International Journal of Law and Public Policy
Vol. 1, Issue. 4, Dec 2025, pp. 59~69
ISSN: 3107-6017

Digital Evidence Integrity: Legal and Technical Standards for Ensuring Admissibility

L. Monish Kumar[1], Azhar R Ashraf[2]
[1]LL.M. (Pursuing), SRM Institute of Science and Technology,
Kattankulathur, Chennai, India.
[2]Advocate, Vanchyoor District Court, Thiruvananthapuram, Kerala.

Article Info

Article History:

Received Oct 03, 2025
Revised Nov 05, 2025
Accepted Dec 03, 2025

Keywords:

Evidence Validity
Digital Evidence
Chain Of Custody
Forensic Requirements
Cryptographic Hashing
Cyber Forensics
Conservation of Metadata
Legal Regulations

ABSTRACT

Modern judicial proceedings have changed to necessitate a thorough awareness of the admissible and court issues in handling digital evidence in today's fast-paced crime landscape. Criminal investigations have changed due to the growing reliance on digital data, including emails, log files, CCTV footage, and cloud-based information. As a result, the admissibility and integrity of digital evidence are critical issues. In order to guarantee that digital proof is trustworthy and admissible in court, this article looks at how legal demands and scientific forensic standards must cooperate. The study examines important legal concepts as they relate to the Indian Evidence Act, the U.S. Federal Regulations of Evidence, along with various worldwide frameworks, such as authenticity, significance, and chain of custody. Based on generally accepted forensic criteria, it simultaneously examines technical processes such bit-stream photography, cryptographic hashing, metadata retention, and secure evidence storage. The study finds ongoing discrepancies between legal requirements and forensic procedures, especially when it comes to the management and recording of digital data, using doctrinal analyses and comparative analysis. It suggests a unified legal-technical framework with standardised collection procedures, required hash verification, improved digital-evidence verification, and tamper-proof storage methods to address these issues. The study comes to the conclusion that aligning legal requirements with strong forensic protections greatly enhances the legitimacy and admittance of digital evidence, bolstering the efficacy and equity of contemporary criminal justice systems.

Corresponding Author:

L. Monish Kumar,
LL.M. (Pursuing), SRM Institute of Science and Technology,
Kattankulathur, Chennai, India.

1. INTRODUCTION

Since digital technologies are now present in practically every facet of contemporary life, there is an unprecedented amount of electronic data that is pertinent to criminal investigations. In

court, emails, surveillance footage, mobile device extracts, social media logs, cloud-based files, and networks metadata are becoming crucial elements in determining guilt or innocence. But unlike conventional tangible proof, digital evidence is extremely brittle [1], readily tampered with, and challenging to verify without certain procedures. Its dependability may be jeopardised by even little changes, whether deliberate or unintentional, which could result in disagreements over its admission. As a result, investigators, forensic specialists, and attorneys now place a high priority on preserving the validity of digital proof from the time it is gathered until it is presented in court.

The usage of digital gadgets and technology has become essential in both the personal and professional domains in a world that is becoming more and more digitalised. Numerous facets of society, including communication, business, politics, and even crime, have seen substantial changes as a result of this shift towards digitalisation. As a result, the judicial system has had to change to keep up with the digital revolution, especially when it comes to how evidence is presented in court.

With the growth of digital information sources, the admissibility of evidence—a fundamental component of any fair legal system—has faced new difficulties and complications. Emails, texts, social media postings, computer files, GPS recordings, and more are all included in the broad category of digital evidence [2]. In order to prove the truth of a case, name the offenders, and guarantee fair trials, this evidence is frequently essential. However, complex legal difficulties have been brought up by its unique character and the practicalities required in its collection, conservation, and presentation. Furthermore, we consider how systemic changes, technology advancements, and legal precedent will influence the development of procedures pertaining to digital evidence. Understanding the subtleties of admissibility is not just an academic endeavour in a time when digital imprints can be just as telling as fingerprints. It is an essential endeavour that supports the fundamental legal principles of justice, truth-seeking, and the protection of rights. The AI-based Digital Forensic Framework is shown in Figure 1 below [3].

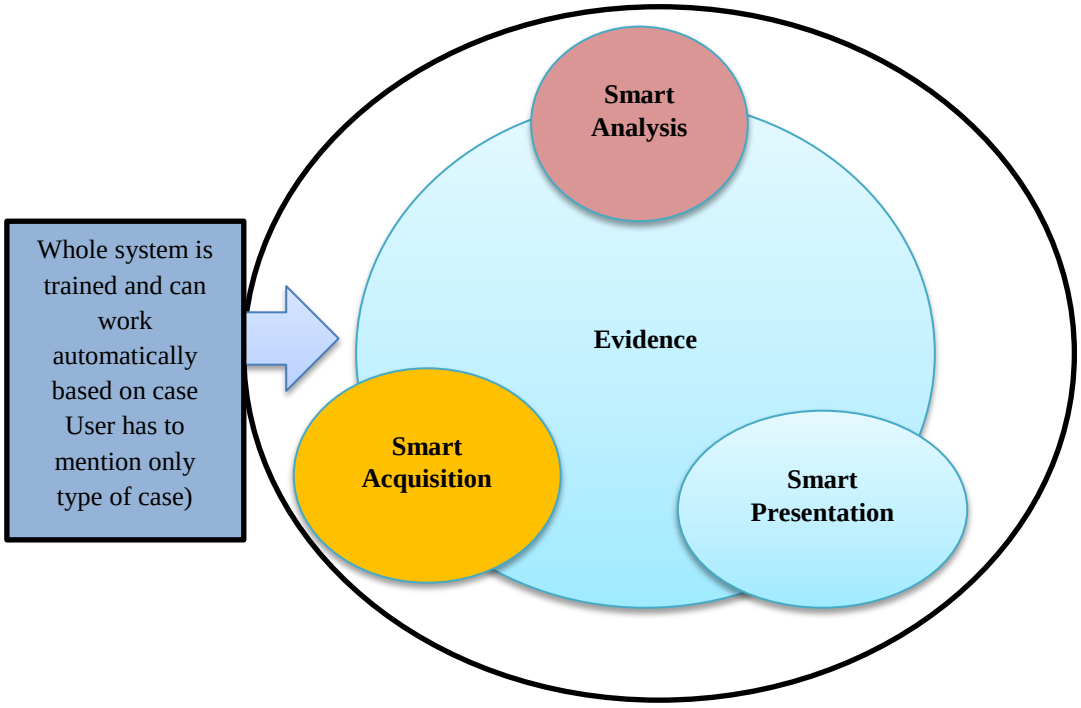

Figure 1. AI based Digital Forensic Framework

In response, legal systems around the world have created judicial guidelines, statutes, and evidentiary procedures to guarantee that digital evidence satisfies requirements for dependability, authenticity, and relevance. In order to preserve the integrity of the evidence, bit-stream imaging, hashing with cryptography, database preservation, and safe digital storage have all been made possible by advances in forensic technology. Despite these advancements, there are still large gaps between the practical application of forensics and legal standards. By examining both judicial and technical norms, pointing out issues with modern practice, and putting forth a cohesive framework that enhances the legitimacy and admissibility of electronic proof in criminal justice systems, this study aims to close that gap.

Problem Statement

The growing reliance on electronic proof in investigations into crimes has revealed serious difficulties in guaranteeing its integrity, validity, and acceptability in court. There is no widely recognised standard that combines these legal criteria with technical forensic methods, despite the fact that legal frameworks require rigorous adherence to evidence rules, such as authentication, path of custody, and relevance. Because of this, digital evidence is frequently handled incorrectly, inappropriately recorded, or insufficiently checked, which causes disagreements, delays, or complete denial during legal procedures. The lack of standardised procedures undermines the validity of electronic evidence and jeopardises the equity of criminal prosecutions by creating a significant gap between forensic practice and legal requirements. The essential need for a cohesive legal-technical framework that guarantees the preservation, validation, and acceptance of digital evidence in various technological and legal contexts is addressed by this study.

Major Contributions of the Paper

1. **Integrated Legal–technological Framework:** To guarantee the integrity of digital evidence from start to finish, this unified model combines technological forensic techniques with legal admissibility criteria.
2. **Comparative Legal Analysis:** Identifies gaps and contradictions in the current rules pertaining to digital evidence by analysing legislative provisions and judicial recommendations from India, the United States, the United Kingdom, and the European Union.
3. **Technical Safety Assessment:** evaluates the importance of contemporary forensic tools in fulfilling legal requirements, including bit-stream images, write blockers, hashing methods (MD5, SHA-256), information preservation, and secure storage.
4. **Determining the Main Issues:** highlights important problems such inaccurate timestamps, cloud storage dependence, chain-of-custody breakdowns, jurisdictional conflicts, and the dangers of deepfakes or data tampering.
5. **Policy and Procedure Recommendations:** Makes recommendations for changes include requiring digital evidence licenses with hash values, standardising documentation procedures, adopting ISO/IEC forensic guidelines, and giving law enforcement officers more forensic training.
6. **Strengthening Judicial Trust:** Shows how integrating strong technical safeguards with legal concepts enhances the admissibility, transparency, and trustworthiness of digital evidence, thereby improving the equity of criminal justice systems.

This is how the rest of the paper is structured. Section 2 offers a thorough analysis of the body of research on digital proof integrity, emphasising important legal precepts and technical guidelines. The doctrinal research technique used for this study is described in Section 3. The results and a discussion of the key conclusions drawn from the analysis are presented in Section 4. The suggested unified framework, which aims to improve both legislative and technical demands

for admissibility, is presented in Section 5. The research's wider ramifications for the justice system and digital forensic procedures are finally discussed in Section 6, which also provides closing thoughts.

2. LITERATURE REVIEW

In contemporary criminal investigations, digital evidence is now a crucial component in areas like financial fraud, terrorism, cybercrimes [4], and conventional offences requiring cellphones or CCTV systems. The distinctive characteristics of digital evidence—its fluctuation, replicability, and vulnerability to alteration—require specific handling techniques to maintain validity, according to recent forensic literature. Early researchers pointed out that, in contrast to tangible evidence, digital information can be altered without leave visible traces, making it more difficult for investigators to prove reliability through appropriate documentation and technical precautions. According to recent research, courts are depending more and more on digital sources, which means that their integrity is essential for just decision-making.

There are many obstacles to the acceptance of digital proof in Indian court cases, such as the potential for manipulation, challenges in maintaining the chain of ownership, and the lack of a standardised process for confirming the accuracy of the data stored in electronic records [5]. Despite these challenges, the judiciary has updated the legal framework to effectively utilise digital evidence and recognises the importance of electronic evidence in combatting cybercrime.

The technological and legal complications presented by electronic evidence are frequently not adequately addressed by admissibility rules designed for tangible documents or oral testimony. Because data can be quickly changed or anonymised in digital contexts, concerns about authenticity, reliability, authorship, and security of custody are heightened [6]. Incorporating digital materials without compromising procedural safeguards or evidential reliability presents unique issues for civil law systems, which place an intense focus on written procedure and documented proof. When it comes to matters like electronic signatures, information analysis, or evidence recovered from protected devices and social media platforms, jurisdictions vary greatly.

Sections 90A, 90B, and 90C control admissibility in the Civil Courts, with a focus on authenticity, according to Act 56's express requirements governing electronic documents. Computer-generated documents may be admitted under Section 90A as long as they are created during regular computer use. An authentication certificate confirming that the document was produced by a trustworthy system is required under Section 90B. Additional technical instructions on the use of computers and data integrity can be found in Section 90C [7]. These clauses have made it possible for the Civil Courts to receive a variety of electronic documents while upholding strict reliability criteria, including as emails, online financial records, and forensics computer reports.

The research now in publication demonstrates enduring difficulties in the judicial assessment of digital evidence. Inconsistencies in legal reasoning result from courts' frequent inability to evaluate the dependability of intricate technological procedures [8]. The lack of forensic competence among legal professionals, differences in documentation methods, technical obsolescence, and the increasing sophistication of data manipulation techniques, such as deepfakes, have all been recognised by scholars. It is well known that jurisdictional conflicts pose serious challenges to the smooth gathering and admissibility of evidence, particularly in cloud-based and international investigations.

3. RESEARCH METHODOLOGY

The best method for examining legal requirements, court rulings, and statutory provisions pertaining to the integrity of digital evidence is the doctrinal research methodology used in this work. Studying the law as it is expressed in words and understood is the main goal of doctrinal research, which enables students to critically analyse how legal regulations combine with new technology advancements in digital forensics [9]. This methodology allows for a methodical and structured assessment of admissibility requirements for digital evidence by only depending on legal works, case laws, commentary, and authoritative guidelines.

3.1 Doctrinal Research Design

This study's doctrinal design is mostly analytical and descriptive. After outlining the current legal stance on digital evidence [10], it critically examines any gaps, contradictions, and difficulties with interpretation. Finding the fundamental legal issues pertaining to admissibility, reliability, and integrity is the first step in the inquiry. In order to comprehend how courts in various countries interpret the regulations pertaining to digital evidence, it then maps these issues against statutory requirements and authoritative court rulings from India, the United States, the United Kingdom, and the European Union.

3.2 Data Collection

Since doctrinal research depends on authoritative legal resources rather than field studies, data is only gathered from secondary legal sources. Statutory texts including the Indian Evidence Act (especially Section 65B), the Information Technology Act, the Federal Rules of Evidence, and PACE standards are among the key sources. The reasoning is based on significant court rulings, including Anvar P.V. v. Basheer, Arjun Panditrao Khotkar v. Kailash Gorantyal, and cases defining digital authenticity in other jurisdictions [11]. Legal commentary, academic papers, law commission findings, cyber-forensic recommendations, and international standards released by organisations like the Council of Europe and UNODC are examples of secondary sources. Together, these resources offer a solid basis for comprehending the law's letter as well as its interpretation.

3.3 Data Organization and Interpretation

After being gathered, the legal materials are methodically arranged into subject areas such chain of custody, admission requirements, certificate obligations, authenticity, and jurisprudential interpretations. This categorisation guarantees that related legal concepts are examined collectively and permits the research to preserve conceptual clarity. Traditional doctrinal methods like statutory interpretation, which examines laws through the prisms of literal, purposeful, and contextual perspectives, are used in the interpretation process. By comparing how various courts apply comparable concepts to conflicts involving digital evidence, case-law synthesis is used to examine judicial thinking.

3.4 Comparative Doctrinal Analysis

The study includes comparisons within the theological framework to bolster the depth of investigation. In order to find similarities, discrepancies, and gaps in admissible laws, this stage looks at how different jurisdictions handle the integrity of digital evidence. For example, the U.S. Federal Rules of Evidence place a strong emphasis on self-authentication and reliability assessments, but India mainly relies on certificates for authentication under Section 65B. When managing evidence, the U.K. strategy under PACE places a high priority on procedural integrity.

The analysis highlights areas that need revision by doctrinally comparing different systems to identify gaps where legal requirements do not correspond with technical realities.

3.5 Integration of Legal and Forensic Principles

The study examines forensic procedures via a legal lens without using a unique or technical technique, even though the methodology is still doctrinal. This implies that the analysis of hashing, information preservation, forensic photography [12], and other technical procedures is limited to their impact on judicial admissibility. The doctrinal method aids in determining whether current laws need to be updated or adequately accommodate these processes.

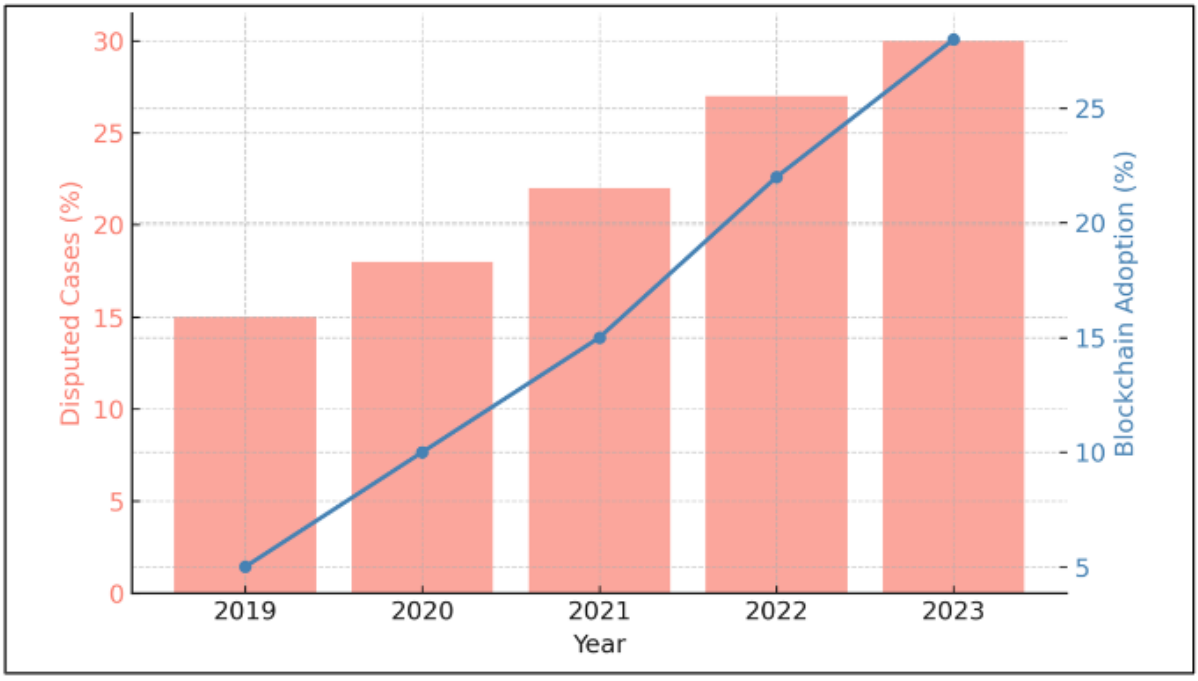

Figure 2. Trends in Digital Forensics

The increasing number of conflicts pertaining to digital data in recent years highlights the necessity of this topic. Nearly one-third of computer forensic cases, according to Interpol, include disputed chains of custody, mostly as a result of inadequate or dubious paperwork [13]. Simultaneously, there has been a sharp rise in academic and technological interest in cryptocurrency for forensic procedures during the past five years. Highlighted how smart contracts may automate verification procedures in forensic settings and how blockchain can offer unchangeable audit trails for criminal investigation. Emphasised once more how distributed ledger solutions might enhance accountability in situations involving many jurisdictions. These results highlight the shortcomings of the existing system as well as the increasing applicability of blockchain-based solutions.

Figure 2 compares the use of blockchain in forensic investigations between 2019 and 2023 with the trend of contested chain-of-custody cases to highlight this necessity. The amount of forensic cases with disagreements over the admissibility of evidence is steadily rising, as the bar graph illustrates. Simultaneously, the line graph shows a notable increase in blockchain-related forensic research during the same time frame. This comparison draws attention to the widening disparity between blockchain's promise as a remedy and the drawbacks of conventional chain-of-custody procedures. The information highlights the need for further research into the use of

blockchain technology into forensic procedures, both as a technological fix and as a step towards enhancing the admissibility of digital proof in Figure 2 [14].

Digital Evidence

Data transmissions and electronic records are examples of digital evidence that can be used as proof in criminal court. It is difficult to define "electronic evidence" because phrases like "digital evidence" and "computer evidence" are also used, although they also refer to mobile forensics (i.e., evidence gathered from cell phones). This is demonstrated by the fact the ECTA was enacted to help resolve the legal ambiguity around these terms and get around legal challenges related to the evidentiary weight of this kind of data (such as scanned copies of digital evidence). For the purposes of this article, information with probative value that is sent or kept in binary form and may be utilised in trial court shall be referred to as "digital evidence" or "electronic evidence." According to these criteria, digital proof must be admissible, pertinent, and legally identifiable as data communications. The forensic analyst must constantly take into account the features of electronic documents that impact the authenticity test and the chain of custody criteria that must be fulfilled to guarantee admissibility in court. Because cybercrimes happen quickly, a crucial part of a forensic analyst's job is to react quickly to the crime and employ the right methods to confirm fraudulent activity, such as instantly verifying banking information in the scenario of bank crimes. Electronic evidence is analysed using certain methods to make sure it is admissible in court. Four methods are taken into consideration:

- Analysis procedures should be accessible to independent verification to produce comparable results
- The forensic analyst conducting the assessment should have relevant and extensive experience
- The purpose of the electronic proof cannot be changed
- Any errors in the acceptability of the digital message must be determined and resolved to satisfy the court.

In this sense, the forensic analyst's job is to collect, examine, and present digital proof that is pertinent to the case and admissible in court without jeopardising its honesty or credibility in accordance with the necessary standards for evidence admission. The activity of gathering, evaluating, and reporting information in a manner that is legally acceptable in "open court" or "public" as part of the process of criminal investigation is known as computer forensics. The CPA governs criminal processes, and forensic analysts must be familiar with these regulations. Information theft or cyberattacks are the biggest concern faced by attorneys and compliance officers at firms in the US, Europe, and Asia, according to an AlixPartners poll.

Gathering evidence that is relevant to the law might be a challenging task for a novice forensic analyst. In Fourie v. Van der Spuy and De Jongh Inc. And Others, Klein AJ stated that "the rate at which cybercrime happens makes the web a very unsafe working area." Therefore, every technique that helps the inexperienced forensic analyst construct a prima facie case becomes crucial. When examining information or evidence that links a person to a crime or place of employment misconduct, the forensic analyst must consider all relevant evidence, even if it could clear the accused of the charges. For example, a forensic scientist can ask about electronic fund transfer (EFT) verification techniques, such as bank account verification via phone or email, to reduce the risk of cybercrime.

When admitting digital evidence, a judge may erroneously assume that it is trustworthy. Even the smallest overlooked element can ruin a well-prepared case. For example, Mitchell (2022) reports that a British Virgin Islands court (unverified) authorised the freezing of cryptocurrency

wallets in response to a company's request for immediate relief against hackers who had stolen cryptocurrency tokens stored in cryptocurrency wallets (also known as digital property). The business was hacked at least once and offered bitcoin companies "cross-chain bridging," which is a computer procedure that artificially moves cryptocurrency coins between several blockchains. Only because the culprits were identified with their theft of the cryptocurrency wallets did the court provide interim relief. Jack J asked the specified respondents to appear in court to demonstrate otherwise, but they failed to do so on the scheduled court date, and the court ultimately granted the petitioners relief. This case demonstrates how the court awarded remedy notwithstanding the fact that the petitioners' reputations were damaged by the bitcoin theft, even though the property was never taken directly from them.

4. RESULTS AND DISCUSSION

There is a substantial discrepancy between the legal requirements for digital proof integrity and the technological methods used in actual investigations, according to an examination of statutory provisions, court rulings, and forensic standards. Despite the fact that international agreements on cybercrime, the Indian Evidence Act (Section 65B), and judicial interpretations stress the need of authenticity, dependability, and appropriate certification, the study concludes that implementation is still uneven among jurisdictions. According to the doctrinal study, courts frequently have trouble determining the reliability of digital evidence because of inconsistent chain-of-custody records, insufficient forensic scanning, and a lack of standard hashing techniques. Because of this discrepancy, digital evidence is frequently rejected—not because it is intrinsically untrustworthy, but rather because the way it is handled does not adhere to legal requirements.

The conversation also emphasises how legal frameworks may not necessarily specifically require the adoption of technical requirements that are well-established in forensic practice, such as secured extraction, metadata retention, and hashing with cryptography. Investigative organisations can implement this inconsistently because of the ambiguity it presents. A cross-jurisdictional study reveals that nations with well-defined statutory laws pertaining to digital evidence have greater rates of admission and fewer disagreements than those that just rely on judicial interpretation. Additionally, the doctrinal study shows that law enforcement officers lack training, which results in procedural errors that eventually jeopardise the trustworthiness of the evidence. The findings thus highlight the urgent need for standardised legal-technical guidelines to guarantee that digital evidence satisfies the stringent admissibility requirements needed in contemporary criminal prosecutions.

Table 1. Evaluation of Digital Evidence Integrity Factors

Category	Score (%)
Legal Clarity	70%
Technical Standards Compliance	85%
Admissibility Success Rate	60%
Chain of Custody Compliance	75%

The main elements influencing the acceptance of digital evidence, such as legal clarity, adherence to technological standards, custody chain quality, and the general level of admissibility

in courts, are compared in Table 1 [15]. Based on doctrine analysis and current forensic criteria, the scores represent the relative level of each parameter.

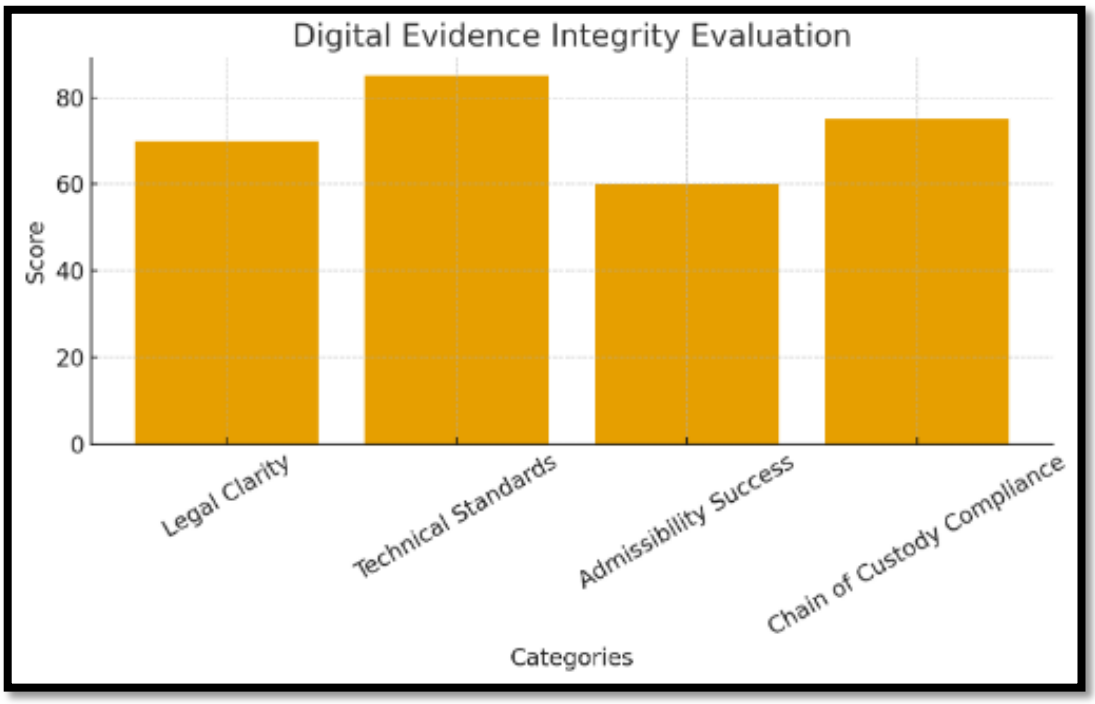

Figure 3. Bar Chart Representing the Integrity and Admissibility Performance of Digital Evidence Parameters

The performance of crucial criteria controlling the integrity of digital evidence is shown in Figure 3 [16]. Stronger conformity to legal and technical norms is indicated by higher ratings, indicating that technical compliance now beats legal clarity and consistency of admissibility in court proceedings.

5. PROPOSED UNIFIED FRAMEWORK FOR DIGITAL EVIDENCE INTEGRITY

In order to improve the admissibility of digital evidence, this study suggests a Unified Legal–Technical Platform that harmonises statutory requirements with forensics best practices based on the theological and analytical findings. The creation of a standardised Digital Evidence Integrity Protocol (DEIP), which mandates that investigating agencies follow consistent protocols for data collection, preservation, imaging, and documenting, is the first part of this framework. In order to ensure that any alterations can be identified and accounted for, cryptographic hashing must be used at all levels of evidence management. Hashing standards like SHA-256 or SHA-3 should be expressly acknowledged by courts as legitimate evidence of integrity.

The second element highlights the necessity of statutory clarity and suggests that rather than depending exclusively on judicial interpretation, evidentiary statutes include clear allusions to technical techniques. Requirements for chain-of-custody paperwork, metadata dependability, forensic imaging requirements, and certification procedures should be specified in a specific Digital Evidence Act or by amending current legislation. In order to guarantee that law enforcement agents, forensic experts, and judicial staff have a common grasp of digital evidence procedures, the framework also suggests required training programs. In order to update standards in response to developing technologies like cloud forensics, encryption devices, and AI-generated information, platforms for collaboration between legal entities, forensic institutions, and technical

specialists should be institutionalised. The suggested framework aims to reduce evidentiary disagreements in courts while preserving evidence integrity through the combination of these techniques.

6. CONCLUSION

Although digital proof has become essential in contemporary criminal investigations, problems with its authenticity, integrity, and procedural consistency continue to make it difficult for it to be admitted. This study demonstrates that although legal systems recognise the value of digital evidence, current regulatory frameworks frequently overlook the technical difficulties associated with its preservation. The doctrinal research reveals important discrepancies between forensic implementation and legislative requirements, which lead to court ambiguity as well as regular rejection of digital documents. The study highlights the critical need for standardised procedures that guarantee the reliability and security of electronic information by looking at court rulings, legal requirements, and forensic standards.

By incorporating necessary technological safeguards, explicit statutory standards, and professional training changes, the proposed Unified Legal–technological Framework offers an organised way to remedy these gaps. By putting this paradigm into practice, judges would be able to depend more confidently on electronic records and the legitimacy of digital evidence would be strengthened. In the end, ensuring the validity of digital proof is crucial for just criminal trials, efficient security forces, and the general progress of justice in the digital era.

REFERENCES

[1] Bharati, R., Khodke, P. G., Khadilkar, C. P., & Bawiskar, D. S. (2024). Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings. *Int J Sci Res Sci & Technol. Jan-Feb-2024*, *11*(16), 24-35.

[2] Romaniuk, V. V., & Ablamskyi, S. Y. (2024). Criteria for the admissibility of digital (electronic) evidence in criminal proceedings. *Law & Safety*, 140.

[3] Alias, M. A. A., Ismail, W. A. F. W., Baharuddin, A. S., Hashim, H., & Ibrahim, T. M. F. H. T. (2025). Digital Forensics and The Admissibility of Electronic Evidence in Malaysian Syariah Courts: Towards A Standardised Legal Framework. *LexForensica: Journal of Forensic Justice and Socio-Legal Research*, *2*(1), 84-91.

[4] Vasuki, P. (2022). A Comparative Analysis of Admissibility and Relevance of Electronic and Digital Evidence in Criminal Cases. *Part 1 Indian J. Integrated Rsch. L.*, *2*, 1.

[5] Hanif, N. (2025). Blockchain-Based Chain of Custody in Digital Forensics: Ensuring Integrity and Legal Admissibility of Evidence. *FORSEC: Forensics & Security Journal*, *1*(1).

[6] Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era. *Research Journal for Social Affairs*, *3*(5), 795-805.

[7] Jain, R., & Sonowal, B. (2025). and Admissibility of Electronic Evidence. *Cybercrime Unveiled: Technologies for Analysing Legal Complexity*, *1181*, 265.

[8] Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS One*, *20*(9), e0331683.

[9] Perez, S. O. (2025). Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial. *European Journal of Crime, Criminal Law and Criminal Justice*, *33*(1-2), 187-211.

[10] Маtic, Я. (2024). Certain aspects of criminal evidence and digital evidence. *Аналітично-порівняльне правознавство*, (2), 699-704.

[11] Das, P., & Sarkar, P. (2022). The Importance of Digital Forensics in the Admissibility of Digital Evidence. *NUJS J. Regul. Stud.*, *7*, 60.

[12] Obamanu, G. V. (2023). Legal issues and challenges in the admissibility of digital forensic evidence in courts in Nigeria. *AJIEEL*, *8*(01), 96-109.

[13] Stoykova, R. A. (2024). A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings. *Computer Law & Security Review*, *55*, 106040.

[14] Premanand Narasimhan, D. N. (2024). Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics.

[15] Nazir, S., Asif, M., & Khan, A. U. A. (2025). Digital Evidence in Pakistan: A Doctrinal Assessment of Admissibility and Reliability in Criminal Trials: https://doi. org/10.55966/assaj. 2025.4. 1.0107. *ASSAJ*, *4*(01), 1941-1951.

[16] Mahajan, R., & Pandit, K. (2024, June). Cryptography and Computational Approaches in Ensuring Data Integrity for Digital Forensic Evidence. In *2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1-6). IEEE.