VOLUME 5 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

# AUTHENTICATION OF ELECTRONIC RECORDS BY USE OF ASYMMETRIC CRYPTO SYSTEM AND HASH FUNCTION: ANALYSIS OF ISSUES AND CHALLENGES

- Vardhan Deshmukh[1]

## ABSTRACT

*The growing reliance on digital transactions and records has underscored the need for robust methods to authenticate electronic evidence within India's legal framework. This paper critically analyzes the role of asymmetric cryptosystems and hash functions in verifying the authenticity and integrity of electronic records, focusing on their implementation under Section 65B of the Indian Evidence Act, 1872. Asymmetric cryptography, through digital signatures, and hash functions provide essential safeguards against tampering by ensuring data origin and integrity. However, the study reveals significant challenges in their practical application, including technical vulnerabilities, inconsistent judicial interpretations of certification requirements, regulatory ambiguity, and limited technical expertise within the judiciary. Landmark judgments such as Anvar P.V. v. P.K. Basheer and Arjun PanditraoKhotkar v. Kailash KushanraoGorantyal illustrate the evolving but inconsistent application of cryptographic authentication in Indian courts. Furthermore, the paper highlights operational and economic barriers that hinder widespread adoption among smaller entities. To address these challenges, the study proposes a hybrid approach combining blockchain with traditional cryptography, clearer guidelines for Section 65B certification, judicial training on cryptographic methods, and cost-effective solutions for small businesses and individuals. The analysis concludes that while asymmetric cryptosystems and hash functions are vital for digital evidence, aligning technological measures with consistent legal standards and improved technical understanding is essential to ensure the reliable and uniform admissibility of electronic records, thereby strengthening trust in India's digital legal ecosystem.*

[1] Student at NLU Nagpur



© 2025 International Journal of Advanced Legal Research

## INTRODUCTION

The digitalization of information and transactions has transformed the way evidence is managed, stored, and authenticated, making the verification of electronic records crucial under Indian Evidence Law. [2]The inherent risk of electronic records being modified or tampered with requires robust mechanisms to establish their authenticity in legal settings. Recognizing this need, India introduced significant changes to its legal framework through the Information Technology Act, 2000, which amended the Indian Evidence Act, 1872. These amendments included the addition of Section 65B, setting forth specific conditions that electronic records must satisfy to be considered admissible evidence in court.

Under Section 65B, electronic records can only be deemed admissible if they meet certain procedural requirements. This provision aims to ensure that digital evidence presented in court has not been altered, thus safeguarding its integrity. However, merely meeting the requirements of Section 65B does not guarantee that an electronic record is authentic; it merely enables it to be considered. For authenticating such records, courts rely heavily on digital signatures and data integrity mechanisms provided by cryptographic technologies.

Asymmetric cryptography, also known as public-key cryptography, plays a pivotal role in this authentication process. By using a pair of keys—public and private—a sender can create a digital signature that allows the receiver to verify the origin and integrity of the message or document. This digital signature, recognized under Indian law, provides a method for validating the authenticity of the electronic record and is an essential component of ensuring that the document remains unchanged.

Hash functions complement this process by creating a unique “digital fingerprint” for a document or piece of data. Even the slightest alteration in the electronic record changes the hash, making it an effective tool for verifying data integrity. Together, digital signatures and hash functions establish a framework for maintaining and verifying the authenticity of electronic records.

Despite the clear advantages of these cryptographic methods, several challenges affect their implementation in India.[3] These include the technical complexity of setting up and maintaining secure cryptographic systems, the varied understanding and application of Section 65B across

[2]S. Sundaram, Information Technology Act, 2000: A Comprehensive Guide, 3rd ed. (Bharati Law House, 2015)
[3]TechCrunch India, "Understanding Digital Signatures and Their Legal Implications," TechCrunch India (2024), https://techcrunch.com/india/digital-signatures.



© 2025 International Journal of Advanced Legal Research

different judicial rulings, and compliance issues among individuals and organizations. Courts have, on occasion, differed in their interpretation of what qualifies as a valid electronic record under Section 65B, adding further uncertainty.

This paper examines these challenges to electronic record admissibility in India and discusses potential advancements that could enhance the robustness and reliability of electronic evidence authentication, thereby strengthening the legal framework surrounding digital evidence in the Indian judiciary.[4]

## RESEARCH AIM

The aim of this research is to explore and critically analyze the role of asymmetric cryptosystems and hash functions in the authentication of electronic records. This study will examine the technical and legal aspects involved in ensuring the integrity and security of electronic records, identify the challenges inherent in these cryptographic methods, and propose potential solutions for enhancing digital transaction security and reliability.

## STATEMENT OF THE PROBLEM

The authentication of electronic records via asymmetric cryptosystems and hash functions faces technical, regulatory, and operational challenges, affecting the reliability of data integrity, the security of digital interactions, and their recognition under legal frameworks. These issues present significant risks in the global push towards digitalization and necessitate a critical evaluation of the technology's current limitations and future enhancements.

## RESEARCH OBJECTIVES

1. To examine the roles of asymmetric cryptosystems and hash functions in authenticating electronic records.
2. To identify the technical, regulatory, and operational challenges in using these methods for record authentication.
3. To analyse real-world applications and case studies to illustrate the limitations and effectiveness of current authentication frameworks.

[4]R. Chakraborty, "Electronic Evidence and Admissibility in Indian Courts: Challenges and Remedies," Journal of Information Technology and Law, 12(2), 113-129 (2020), at 120.



© 2025 International Journal of Advanced Legal Research

## RESEARCH QUESTIONS

1. How do asymmetric cryptosystems and hash functions contribute to the secure authentication of electronic records?
2. What are the key challenges and limitations in using these methods for electronic record authentication?
3. How have these authentication methods been applied in practice, and what improvements are required?

## REVIEW OF LITERATURE

Literature on asymmetric cryptosystems and hash functions demonstrates that these cryptographic techniques are foundational to securing electronic records. Asymmetric cryptography, utilizing a key pair for encryption and decryption, allows for secure transmission and verification without exposing private data. Studies indicate that, despite their effectiveness in authentication, these systems are vulnerable to quantum computing, algorithmic flaws, and high computational costs, highlighting a need for enhanced methods to counter these vulnerabilities.

In addition to technical evaluations, there are discussions around the legal recognition of digital signatures and records authenticated through cryptographic means, particularly with respect to cross-jurisdictional compliance. Regulatory frameworks vary, with some countries having implemented robust standards while others lag, leading to fragmented global recognition. Literature suggests that for cryptographic authentication to be widely accepted, technical improvements must be coupled with legal standardization and policy reform to align with emerging digital transaction practices.

## RESEARCH METHODOLOGY

This paper employs a doctrinal analysis method, focusing on qualitative research of academic publications, case studies, security reports, and legal frameworks related to electronic record authentication. The research draws on sources that evaluate the technical principles of asymmetric cryptosystems and hash functions as well as the regulatory and operational challenges they face in practical applications. This approach enables a comprehensive understanding of both the strengths and limitations of cryptographic authentication mechanisms.



© 2025 International Journal of Advanced Legal Research

## SCOPES AND LIMITATIONS

The scope of this study is limited to analyzing the technical and legal challenges in the authentication of electronic records through asymmetric cryptography and hash functions. While other cryptographic innovations, such as quantum-resistant algorithms, are emerging, this paper restricts its focus to current mainstream methods. This limitation ensures a concentrated study of the technology most commonly implemented in electronic authentication today, while acknowledging that future research may explore broader cryptographic advances.

## HYPOTHESIS

The hypothesis of this study is that while asymmetric cryptosystems and hash functions are critical to securing electronic records, their current application is insufficient to fully protect data integrity and ensure broad legal acceptance due to technical and regulatory challenges. It is proposed that a hybrid approach, integrating supplementary cryptographic techniques, could better address these challenges and enhance the reliability of electronic record authentication.

## HISTORY

The incorporation of asymmetric cryptography and hash functions into India's legal system represented a landmark shift toward secure digital authentication, essential for the country's expanding digital economy. The Information Technology Act, 2000, was pivotal in this transformation, as it officially recognized digital signatures, aligning India with global norms for electronic transactions. This legal framework underscored the importance of validating the authenticity and integrity of electronic records, especially in a landscape increasingly susceptible to data breaches, cyber fraud, and unauthorized modifications.[5]

Section 65B of the Indian Evidence Act, 1872, codified these requirements, setting out strict criteria for the admissibility of electronic records in court.[6] Under this provision, electronic records must be certified by a person with lawful control over them, providing an assurance of their originality and reliability. This certification often involves advanced cryptographic techniques, such as digital signatures and hash functions, which act as digital safeguards.

[5]K. Rattan, Legal Aspects of Digital Signatures and Electronic Evidence, 2nd ed. (LexisNexis, India, 2020), at 125.

[6]A. Kumar, "Digital Authentication and Cryptographic Standards: A Legal Perspective," Indian Cyber Law Review, 8(1), 45-56 (2018), at 51.



© 2025 International Journal of Advanced Legal Research

Digital signatures utilize asymmetric cryptography to create a secure, verifiable link between a document and its originator, while hash functions generate a unique "fingerprint" for data integrity checks, highlighting any alterations.[7] Together, these technologies form a robust framework to uphold the integrity of electronic records, thereby strengthening the evidentiary reliability of digital information in Indian courts.

## ASYMMETRIC CRYPTOSYSTEM AND HASH FUNCTIONS IN AUTHENTICATION UNDER INDIAN LAW

Asymmetric cryptosystems and hash functions play a foundational role in the authentication of electronic records under Indian law, primarily through the combined application of public and private keys to create digital signatures. These digital signatures, mandated under the Information Technology Act, 2000, are essential for verifying the origin and integrity of electronic documents and transactions, thus meeting the evidentiary requirements set forth in Section 65B of the Indian Evidence Act, 1872. This section explicitly stipulates that electronic records must be certified to ensure their authenticity and admissibility in court, and digital signatures serve as the technical basis for this certification.

An asymmetric cryptosystem operates by generating two related keys: a public key, which is openly accessible, and a private key, which remains confidential to the owner. When an electronic record is signed using the private key, a unique digital signature is created that can only be verified by the corresponding public key.[8] This pairing allows a third party to authenticate the identity of the sender without compromising the security of the data itself, as only the original signer can produce a valid signature with their private key. Under the Indian legal framework, this process is crucial for establishing both the integrity and origin of an electronic record.

In addition to digital signatures, hash functions provide another layer of security by ensuring data integrity. A hash function generates a unique value—a "hash"—based on the specific content of the electronic record. Even a minor alteration in the data will produce a completely different hash, alerting the verifier to any unauthorized changes. Therefore, hash values serve as digital fingerprints, reinforcing the trustworthiness of electronic records. Together, the digital signature and hash value safeguard the record against forgery and tampering.

[7]R. Mohan, Cyber Law in India: Legal and Regulatory Perspectives (Eastern Book Company, 2017), at 56.
[8]India Today, "Challenges in Implementing Digital Signature Authentication in India," India Today (2023), https://www.indiatoday.in/technology/features/story



© 2025 International Journal of Advanced Legal Research

Under Section 65B, it is required that electronic records presented as evidence be accompanied by a certificate from a person with lawful control over the data. This certificate must attest that the electronic record meets all necessary conditions for admissibility, including proof of authenticity and originality.[9] The combined use of asymmetric cryptography and hash functions forms the technical basis for these certifications, establishing a standard for electronic records that aligns with global best practices.

The Information Technology Act, 2000, and Indian Evidence Act aim to integrate such technological standards into the legal system. However, challenges persist in practical applications. Courts have at times varied in their interpretation of Section 65B, leading to inconsistency in what constitutes a properly authenticated electronic record.[10] Additionally, the complexity of cryptographic technology poses compliance difficulties for smaller businesses or individuals lacking the resources for sophisticated digital infrastructure.

Despite these challenges, India's commitment to integrating cryptographic standards in electronic authentication reflects a significant step toward enhancing the legal reliability of digital evidence, thereby supporting the judicial process in an era of digital transformation.

## KEY ISSUES AND CHALLENGES IN AUTHENTICATION UNDER INDIAN EVIDENCE LAW

Asymmetric cryptosystems and hash functions, despite their robustness in ensuring the security and authenticity of electronic records, face multiple challenges within the Indian legal context. These challenges can be divided into technical, regulatory, and operational issues, each adding a layer of complexity to the consistent and reliable application of cryptographic methods for electronic evidence authentication in court.[11]

### Technical Vulnerabilities and Judicial Interpretations of Section 65B

Although asymmetric cryptosystems and hash functions are theoretically secure, they are not entirely free from technical vulnerabilities, which impact their reliability in legal applications. The Indian Evidence Act, under Section 65B, mandates that electronic records must be certified for admissibility, a requirement that courts have interpreted in varying ways. While

[9]H. Patel & P. Mehta, "Hash Functions and Data Integrity in Electronic Records," Indian Journal of Cyber Law, 5(4), 232-246 (2019), at 240.
[10]Centre for Internet and Society (CIS), India, "Blockchain Technology and the Law," Centre for Internet and Society (2022), https://cis-india.org/blockchain.
[11]Indian Cyber Crime Coordination Centre (I4C), "Digital Evidence and Cyber Law in India," I4C (2023), https://i4c.gov.in/digital-evidence.


© 2025 International Journal of Advanced Legal Research

some courts enforce a strict reading of Section 65B, requiring electronic evidence to be accompanied by digital signatures, others are more lenient, sometimes accepting printed copies of digital records without demanding full compliance with cryptographic standards.

This inconsistency has created a fragmented approach to electronic evidence. For example, certain judgments have upheld that only original electronic records with digital signatures and appropriate Section 65B certification are admissible, placing stringent demands on parties submitting evidence.[12] In contrast, other courts have taken a flexible stance, admitting printed copies as evidence without requiring the rigorous standards of digital certification, particularly when such records are undisputed. This variability can make it difficult for legal practitioners to ascertain which evidence will meet the court's standards, as the requirements for digital signatures and certifications are not uniformly enforced across cases, causing uncertainty in how to secure electronic records effectively.

**Regulatory Challenges and Lack of Standardization**

The Information Technology Act, 2000, and the Indian Evidence Act, 1872, both recognize digital signatures and hash functions as mechanisms for validating electronic records. Yet, these Acts lack precise, standardized guidelines on applying these cryptographic methods across judicial and administrative scenarios.[13] This absence of uniformity has led to contradictory rulings where electronic records are admitted in one case but may be dismissed in another, resulting in confusion for practitioners and individuals seeking to use digital records as evidence.

Without a nationwide standard, legal practitioners face challenges in navigating the requirements for electronic records, especially when certification requirements vary from one court to another. For example, some courts insist on a Section 65B certificate signed by a qualified individual with lawful control over the record, verifying that the digital evidence is accurate and unaltered. Other courts view such a certificate as optional, particularly if the document’s authenticity is uncontested or if a certified hard copy is provided. This lack of consistency across judicial decisions undermines the reliability of cryptographic methods as evidence mechanisms, as it becomes challenging to predict how a particular court will interpret

[12]R. Chakraborty, "Electronic Evidence and Admissibility in Indian Courts: Challenges and Remedies," Journal of Information Technology and Law, 12(2), 113-129 (2020), at 113.
[13]Ministry of Electronics and Information Technology, Government of India, "Digital Signature and Cryptography in India," Ministry of Electronics and Information Technology (2024), https://www.meity.gov.in/digital-signatures.


© 2025 International Journal of Advanced Legal Research

the admissibility requirements for electronic records.[14] This regulatory ambiguity further diminishes the efficiency of asymmetric cryptosystems and hash functions in Indian law.

**Operational Challenges and Limited Technical Expertise in Indian Courts**

Operationally, one of the major issues is the limited availability of technical expertise within the Indian judicial system to effectively evaluate electronic records authenticated by cryptographic methods. Asymmetric cryptosystems and hash functions are complex technological tools, and while they are widely used in sectors like finance and IT, their application in legal contexts requires specialized understanding. Many judges, court staff, and legal practitioners may lack the technical training to properly assess the validity and security of cryptographic evidence.

This lack of expertise has practical implications. Courts sometimes favor paper-based evidence or simpler forms of verification that do not accurately reflect the digital nature of the original records. As a result, digital records authenticated by cryptographic methods may be viewed with skepticism or, in some cases, misunderstood. In certain scenarios, courts have struggled to evaluate whether digital evidence has been tampered with or altered, potentially compromising the integrity of the evidence being presented. This issue underscores the need for greater technological understanding within the judiciary to evaluate electronic records effectively and consistently.

**Cost and Complexity Barriers for Small Entities and Individuals**

The cost and complexity associated with implementing cryptographic systems like digital signatures and hash functions pose significant obstacles, particularly for smaller entities or individuals. Securing a digital signature, ensuring compliance with cryptographic protocols, and meeting Section 65B's certification requirements can be resource-intensive.[15] Obtaining digital certification often requires specialized software, cryptographic keys, and other technical infrastructure, all of which may be beyond the reach of smaller businesses or individuals without access to such resources.

This financial and logistical burden disproportionately affects individuals and smaller enterprises. For instance, large corporations and government agencies may have the

[14]K. Rattan, Legal Aspects of Digital Signatures and Electronic Evidence, 2nd ed. (LexisNexis, India, 2020), at 142.

[15]Legal Service India, "The Role of Section 65B in Electronic Evidence," Legal Service India (2021), https://www.legalserviceindia.com/article/1216-Section-65B-of-Indian-Evidence-Act.html.



© 2025 International Journal of Advanced Legal Research

infrastructure and financial capacity to support secure electronic documentation, but small business owners or individuals may struggle to meet these technical requirements. They may lack not only the tools but also the guidance on how to implement secure digital authentication methods, creating disparities in access to justice. Consequently, those without adequate resources might resort to less reliable forms of evidence, such as printed copies without proper digital certification, which could be dismissed in court due to non-compliance with Section 65B standards.[16] This economic barrier prevents uniformity in the application of cryptographic evidence, highlighting the need for accessible solutions to support the fair use of digital records across different segments of society.

These challenges underscore the complexity and obstacles in adopting asymmetric cryptography and hash functions within the Indian legal system, despite their potential to secure and authenticate electronic records reliably.[17] Addressing these technical, regulatory, and operational issues is essential to creating a more consistent and reliable framework for electronic evidence authentication in Indian courts.

## LANDMARK JUDGMENTSON ELECTRONIC RECORD AUTHENTICATION

### Anvar P.V. v. P.K. Basheer (2014)

The Supreme Court in *Anvar P.V. v. P.K. Basheer* (2014) is a landmark case that underscores the importance of using cryptographic methods such as digital signatures for the authentication of electronic records. In this case, the Court emphasized the mandatory requirement of Section 65B certification for admitting electronic records as evidence. The role of asymmetric cryptosystems is central here because digital signatures, which form the backbone of Section 65B certification, are based on public and private key pairs characteristic of asymmetric encryption.

Digital signatures, created using asymmetric cryptosystems, ensure that an electronic record has not been tampered with, as the signature can only be generated using the private key of the signer, and it can be verified using the public key. This process ensures both data integrity and non-repudiation, two essential elements in ensuring the reliability of electronic records. The

[16]A. Kumar, "Digital Authentication and Cryptographic Standards: A Legal Perspective," Indian Cyber Law Review, 8(1), 45-56 (2018), at 49.
[17]TechCrunch India, "Understanding Digital Signatures and Their Legal Implications," TechCrunch India (2024), https://techcrunch.com/india/digital-signatures.


© 2025 International Journal of Advanced Legal Research

*Anvar* judgment firmly established that the absence of a Section 65B certificate, which is typically tied to the use of asymmetric cryptography, renders electronic records inadmissible, regardless of whether the content is otherwise truthful or accurate.

**Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020**

In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), the Supreme Court further explored the complexities surrounding electronic evidence and certification requirements under Section 65B. While the case primarily focused on the use of secondary evidence, it also highlighted the relevance of hash functions in ensuring the integrity of digital evidence.[18]

A hash function is a cryptographic algorithm that takes an input (or "message") and returns a fixed-size string of bytes. This fixed-size output, known as the hash value, is unique to the input data, meaning even a small change in the original data will result in a drastically different hash value. In the context of Section 65B certification, hash values are used to prove that the electronic record presented in court has not been altered since it was originally created. The use of hash functions ensures that the content remains intact, providing a cryptographic fingerprint that can verify its authenticity.

Although *Arjun Panditrao Khotkar* did not directly address hash functions, the principles established by the Court regarding secondary evidence and certification indirectly affect how hash functions are used to authenticate electronic records. As Section 65B often requires certification of the record by a person in lawful control of the record, the use of cryptographic hash functions further supports this certification by ensuring that the content of the record is preserved in its original state, providing a secure basis for its admissibility in court.

**Shafhi Mohammad v. State of Himachal Pradesh (2018)**[19]

The case of *Shafhi Mohammad v. State of Himachal Pradesh* (2018) delves into the practical application of electronic records as evidence, touching upon the certification requirements for such records under Section 65B. In particular, this case reinforces the importance of both asymmetric cryptosystems (via digital signatures) and hash functions in ensuring the integrity of electronic records. While the Supreme Court in this case did not directly focus on

[18]S. Sundaram, Information Technology Act, 2000: A Comprehensive Guide, 3rd ed. (Bharati Law House, 2015), at 85.

[19]Cyberlaw Times, "Cryptography and Electronic Evidence in Indian Courts," Cyberlaw Times (2023), https://www.cyberlawtimes.com/cryptography-evidence-india.



© 2025 International Journal of Advanced Legal Research

cryptographic methods, it underscored the role of Section 65B certificates in authenticating the integrity of electronic evidence.

As digital signatures are derived from asymmetric cryptography, and hash functions play a critical role in verifying the integrity of digital data, this case reaffirms that cryptographic methods are essential for the authentication of electronic records. Digital signatures ensure that the record is authentic and was signed by the authorized party, while hash functions ensure that the record has not been tampered with in any way. In the absence of these cryptographic measures, courts may have a difficult time accepting electronic records as valid evidence.

**Regulatory Guidelines: Reserve Bank of India (RBI)**[20]

While not a judicial case, the Reserve Bank of India's (RBI) guidelines on digital signatures in the financial sector also highlight the importance of asymmetric cryptosystems for secure electronic transactions. In the financial sector, digital signatures are required for a wide range of transactions, including e-banking services, to ensure that the integrity of the data is preserved. The RBI mandates the use of asymmetric cryptosystems to generate digital signatures that verify the authenticity of financial transactions.

Asymmetric cryptography in the form of public-private key pairs ensures that only the designated individual can sign a transaction, and the public key can be used to verify the signature's validity. Hash functions are also employed in financial transactions to verify that the transaction data has not been altered in transit. The adoption of these cryptographic methods by the RBI ensures the security and legitimacy of digital transactions, aligning with broader statutory requirements, including Section 65B of the Indian Evidence Act.

## ANALYSIS

The challenges faced in using asymmetric cryptosystems and hash functions within Indian Evidence Law reveal a significant gap between the technological capabilities of cryptographic methods and the legal requirements set out by Indian courts. While asymmetric cryptography (through digital signatures) and hash functions are widely accepted as global standards for authenticating electronic records and ensuring data integrity, their implementation within the Indian legal system remains inconsistent. This inconsistency arises primarily due to varied judicial interpretations of Section 65B of the Indian Evidence Act, 1872, which governs the admissibility of electronic records. While some courts strictly enforce the requirements for

[20]R. Mohan, Cyber Law in India: Legal and Regulatory Perspectives (Eastern Book Company, 2017), at 67.



© 2025 International Journal of Advanced Legal Research

certification under Section 65B, others have demonstrated flexibility or lack clarity in their approach, resulting in contradictory rulings and legal uncertainty.

Another critical challenge is the limited technical expertise available in many Indian courts to assess the validity and authenticity of digital signatures and hash functions.[21] These cryptographic tools require specialized knowledge to evaluate their effectiveness and to verify their proper application in authenticating electronic records.[22] Without adequate technical support, judges may be unable to determine whether the electronic evidence presented in court is truly secure and unaltered, which compromises the reliability of such records in legal proceedings.

As a result, the reliance solely on asymmetric cryptosystems and hash functions is not sufficient to ensure the security and admissibility of electronic records. To bridge this gap, both legal and technical improvements are necessary. The legal framework must provide more standardized guidelines for the use of these cryptographic methods, and courts must be equipped with the requisite expertise to properly assess and apply them in the context of electronic evidence. This will help uphold data integrity and ensure that electronic records remain reliable and secure in legal proceedings.

## SUGGESTIONS

### 1. Hybrid Approach Combining Traditional Cryptography with Blockchain

The integration of emerging technologies like blockchain with traditional cryptographic methods can significantly enhance the security and authenticity of electronic records. Blockchain offers a decentralized and immutable ledger, which ensures that once a record is created, it cannot be altered, providing an additional layer of protection against data manipulation. When combined with asymmetric cryptography (through digital signatures) and hash functions, blockchain can further solidify the legal framework for authenticating electronic evidence. This hybrid approach would ensure greater data integrity and enable more secure, transparent, and tamper-proof record-keeping, aligning with both legal requirements and technological advancements.

[21]Indian Cyber Crime Coordination Centre (I4C), "Digital Evidence and Cyber Law in India," I4C (2023), https://i4c.gov.in/digital-evidence.
[22]H. Patel & P. Mehta, "Hash Functions and Data Integrity in Electronic Records," Indian Journal of Cyber Law, 5(4), 232-246 (2019), at 235.


© 2025 International Journal of Advanced Legal Research

**2. More Detailed Guidelines and Consistent Interpretations of Section 65B**

One of the critical challenges in electronic record authentication is the inconsistent interpretation of Section 65B of the Indian Evidence Act, 1872. To address this, it is essential to develop more detailed and comprehensive guidelines that provide clarity on the certification process for electronic records. Clear guidelines would eliminate ambiguity and create a standardized approach to the admissibility of digital evidence. By ensuring that courts across India adopt a consistent interpretation of Section 65B, the legal system can avoid contradictory rulings and provide more predictability in the handling of electronic records. This consistency is crucial for establishing trust in the judicial process concerning digital evidence.

**3. Training for Judicial Officers on Cryptographic Methods**

To improve the reliability of court rulings concerning the admissibility of electronic records, judicial officers must be trained in the technical aspects of cryptographic methods, including digital signatures and hash functions. Judges often lack the specialized knowledge required to evaluate the integrity of electronic evidence, which can lead to challenges in understanding and applying cryptographic technologies accurately. Training programs specifically focused on these technologies, developed in collaboration with experts in the field, would enable judicial officers to better comprehend the intricacies of electronic records. This enhanced technical understanding would foster more informed decision-making, ensuring that digital evidence is treated with the same rigor as traditional forms of evidence.

**4. Implementing Cost-Effective Solutions for Smaller Entities**

Smaller entities, such as small businesses and individual practitioners, often face financial barriers when it comes to adopting secure methods for digital record-keeping, including the use of digital signatures and certifications. To bridge this gap, the government should consider implementing subsidized or cost-effective solutions for digital certification, enabling these entities to comply with legal requirements. This could include offering financial incentives, subsidies for certification fees, or the development of low-cost certification schemes. By making these resources more accessible, the legal system can ensure that smaller businesses and individuals are not excluded from the benefits of secure, authenticated electronic records, contributing to broader adoption and improved legal compliance across the economy.



© 2025 International Journal of Advanced Legal Research

## CONCLUSION

In conclusion, asymmetric cryptosystems and hash functions are integral to the authentication of electronic records under Indian Evidence Law, playing a crucial role in ensuring data integrity and preventing tampering. However, their effectiveness is hindered by a range of technical and legal challenges.[23] While these cryptographic methods are globally recognized standards, their implementation in India has been compromised by inconsistent judicial interpretations and a lack of specialized technical expertise within the judiciary.[24] This fragmentation in legal approaches has led to uncertainty regarding the admissibility of electronic records, creating obstacles in the reliable application of these authentication methods.

To address these challenges, a dual approach involving both policy reforms and technological advancements is necessary. Clearer legal guidelines, consistent judicial interpretations, and comprehensive training for judicial officers are essential to ensuring that asymmetric cryptosystems and hash functions are used effectively and uniformly in Indian courts.[25] Moreover, technological advancements such as integrating blockchain alongside traditional cryptography could provide an additional layer of security, further enhancing the reliability of electronic record authentication.

Ultimately, the success of electronic record authentication in India depends on aligning technological innovation with legal clarity.[26] By addressing current gaps and adopting a forward-looking approach, India can ensure that electronic records are securely authenticated, their admissibility is predictable, and the judicial process remains credible in the era of digital transformation.

## BIBLIOGRAPHY

### Books

1. Rattan, K. (2020). *Legal Aspects of Digital Signatures and Electronic Evidence.* 2nd ed. LexisNexis, India.

[23]Centre for Internet and Society (CIS), India, "Blockchain Technology and the Law," Centre for Internet and Society (2022), https://cis-india.org/blockchain.
[24]India Today, "Challenges in Implementing Digital Signature Authentication in India," India Today (2023), https://www.indiatoday.in/technology/features/story.
[25]Cyberlaw Times, "Cryptography and Electronic Evidence in Indian Courts," Cyberlaw Times (2023), https://www.cyberlawtimes.com/cryptography-evidence-india.
[26]Ministry of Electronics and Information Technology, Government of India, "Digital Signature and Cryptography in India," Ministry of Electronics and Information Technology (2024), https://www.meity.gov.in/digital-signatures.



© 2025 International Journal of Advanced Legal Research

2. Sundaram, S. (2015). *Information Technology Act, 2000: A Comprehensive Guide.* 3rd ed. Bharati Law House.

3. Mohan, R. (2017). *Cyber Law in India: Legal and Regulatory Perspectives.* Eastern Book Company.

**Articles**

1. Chakraborty, R. (2020). "Electronic Evidence and Admissibility in Indian Courts: Challenges and Remedies." *Journal of Information Technology and Law,* 12(2), 113-129.

2. Kumar, A. (2018). "Digital Authentication and Cryptographic Standards: A Legal Perspective." *Indian Cyber Law Review,* 8(1), 45-56.

3. Patel, H., & Mehta, P. (2019). "Hash Functions and Data Integrity in Electronic Records." *Indian Journal of Cyber Law,* 5(4), 232-246.

**Webliography**

1. National Law University, Delhi. (2023). "Section 65B of the Indian Evidence Act: Analysis and Application." https://www.nludelhi.ac.in/section-65b-analysis

2. Ministry of Electronics and Information Technology, Government of India. (2024). "Digital Signature and Cryptography in India." https://www.meity.gov.in/digital-signatures

3. Indian Cyber Crime Coordination Centre (I4C). (2023). "Digital Evidence and Cyber Law in India." https://i4c.gov.in/digital-evidence

4. Centre for Internet and Society (CIS), India. (2022). "Blockchain Technology and the Law." https://cis-india.org/blockchain

5. Legal Service India. (2021). "The Role of Section 65B in Electronic Evidence." https://www.legalserviceindia.com/article/1216-Section-65B-of-Indian-Evidence-Act.html

6. TechCrunch India. (2024). "Understanding Digital Signatures and Their Legal Implications." https://techcrunch.com/india/digital-signatures



© 2025 International Journal of Advanced Legal Research

7. Cyberlaw Times. (2023). "Cryptography and Electronic Evidence in Indian Courts." https://www.cyberlawtimes.com/cryptography-evidence-india

8. India Today. (2023). "Challenges in Implementing Digital Signature Authentication in India." https://www.indiatoday.in/technology/features/story



© 2025 International Journal of Advanced Legal Research