MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2332-2336

METADATA, HASH VALUES AND DIGITAL SIGNATURE: TECHNICAL SAFEGUARDS WITHIN THE INDIAN LEGISLATION.

[1]Ms. Vratika Singh
[2]Prof. (Dr.) Bindu Jindal
[3] Ms. Bhawana Girdhar
[4]Dr. Sujata Dahiya
[1a]Ph.D. Scholar, Department of Law, Maharishi Markandeshwar(Deemed to be University) Mullana-Ambala, Haryana, India, vratika303@gmail.com
[1b]Assistant Professor, Department of Law, Maharishi Markandeshwar(Deemed to be University) Mullana-Ambala, Haryana, India, vratika303@gmail.com
[2]Head & Dean, Department of Law, Maharishi Markandeshwar(Deemed to be University) Mullana-Ambala, Haryana, India, bindujindal1994@gmail.com
[3]LL.M. Scholar, Department of Law, Maharishi Markandeshwar(Deemed to be University) Mullana-Ambala, Haryana, India, girdharbhawana2@gmail.com
[4]Assistant Professor, Department of Law, Maharishi Markandeshwar(Deemed to be University) Mullana-Ambala, Haryana, India, sujata.dahiya@mmumullana.org

Abstract
In the digital age, the Indian courts are becoming more dependent on electronic documents, including emails, WhatsApp messages, and CCTV footage, call detail records, online agreements, and documents stored in the clouds to establish rights and liabilities. Since the administration of governance, trade, and individual communication have shifted to online platforms, court cases have not been far behind. But, unlike the documents of the past, which were made of paper, electronic records are immaterial and can be copied, changed and manipulated easily without any tracks. This raises serious issues of authenticity and integrity and makes vital questions on how courts can trustfully depend on digital evidence.This paper will discuss three essential technical security measures that can be used to deal with these issues: metadata, hash values and digital signatures. Metadata gives account related background facts concerning a digital file like the time in which it was created, edited, or viewed thus helping in the determination of authorship and timeline. The value of hashes is cryptographic generated numbers that serve as digital fingerprints to confirm the possibility of alteration of a file. Asymmetric cryptography is used to create digital signatures which provide legally accepted ways of authentication as well as provide a secure electronic communication. These tools when combined create credibility to the electronic records when they appear before courts.
The discussion is contextualized in the legal framework of the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023 which is a combination of laws that regulate and govern the admissibility and authentication of electronic evidence in India. The article provides an analysis of the integration of technological safeguards into Indian law, through a doctrinal and analytical approach, assisted by little comparative information, and identifies the areas where gaps still exist.
The research concludes that despite the definite statutory status of digital signatures, the factual role of metadata and hash verification has not yet been developed and is highly reliant on expert testimony. It ends with the suggestion of precise statutory provisions, standard forensic practices, and further training of judges on digital literacy in order to make technological innovation work towards and not against the transparency and credibility of the justice system.
Keywords: Electronic Evidence; Metadata; Hash Values; Digital Signatures; Digital Authentication; Data Integrity; Cyber Forensics; Information Technology Act, 2000; Bharatiya Sakshya Adhiniyam, 2023; Admissibility of Electronic Records.

Introduction

The justice system in the present day is in a more digitalized world. Discussions that were previously done in person or via handwritten letters are now being conducted via emails, messaging apps and social media. Business is transacted electronically, contracts are signed over the internet and every action is recorded by surveillance systems in real time. Because of this, the electronic recordings of WhatsApp chats, CCTV footage, bank transactions records, and digitally signed agreements, among other types, are often requested in court across India. In most instances, this material is not just a supportive evidence; in fact it is the core of the dispute.The change has resulted in opportunities and challenges. On the one hand, digital records have the ability to give accurate timestamps, location information, and elaborate transaction logs. Conversely, electronic files can be duplicated, altered and manipulated relative easily and in most cases they leave no trace of it. Digital evidence is unrealistic and technologically sophisticated, unlike the paper documents of the past. The mentioned features cast significant doubts on the authenticity, reliability, and fairness central principles, which are at the center of evidentiary law. Making sure the electronic records can be trusted by the courts without jeopardizing the due process has thus emerged as an urgent legal issue.

Background

The law of evidence in India has been formed based on a period where documents were tangible and physical. The sudden development of digital communication meant that this traditional structure had to be reconsidered. The passage of the Information Technology Act, 2000 was a historic move since it accorded legal status to electronic records and digital signatures. Recently, Bharatiya Sakshya Adhiniyam, 2023 has attempted to update rules of evidence to meet the needs of the technology and increasing dependence on digital technologies.However, as much as legislation recognizes electronic records, there are practical issues. Courts frequently struggle with the issue of whether or not there was some tampering of a digital file or whether the due requirements of certification were met or whether or not the technical evidence has been fully discussed. In most of the cases, experts testify so that the judges and lawyers can rely on them to comprehend the technological processes. This brings in confusion and even inconsistency in the application of the law at times.These doubts are what have underpinned the rationale of this study. The research aims to address the gap between legal and technological reality by analyzing the functionality of metadata, hash values and digital signatures as technical protective measures.

India Rises as the Digital Evidence.

The high pace of digitization in India has transformed the nature of litigation drastically. The growth of online banking, online shopping, e-governance applications, and users of smartphones have created a monumental mass of electronic information. Facebook and Twitter updates and personal correspondence often find their way to court as witnesses of crime and civil conflicts. Corporate litigation can be based on email trails and digital contracts, whereas cybercrime investigations are based on server logs, IP addresses, and forensic imaging.
This influx of digital evidence has imposed new burden on the courts. Courts are now required to review sophisticated technological material in order to address compliance with the evidentiary standards. The advent of such technologies like artificial intelligence, cloud storage, and blockchain only makes it more difficult to address elements of traditional ideas of proof. With digital content taking over adjudication, the technical processes to establish authentication and integrity are no longer optional they are necessary.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2332-2336

Electronic Records under the Bharatiya Sakshya Adhiniyam, 2023.

The Bharatiya Sakshya Adhiniyam, 2023 is a contemporary strategy of the evidence law in India. The Act has clearly taken into account the digital revolution of the society as evidenced by incorporation of electronic records in the scope of documentary evidence. This implies that electronic records like emails, electronic contracts, audio-video records, or data on servers are jurisdictional records and can be used in court provided that they are in accordance with the statutory requirements.

The Act represents a significant change of thought. It recognizes the fact that in the contemporary world, evidence is usually produced and stored in an electronic format as opposed to being on paper. Simultaneously, it does not approach electronic records carelessly. Rather, it focuses on procedural protection to make sure that such records are valid and genuine and can be depended upon in court. To put it simply, the law admits digital evidence as long as it can prove that it is not tampered with.

The Information Technology Act, 2000 formed the basis of the acknowledgment of electronic records in India. This Act is quite broad in defining what an electronic record is by considering any information, image, sound or data which is created, sent, received or stored in electronic format as an electronic record. This definition is specifically broad based so that the law may be modified as technology evolves.

Notably, the IT Act does not only define electronic records by rendering them legally binding. It is also aware of the digital signatures, secure electronic records and thus it is able to offer a means of authentication. This was a major breakthrough particularly in online contracts, e-banking and e-governance.The IT Act made the electronic records as legally equivalent to traditional documents, and this worked in favor of the digital economy of India to operate under legal certainty. Nonetheless, it also necessitated the need to come up with sound technical measures to guard the integrity of such records.

Nature and Characteristics of Digital Evidence.

There are some peculiarities of the digital evidence which may be compared with the traditional evidence:

i. Intangible Nature- Electronic records can not be touched or evaluated physically as paper documents can. They are in digital form and they need machines to retrieve them.
ii. The simplicity of copying- Digital files can be copied without any loss of quality. Although this simplifies the preservation process, it complicates the issue of determining the original version.
iii. Volatility- Temporary system data and other volatile digital data may be lost in no time unless well maintained.
iv. Manipulation Risk Digital files can be manipulated with advanced tools. In some cases, such changes are not easily observed without technical knowledge.
v. Embedded Information (Metadata) - Each digital file has some secret data regarding the time and manner of its creation or editing. It may be of great help in establishing authenticitybut it may also be manipulated.

Metadata as Evidentiary Protective Measure.

There is a story behind every file in the realm of the digital world. In addition to the apparent content of a document, picture, or video, there is the information that is hidden and, as such, registers how, when, and sometimes by whom the file was created, accessed, or modified. This is an under-meta-form of information otherwise known as metadata that has gained prominence in current litigation. Although the content that is visible can depict a certain narrative, metadata can either affirm it or refute it.

Metadata can be crucial in a case of forgery, backdating, tampering or fabrication claims. It serves as a technical protection as it assists the courts in verifying the authenticity and integrity of electronic records. Even though the use of an Indian legislation like the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023 does not specifically expound on metadata, its evidentiary value is becoming increasingly acknowledged by the forensic practice and logic in a court of law.

There is a name, metadata, which means, literally, information about information. It is the background information that is automatically created and saved in an electronic file. Such information can be in the form of:

i. Date and time of creation
ii. Date and time of the last modification.
iii. Author or user identity
iv. Device or software used
v. File size and format
vi. In some instances, location data.

Metadata can be broadly classified into three:

i. Descriptive Metadata - Determines the fundamental characteristics of a file, e.g. title, author and keywords.
ii. Structural Metadata - describes the organisation or association of various elements of a digital file.
iii. Administrative Metadata - This contains technical data regarding file creation, history of modification, access logs and system specifications.

In practical explanation, metadata offers a digital footprint. To give a case in point, in case a contract is said to have been signed on this date the metadata can show whether the document was created or modified afterwards. Likewise, metadata is used in criminal investigations to prove location and time by utilizing photographs or videos.

Relevance of Metadata in Litigation

Metadata comes in handy especially when authenticity is being challenged. It can assist courts in:

i. Painting authorship or user identity.
ii. Negotiating schedules and order of events.
iii. Identification of changes or unauthorized changes.
iv. Impeaching or supporting witness testimony.

Examples include the metadata aspect of emails where it can be used in proving whether an email has been dispatched at a specific time in case of a corporate dispute. Metadata on the digital photographs or chat messages can be used in matrimonial or criminal cases to confirm its source. Regarding the evidence substantiation, metadata reinforces the integrity of the electronic records by providing objective system-generated information. Digital systems automatically capture metadata, unlike oral testimony which can be subjective or affected by the memory. Well-maintained, validated, it is a highly effective corroborative instrument. Its applicability and strength however will be determined by the adherence to statutory provisions by the Indian evidence law and their forensic management. The Indian courts have slowly started to recognize the relevance of technical verification in the digital evidence cases. Though the statutory framework mainly concerns the condition of admissibility and certification, courts have been more inclined to use the forensic analysis to ascertain authenticity. When it comes to electronic communications, the courts have considered technical evidence, including timestamps, server logs and device details. Metadata is not frequently discussed on its own, but it is commonly included in the expert testimony provided to prove the authenticity of digital content.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2332-2336

There is reserved acceptance under judicial practice. Before courts put much trust in metadata, they normally demand that it is properly certified and verified by the experts. In cases of suspicion of tampering or manipulation, it can be reasonable to deny the assignment of probative value by the court unless the presence of technical safeguards.

Although greater recognition is being given to it, there is little explicit judicial commentary on metadata standards per se and a lot of it rests on forensic practice as opposed to statutory direction.

Authentication and Manipulation Risk Challenges.

Although metadata may be used as a good evidentiary protection, it is not an impervious barrier to manipulation. Metadata fields can be changed using advanced software, timestamps can be changed or document properties themselves can be changed. There are also instances where metadata may be distorted by accidental copying/transferring of files between devices, leading to confusion of authenticity.

Key challenges include:

i. Absence of homogenous forensic standards.
ii. Overall, poor digital literacy among lawyers.
iii. Possibility of intentional interference.
iv. Problems with maintaining original metadata in investigation.

Also, when the electronic records are printed or changed to other formats, important metadata can be forgotten. This casts some doubts on the reliability of courts to always scrutinize the most credible copy of the digital file.

In response to these issues, effective forensic practices, appropriate chain-of-custody reports, and technological sensitivity in the courts of law are necessitated. Though metadata is useful, other security measures like hash verification and digital signatures should be used to supplement it, in order to protect the digital evidence fully.

Hash Values and Integrity of Data.

The most important and yet simple issue concerning digital evidence is the following: how can a court be certain that a file is not modified? This is unlike paper document where every overwrite or a physical interference may leave some trace yet digital files can be altered in a few seconds without any obvious mark. It raises the problem of integrity as a core to electronic evidence.

A solution to this problem is the use of hash values which is practical and reliable. A hash value, also known as a digital fingerprint, is used to identify whether the electronic data has been altered in any way since the time it was gathered to the time it is admitted in court. Although the Indian laws like the Information technology act, 2000 and the Bharatiyasakshya Adhiniyam, 2023 do not explicitly stipulate the details of the hash technology, it is regularly used by forensic specialists in India to ensure the authenticity of digital evidence.

A hash function is a mathematical activity that transforms digital information like a document, image, audio file or a whole hard drive into a fixed length series of characters called a hash value. This is a unique output of that given data. Any single modification made to the original file (adding even a single letter or pixel) will produce an entirely new hash value.

Simply, when two files possess the same hash value, they are the same. When there is a change in the hash values then something has changed. Contemporary cryptographic hash functions, including the variants of Secure Hash Algorithms (SHA) are built as being trustworthy and proving tamper-sensitive. They have key properties:

i. The input will always want the same output.
ii. Different inputs have different outputs.
iii. The hash cannot be used to rebuild the original file.
iv. The slightest change has a drastic impact on the hash outcome.

Practically, in cases where the investigators extract the digital evidence, they calculate a hash value on the fly. The hash is re-calculated later when the evidence is checked or put in the court. When the values are the same, then it is an assurance that the data is unaltered.

Use of Hash Values to reveal Proof of Authenticity and Integrity.

The hash values are mostly used to establish integrity, which is the absence of modifications in the file. They will not directly establish the person who made the file, but will ensure that the file contains no alterations.

This renders hash verification very significant in situations where there are claims of tampering. For example:

i. When the crime involves cybercrime, the hard disks or phones will be seized and duplicated to be examined.
ii. In financial fraud cases, the digital records are obtained in servers.
iii. In the criminal cases, CCTV records or computer records are depended on.

In both of these scenarios, hash values can be used to offer objective technical assurance. Rather than relying on oral testifying, the courts can also apply scientific approach that will ensure that the evidence is not tainted. In this regard, hash values are silent successors of digital integrity.

Indian Courts: Hash Value Forensics.

In India, hash verification is frequently used in the laboratories of forensic science on the work with the digital evidence. In cases where a device is taken, it is common to have experts generate a forensic image, a full copy of the device on a digital basis instead of utilizing the original device. Both the original and the copy are generated with hash values. When they are similar, it demonstrates that the copy is correct and has not been distorted.

Despite the fact that the algorithm used in hash may not be discussed in detail in court judgments, it is likely that forensic reports mention it. Expert witnesses assist the judges to describe how the hash comparison can be used to prove integrity. Such a procedure enhances the reputation of electronic evidence when properly documented.

Nonetheless, the technical knowledge can be different in various courts. Even though there is a growing tendency of the higher courts toward the necessity of scientific validation, the trial courts may occasionally rely heavily on expert interpretation. This brings to the fore the fact that there should be more technological awareness in the judicial system.

Chain of Custody Standards and Preservation Standards.

Hash values are directly related to the term chain of custody the registered account of evidence gathering, treatment, custody, and transference. It is due to the fact that digital files are not only easy to copy or alter that strict procedures of handling them are crucial.

A good forensic practice usually comprises of:

i. Creation of hash values right after seizure.
ii. Production of forensic images rather than the investigation of original devices.
iii. Storing the original media in a secure manner.
iv. Enhancing records of all transfers or access.
v. Recomputation of hash values during various stages of investigation.

Failure to follow these steps means that the integrity of the evidence can be doubted. The courts can then diminish its weight of evidence or even dismiss it.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2332-2336

Although the use of hash verification in forensic practice is widely used, India is yet to address the issues of statutory guidelines that provide a clear definition of standardized digital preservation practices. A lot is based on laboratory procedures and professional skills. The confidence in digital evidence would be increased by bolstering formal standards and judicial training.

Digital Signature and Legality.

The real world is commonly used to bring out authenticity by means of a handwritten signature. Courts compare the handwriting, test the ink or use witnesses. Such old ways cannot work in the digital world. Electronic documents are transferred across networks immediately, they can be copied endlessly, and they can be modified without any traces. This brings up a basic legal issue; how do we know with the certainty that an electronic document was signed by a specific person and that it was not altered?

It is on this concern that digital signatures were introduced. They are not copied pictures of handwritten signatures but they are state-of-the-art tools that are installed to make sure that there is authenticity and integrity. Digital signatures are legally established in Indian law and thus, secure electronic transactions, governance, and reliability of evidence in courts are achieved.

Digital signatures use the so-called asymmetric cryptography system that has two keys that are interrelated:

i. A secret key, which is known to the signer.
ii. Public key, which is visible in a manner that anyone who has to verify the signature.

Digital signatures, in which an individual signs a document with the help of the personal key, produce a unique encrypted code. It is a mathematically connected code to the content of the document by a hash value. Should there be any small change to the document following the signing of such documents such as the addition of a comma or changing the number in any way the hash value will change resulting in the invalidity of the signature.

The public key can then be used by the recipient to arrive at the signature. Effective certification establishes two important facts:

i. The signatory was the one that holds the private key.
ii. The content has not been varied since then of signing.

In this way, the digital signatures will be used with two purposes: to verify the identity of the signer, and to ensure that the document is not altered. The combination of this makes them especially useful in court.

Legal Recognition in the Information Technology Act, 2000

Digital signatures within India are given statutory basis by Information Technology Act, 2000. Section 3 elaborates on the technical process of authentication of asymmetric cryptography and hash functions. The law does not solely rely on technological practice to leave the issue of digital verification to it, but these concepts are explicitly introduced in it.

Section 5 goes even further to reinforce this framework by providing legal status to electronic and digital signatures. It explains that in case law needs a signature then the need is met as long as the document is signed with a legalized electronic procedure. As a matter of practicality, this puts digital signatures at the same legal status as handwritten signatures, assuming that the specified conditions of the statutes are met.

This appreciation has been revolutionary. It has made electronic contracts, online filings, government services and corporate compliance processes to operate with legal confidence.

The legal establishment also presents the notion of safe electronic records. An electronic record can be deemed secure by law when security procedures are adhered to by the prescribed procedures. Where there is such a case, the court can assume that the record has not been distorted, unless proven to the contrary.

This assumption has an influential evidentiary purpose. Rather than putting the whole burden on the party which is depending on the electronic document, the law can impose the burden on the other party to prove tampering or invalidity. These assumptions lead to a greater trust in the digitally signed records, particularly in business and governmental areas.

These protections are however not automatic. They are used in those situations where the procedural and technical protection measures, which are established by the law, will be followed strictly. Evanescent evidentiary strength can be compromised by improper issuance, lax security practices or weakened private key.

Certifying Authorities Role.

It is the trust in the system that issues the digital signatures that ultimately determines the reliability of digital signatures. Certifying Authorities (CAs) are important at this point. These licensed bodies identify the identity of individuals or organizations and give out Digital Signature Certificates (DSCs).

The Certifying Authorities are supervised by the regulatory authority to achieve:

i. appropriate identity check.
ii. Adequate generation and control of keys.
iii. Observation of maintenance of prescribed technical standards.
iv. Cancellation or suspension of certificates when required.

The system progresses by instituting controlled supervision and goes beyond trust arrangements at the individual level and establishes institutional credibility. The courts are not just limited to the claims made with regards to technology but have a systematic system of certification with the support of statutory mandate.

Judicial Interpretation

The electronic evidence in India has, in most respects, been a judicial story. Whereas the statutory framework was laid down by Parliament, it did not have to interpret how these provisions would work in the actual courtroom circumstances but it was the courts which had to interpret. The use of judges with fast changing technology CDs, call data records, emails, and server logs were presented at a time when procedural clarity was still in its early stages. The Supreme Court over a span of cases gradually tightened the legal stance, away from being flexible and then strict compliance before settling on a more sensible and moderate stance.

In ***State (NCT of Delhi) v. Navjot Sandhu*** also commonly known as the Parliament Attack case, the Supreme Court was forced to examine the admissibility of electronic evidence like the call data records.

The section 65B certification law then was still new and not well comprehended. The Court was flexible in its perspective. It was presumed that where the particular certificate that is necessary under Section 65B was not produced, electronic evidence could still be provided according to other provisions in connection with secondary evidence.This method signified an expedient issue: the Court did not wish the vital evidence to be omitted only on technical reasons. Nonetheless, the decision was well-intended but it generated uncertainty. So, what was the purpose of the existence of Section 65B had it not been mandatory? Different standards were introduced in trial courts and this created inconsistency. Almost ten years later the Supreme Court took up the case again in ***Anvar P.V. v. P.K. Basheer***. This ruling headed a new beginning. The Court reversed Navjot Sandhu and concluded that the requirements of adhering to Section 65B is applicable when the electronic evidence is generated in a secondary form (as in CDs, printouts, or copied files). The certificate requirement ceased being optional and made obtainment of a certificate a mandatory admissibility requirement.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1, 2026, Pages: 2332-2336

This argument was simple: electronic records are not similar to paper records. They can be easier changed and manipulated. Thus, the legislature wittingly made a special procedure to protect their originality. By referencing general clauses of evidence law, the courts could not circumvent such a procedure.

Although this ruling provided a doctrinal clarity, it caused difficulties practical challenges. Litigants frequently found it hard to get as well as get the certificates, particularly when the pertinent electronic records were in the power of third parties, e.g., telecom providers or corporate bodies. In numerous situations, the electronic evidence was denied just due to the lack of the certificate.

On realizing the misunderstanding and suffering that had encircled the case, the Supreme Court attempted to look at the matter in the case of ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.***

The Court reiterated that the certificate requirement is actually binding. Nevertheless, it helped to understand a number of significant things: The certificate must be made in the case of an electronic evidence production in secondary form. In case the original device itself is manufactured prior to the court, it might not require certification.

In the event that one of the parties is truly incapable of getting the certificate though acting in good faith, the court can permit some proper procedural measures to facilitate adherence.

This sentence brought about sanity. It upheld statutory discipline and accepted practical realities. The Court stated that procedural rules must not subvert substantive justice, particularly in a time when electronic records are the overwhelming hours in business and criminal litigation.

Conclusion

The Indian legislation of evidence has experienced a radical change with regard to digitalization. Electronic records cannot be considered extraordinary anymore, as they tend to be the main piece of evidence. India has grown in a systematic approach of dealing with the issues of authenticity and integrity through a legislative change and scope of judicial interpretation.

The technical security measures like metadata analysis, hash verification and digital signature are important in guaranteeing reliability. Meanwhile, the success of such a framework is determined by well-built forensic institutions, judicial effectiveness, and dynamic legal norms.

The digital age is turning to the invisible technological processes in the pursuit of justice which is not based on physical documents. The issue facing the Indian legal system is not that it should accept electronic evidence, but that they should know it fully and make it work in a prudent manner. At the same time, as institutional strengthening, further reform, and informed adjudication, digital evidence may contribute more than complicate the quest to seek fairness and due process.

References

1) State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
2) Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
3) Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
4) Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
5) Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570.
6) Avtar Singh, *Cyber Law and Information Technology*, 3rd edn., Eastern Book Company, Lucknow (2021).
7) Yatindra Singh, *Cyber Laws*, 5th edn., Universal Law Publishing Co., New Delhi (2018).
8) Aparna Viswanathan, *Cyber Law: Indian and International Perspectives*, 1st edn., LexisNexis Butterworths, New Delhi (2007).
9) Stephen Mason & Daniel Seng, *Electronic Evidence and Electronic Signatures*, 5th edn., Institute of Advanced Legal Studies, London (2021).
10) Paul R. Rice, *Electronic Evidence: Law and Practice*, 3rd edn., American Bar Association, Chicago (2018).
11) Law Commission of India, 185th Report on Review of the Indian Evidence Act, 1872 (2003).
12) Stephen Mason, "Electronic Evidence and the Challenges of Digital Authentication," *Computer Law & Security Review*, Vol. 26, Issue 4 (2010).
13) National Institute of Standards and Technology (NIST), *Guidelines on Mobile Device Forensics*, Special Publication 800-101 Rev. 1 (2014).
14) Ministry of Electronics and Information Technology (MeitY), Government of India, available at: https://www.meity.gov.in (last visited on 20 February 2026).
15) e-Committee, Supreme Court of India, available at: https://ecourts.gov.in (last visited on 20 February 2026).
16) Controller of Certifying Authorities (CCA), Government of India, available at: https://cca.gov.in (last visited on 20 February 2026).
17) National Cyber Crime Reporting Portal, Ministry of Home Affairs, available at: https://cybercrime.gov.in (last visited on 20 February 2026).
18) National Institute of Standards and Technology (NIST), U.S. Department of Commerce, available at: https://www.nist.gov (last visited on 20 February 2026).
19) The United Kingdom Judiciary, available at: https://www.judiciary.uk (last visited on 20 February 2026).
20) United States Courts – Federal Rules of Evidence, available at: https://www.uscourts.gov (last visited on 20 February 2026).