IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

Authentication of Electronic Records and Digital Signature Under Evidence Law

Pratheesh C[1] and V. Mahalingam[2]
[1]B..Com.Llb (Hons) & [2]Assistant Professor
SRM School of Law, SRM Institute of Science and Technology, Kattankulathur

Abstract: *The rapid development of technology has transformed the way information is created, stored, and communicated. In modern legal systems, electronic records and digital signatures have become essential components of evidence. Courts are increasingly required to deal with electronic documents such as emails, online transactions, digital contracts, and electronic communications. Therefore, the authentication of such records has become a crucial aspect of evidence law.*

This paper examines the concept of authentication of electronic records and digital signatures under the framework of the Bharatiya Sakshya Adhiniyam, 2023 and the Information Technology Act, 2000. It explains the legal provisions, admissibility, methods of proof, and judicial interpretation relating to electronic evidence. The study also highlights the importance of ensuring reliability, integrity, and security of digital records in legal proceedings.

The objective of this research is to provide a comprehensive understanding of how electronic records are authenticated and how digital signatures function as a tool of verification. It also addresses the challenges faced in proving electronic evidence and the evolving role of courts in adapting to technological advancements.

Keywords: Electronic Records, Digital Signature, Evidence Law, Authentication, Admissibility, Bharatiya Sakshya Adhiniyam 2023, Information Technology Act 2000, Cyber Law, Electronic Evidence

I. INTRODUCTION

The law of evidence plays a vital role in ensuring that justice is delivered based on reliable and admissible facts. With the advancement of technology, traditional forms of evidence are gradually being replaced by electronic records. Today, most communications, transactions, and agreements are carried out in digital form, making electronic evidence an integral part of legal proceedings.

Electronic records include emails, digital documents, online contracts, audio recordings, and other forms of data stored electronically. However, unlike traditional documents, electronic records are more vulnerable to tampering, alteration, and unauthorized access. Therefore, authentication becomes essential to prove their genuineness and reliability before the court.

Digital signatures serve as a key tool in verifying electronic records. They ensure that the document has not been altered and that it originates from a verified source. The Bharatiya

Sakshya Adhiniyam, 2023 recognizes electronic records and provides legal provisions for their admissibility and authentication.

Thus, the study of authentication of electronic records and digital signatures is essential in understanding the modern law of evidence.

II. MEANING OF ELECTRONIC RECORD

An electronic record refers to any information that is created, stored, or transmitted in digital form. It includes data generated, sent, received, or stored in electronic devices such as computers, mobile phones, and servers.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

Electronic records are widely used in business, banking, communication, and government transactions. Examples include emails, SMS messages, digital contracts, online invoices, and electronic databases.

Unlike traditional paper documents, electronic records exist in intangible form. This makes them easier to store and transfer but also raises concerns regarding their authenticity and security.

Therefore, courts require proper authentication to ensure that such records are genuine and have not been tampered with.

III. DIGITAL SIGNATURE

A digital signature is a method of verifying the authenticity of an electronic record. It is a secure electronic code attached to a document to confirm the identity of the sender and ensure that the content has not been altered.

In addition to the existing legal provisions, the increasing dependence on electronic records has made it necessary for courts to develop a deeper understanding of technological processes. Judges and legal practitioners are now required to interpret complex digital data, which often involves technical concepts such as encryption, metadata, and data recovery. This shift has created a need for specialized training and expert assistance in handling electronic evidence. Without proper technical knowledge, there is a risk of misinterpretation or incorrect evaluation of digital records. Therefore, the integration of law and technology has become essential in modern judicial systems. Courts must ensure that while relying on electronic evidence, they do not compromise on the principles of fairness, accuracy, and justice. This highlights the evolving nature of evidence law, which must continuously adapt to technological advancements.

Digital signatures are based on cryptographic technology. They use a pair of keys:

• Private key – used to sign the document
• Public key – used to verify the signature Digital signatures provide:
• Authentication of identity
• Integrity of data
• Non-repudiation (cannot deny signing)

Thus, digital signatures play a crucial role in ensuring the reliability of electronic records.

IV. LEGAL FRAMEWORK

The legal recognition of electronic records and digital signatures in India is mainly governed by:

• Bharatiya Sakshya Adhiniyam, 2023
• Information Technology Act, 2000

These laws provide that electronic records are admissible as evidence if they satisfy certain conditions.

Another important aspect of authentication of electronic records is the concept of data integrity. Data integrity refers to the assurance that information has remained complete, accurate, and unaltered from the time it was created to the time it is presented in court. In the digital environment, maintaining data integrity is a significant challenge due to the ease with which electronic records can be modified. Even a small alteration in a digital file can change its meaning and legal implications. Therefore, courts rely on tools such as hash values and digital signatures to verify whether the data has been tampered with. These tools create a unique digital fingerprint of the document, which helps in detecting any unauthorized changes. Ensuring data integrity is crucial for maintaining trust in electronic evidence and for preventing misuse or manipulation of digital records.

The law also recognizes digital signatures as a valid method of authentication. Certifying Authorities are appointed to issue digital signature certificates.

Thus, the legal framework ensures that electronic evidence is treated on par with traditional evidence.

V. ADMISSIBILITY OF ELECTRONIC EVIDENCE

Electronic records are admissible in court if they are properly authenticated. The law requires that:

• The record must be relevant
• It must be genuine

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, May 2026 Impact Factor: 8.2

• It must be produced in proper form

The role of cyber laws and regulatory mechanisms has also become increasingly important in the context of electronic evidence. Governments and legal institutions are continuously updating laws and policies to address new challenges arising from digital technologies. Issues such as cybercrime, data breaches, identity theft, and online fraud have highlighted the need for strong legal safeguards. Electronic records often play a central role in investigating and prosecuting such offences, making their authentication even more critical. At the same time, privacy concerns must also be taken into account while handling electronic data. Courts must strike a balance between the need for evidence and the protection of individual rights.

This requires a careful and responsible approach in dealing with electronic records, ensuring that they are used only for legitimate purposes and in accordance with the law.

Courts also require a certificate (similar to Section G5B concept) to prove the authenticity of electronic records.

This ensures that electronic evidence is reliable and trustworthy.

VI. AUTHENTICATION OF ELECTRONIC RECORDS

Authentication means proving that an electronic record is genuine and has not been altered.

Methods of authentication include:

• Digital signatures
• Hash values
• Metadata analysis
• Expert testimony

Authentication ensures that the record is accurate and reliable for judicial purposes.

VII. ROLE OF CERTIFYING AUTHORITIES

Certifying Authorities are responsible for issuing digital signature certificates.

Their functions include:

• Verifying identity of users
• Issuing certificates
• Maintaining security

Looking towards the future, the importance of authentication of electronic records and digital signatures is expected to grow even further with the advancement of emerging technologies such as artificial intelligence, blockchain, and cloud computing. These technologies have the potential to enhance the security and reliability of electronic records, making authentication more efficient and trustworthy. For instance, blockchain technology provides a decentralized and tamper-proof system for storing data, which can significantly reduce the risk of manipulation.

Similarly, artificial intelligence can be used to detect anomalies and verify the authenticity of digital documents. However, these advancements also bring new challenges that require continuous legal adaptation. The law must evolve alongside technology to ensure that it remains effective in regulating digital evidence. Thus, the future of evidence law will largely depend on its ability to integrate technological innovations while upholding the fundamental principles of justice.

They play a crucial role in ensuring trust in digital transactions.

VIII. PROOF OF DIGITAL SIGNATURE

Digital signatures can be proved by:

• Producing the certificate
• Verifying through public key
• Expert evidence

Courts rely on technical and legal evidence to verify signatures.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

IX. ROLE OF COURTS

Courts play an important role in evaluating electronic evidence. They examine:

- Authenticity
- Integrity
- Reliability

Courts ensure that only genuine electronic records are accepted.

X. IMPORTANT CASE LAWS

- Anvar P.V. v. P.K. Basheer – Electronic evidence must follow proper certification
- Arjun Panditrao Khotkar v. Kailash Kushanrao – Clarified admissibility rules

These cases highlight judicial approach.

XI. COMPARISON WITH TRADITIONAL EVIDENCE

Electronic evidence differs from traditional evidence:

- Easily transferable
- Easily tampered
- Requires technical verification Thus, stricter rules are applied.

XII. CYBER SECURITY ISSUES

Electronic records face risks like:

- Hacking
- Data manipulation
- Identity theft

Security measures are essential.

XIII. CHALLENGES

- Difficulty in authentication
- Lack of technical knowledge
- Risk of misuse

Courts must handle these carefully.

XIV.CRITICAL ANALYSIS

Advantages:

- Fast and efficient
- Easy storage Disadvantages:
- Risk of tampering
- Technical complexity

Thus, balance is needed.

XV. PRACTICAL IMPORTANCE

Electronic evidence is widely used in:

- Banking
- E-commerce
- Criminal cases

It ensures quick justice.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, May 2026
Impact Factor: 8.2

1C. FUTURE SCOPE

With AI and blockchain:

- Authentication will improve
- Security will increase Law will continue evolving.

XVI. CONCLUSION

Authentication of electronic records and digital signatures is essential in modern evidence law. It ensures reliability, security, and fairness in legal proceedings. Courts play a key role in adapting to technological changes.

XVII. BIBLIOGRAPHY

Bare Acts

- Bharatiya Sakshya Adhiniyam, 2023
- Information Technology Act, 2000

Books

- Ratanlal & Dhirajlal – Law of Evidence

Case Laws

- Anvar P.V. v. P.K. Basheer
- Arjun Panditrao Khotkar v. Kailash Kushanrao