Deepfakes, AI, and Cloud Forensics: Rethinking the Admissibility of Secondary Electronic Evidence in India and the United States

[1]Ram Krishna Baghel, [2]Dr. Rajeev Kumar Singh
[1]B.A. LL.B (Hons) 5th Year, [2]Assistant Professor
[1]Amity Law School, Lucknow
[1]Amity University Uttar Pradesh, Lucknow Campus

Abstract : **The admissibility of electronic evidence is undergoing a critical transformation, shaped by the rise of deepfakes, cloud-native data, and AI-generated content. This paper presents a comparative legal analysis of secondary electronic evidence in India and the United States, focusing on authentication protocols and evolving admissibility standards.**

India's Bharatiya Sakshya Adhiniyam, 2023 (BSA) retains the certification requirement for electronic records under Section 65B, yet struggles to address the complexities of synthetic media and decentralized digital storage. Judicial interpretations—from *Anvar P.V. to Arjun Panditrao Khotkar*—reveal tensions between procedural rigidity and technological realities. The paper examines the evidentiary role of hash values, metadata, and expert opinion under Section 39(2), alongside the institutional function of the Examiner of Electronic Evidence.

In contrast, the U.S. Federal Rules of Evidence (FRE) adopt a more flexible approach. Rule 901 allows contextual authentication, while Rules 902(13) and 902(14) permit self-authentication of machine-generated records. Cases such as United States v. Jackson and United States v. Thomas illustrate how courts engage with digital evidence using forensic tools and expert validation, often without rigid procedural constraints.Employing doctrinal analysis and forensic protocol review, this paper identifies key divergences in admissibility thresholds, burdens of proof, and treatment of synthetic media. It proposes a hybrid model integrating technical validation such as blockchain timestamps and AI-detection algorithms within a coherent legal framework.

The paper concludes by advocating statutory reform in India to define synthetic media, recognize presumptive admissibility for verified forensic tools, and harmonize evidentiary standards with global best practices. By bridging legal doctrine with forensic innovation, this research contributes to the evolving discourse on digital truth and the future of cybercrime adjudication.

IndexTerms **- Electronic Evidence, Authentication, Synthetic Media, Forensic Protocols, Comparative Law.**

I. INTRODUCTION

In today's courtrooms, digital evidence is no longer an occasional supplement — it often decides the case. Under the *Bharatiya Sakshya Adhiniyam, 2023* (BSA), electronic records are firmly recognised, yet the old Section 65B-style certificate requirement is still anchored in Section 63(4)[1]. This safeguard aims to ensure authenticity, but in practice it feels inflexible when evidence is drawn from decentralised systems, cross-border cloud services, or even AI-generated sources. The legal reality is that most data today is stored or transmitted through distributed ledgers, blockchain-anchored archives, and multi-jurisdiction SaaS platforms, which means courts and litigants often rely on *secondary electronic evidence* server logs, exported datasets, or forensic images collected from providers beyond India's territorial reach[2]. Alongside these practical hurdles are serious integrity threats: deepfake content produced by *Generative Adversarial Networks (GANs)*[3], altered metadata designed to mislead on timestamps or geolocation[4] and deliberate hash manipulation to pass off tampered files as original[5]. Indian courts, through rulings such as *Anvar P.V. v P.K. Basheer* and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, have reinforced that certification is mandatory[6], yet compliance becomes near-impossible when foreign custodians do not cooperate[7]. The BSA also has no dedicated framework for synthetic or AI-created media, leaving judges to work within general evidentiary rules, the Information Technology Act, 2000, and expert opinion. This contrasts sharply with the *U.S. Federal Rules of Evidence* (FRE), where provisions like Rules 901 and 902(13)–(14) allow more adaptive authentication for machine-generated and cloud-sourced material[8]. Against this backdrop, the present study will: (i) assess admissibility thresholds for secondary electronic evidence under the BSA; (ii) compare these with the FRE's approach; (iii) examine the robustness of current authentication protocols from cryptographic hashes and blockchain timestamps to metadata forensics and AI-deepfake detection; and (iv) propose a hybrid reform model that blends forensic science with statutory safeguards to protect evidentiary integrity while accommodating modern technology[9]. The methodology combines doctrinal and comparative legal analysis, review of technical protocols, and policy evaluation using authoritative sources such as Law Commission reports, government advisories, and international best-practice guidelines, ensuring that the conclusions are both legally sound and technologically relevant[10].

---

[1] Bharatiya Sakshya Adhiniyam 2023, s 63(4).
[2] Ministry of Electronics & Information Technology, *India Cloud Strategy* (2021) <https://www.meity.gov.in>.
[3] S Gill, 'Deepfakes and Indian Law' (2024) 6(2) *NLUJ L Rev* 45.
[4] NIST, *Guide to Integrating Forensic Techniques into Incident Response* (SP 800-86, 2020).
[5] X Wang and H Yu, 'How to Break MD5 and Other Hash Functions' (2005) 21(3) *Advances in Cryptology* 19.
[6] *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473; *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
[7] P Kumar, 'E-Evidence and Cloud Jurisdiction' (2022) 14(1) *Indian Journal of Law & Tech* 77
[8] Federal Rules of Evidence, rr 901, 902(13) – (14).
[9] UNODC, *Handbook on Identity-Related Crime* (2023) ch 6.
[10] Council of Europe, *Guidelines on Electronic Evidence in Criminal Proceedings* (2019).

II. LEGAL FRAMEWORK FOR ADMISSIBILITY OF SECONDARY ELECTRONIC EVIDENCE IN INDIA

The admissibility of secondary electronic evidence in India is founded on a combination of procedural safeguards and substantive definitions embedded in the *Bharatiya Sakshya Adhiniyam, 2023* (BSA) and supplemented by the *Information Technology Act, 2000* (IT Act). Within Chapter V of the BSA dedicated to documentary evidence, Section 58 defines "secondary evidence" to include, inter alia, counterparts of documents and reproductions made by mechanical or electronic processes that ensure accuracy.[11] In the digital context, Section 63 lays down special provisions for electronic records, confirming that they are documents when produced in compliance with statutory conditions. Central to admissibility is Section 63(4), which is effectively the procedural successor to the erstwhile Section 65B (4) of the Indian Evidence Act, 1872, mandating a certificate that specifies the identity of the electronic record, the manner of production, and relevant device particulars, authenticated by a person in a responsible official position[12]. The provision operates as a statutory authentication mechanism, ensuring that courts receive electronic records accompanied by verifiable assurance of integrity. Furthermore, Section 39(2) empowers courts to rely on the opinion of specially skilled persons for matters relating to electronic evidence, a route often invoked in cases involving forensic examination of metadata, hash verification, or detection of synthetic media[13].

The IT Act complements this procedural structure by supplying the overarching definitions and offences that frame evidentiary relevance. Section 2(1)(t) provides a broad definition of "electronic record", encompassing data, images, sounds, and any information generated, sent, received, or stored in electronic form, thereby covering not only traditional digital files but also algorithmically generated content[14]. Provisions such as Section 66C (punishing identity theft) and Section 66D (cheating by personation through computer resources) address offences where electronic evidence is critical to establishing culpability[15]. Section 67B, criminalising child sexual abuse material in electronic form, further illustrates Parliament's acknowledgement of the evidentiary complexities and sensitivities involved in handling certain categories of data[16]. Taken together, the BSA prescribes the procedural gatekeeping requirements for admissibility, while the IT Act frames the substantive legal context in which such evidence is evaluated. This twin-statute framework ensures that secondary electronic evidence is subjected to both rigorous authentication protocols and clear statutory definitions before it is admitted for judicial consideration.

2.1 Judicial Interpretation

Judicial interpretation has played a decisive role in shaping the admissibility standards for secondary electronic evidence, and these principles, though evolved under the now-repealed Indian Evidence Act, continue to inform the operation of the *Bharatiya Sakshya Adhiniyam, 2023* (BSA). In *Anvar P.V. v. P.K. Basheer* (2014), the Supreme Court departed from earlier leniency on production of electronic evidence, holding that primary evidence in electronic form must either be produced in its original device or, if adduced as secondary evidence, be accompanied by the statutory certificate under Section 65B (4) of the 1872 Act[17]. The Court clarified that oral evidence or mere production of print-outs without certification would not suffice a principle now squarely mapped onto Section 63(4) of the BSA. This insistence on procedural compliance was reinforced in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), where a larger bench affirmed that the certificate requirement is *mandatory*, save where the party has no lawful means to obtain it, in which case the Court may permit alternative proof[18]. Although decided in the context of the predecessor legislation, the reasoning applies directly under the BSA, given the functional equivalence of the provisions.

More recently, in *Vijay v. Union of India* (2023), the Supreme Court addressed the *burden and standard of proof* in relation to electronic evidence. The Court reiterated that the party relying on an electronic record must first establish its admissibility by fulfilling the statutory prerequisites including the certificate under Section 63(4) before its probative value can be assessed[19]. It further observed that where the genuineness of an electronic record is challenged, the standard of proof remains that of a prudent judicial mind satisfied on the balance of probabilities in civil matters and beyond reasonable doubt in criminal trials[20]. These judgments collectively anchor the interpretive approach under the BSA: certification operates as a gateway, expert evidence under Section 39(2) can assist in technical authentication, and judicial discretion is preserved only in narrowly-defined exceptional circumstances. The resulting jurisprudence underscores that compliance with procedural formalities is not a mere technicality but an essential evidentiary safeguard in an era where manipulation of digital artefacts — whether through metadata alteration, hash spoofing, or synthetic media generation — is increasingly sophisticated.

2.2 Authoritative Reports and Technical Guidelines

1. Law Commission of India — Report No. 185 (2003)[21]
    a) Comprehensive review of the *Indian Evidence Act, 1872*, including detailed analysis of Section 65B on electronic record.
    b) Recommended retention of certification requirements to safeguard authenticity and reliability.
    c) Advocated expert assistance in technologically complex matters — a principle echoed in the *Bharatiya Sakshya Adhiniyam, 2023* (BSA).
    d) Core themes of authenticity, reliability, and procedural safeguards remain directly applicable to BSA interpretation.

---

[11] Bharatiya Sakshya Adhiniyam 2023, s 58.
[12] BSA 2023, s 63(4); cf. Indian Evidence Act 1872, s 65B (4) (repealed).
[13] BSA 2023, s 39(2).
[14] Information Technology Act 2000, s 2(1)(t).
[15] IT Act 2000, ss 66C–66D.
[16] IT Act 2000, s 67B.
[17] *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473.
[18] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
[19] *Vijay v Union of India* 2023 SCC OnLine SC 125.
[20] ibid [42] – [45].
[21] Law Commission of India, *185th Report on Review of the Indian Evidence Act, 1872* (2003) paras 5.16–5.22.

2. Ministry of Electronics and Information Technology (MeitY) — Digital Forensic Methodologies Guidelines[22]
    a) Provides SOPs for the identification, acquisition, preservation, analysis, and documentation of electronic evidence.
    b) Stresses maintaining chain of custody, generation of hash values, and admissibility-ready record-keeping.
    c) Though non-binding, frequently relied upon in investigative and prosecutorial contexts as a benchmark for forensic integrity.

2.3 Key Issues

1. Statutory Silence on Deepfakes and AI-Generated Outputs[23]
    a) Neither the BSA nor the IT Act defines *synthetic media* or specifically regulates AI-created evidence.
    b) Courts currently address such material via analogy to forgery or falsification offences, coupled with expert testimony.
    c) This gap generates interpretive uncertainty in admissibility and weight of evidence.
2. Certification Challenges for Decentralised/Foreign Cloud Sources[24]
    a) BSA-compliant certification often unattainable when data resides on decentralised or foreign-controlled servers.
    b) Overseas service providers may fall outside Indian legal process, producing evidentiary lacunae.
    c) Persistent problem noted in case law, indicating a need for legislative or treaty-based intervention.

III. ADMISSIBILITY IN THE AGE OF DEEPFAKES, CLOUD FORENSICS, AND AI EVIDENCE

The contemporary evidentiary framework faces unprecedented stress from the simultaneous rise of *synthetic media*, *globally distributed cloud storage*, and *autonomously generated content*. The *Bharatiya Sakshya Adhiniyam* ("BSA") provides a technologically neutral definition of "document" and "electronic record" but lacks explicit provisions addressing these emergent formats, compelling courts to interpret existing rules purposively to uphold procedural fairness and accuracy in fact-finding.

3.1 Deepfake Challenges

Despite the socio-legal urgency, neither the BSA nor the ITA articulates an explicit statutory definition of "deepfake" or "synthetic media". Current reliance is on general offences of forgery, fraud, and misrepresentation under the BNS (ss 336–341) and the ITA's penal provisions (ss 66D–66E)[25]. From a procedural justice perspective, the absence of definitional clarity risks inconsistent admissibility determinations, particularly when defence counsel challenges the *reliability threshold* under s 136 BSA. Authentication demands sophisticated forensic examination. Expert testimony now frequently involves AI forensic analysis—detecting generative adversarial network (GAN) artefacts, inconsistencies in eye-blinking patterns, micro-expression anomalies, and irregular compression signatures[26]. Such evidence must meet both the relevance requirement (s 4 BSA) and the balancing test for unfair prejudice, with the judge's gatekeeping role ensuring that fabricated yet technically impressive exhibits do not mislead the trier of fact.

3.2 Cloud Forensics

The increasing use of foreign-hosted cloud services for personal, corporate, and governmental data storage generates profound jurisdictional complexity. Section 75 ITA provides for extra-territorial application, yet in practice, compelling disclosure from non-treaty jurisdictions often depends on *de facto* negotiation or diplomatic channels, rather than enforceable judicial writs[27].
From an evidentiary chain-of-custody standpoint, cloud-stored data challenges the procedural requirement under s 63(2) BSA and s 65B ITA to demonstrate integrity from the moment of collection. Issues include multi-node replication, elastic storage re-allocation, and automated retention-policy deletions. Maintaining procedural fairness therefore requires forensically sound acquisition-imaging data in situ, securing contemporaneous hash validations, and documenting each transfer or extraction step in an audit-compliant log[28].

3.3 AI-Generated Evidence

AI-produced evidence occupies a liminal legal space between expert-assisted demonstratives and autonomous fabrications. The former such as algorithmic accident reconstructions or predictive crime-mapping outputs prepared under judicial or investigative mandate may assist fact-finding if their underlying models are transparent, datasets are validated, and methodology satisfies scientific reliability tests.

By contrast, manipulative falsifications intentionally distort the factual record. Here, the "liar's dividend" phenomenon[29] compounds the challenge: litigants may claim genuine footage or recordings are "AI-generated" to manufacture reasonable doubt. Procedural justice demands that courts develop provenance verification standards disclosing metadata lineage, AI model specifications, and, where possible, the cryptographic signing of outputs at source to distinguish lawful reconstructions from deceptive forgeries.

---

[22] Ministry of Electronics & Information Technology, *Guidelines for Digital Evidence Examination and Forensic Methodologies* (2022) <https://www.meity.gov.in> accessed 02 August 2025.
[23] Information Technology Act 2000, ss 66C–66E; Bharatiya Nyaya Sanhita 2023, ch XVIII.
[24] P Kumar, 'E-Evidence and Cloud Jurisdiction' (2022) 14(1) *Indian Journal of Law & Technology* 77, 84–85.
[25] Bharatiya Nyaya Sanhita 2023, ss 336–341; Information Technology Act 2000, ss 66D–66E.
[26] *Guidelines for Examination of Digital Evidence* (2022).
[27] *State of Karnataka v M R Hiremath* (2019) 7 SCC 515.
[28] Information Technology Act 2000, s 65B; Bharatiya Sakshya Adhiniyam 2023, s 63(2).
[29] Danielle K Citron and Robert Chesney, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 Cal L Rev 1753.

3.4 Forensic Tools and Methodologies

Judicial assessment of admissibility in such cases increasingly leverages technical integrity tools, including:

- Cryptographic hashing - SHA-256 as the preferred algorithm, with MD5 used only alongside corroborative checks given its vulnerability to collisions;[30]
- Metadata analysis (e.g., EXIF timestamps, camera serial identifiers, and modification logs) to corroborate asserted timelines;
- Blockchain-based evidence sealing—anchoring a hash of the artefact in a distributed ledger to provide immutable proof of unaltered state from the moment of sealing;[31]
- AI-assisted detection suites employing multi-modal analytics (visual, acoustic, and linguistic channels) to identify patterns characteristic of synthetic generation.

From a statutory interpretation viewpoint, the BSA's technologically neutral language accommodates such tools, but expert admissibility remains subject to the court's satisfaction that the methodology has demonstrable reliability and that the audit trail is unbroken.[32]

3.5 Doctrinal and Policy Considerations

The doctrinal trajectory points toward purposive construction of existing evidentiary provisions, adapting them to technological realities without undermining the principles of natural justice. Legislative intervention may still be warranted—either to define emerging categories such as deepfakes or to codify minimum technical standards for admissibility.

Policy measures could include:

- Judicial capacity-building through specialist training in digital forensics;
- Establishment of nationally accredited forensic laboratories capable of verifying AI-linked evidence;
- Integration of provenance tracking protocols into law-enforcement evidence-handling SOPs;
- Strengthening cross-border mutual legal assistance frameworks for timely access to cloud-stored data.

Such steps would align evidentiary law with both the right to a fair trial and the constitutional mandate for procedural due process, ensuring that technological sophistication enhances rather than erodes the justice system.

IV. ADMISSIBILITY PROCEDURE IN THE USA FOR SECONDARY ELECTRONIC EVIDENCE

The United States employs a flexible, process-driven evidentiary framework for the authentication and admission of secondary electronic records, principally governed by the *Federal Rules of Evidence* ("FRE"). The FRE's technologically neutral drafting permits adaptation to evolving data formats, including cloud-stored logs, AI-generated files, and social-media-based material, without necessitating statutory overhaul.

4.1 Statutory Framework

Rule 901(a) FRE sets the baseline: evidence must be authenticated by "*evidence sufficient to support a finding that the item is what the proponent claims it is*"[33]. This is an illustrative standard rather than a closed list, with Rule 901(b) enumerating non-exhaustive methods, such as witness testimony with direct knowledge (901(b)(1)), comparison by an expert (901(b)(3)), distinctive characteristics and contextual cues (901(b)(4)), and authentication via description of process or system (901(b)(9))[34].

The 2017 amendments introduced Rules 902(13) and 902(14) to address efficiency in admitting machine-generated records. Rule 902(13) provides for self-authentication of records generated by an electronic process or system that produces an accurate result, upon presentation of a certification by a qualified person. Rule 902(14) extends this to data copied from electronic devices, storage media, or files, if authenticated by a digital identification process. These provisions significantly reduce the need for live testimony when the integrity of the process or copy is not seriously disputed, streamlining admissibility without sacrificing reliability safeguards[35].

4.2 Key Precedents

In *United States v Jackson* (2000), the Seventh Circuit declined to admit web-based materials allegedly authored by a gang member because the proponent failed to prove authorship or authenticity emphasising that online content is inherently susceptible to alteration and impersonation[36]. The case underscores the FRE's insistence on corroborating indicia before admitting secondary digital evidence.

United States v Bansal (2011) involved evidence from the Internet Archive's "Wayback Machine." The Third Circuit accepted archived web pages after testimony from an Archive official described the technical process and reliability controls, satisfying Rule 901(b)(1) and (b)(9)[37]. This demonstrates judicial willingness to accept expert-authenticated process evidence for large-scale, automated archives.

In *Tienda v State* (2012), the Texas Court of Criminal Appeals upheld admission of social media profiles allegedly belonging to the accused. The Court relied on contextual evidence — such as photographs, music playlists, and messages containing unique

---

[30] NIST, *Secure Hash Standard* (FIPS 180-4, 2015).
[31] European Union Agency for Cybersecurity (ENISA), *Blockchain and Digital Evidence* (2021).
[32] *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801.

[33] Federal Rules of Evidence, Rule 901(a).
[34] ibid, Rule 901(b).
[35] Federal Rules of Evidence, Rules 902(13) and 902(14) (added 2017).
[36] *United States v Jackson* 208 F 3d 633 (7th Cir 2000).
[37] *United States v Bansal* 663 F 3d 634 (3d Cir 2011).

personal details — to authenticate the material under Rule 901(b)(4)[38]. This ruling shows that circumstantial linkage can suffice, illustrating the FRE's flexible, content-based approach to authentication.

4.3 Procedural Distinctions and Judicial Discretion

Three salient procedural distinctions emerge when comparing the FRE with India's BSA 2023 s 63(4) regimes:

1. **Absence of Mandatory Certification**: The FRE does not impose a universal, formal certification requirement as a *sine qua non* for electronic evidence. Certification is one permissible route, particularly under Rules 902(13) and (14), but not the exclusive method[39].
2. **Multiplicity of Proof Methods**: FRE Rule 901's non-exhaustive methods allow authentication via direct witness testimony, expert opinion, circumstantial evidence, or process verification, depending on the nature of the dispute and the record in question. This accommodates rapidly evolving technologies that may render prescriptive formalities obsolete.
3. **Role of Judicial Discretion**: Under Rule 104(a), the judge decides preliminary questions about admissibility — including whether there is enough foundation for authentication — applying a preponderance of the evidence standard. Under Rule 104(b), when relevance depends on a fact, the court admits the evidence conditionally, leaving the fact-determination to the jury once a prima facie link is shown[40]. This division of responsibility aligns with adversarial fairness: judicial screening ensures baseline reliability, while the trier of fact assesses weight and credibility.

4.4 Relevance to Procedural Justice and Comparative Reform

The US model illustrates how procedural flexibility can coexist with robust evidentiary safeguards. By permitting diverse authentication methods and reserving rigid certification only for defined contexts, the FRE minimises exclusion of probative material due to purely procedural defaults — a recurrent issue in India under strict application of s 63(4) BSA. At the same time, the US framework relies heavily on cross-examination, expert scrutiny, and fact-finder evaluation to safeguard against manipulation, echoing the values of transparency and accountability central to procedural justice.

For Indian reform discussions, the FRE's adaptive design offers a template for calibrated relaxation: introducing alternative authentication routes for cases where formal certificates are unattainable, especially in relation to foreign-hosted data or emergent AI-generated content. Such adaptations could be legislated without abandoning the evidentiary discipline that certification presently enforces.

V. LEGAL PROPOSALS

5.1 For India under the Bharatiya Sakshya Adhiniyam

- **Define synthetic media across statutes:** Insert a cross-referenced definition in BSA harmonised with the Information Technology Act (ITA) and Bharatiya Nyaya Sanhita (BNS). Drafting suggestion: "Synthetic media means audio, visual, or audiovisual content generated or materially altered using computational techniques, including machine learning or generative models, such that it purports to depict persons, speech, or events that did not occur as represented; and includes deepfakes, voice cloning, and AI-generated text-to-image/video, whether wholly synthetic or composited with authentic content." The definition should be tethered to existing ITA terms (computer resource, data, information) and BNS offences on electronic records/forgery to ensure doctrinal coherence and downstream enforcement[41].
- **Presumptive admissibility for accredited forensic outputs:** Create a rebuttable presumption of authenticity and integrity for outputs (hash values, verification logs, AI-manipulation detection reports) produced by labs/tools accredited by a notified authority (e.g., NFSU-led scheme aligned to ISO/IEC 27037/27043). The presumption should be conditional on: Tool versioning and validation records; Reproducible methodology; Audit-ready chain-of-custody; Disclosure of known error rates. This reduces live-testimony burdens without insulating bad methods from challenge[42].
- **Alternative authentication when BSA s 63(4) is impracticable:** Codify a safety valve where the certificate is not reasonably obtainable with due diligence (foreign custodians, defunct platforms, or urgent risk of loss). Permit authentication via: Hash-matching against known-good images; Process-or-system description by a qualified person; Distinctive characteristics and corroborative circumstantial links; — Independent service-metadata or business records. This mirrors FRE 901's plurality of methods and avoids exclusion of probative evidence purely for formal defects[43].
- **Structured notice-and-challenge procedure:** Require the proponent to serve a disclosure pack (hashes, tool logs, process description) 14 days before tender. The opponent must articulate specific, testable objections (method, integrity, identity). Courts decide preliminary admissibility on a preponderance standard; residual disputes go to weight. This channels adversarial scrutiny to reliability rather than paperwork[44].
- **Capacity building on AI forensics:** Establish judicial colloquia and prosecution-defence joint trainings on: AI-manipulation typologies and detection limits; Error-rate literacy and overfitting risks; Reading and cross-examining forensic reports; Preservation and triage of volatile cloud artefacts. Integrate bench books and model orders for consistent practice[45].
- **Cloud-era cooperation instruments:** Negotiate MLAT addenda and executive agreements with major data-hosting jurisdictions for expedited preservation and disclosure, aligned with privacy safeguards. Provide statutory hooks for direct

[38] *Tienda v State* 358 SW 3d 633 (Tex Crim App 2012).
[39] ibid Rules 902(13) – (14).
[40] Federal Rules of Evidence, Rules 104(a) and 104(b).

[41] Bharatiya Sakshya Adhiniyam 2023; Information Technology Act 2000; Bharatiya Nyaya Sanhita 2023.
[42] ISO/IEC 27037:2012; ISO/IEC 27043:2015; National Forensic Sciences University accreditation initiatives.
[43] Federal Rules of Evidence rr 901, 902(13) – (14).
[44] Federal Rules of Evidence r 104; analogous notice periods in r 902 practice.
[45] Judicial training best-practice frameworks; bench book models for digital evidence.

provider orders where comity permits, and adopt Budapest-style standards on preservation and rapid assistance even pending accession[46].

5.2 For the United States under the Federal Rules of Evidence

- **Standardised protocols for AI-linked evidence:** Promulgate nationally recognised protocols (Judicial Conference/NIST/SWGDE) for authentication of: AI-generated or AI-altered media (model cards, provenance signals, detection reports, error rates); Automated system logs and cloud artefacts (time-sync, hashing, environment capture). Cross-reference with Daubert to anchor admissibility of expert explanations of model behaviour and detection reliability[47].
- **Textual clarification in FRE:** Consider an amendment or Committee Note clarifying that Rules 901(b)(9) and 902(13) – (14) encompass AI-forensic workflows, including detector-tool certifications and cryptographic provenance (e.g., C2PA manifests), to reduce needless live testimony where integrity is uncontested[48].
- **Blockchain-supported chain of custody (optional but encouraged):** Encourage agencies to pilot permissioned-ledger registries for evidence-handling events (ingest, hashing, transfers, access). Treat ledger proofs as business records subject to Rule 803(6), not as per se authenticators; authenticity remains rebuttable via concrete integrity challenges. Pair with conventional logs to avoid single-point failure or vendor lock-in[49].

5.3 Hybrid model for cross-jurisdictional robustness

- **Merge safeguards with flexibility:** Retain BSA's discipline of documentation and accountability but add FRE-style alternative routes when certificates are impracticable or disproportionate. The touchstone becomes demonstrable integrity and identity, not formalism[50].
- **Codify technically validated presumptions with rebuttals:** Create statutory presumptions of authenticity where: Cryptographic hashes match across independent acquisitions; Provenance manifests (e.g., C2PA) verify an unbroken content history; Blockchain or WORM-logged custody shows tamper-evident handling; Accredited AI-detection tools report manipulation likelihood below a notified threshold. Each presumption must be explicitly rebuttable on proof of tool error, compromised workflows, or inconsistent corroboration[51].
- **Provenance-first disclosure and fairness:** Mandate early disclosure of all validation artefacts (hash trees, tool versions, thresholds, calibration sets where feasible) and provide funding for defence experts in indigent cases. Fair access is the predicate for meaningful rebuttal[52].

5.4 Drafting notes and model clauses

- **Synthetic media definition (BSA):** "Synthetic media means audio, visual, or audiovisual content generated or materially altered using computational techniques, including generative or machine-learning systems, depicting or purporting to depict persons, speech, or events in a manner that does not correspond to an actual occurrence, and includes deepfakes, voice cloning, and text-to-image/video outputs." Cross-define by reference to ITA "computer resource," "data," and "information[53]."
- **Alternative authentication clause (BSA):** "Where compliance with subsection 63(4) is impracticable despite due diligence, the Court may admit electronic evidence upon a prima facie showing of authenticity by any reliable means, including cryptographic hashing, process-or-system description by a qualified person, distinctive characteristics with corroboration, or independent business records, without prejudice to weight[54]."
- **Presumption for accredited tools (BSA):** "Outputs produced by a forensic laboratory or tool accredited by a notified authority shall be presumed authentic and accurate, subject to rebuttal by showing specific deficiencies in validation, methodology, or application in the instant case[55]."
- **Provenance notice (FRE/Practice):** "A party intending to rely on AI-forensic outputs or provenance manifests shall provide notice and a certification under Rule 902(13)/ (14) at least 14 days prior to trial, with supporting materials adequate to evaluate reliability[56]."

5.5 Rationale and safeguards

- **Why this set works:** These reforms prevent exclusion of probative material solely for certificate defects, yet raise the bar on technical transparency. Rebuttable presumptions reward validated methods without immunising them from attack. Notice-and-challenge structures move disputes to where they belong: reliability, bias, error rates, and integrity.
- **Guardrails against over-reliance on automation:** Require disclosure of detector limitations, confidence thresholds, and known failure modes; mandate human-in-the-loop review for close-call classifications; and forbid treating any single automated flag as conclusive of authenticity or manipulation.

---

[46] Budapest Convention on Cybercrime (2001); US CLOUD Act (2018); MLAT practice guides.
[47] Daubert v Merrell Dow Pharmaceuticals, Inc 509 US 579 (1993); SWGDE best practices; NIST AI Risk Management Framework 1.0 (2023).
[48] Federal Rules of Evidence rr 901(b)(9), 902(13)–(14) and Advisory Committee Notes.
[49] NISTIR 8202: Blockchain Technology Overview; business-records exception under r 803(6).
[50] Bharatiya Sakshya Adhiniyam 2023 s 63(4); Federal Rules of Evidence r 901.
[51] Coalition for Content Provenance and Authenticity (C2PA) specifications; cryptographic hashing standards (e.g., SHA-256).
[52] Principles of fair trial and equality of arms; publicly funded expert assistance in complex evidence cases.
[53] Information Technology Act 2000 s 2; definitional harmonisation practice.
[54] Comparative models inspired by FRE r 901 and conditional relevance under r 104(b).
[55] Presumption-rebuttal structures in evidence law; accreditation logic under ISO frameworks.
[56] Federal Rules of Evidence rr 902(13)–(14) certification practice.

VI. CONCLUSION

6.1 Findings

The *Bharatiya Sakshya Adhiniyam, 2023* (BSA) is, in substance, a lineal successor to the evidentiary philosophy of the *Indian Evidence Act, 1872*, maintaining the centrality of authenticity, reliability, and procedural safeguards as the gatekeepers for admissibility. Its adoption of a certificate regime under s 63(4) continues the IEA's emphasis on formal validation of electronic records, ensuring that courts are not misled by inauthentic or altered data[57]. However, this static textual model now operates in an environment defined by dynamic and technologically complex threats: the proliferation of deepfakes generated by advanced machine-learning architectures, the evidentiary opacity of AI-manipulated media, and the jurisdictional as well as technical fragility of cloud-based artefacts.

Judicial interpretation under cases such as *Anvar P.V.*, *Arjun Panditrao*, and *Vijay* has fortified the mandatory character of certification, but has also exposed procedural bottlenecks where compliance is practically impossible. In practice, these rigidities risk excluding probative, high-integrity evidence solely for want of a formal document a situation exacerbated in cross-border and decentralised data environments. The absence of statutory recognition for synthetic or AI-generated evidence leaves courts to improvise under general provisions, often without the benefit of uniform forensic or procedural standards. As demonstrated in the comparative analysis, the Federal Rules of Evidence (FRE) in the United States embody a markedly more adaptable approach, permitting multiple authentication pathways and leveraging judicial discretion to admit technically sound evidence while still guarding against unreliability.

6.2 Future Direction

Sustaining evidentiary integrity in this environment will require statutory precision paired with procedural innovation. On the Indian side, this means:

- Incorporating explicit definitions of "synthetic media" harmonised across the BSA, ITA, and BNS;
- Recognising outputs of accredited forensic processes through rebuttable presumptions;
- Allowing alternative, reliability-centred authentication routes when s 63(4) certificates are unattainable; and
- Embedding a notice-and-challenge culture focused on substance rather than form.

For the United States, the next step lies in codifying and standardising AI-evidence protocols, expanding blockchain-anchored chain-of-custody practices, and refining Committee Notes to eliminate residual ambiguity around emerging forensic processes.
In both jurisdictions, the strategic aim should be harmonisation — blending the BSA's procedural discipline with the FRE's evidentiary flexibility to form a technology-integrated, jurisdiction-convergent framework. Such a hybrid model would:

- Secure authenticity through verifiable technical markers (hashing, blockchain sealing, provenance manifests, AI-detection reports);
- Preserve adversarial testing by making all such validations transparent and open to rebuttal; and
- Enhance procedural fairness by preventing exclusion of high-value evidence on grounds of avoidable formal defects.

In doing so, courts across jurisdictions can be equipped to meet the dual imperatives of truth-seeking and due process, ensuring that in the algorithmic age, the evidentiary system remains both resilient to manipulation and faithful to the principles of justice[58].

[57] Bharatiya Sakshya Adhiniyam 2023, s 63(4); Indian Evidence Act 1872 (repealed), s 65B(4); *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473; *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1; *Vijay v Union of India* 2023 SCC OnLine SC 125.

[58] Federal Rules of Evidence rr 901, 902(13)–(14); Council of Europe, *Guidelines on Electronic Evidence in Criminal Proceedings* (2019); Budapest Convention on Cybercrime (2001).