules on hashing, metadata and imaging.

Third, forensic capacity need to be expanded. If notified laboratories cannot examine devices within a reasonable time, the news certificate requirement risks becoming a sources of delay rather than reliability. Accreditation of private experts, with transparent criteria, would also help give content to the idea of an "expert" that the Supreme Court has left open.

Fourth, Parliament or the rule- making authority should consider providing for the authentication of synthetic media. A short provision requiring courts to consider the possibility of alteration, and permitting them to order examining of metadata or sources files where a recording is seriously disputed, would be a modest and useful step. The law commission had already pointed to the need to modernise evidence law for electronic material in its review of the Evidence Act, and that work has not kept pace with technology.[24]

Fifth, trial courts should be encouraged to decided objections to electronic evidence at the stage of marking, rather than leaving them to be argued at the end. Given the reasoning in sonu, an early and reasoned ruling would benefit both sides.

11.Conclusion:

Indian law on digital evidence has moved in a fairly clear direction over the last twenty years: away from the relaxed approach of Navjot Sandhu, through the strict rule of Anvar and the settling effect of Khotkar, to a certificate under the BSA that requires a hash value and an expert's signature. The 2026 decision upholding Section 63(4) confirms that the courts see this added rigour as justified by the nature of the evidence.

But a certificate is only a statement it does not by itself prove that a phone was handled properly, that a CCTV system kept correct time or that a video is real. Those facts depend on investigators, forensic examiners and the question asked in court. The real test of the new framework will therefore not be how often the certificate is filed, but how often courts are prepared to look behind it. If they do, the law can make digital evidence more reliable. If they do not, there is a danger that the form of authenticity will be mistaken for the substance.

[24] Law Commission of India, 185th Report on the Review of the Indian Evidence Act, 1872 (March 2003).

Bibliography

Statutes

- Bharatiya Nagarik Suraksha Sanhita, 2023.
- Bharatiya Sakshya Adhiniyam 2023.
- Indian Evidence Act, 1872.
- Information Technology Act, 2000.

Cases

1. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
3. Justice K.S. Puttaswamy (Retd) v. Union of India (2017) 10 SCC 1.
4. Pooran Mal v. Director of Inspection (Investigation)(1974)1 SCC 345.
5. Pune Bar Association v. Union of India, WP (c) no 599 of 2026 (SC,22 May 2026)
6. R.M. Malkani v. State of Maharashtra (1973)1 SCC 471.
7. Selvi v. State of Karnataka (2010) 7 SCC 263.
8. Shafhi Mohammed v. State of Himachal Pradesh (2018) 2 SCC 801.
9. Sonu @ Amar v. State of Haryana (2017) 8 SCC 570.
10. State (NCT of Delhi) v. Navjot Sandhu (2005)11 SCC 600.
11. Tomaso Bruno v. state of Uttar Pradesh (2015) 7 SCC 178.

Book and Reports:

- Law Commission of India, 185th Reports on the Review of the Indian Evidence Act,

1872(2003).

- Mason, S., & Seng, D. K. B. (2021). Electronic evidence and electronic signatures. In *University of London Press eBooks*. https://doi.org/10.14296/2108.9781911507246

- Ranchhoddas, R., & Thakore, D. K. (2010). *Ratanlal & Dhirajlal's The Law of Evidence (Act I of 1872): Enlarged Edition on a Wider Format...*