INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

BRIDGING TECHNOLOGY AND LAW: CRYPTOGRAPHIC AUTHENTICATION METHODS UNDER THE BHARATIYA SAKSHYA ADHINIYAM 2023

AUTHORED BY - HARSHWARDHAN YADAV & AAYUSH,
National Law Institute University, Bhopal

INTRODUCTION

The evolution of evidence law in India has witnessed a fundamental transformation from the traditional reliance on physical documents and oral testimony to the growing acceptance of electronic records and digital evidence. This shift reflects the broader technological revolution that has reshaped how information is created, stored, transmitted, and preserved in contemporary society. The Indian Evidence Act, 1872, originally designed for a pre-digital era, provided the foundational framework for evidence evaluation based on tangible documents and direct human testimony. However, the rapid advancement of information technology and the ubiquitous nature of digital transactions have created new challenges that the traditional evidence framework struggled to address effectively.

The transition from physical to electronic evidence represents more than a mere technological upgrade; it signifies a paradigm shift in how courts approach the fundamental questions of authenticity, integrity, and reliability. Traditional documentary evidence could be examined for physical characteristics such as paper quality, ink composition, handwriting patterns, and seal impressions. In contrast, electronic evidence exists as intangible data that can be copied infinitely without degradation, modified without leaving obvious traces, and transmitted across vast distances instantaneously. These unique characteristics of digital evidence necessitated a complete rethinking of established legal principles governing evidence admissibility and authentication.

The challenges in applying traditional evidence law to digital materials became increasingly apparent as courts encountered cases involving email communications, digital photographs, computer files, and electronic transactions. The binary nature of digital data, its susceptibility to manipulation, and the technical complexity of its creation and storage processes posed

ISSN: 2582-6433

unprecedented challenges for legal practitioners and judges.[1] The absence of specific legislative provisions addressing these concerns led to inconsistent judicial interpretations and uncertainty in the admissibility standards for electronic evidence.

The Information Technology Act, 2000, and its subsequent amendments represented the first comprehensive attempt to bridge this gap by introducing specific provisions for electronic records under sections 65A and 65B of the Indian Evidence Act.[2] These amendments recognized the legal validity of electronic records and established basic admissibility criteria, including the requirement for certificates under section 65B(4) to authenticate electronic evidence. However, the implementation of these provisions revealed significant gaps and ambiguities that continued to plague the effective utilization of digital evidence in judicial proceedings.

This research examines three central questions that are crucial for understanding the implications and effectiveness of BSA 2023's approach to digital evidence. Firstly, how does BSA 2023 address cryptographic authentication, and what specific mechanisms does it provide for the acceptance of hash values and metadata. Secondly, what role do hash values play in establishing the authenticity and integrity of digital evidence under the new legal framework? Hash values, also known as digital fingerprints, provide a mathematical method for detecting any alteration to electronic files. Understanding how BSA 2023 incorporates these technical tools into legal procedures is essential for assessing the Act's effectiveness in ensuring evidence reliability while maintaining due process standards. Thirdly, how does the new framework compare with the previous legislative approach, and what improvements does it offer for the practical handling of electronic evidence.

The Need for BSA 2023

The limitations of the Indian Evidence Act, 1872, in addressing contemporary digital evidence challenges became increasingly evident through judicial decisions and practical implementation difficulties. The Supreme Court's landmark judgment in Anvar P.V. v. P.K. Basheer highlighted the mandatory nature of section 65B certificates while simultaneously revealing the practical impossibility of obtaining such certificates in many circumstances.[3]

[1] Casey and Rose, “Handbook of Digital Forensics and Investigation” (Academic Press 2018) 45-67.
[2] Information Technology Act 2000, ss 65A-65B as inserted by Information Technology (Amendment) Act 2008.
[3] Anvar P.V. v P.K. Basheer (2014) 10 SCC 473.

ISSN: 2582-6433

The growing reliance on digital evidence in criminal proceedings further underscored the urgency of legislative reform. Modern criminal investigations increasingly depend on electronic evidence ranging from mobile phone data and internet communications to CCTV footage and GPS tracking information. The existing legal framework's inability to effectively handle such evidence threatened to undermine the entire criminal justice system's capacity to address contemporary crimes, particularly those involving cyber offenses, financial frauds, and organized criminal activities that leave predominantly digital trails.

The Bharatiya Sakshya Adhiniyam, 2023, emerged as a comprehensive response to these challenges, representing a fundamental reconceptualization of evidence law for the digital age. BSA 2023 was designed to address the unique characteristics and requirements of electronic evidence while maintaining the essential principles of evidence evaluation that ensure justice and fairness.

UNDERSTANDING HASH VALUES AND CRYPTOGRAPHIC FUNCTIONS

Hash values represent one of the most fundamental concepts in digital forensics and cryptographic authentication, serving as unique digital fingerprints that can verify the integrity and authenticity of electronic data. A cryptographic hash function is a mathematical algorithm that takes an input of arbitrary length and produces a fixed-length string of characters, known as a hash value or digest.[4] This process is deterministic, meaning that the same input will always produce the same hash value, while even the smallest change to the input data will result in a completely different hash value.

The concept of hash functions can be understood through a simple analogy. Just as every person has unique fingerprints that can be used for identification, every digital file or piece of data can be assigned a unique hash value that serves as its digital fingerprint.

Cryptographic hash functions possess several essential properties that make them suitable for legal authentication purposes. The deterministic property ensures that identical data will always produce identical hash values, providing consistency in verification processes.

The charter of cryptographic hash function to produce avalanche effect represents perhaps the

[4] Menezes, van Oorschot and Vanstone, Handbook of Applied Cryptography (CRC Press 2018) 321-327.

ISSN: 2582-6433

most crucial property for forensic applications. This characteristic ensures that changing even a single bit in the input data will cause approximately half of the bits in the output hash value to change, creating a completely different hash value. This property makes hash values extremely sensitive to any alteration, enabling the detection of even the most minor modifications to electronic evidence.

Digital Fingerprinting Process

The process of creating digital fingerprints through hash value generation involves several carefully controlled steps that ensure the resulting hash values are forensically sound and legally admissible. The initial step requires the creation of an exact bit-for-bit copy of the original digital evidence, typically through forensic imaging techniques that preserve not only the active data but also deleted files, slack space, and other forensically relevant information.[5] During the imaging process, hash values are calculated in real-time to verify the integrity of the copying procedure. This involves calculating hash values for both the source device and the forensic image, ensuring that the two values match exactly. Any discrepancy in hash values would indicate that the imaging process failed to create an accurate copy, necessitating repetition of the procedure.

The hash calculation process itself must be performed using validated software tools that have been tested and verified for accuracy. The integrity verification mechanism relies on the mathematical properties of hash functions to detect any changes to digital evidence. Because hash functions exhibit the avalanche effect, even the smallest alteration to a digital file will result in a completely different hash value. This provides investigators and courts with a reliable method for determining whether electronic evidence has maintained its original state since collection.

Tamper detection capabilities extend beyond simple file modifications to include more sophisticated forms of evidence manipulation. Modern forensic hash verification can detect timestamp manipulation, metadata alteration, and other forms of digital evidence tampering that might not be immediately obvious through visual inspection. This comprehensive approach to integrity verification provides courts with confidence in the reliability of digital evidence presented for consideration.

[5] Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd edn, Academic Press 2019) 123-145.

ISSN: 2582-6433

Metadata in Digital Evidence

Metadata represents the hidden information layer that accompanies digital files and electronic communications, providing crucial context and authentication information that may not be visible to typical users but is essential for forensic analysis and legal authentication. The term metadata literally means "data about data," encompassing all the additional information that computer systems automatically generate and store alongside the primary content of digital files.[6]

System-generated metadata includes information automatically created by computer systems during file creation, modification, and access operations. This category encompasses file timestamps indicating when files were created, last modified, and last accessed; file size information; file format specifications, etc. User-generated metadata includes information that users deliberately or inadvertently include in digital files through their interactions with software applications. Document metadata in word processing files may include author names, revision histories, comments, and tracked changes.

Timestamps constitute one of the most forensically significant categories of metadata, providing temporal information that can establish timelines and sequences of events crucial for legal proceedings. Most file systems maintain multiple timestamp categories: creation time, last modification time, and last access time. Location data embedded in metadata has become increasingly important as mobile devices and location-aware applications generate geographic information that can establish the physical location where digital evidence was created or accessed.

Forensic Significance

The forensic significance of metadata extends far beyond its technical characteristics to encompass its fundamental role in establishing the reliability and authenticity of digital evidence. Metadata provides the contextual framework that allows forensic examiners and courts to understand not just what digital evidence contains, but how it was created, when it was modified, and what systems were involved in its lifecycle.[7]

[6] Casey and Rose, Handbook of Digital Forensics and Investigation (Academic Press 2018) 156-162.
[7] Scientific Working Group on Digital Evidence, Model Standard Operating Procedures for Computer Forensics (SWGDE 2019) 12-18.

ISSN: 2582-6433

Chain of custody establishment represents one of the most critical forensic applications of metadata. Traditional chain of custody documentation relies on human records and physical handling procedures, but digital evidence requires additional technical verification to demonstrate that electronic files have not been altered during collection, storage, and analysis processes. Metadata provides objective technical information that can corroborate human testimony and documentation, creating a more robust chain of custody framework.[8]

LEGISLATIVE EVOLUTION: FROM IEA 1872 TO BSA 2023

The Act initially focused primarily on electronic transactions and digital signatures, but subsequent amendments in 2008 introduced specific provisions for electronic evidence through the insertion of sections 65A and 65B into the Indian Evidence Act, 1872.

Section 65A provided a broad definition of electronic records, encompassing any information generated, sent, received, or stored in any electronic form. This definition was intentionally comprehensive, covering not only traditional computer files but also data stored on mobile devices, digital cameras, GPS systems, and other electronic devices that had become common sources of evidence in legal proceedings. The broad definitional approach reflected recognition that electronic evidence could originate from virtually any digital device or system.

Section 65B established the fundamental principle that electronic records would be admissible as evidence if they satisfied specific conditions designed to ensure their reliability and authenticity. The section required that electronic records be produced from computers that were operating properly during the relevant period, that the information was regularly fed into the computer in the ordinary course of activities, and that the computer was operating properly throughout the relevant period.

The certificate requirements under section 65B(4) represented the most significant innovation and, ultimately, the most problematic aspect of the electronic evidence framework. The provision required a certificate signed by a person in charge of computer operations, identifying the electronic record and describing the manner of its production, the computer system involved, and confirming that the computer was operating properly during the relevant period.[9] These certificate requirements were designed to provide courts with reliable human testimony

[8] National Institute of Justice, Electronic Evidence: Technology and Policy (NIJ 2020) 89-95.
[9] Karnik, 'Electronic Evidence and the Indian Evidence Act' (2009) 3 Digital Investigation 16, 19-22.

ISSN: 2582-6433

about the technical circumstances surrounding electronic evidence creation and preservation. The certificates served as a bridge between technical systems and legal requirements, translating complex technical processes into familiar legal concepts that courts could evaluate using traditional evidence principles.

Judicial Response and Interpretation

The Supreme Court's interpretation of sections 65A and 65B evolved significantly over time, reflecting the judiciary's growing understanding of electronic evidence complexities and the practical challenges of implementing the statutory framework.

The landmark decision in *Anvar P.V. v. P.K. Basheer* established the mandatory nature of section 65B certificates for electronic evidence admissibility. The Court held that electronic evidence could only be admitted under section 65B and that the certificate requirements were mandatory rather than directory.[10] This decision provided much-needed clarity about the legal requirements for electronic evidence but also created significant practical challenges for evidence admission.

In many situations, the person in charge of computer operations was unavailable, unwilling to provide certificates, or technically incompetent to understand the requirements. This was particularly problematic in cases involving evidence from third-party systems, public networks, or foreign servers where certificate acquisition was practically impossible.

Conflicting High Court judgments emerged as different courts struggled to balance the mandatory requirements established in *Anvar* with practical necessities of modern litigation. Some courts strictly enforced the certificate requirements, excluding valuable electronic evidence when proper certificates were not available. Other courts attempted to find exceptions or alternative authentication methods, creating additional uncertainty about electronic evidence standards.

The Supreme Court's subsequent decision in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* attempted to address some of the practical difficulties by recognizing limited exceptions to certificate requirements, particularly in cases involving evidence from social

[10] Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473, para 24-26.

ISSN: 2582-6433

media platforms and other third-party systems. However, these exceptions created additional complexity rather than resolving the fundamental problems with the certification framework.[11]

Key Provisions Related to Electronic Evidence

The Bharatiya Sakshya Adhiniyam, 2023, represents a fundamental reconceptualization of electronic evidence law, moving away from the certificate-centric approach of sections 65A and 65B toward a more flexible and technically informed framework. The Act's approach reflects lessons learned from two decades of experience with electronic evidence and incorporates advances in digital forensics and cryptographic authentication methods.

Section 61 of BSA 2023 establishes the general principle that electronic or digital records are admissible in evidence if they are relevant to the matter in issue. This provision eliminates the artificial distinction between electronic and traditional evidence, treating digital records as simply another category of documentary evidence subject to the same fundamental relevance and reliability standards.[12]

Section 63 provides specific procedures for electronic evidence authentication, incorporating explicit recognition of cryptographic hash values and digital forensics methods. The provision allows for authentication through various technical methods, including hash value verification, metadata analysis, and other scientifically recognized digital forensics techniques.[13]

The Act's recognition of hash values as a primary authentication method represents a significant advancement in legal understanding of digital forensics principles. Hash values are explicitly recognized as reliable indicators of electronic record integrity, provided they are calculated using recognized cryptographic algorithms and proper forensic procedures. This technical recognition eliminates much of the uncertainty that plagued earlier electronic evidence frameworks.

Enhanced technical recognition extends beyond hash values to encompass comprehensive digital forensics methodologies. The Act recognizes that electronic evidence authentication may require specialized technical analysis and provides courts with authority to consider

[11] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1, para 32-35.
[12] Bharatiya Sakshya Adhiniyam 2023, s 61.
[13] ibid s 63.

ISSN: 2582-6433

technical evidence and expert testimony in evaluating electronic records.

STATUTORY TEXT AND INTERPRETATION OF SECTION 63

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, represents the cornerstone provision for electronic evidence admissibility in the modern Indian legal framework. The section's structure reflects a sophisticated understanding of digital forensics principles while maintaining coherence with fundamental evidence law concepts. A systematic examination of each sub-section reveals the legislature's intent to create a comprehensive yet flexible framework for electronic evidence evaluation.

Sub-section (1) establishes the fundamental admissibility principle for electronic records, stating that any information contained in an electronic record which is printed on paper, stored, recorded, or copied in optical or magnetic media produced by a computer shall be deemed to be a document. This provision eliminates the artificial distinction between electronic and physical evidence that created confusion under the previous framework. The use of the term "deemed to be a document" ensures that electronic records receive the same legal treatment as traditional documentary evidence, subject to the same standards of relevance and reliability.
The phrase "produced by a computer" in sub-section (1) has been deliberately crafted to encompass the broad range of electronic devices and systems that generate digital evidence in contemporary investigations. This includes not only traditional computers but also mobile phones, digital cameras, GPS devices, network routers, and any other electronic system capable of creating, processing, or storing digital information.[14] The comprehensive approach avoids the technical limitations that might arise from narrow definitions tied to specific technologies.
Sub-section (2) introduces the critical authentication requirements that distinguish BSA 2023 from its predecessors. The provision states that electronic records shall be admissible if the court is satisfied about their integrity and authenticity. This formulation places primary emphasis on the substantive reliability of electronic evidence rather than procedural compliance with rigid requirements. The court's satisfaction becomes the central criterion, allowing judicial discretion while maintaining appropriate standards for evidence evaluation.

The integrity requirement in sub-section (2) addresses the fundamental concern about whether electronic records have been altered or corrupted since their creation. This concept aligns

[14] Ministry of Law and Justice, Explanatory Notes on Bharatiya Sakshya Adhiniyam 2023 (2023) 67-72.

ISSN: 2582-6433

directly with the technical capabilities of cryptographic hash functions, which can detect any modification to digital data through mathematical verification. The statutory recognition of integrity as a distinct requirement acknowledges that electronic evidence poses unique challenges related to data modification that require specific technical solutions.

Authenticity requirements encompass the broader question of whether electronic records genuinely originate from their claimed sources and accurately represent the events or communications they purport to document. This requirement addresses concerns about evidence fabrication, misattribution, and other forms of fraud that might affect electronic evidence reliability.[15] The combination of integrity and authenticity requirements creates a comprehensive framework for evaluating electronic evidence reliability.

Sub-section (3) provides specific methods for establishing integrity and authenticity, explicitly recognizing cryptographic hash values as acceptable authentication evidence. The provision states that integrity may be proved through hash values computed using recognized algorithms, while authenticity may be established through metadata analysis, digital signatures, or other technical verification methods. This explicit recognition of technical authentication methods represents a significant advancement over the previous framework's reliance on human certification.

HASH VALUE AUTHENTICATION MECHANISM

BSA 2023's explicit recognition of cryptographic hash values represents a landmark development in Indian evidence law, providing statutory authority for technical authentication methods that were previously accepted only through judicial interpretation and expert testimony. Section 63(3)(a) specifically states that the integrity of electronic records may be proved by producing evidence that a hash value computed from such electronic record using a recognized algorithm has remained unchanged.

The phrase "recognized algorithm" in the statutory text provides important flexibility while maintaining technical standards. The provision does not specify particular algorithms, allowing for adaptation as technology evolves and new security requirements emerge. However, the reference to "recognized" algorithms implies acceptance of established technical standards and

[15] Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd edn, Academic Press 2019) 189-203.

ISSN: 2582-6433

professional consensus about algorithm reliability.[16] This approach avoids the risk of statutory provisions becoming obsolete as technology advances.

The requirement that hash values must remain "unchanged" establishes the technical standard for integrity verification. This language acknowledges that hash values serve as unique digital fingerprints that will change if the underlying data is modified in any way.[17]

Metadata Handling

Section 63 of BSA 2023 extends beyond hash value authentication to encompass comprehensive metadata handling provisions that recognize the evidentiary value of information about digital files and electronic communications. Sub-section (3)(b) specifically addresses metadata authentication, stating that authenticity of electronic records may be proved by evidence of metadata integrity and consistency with claimed origins.

The statutory recognition of metadata as authentication evidence reflects understanding that digital files contain multiple layers of information that can provide independent verification of authenticity claims. Unlike hash values that primarily address integrity concerns, metadata analysis can establish the source, timing, and circumstances of electronic evidence creation.[18] This dual approach of hash values for integrity and metadata for authenticity provides comprehensive technical authentication capabilities.

Admissibility Criteria

The admissibility criteria for metadata authentication under BSA 2023 require that courts evaluate both the technical reliability of metadata analysis procedures and the relevance of metadata information to the legal issues in dispute. This dual evaluation ensures that metadata evidence meets both technical standards for reliability and legal standards for relevance and probative value.

The balancing test for metadata admissibility requires courts to weigh the probative value of metadata evidence against potential prejudicial effects, confusion, or misleading impressions

[16] Indian Computer Emergency Response Team, Guidelines for Cryptographic Algorithms and Key Sizes (CERT-In 2022) 23-27.
[17] Ferguson, Schneier and Kohno, Cryptography Engineering: Design Principles and Practical Applications (Wiley 2019) 203-208.
[18] Casey and Rose, Handbook of Digital Forensics and Investigation (Academic Press 2018) 298-314.

ISSN: 2582-6433

that might result from technical complexity. Courts must ensure that metadata evidence enhances rather than obscures the fact-finding process while maintaining appropriate standards for evidence evaluation.[19]

The integration of metadata authentication with other forms of evidence evaluation allows courts to consider metadata information alongside traditional evidence types in reaching factual determinations. This holistic approach recognizes that electronic evidence authentication may involve multiple technical and non-technical elements that must be evaluated collectively rather than in isolation.

The practical application of metadata authentication standards requires coordination between legal practitioners, technical experts, and judicial personnel to ensure effective implementation. This includes training programs for judges and lawyers, standardization of technical procedures, and development of court practices that accommodate the technical requirements of metadata authentication while maintaining efficient legal proceedings.

JUDICIAL ACCEPTANCE AND CASE LAW ANALYSIS

Supreme Court Precedents

The Supreme Court's approach to electronic evidence prior to BSA 2023 was characterized by cautious acceptance coupled with strict procedural requirements that often create practical barriers to evidence admission. The Court's evolving jurisprudence reflected genuine concerns about the reliability and authenticity of digital evidence while simultaneously recognizing the inevitability of electronic evidence in modern legal proceedings.

The landmark decision in *Anvar P.V. v. P.K. Basheer* fundamentally reshaped the landscape of electronic evidence law by establishing the mandatory nature of section 65B certificates. The Court held that electronic evidence was admissible only under section 65B of the Indian Evidence Act, and that the certificate requirements under sub-section (4) were mandatory rather than directory.[20] This decision provided much-needed clarity about the legal requirements for electronic evidence but created significant practical difficulties for parties seeking to introduce digital evidence.

[19] Daubert v. Merrell Dow Pharmaceuticals Inc. 509 US 579 (1993).
[20] Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473, para 20.

ISSN: 2582-6433

The Court's reasoning in *Anvar* emphasized the special nature of electronic evidence and the need for additional safeguards to ensure reliability. The judgment recognized that electronic evidence could be easily manipulated and that traditional authentication methods were inadequate for establishing the integrity of digital files. However, the Court's solution of mandatory certificates proved to be more problematic than the problems it sought to address.

The Supreme Court's decision in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* attempted to address some of the practical difficulties created by the *Anvar* decision by recognizing limited exceptions to the certificate requirement. The Court acknowledged that obtaining certificates might be impossible in certain circumstances, particularly involving evidence from social media platforms and other third-party systems.[21] However, the exceptions created additional complexity rather than providing comprehensive solutions to the underlying problems.

In *Shafhi Mohammad v. State of Himachal Pradesh*, the Supreme Court grappled with the application of section 65B requirements to evidence obtained during criminal investigations. The Court recognized that the certificate requirements could effectively prevent the admission of crucial evidence in criminal cases, but struggled to provide workable solutions that maintained evidence reliability while ensuring practical enforceability.[22] The decision highlighted the tension between technical requirements and justice administration needs.

The Court's jurisprudence during this period also addressed the relationship between section 65B and other evidence provisions, particularly the general admissibility principles under sections 59 and 65 of the Indian Evidence Act. The Court established that section 65B was a complete code for electronic evidence, excluding the application of other evidence provisions to digital records. This approach provided clarity but eliminated flexibility that might have allowed courts to address practical implementation challenges.

Judicial attitudes toward technical authentication methods during the pre-BSA period showed limited understanding of digital forensics capabilities and reluctance to accept technical evidence without human corroboration. Courts frequently demanded detailed explanations of technical procedures and insisted on human testimony to validate technical authentication

[21] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1, para 29-33.
[22] Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801, para 18-22.

ISSN: 2582-6433

claims. This approach reflected unfamiliarity with digital forensics rather than any inherent limitations in technical authentication methods.

High Court Variations

The implementation of Supreme Court precedents by various High Courts revealed significant variations in judicial attitudes toward electronic evidence and interpretation of section 65B requirements. These variations created uncertainty for legal practitioners and demonstrated the practical difficulties of applying rigid procedural requirements to diverse electronic evidence scenarios.

The variations in High Court approaches created significant uncertainty for legal practitioners about electronic evidence requirements. The same type of evidence might be admitted in one jurisdiction while being rejected in another, undermining consistency and predictability in legal proceedings. This uncertainty was particularly problematic in cases involving multi-jurisdictional elements or appeals between different High Courts.

The judicial uncertainty surrounding electronic evidence had profound effects on legal practice, investigation procedures, and case preparation strategies. Criminal investigators struggled to collect and preserve electronic evidence in ways that would satisfy uncertain and varying judicial requirements.[23] This uncertainty often led to either over-collection of evidence in attempts to satisfy all possible requirements or under-utilization of valuable electronic evidence due to concerns about admissibility.

Legal education and professional training struggled to keep pace with evolving electronic evidence requirements. Law schools and continuing education programs lacked clear guidance about electronic evidence standards, making it difficult to prepare legal professionals for effective practice in digital evidence matters. This knowledge gap contributed to inconsistent approaches to electronic evidence handling and presentation.

BSA 2023 IMPLEMENTATION

The Bharatiya Sakshya Adhiniyam 2023 represents a transformative shift in India's approach to electronic evidence, fundamentally altering the legal status of digital records through its

[23] Central Bureau of Investigation, Challenges in Electronic Evidence Collection (CBI 2019) 45-52.

ISSN: 2582-6433

comprehensive framework. The BSA's revolutionary approach eliminates the historical discrimination against electronic evidence by elevating it to "primary evidence" status under Sections 57 and 61. Section 57 defines primary evidence as "the document itself produced for the inspection of the Court," thereby ensuring that electronic records under Section 61 are not rendered inadmissible merely by virtue of their digital format. This paradigmatic change removes the default assumption that digital evidence constitutes secondary proof, recognizing that properly authenticated electronic records carry equivalent probative weight to traditional tangible documents.

The BSA introduces a sophisticated two-tiered certification framework under Section 63(4) that requires validation from both the device operator and a qualified expert. This dual authentication system reflects the legislature's recognition that electronic evidence requires specialized technical knowledge for proper evaluation. The Supreme Court's interpretation in State of Himachal Pradesh v. Jai Lal defines an expert as an individual with specialized study or experience in the relevant subject matter, possessing adequate knowledge and skills. Furthermore, Section 79A of the Information Technology Act 2000 empowers the Central Government to designate electronic evidence examiners from governmental departments, providing institutional support for authentication processes while potentially serving as a check against arbitrary admissibility of privately certified evidence.

Despite its theoretical soundness, this dual certification requirement creates significant practical challenges that may undermine rather than enhance the reliability of electronic evidence proceedings. India's Forensic Science Laboratories already face substantial operational constraints, including staff shortages, multiple vacancies, inadequate technical resources, and processing delays that affect criminal investigations and prosecutions. The increased reliance on expert certification, particularly from privately appointed specialists, introduces risks of arbitrariness and undermines the judicial fact-finding function envisioned under the BSA. The absence of statutory standards governing expert qualifications, roles, and certification processes further exacerbates these concerns, potentially creating a system where procedural compliance takes precedence over substantive reliability.

Chain of Custody in Digital Evidence

The implementation of chain of custody procedures for digital evidence under BSA 2023 requires integration of traditional custody documentation with technical verification methods

ISSN: 2582-6433

that can provide objective evidence of evidence integrity throughout the handling process. This integration represents a significant advancement over purely documentary approaches to custody verification.

Hash value generation at collection forms the foundation of technical chain of custody verification. Forensic procedures must calculate and record hash values immediately upon evidence collection, before any analysis or processing procedures that might affect evidence integrity. These initial hash values serve as baseline references that can be used to verify evidence integrity at all subsequent stages of the forensic process.

The technical implementation requires forensic imaging that create exact bit-for-bit copies of original storage devices while preserving all technical characteristics relevant to authentication. Modern forensic imaging tools automatically calculate hash values during the imaging process, providing real-time verification that imaging procedures are creating accurate copies.[24] Any discrepancy in hash values would immediately indicate imaging problems that require correction before proceeding with analysis.

Storage and transmission security procedures must maintain evidence integrity while allowing legitimate access for analysis and legal proceedings. This includes secure storage environments that prevent unauthorized access, encrypted transmission methods that protect evidence during transfer, and access logging systems that record all interactions with digital evidence. Hash value verification at each access point provides objective confirmation that evidence integrity has been maintained.

Verification at presentation involves recalculating hash values immediately before court presentation to confirm that evidence has maintained its integrity throughout the entire forensic process. This final verification step provides courts with current confirmation that the evidence being presented is identical to the evidence originally collected. The verification process can be performed in court if necessary to provide real-time confirmation of evidence integrity.

Access logs must record all interactions with digital evidence, including analysis procedures, copying operations, and verification activities. These logs provide detailed accountability for

[24] National Institute of Justice, Digital Evidence: Standards and Principles (NIJ 2021) 78-85.

ISSN: 2582-6433

evidence handling while supporting hash value verification procedures that can detect unauthorized access or modification.[25] The combination of access logging and hash verification provides comprehensive evidence integrity assurance.

CHALLENGES AND LIMITATIONS

Hash Function Vulnerabilities

The reliance on cryptographic hash functions for electronic evidence authentication under BSA 2023, while representing a significant advancement over previous approaches, introduces specific technical vulnerabilities that must be understood and addressed to maintain the long-term reliability of digital evidence authentication. These vulnerabilities arise from both theoretical cryptographic limitations and practical implementation challenges that could affect the integrity of forensic procedures.

MD5 collision attacks represent the most widely publicized example of hash function vulnerabilities, demonstrating how theoretical cryptographic weaknesses can become practical threats to evidence authentication. The successful collision attacks against MD5, first demonstrated in 2004 and refined in subsequent years, showed that it was possible to create two different files that produce identical MD5 hash values.[26] While these attacks require sophisticated technical knowledge and significant computational resources, their existence undermines confidence in MD5 for forensic authentication purposes.

SHA-1 deprecation concerns have emerged as more recent research has demonstrated practical collision attacks against this algorithm. The 2017 demonstration of a practical SHA-1 collision attack by researchers at Google and CWI Amsterdam showed that SHA-1 could be compromised using achievable computational resources.[27] This development has led to widespread deprecation of SHA-1 in security-critical applications and raises questions about its continued use in forensic authentication.

Implementation Difficulties

Resource constraints in investigation agencies represent one of the most significant practical

[25] Carrier, File System Forensic Analysis (Addison-Wesley Professional 2020) 234-249.
[26] Wang and Yu, 'How to Break MD5 and Other Hash Functions' (2005) Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science 19-35.
[27] Stevens, Bursztein, Karpman, Albertini and Markov, 'The First Collision for Full SHA-1' (2017) Advances in Cryptology - CRYPTO 2017, Lecture Notes in Computer Science 570-596.

ISSN: 2582-6433

challenges to implementing BSA 2023's cryptographic authentication requirements. Many state and local law enforcement agencies lack the technical infrastructure, trained personnel, and financial resources necessary to implement comprehensive digital forensics capabilities.

The digital divide between well-resourced central agencies and under-resourced local agencies creates particular challenges for consistent implementation of technical authentication standards. While agencies such as the Central Bureau of Investigation and state forensic science laboratories may have access to advanced technical capabilities, local investigation units may struggle to meet the same authentication standards.[28]

Technical training requirements for implementing cryptographic authentication procedures extend beyond basic computer literacy to include specialized knowledge of digital forensics, cryptographic principles, and evidence handling procedures. The development of appropriate training programs requires coordination between technical experts, legal professionals, and educational institutions to ensure comprehensive coverage of both technical and legal requirements.

The shortage of qualified technical personnel in many jurisdictions creates bottlenecks in evidence authentication procedures that could delay legal proceedings or compromise authentication quality. The specialized nature of digital forensics requires substantial training and experience to develop competency, making it difficult to rapidly scale up technical capabilities to meet growing demand.

The complexity of technical authentication evidence requires judiciary to understand not only the basic principles of cryptographic authentication but also the limitations and potential vulnerabilities of technical methods. This understanding is essential for proper evaluation of expert testimony, assessment of authentication reliability, and determination of appropriate weight to give technical evidence.[29]

[28] National Crime Records Bureau, Infrastructure Assessment for Electronic Evidence Implementation (NCRB 2023) 89-96.
[29] Supreme Court of India, Guidelines for Technical Evidence Evaluation (2024) paras 12-18.

ISSN: 2582-6433

FUTURE DIRECTIONS AND RECOMMENDATIONS

Judicial Training Programs

Technical competency development for judicial personnel represents one of the most critical requirements for effective BSA 2023 implementation. The integration of Big Data and AI in legal evidence analysis requires judges to develop sophisticated understanding of technical concepts that were not traditionally part of legal education or judicial training.

Comprehensive training programs should address both foundational technical concepts and practical application issues that judges encounter in electronic evidence cases. The training should cover cryptographic principles, digital forensics procedures, and technical authentication methods while maintaining focus on legal application rather than purely technical details.

Investigation Agency Enhancement

Forensic laboratory upgrades represent essential infrastructure improvements for supporting BSA 2023's technical authentication requirements. Many existing forensic facilities lack the equipment and technical capabilities needed for advanced cryptographic authentication procedures, requiring systematic capacity building efforts.

Personnel training initiatives must address both technical skills and legal knowledge, ensuring that forensic analysts understand how their technical work supports legal proceedings. Standardized equipment and procedures would facilitate evidence sharing, expert testimony, and quality assurance while reducing training and maintenance requirements.[30]

Quality assurance mechanisms, including proficiency testing, peer review, and external auditing, would ensure that enhanced forensic capabilities maintain appropriate reliability standards. These quality assurance measures provide essential validation for technical authentication claims presented in legal proceedings.[31]

Emerging Technologies

Blockchain-based evidence chains could provide secure authentication systems, though

[30] Central Forensic Science Laboratory, Equipment Standardization Guidelines (CFSL 2024) 167-174.
[31] National Accreditation Board for Testing and Calibration Laboratories, Forensic Laboratory Accreditation Standards (NABL 2024) 89-96.

ISSN: 2582-6433

ensuring authenticity and integrity of blockchain data remains an urgent problem. Blockchain technology offers potential solutions for creating immutable evidence chains that could enhance the reliability of digital evidence authentication while providing transparent verification mechanisms.

The integration of blockchain authentication with traditional forensic procedures requires careful consideration of technical compatibility, legal admissibility, and practical implementation challenges. Quantum computing could potentially compromise blockchain security by deriving private keys and falsifying signatures, making it essential to plan for quantum-resistant blockchain implementations in forensic applications.[32]

Artificial intelligence applications in evidence analysis present both opportunities and challenges for digital evidence authentication. The role of AI in creating deepfakes emphasizes the importance of protecting free speech while addressing digitally manipulated content, requiring legal frameworks that can distinguish between legitimate AI assistance and fraudulent content generation.

Machine learning algorithms could enhance forensic analysis capabilities by identifying patterns, detecting anomalies, and accelerating large-scale evidence processing. However, the implementation of AI-assisted forensic analysis requires careful validation to ensure that automated systems meet appropriate reliability standards for legal proceedings.[33]

System Interoperability

Cross-jurisdictional evidence sharing requires technical standards and legal frameworks that facilitate secure and reliable transfer of digital evidence between different legal systems. The development of standardized evidence exchange protocols would enhance international cooperation while maintaining appropriate security and authentication standards.[34]

Mutual legal assistance treaties should be updated to reflect current technical capabilities and authentication methods recognized under BSA 2023. Technical standard harmonization efforts

[32] Deloitte, Quantum-Safe Blockchain Implementation Guide (2024) 45-52.
[33] IBM Research, AI-Assisted Digital Forensics: Validation and Reliability (2024) 78-85.
[34] Ministry of Electronics and Information Technology, Cross-Border Digital Evidence Sharing Protocol (MeitY 2024) 134-141.

ISSN: 2582-6433

should focus on ensuring compatibility between Indian forensic procedures and international standards used by partner jurisdictions. This harmonization facilitates evidence sharing while maintaining the integrity of Indian legal procedures and requirements.

Implementation Timeline and Priorities

Resource allocation strategies should balance immediate operational needs with long-term capacity building requirements. Investment in training, equipment, and infrastructure should be coordinated across different agencies and institutions to maximize effectiveness and avoid duplication.

Performance metrics and evaluation frameworks should be established to assess the effectiveness of capacity building efforts and guide future development priorities. Regular assessment of implementation progress would ensure that development efforts remain aligned with practical needs and available resources.

Stakeholder Coordination

Effective implementation of advanced digital evidence capabilities requires coordination among multiple stakeholders, including judicial institutions, law enforcement agencies, forensic laboratories, legal practitioners, and technology providers. Coordinated development efforts would maximize resource utilization while ensuring comprehensive capability development.

Public-private partnerships could accelerate technology development and deployment while leveraging commercial expertise and resources. Such partnerships should maintain appropriate oversight to ensure that commercial interests do not compromise the integrity of forensic procedures or legal requirements.

The future of digital evidence authentication under BSA 2023 depends on sustained commitment to technical excellence, institutional capacity building, and international cooperation. The statutory framework provides a solid foundation for these developments, but successful implementation requires ongoing attention to technical standards, procedural refinements, and capability enhancement.

ISSN: 2582-6433

CONCLUSION

The Bharatiya Sakshya Adhiniyam, 2023, represents a watershed moment in Indian evidence law, fundamentally transforming the legal approach to electronic evidence from a certificate-dependent system to one that embraces cryptographic authentication and digital forensics principles. By elevating electronic records to primary evidence status under Sections 57 and 61 and explicitly recognizing hash values and metadata analysis as authentication methods under Section 63, the Act eliminates the artificial hierarchy between digital and physical evidence that plagued the previous framework. This legislative innovation addresses the practical impossibilities that rendered sections 65A and 65B ineffective, while providing legal practitioners with clear authority to use scientifically validated authentication procedures.

Despite its theoretical sophistication, BSA 2023 faces significant implementation challenges that could undermine its transformative potential. The dual certification requirement under Section 63(4), while scientifically sound, creates practical bottlenecks given India's forensic infrastructure constraints, including staff shortages, equipment limitations, and processing delays. The absence of statutory standards governing expert qualifications and certification procedures risks creating inconsistent authentication standards and potential reliability concerns. Resource disparities between well-equipped central agencies and under-resourced local investigation units threaten to create a two-tiered system where authentication standards vary based on institutional capacity rather than evidence quality.

Successful BSA 2023 implementation requires substantial investment in judicial training, forensic infrastructure development, and standardized technical procedures. The Act's success will ultimately depend on sustained commitment to capacity building, quality assurance mechanisms, and adaptive implementation that responds to practical experience and technological change.