JUDICIAL APPROACHES TO THE ADMISSIBILITY OF DIGITAL EVIDENCE IN MAINLAND TANZANIA: LESSONS FROM INDIAN CRIMINAL JURISPRUDENCE

Donatus Nicholas Nditi, Law Lecturer, University of Iringa, Iringa, Tanzania.

Genoveva Asiimwe Byemelwa, Senior Resident Magistrate, Kagera, Tanzania.

ABSTRACT

Increment in digitization of social, commercial, and criminal activities has transformed the nature of evidence presented before courts. Digital evidence, including electronic communications, computer-generated records, mobile phone data, and digital forensic materials, has become central to modern criminal investigations and prosecutions. However, its admissibility raises complex questions concerning authenticity, reliability, integrity, and procedural safeguards. This article examines judicial approaches to the admissibility of digital evidence in Mainland Tanzania through a doctrinal analysis of statutory provisions, judicial decisions, and comparative jurisprudence from India. It argues that although Tanzania has introduced legislative mechanisms recognizing electronic evidence, judicial engagement with questions of authentication, chain of custody, and technological reliability remains underdeveloped. The article employs a qualitative legal research methodology, analyzing primary legal sources including the Evidence Act, Cybercrimes Act, and reported judicial decisions, alongside Indian jurisprudence under the Indian Evidence Act 1872, particularly section 65B. The article demonstrates that Indian courts have developed more structured principles for admitting electronic records, especially through judicial clarification of certification, authenticity, and reliability requirements. It concludes that Tanzanian courts should develop a clearer jurisprudential framework capable of balancing technological advancement with fair trial guarantees.

Keywords: Digital evidence; electronic records; admissibility; criminal litigation; Tanzania; India; evidence law.

1. Introduction

The emergence of digital technologies has fundamentally altered criminal behaviour and the methods through which criminal conduct is investigated and prosecuted. Contemporary crimes increasingly involve electronic communications, mobile devices, social media platforms, digital financial transactions, and computer-generated records. Consequently, courts across jurisdictions are confronted with the challenge of determining when digital materials should be accepted as legally admissible evidence and what safeguards should govern their use.[1] Digital evidence differs from traditional forms of evidence because it exists in intangible form, can be easily altered, duplicated, transferred, or destroyed, and often requires specialised technical procedures for collection and interpretation.[2] These characteristics create significant evidentiary concerns relating to authenticity, integrity, reliability, and the preservation of the chain of custody.[3]

In Mainland Tanzania, the increasing reliance on electronic evidence has occurred alongside reforms in information technology regulation, particularly through the amendment of evidentiary legislation and the enactment of cybercrime-related laws. The Evidence Act[4] recognizes electronic evidence, while the Cybercrimes Act[5] provides a regulatory framework for computer-related offences and digital investigations. However, despite these legislative developments, Tanzanian judicial practice on the admissibility of digital evidence remains relatively limited and lacks a comprehensive doctrinal framework. The central argument of this article is that Tanzanian courts have not yet fully developed consistent principles for evaluating digital evidence. While courts have demonstrated willingness to admit electronic materials where relevance and reliability are established, questions relating to authentication, forensic integrity, and procedural compliance remain insufficiently articulated. This creates uncertainty for prosecutors, defense counsel, investigators, and trial courts.

India provides a useful comparative jurisdiction because it has confronted similar challenges arising from rapid digital transformation. Indian courts have developed substantial jurisprudence concerning electronic evidence, particularly through interpretation of section

[1] Mason, S., and Seng, D., (eds), *Electronic Evidence and Electronic Signatures,* 5th edn, University of London Press, 2021, pp. 1–3.
[2] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet,* 3rd edn, Academic Press, 2011, pp. 7–10.
[3] Carrier, B., *File System Forensic Analysis,* Addison-Wesley, 2005, pp. 3–5.
[4] Cap. 6 R.E. 2022.
[5] Cap. 443 R.E. 2023.

65B of the Indian Evidence Act 1872. Decisions such as *Anvar PV v PK Basheer*[6] and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[7] have established detailed principles concerning certification, authenticity, and admissibility of electronic records. This article therefore examines whether lessons from Indian jurisprudence can assist Tanzanian courts in developing a coherent approach to digital evidence admissibility. It addresses three principal questions, i.e., what legal standards currently govern the admissibility of digital evidence in Mainland Tanzania?; how have Tanzanian courts approached authentication and reliability of electronic evidence?; and what lessons can Tanzania draw from Indian judicial developments?.

2. Conceptualizing Admissibility of Digital Evidence

Digital evidence refers to information stored or transmitted in digital form that may be used to establish facts in legal proceedings. The concept includes computer files, emails, mobile phone records, digital photographs, internet records, electronic financial transactions, and data extracted from electronic devices.[8] The International Organization for Standardization defines digital evidence as information of probative value that is stored or transmitted in digital form.[9] Unlike physical evidence, digital evidence does not depend upon physical possession but upon maintaining the integrity of electronic data throughout its collection, preservation, analysis, and presentation before court.

The distinctive characteristics of digital evidence create both opportunities and challenges. On one hand, digital records may provide highly accurate information concerning criminal conduct. For example, mobile phone location data may establish the presence of an accused person at a particular place, while electronic transactions may reveal financial offences. On the other hand, digital information may be vulnerable to manipulation, unauthorized access, or incomplete extraction.[10] Accordingly, admissibility requires courts to consider not merely whether digital evidence is relevant, but whether it has been collected and preserved through reliable procedures capable of ensuring authenticity.

[6] (2014) 10 SCC 473.
[7] (2020) 7 SCC 1.
[8] Mason, S., and Seng, D., (eds), Mason, S., and Seng, D., (eds), ibid., p. 45.
[9] ISO/IEC 27037:2012, *Information technology—Security techniques—Guidelines for identification, collection, acquisition and preservation of digital evidence*, para. 3.5.
[10] Casey, E., ibid., pp. 17–19.

3. Legal Foundations for Digital Evidence in Tanzania

The legal framework governing digital evidence in Mainland Tanzania is primarily founded on the Evidence Act[11] and the Electronic Transactions Act,[12] complemented by the Cybercrimes Act,[13] the Criminal Procedure Act,[14] and the National Prosecutions Service Act.[15] These statutes collectively regulate the admissibility, collection, preservation, authentication, and presentation of electronic evidence in judicial proceedings.

3.1. The Constitution of the United Republic of Tanzania.[16]

Although the Constitution does not expressly regulate digital evidence, it provides the constitutional foundation for the admissibility and use of electronic evidence through the protection of fundamental rights and fair trial guarantees. Article 13(6)(a) guarantees every accused person the right to a fair hearing before an independent and impartial court. Consequently, courts admitting digital evidence must ensure that such evidence is authentic, reliable, lawfully obtained, and does not prejudice the accused person's constitutional rights. Likewise, Article 16 guarantees the right to privacy and personal security, requiring investigators to balance the need for electronic evidence against constitutional safeguards relating to private communications and personal data.

3.2. The Evidence Act.[17]

The Evidence Act constitutes the principal legislation governing admissibility of evidence in judicial proceedings. Initially, the Act was drafted before the emergence of digital technology and contained no provisions relating to electronic evidence. However, the enactment of the Electronic Transactions Act in 2015 introduced significant amendments by inserting section 64A on admissibility of Electronic Evidence, thereby expressly recognizing electronic evidence. It explicitly provides that in any proceedings, electronic evidence shall be admissible. This provision abolishes the traditional common-law uncertainty regarding the admissibility of electronic records by recognizing electronic data as legally admissible evidence. Section 64A

[11] Cap. 6 R.E. 2022.
[12] Cap. 442 R.E. 2023.
[13] Cap. 443 Cap. 443 R.E. 2023.
[14] Cap. 20 R.E. 2022.
[15] Cap. 430 R.E. 2022.
[16] Cap. 2 R.E 2002.
[17] Cap. 6 R.E. 2022.

(2) further provides that admissibility and evidential weight shall be determined in accordance with section 18 of the Electronic Transactions Act. Furthermore, section 64A (3) makes clarity by defining electronic evidence as any data or information stored in electronic form or electronic media or retrieved from a computer system, which can be presented as evidence. Accordingly, such data as emails, CCTV recordings, WhatsApp communications, SMS messages, digital photographs, electronic bank statements, GPS records, and computer-generated documents fall within the statutory definition.

3.3. The Electronic Transactions Act.[18]

The Act represents the cornerstone of Tanzania's legal regime governing electronic evidence. According to its long title, the Act was enacted to provide legal recognition of electronic transactions and regulate the collection and admissibility of electronic evidence. Section 18, which is on admissibility and evidential weight, establishes the criteria that courts must consider before admitting electronic evidence. Among the relevant considerations are reliability of the manner in which the electronic record was generated; reliability of the manner in which it was stored; integrity of the information system; manner in which the originator was identified; reliability of the electronic communication system; and any other relevant circumstance affecting authenticity. Unlike India's earlier need for certification requirement,[19] Tanzania adopts a broader reliability-based approach that allows judicial discretion in assessing electronic evidence. Furthermore, the Act legally recognizes electronic records, electronic signatures, secure electronic signatures, electronic record keeping, and electronic certification.[20] These provisions ensure that documents are not rendered inadmissible merely because they exist in electronic form.

3.4. The Cybercrimes Act.[21]

The Act primarily creates cyber offences but also plays an important evidentiary role.

It authorizes investigators to search computer systems; seize electronic devices; preserve computer data; compel disclosure of subscriber information; intercept communications

[18] Cap. 442 R.E. 2023.
[19] S. 65B.
[20] Ss. 4–12.
[21] Cap. 443 R.E. 2023.

pursuant to lawful authority; and obtain traffic data relevant to criminal investigations.[22] These investigative powers ensure that digital evidence is lawfully collected while maintaining evidential integrity and chain of custody.

3.5. The Criminal Procedure Act.[23]

The Act supplements the evidentiary framework by regulating criminal investigations. Its provisions empower police officers to conduct lawful searches, seize computers and digital storage devices, obtain search warrants, and preserve exhibits pending trial. These procedural safeguards are equally applicable where the exhibits comprise computers, mobile phones, servers, flash drives, or cloud-based data accessible through lawful means.

3.6. National Prosecutions Service Act.[24]

The Director of Public Prosecutions bears responsibility for evaluating whether digital evidence satisfies evidential sufficiency before prosecution commences. Digital evidence frequently forms the basis of prosecutions involving cybercrime; corruption; financial crime; money laundering; organized crime; and terrorism. The prosecution must therefore ensure that electronic evidence complies with the admissibility requirements prescribed under the Evidence Act and the Electronic Transactions Act.

3.7. Judicial Interpretation

Although Tanzanian case law on digital evidence is still relatively limited, the courts have increasingly admitted various forms of electronic evidence, including mobile phone data, electronic communications, electronic banking records, and other computer-generated records, provided that their authenticity and reliability satisfy the requirements under section 18 of the Electronic Transactions Act and section 64A of the Evidence Act. Judicial practice demonstrates a preference for examining the authenticity, integrity, reliability, and relevance of electronic evidence rather than excluding it solely because it is produced electronically. This approach aligns with section 18 of the Electronic Transactions Act, which emphasizes reliability over rigid technical formalities.[25]

---

[22] Particularly see parts IV and V.
[23] Cap. 20 R.E. 2022.
[24] Cap. 430 R.E. 2022.
[25] *Republic v Mark Wilson Chacha* [2020] TZHC 386; *Jamii Media Co. Ltd v Attorney General*, Misc. Civil

Therefore, the Tanzanian legal framework governing digital evidence reflects a modern legislative approach that integrates traditional evidentiary principles with emerging technologies. The combined operation of the Evidence Act and the Electronic Transactions Act establishes statutory recognition of electronic evidence while emphasizing authenticity, reliability, and integrity as the principal determinants of admissibility. Additional support is provided by the Cybercrimes Act and the Criminal Procedure Act, which regulate the lawful collection and preservation of digital evidence. Collectively, these statutes provide a coherent legal framework, though continued judicial development and specialized procedural guidance remain necessary to address increasingly complex forms of digital evidence.

4. Legal Standards Govern the Admissibility of Digital Evidence in Mainland Tanzania

Unlike jurisdictions that prescribe rigid procedural prerequisites for the admission of electronic evidence, Tanzanian law adopts a reliability-centered approach, under which the admissibility and evidential weight of electronic evidence depend on its authenticity, integrity, reliability, relevance, and lawful acquisition rather than on its electronic form alone.

4.1. Relevance

The first and most fundamental requirement for the admissibility of digital evidence is relevance. As with all forms of evidence, electronic records must relate to a fact in issue or a relevant fact before they are admissible. Although the Evidence Act does not establish a separate test for digital evidence, electronic records remain subject to the general rules of relevancy contained in Parts I and II of the Evidence Act. Consequently, emails, CCTV recordings, mobile phone data, WhatsApp messages, electronic bank statements, GPS records, and computer-generated documents are admissible only where they logically assist the court in proving or disproving facts in issue.

4.2. Statutory Admissibility of Electronic Evidence

The principal statutory provision governing electronic evidence is section 64A of the Evidence Act, introduced by the Electronic Transactions Act. It expressly provides that in any proceedings, electronic evidence shall be admissible. This provision abolished any common-law uncertainty regarding the admissibility of electronic records merely because they exist in

Cause No. 5 of 2016 (High Court of Tanzania).

electronic form. Instead, electronic evidence is treated as a distinct category of documentary evidence capable of proving facts before Tanzanian courts. Section 64A (2) further provides that the admissibility and evidential weight of electronic evidence shall be determined in accordance with section 18 of the Electronic Transactions Act, thereby integrating the two statutes into a unified evidentiary framework.

4.3. Authenticity

Authenticity requires proof that the electronic record is genuine and has not been fabricated or falsely attributed. Section 18 of the Electronic Transactions Act requires the court to consider the manner in which the electronic record was generated and the manner in which its originator was identified. These statutory safeguards enable the court to determine whether the electronic record accurately represents the information originally created or transmitted. The Act further establishes a presumption of authenticity where there is evidence that the computer system was operating properly or where the record was created in the ordinary course of business, unless evidence to the contrary is produced. This statutory presumption reduces unnecessary evidential burdens while preserving judicial discretion to reject unreliable electronic records.

4.4. Integrity of the Electronic Record

Integrity refers to the assurance that electronic information has remained complete and unaltered from the time it was created until its production in court. Because digital information can easily be modified, deleted or manipulated, Tanzanian law requires courts to consider whether the integrity of the electronic record has been maintained. Section 18(2)(b) specifically directs the court to examine the reliability of the manner in which the integrity of the data message was maintained. Accordingly, where evidence demonstrates that the electronic record has been altered or that the storage system was compromised, the court may reduce its evidential weight or decline to rely upon it.

4.5. Reliability of the Computer System

Unlike jurisdictions that require technical certification as a condition of admissibility, Tanzanian law focuses on the reliability of the electronic system that generated, stored or communicated the electronic record. Section 18(2)(a) requires the court to assess the reliability of the manner in which the electronic record was generated, stored or communicated, while

section 18(3)(a) creates a rebuttable presumption of authenticity where the computer system was operating properly and any malfunction did not affect the integrity of the record. These provisions recognize that electronic evidence derives much of its evidential value from the reliability of the underlying information system.

4.6. Evidential Weight

Admissibility does not automatically determine the persuasive value of electronic evidence. Section 18 distinguishes between admissibility and evidential weight, requiring courts to evaluate the circumstances under which the electronic record was created, stored, maintained and transmitted before determining the weight to attach to it. This approach affords Tanzanian courts flexibility to admit electronic evidence while assigning greater or lesser weight depending upon the quality, reliability and credibility of the evidence presented.

4.7. Lawful Collection of Digital Evidence

Although the Evidence Act principally regulates admissibility, electronic evidence must also be obtained lawfully. Investigators exercising powers under the Criminal Procedure Act and the Cybercrimes Act must comply with statutory procedures governing search, seizure, preservation and production of electronic devices and computer data. Failure to comply with these statutory safeguards may affect both the admissibility and the evidential weight of the electronic evidence.

4.8. Absence of Technical Certification Requirement

A notable characteristic of Tanzanian law is the absence of a mandatory statutory certification requirement comparable to the former section 65B(4) of the Indian Evidence Act, 1872. Instead, the Tanzanian framework leaves the assessment of authenticity and reliability to judicial evaluation under section 18 of the Electronic Transactions Act. This allows courts to admit electronic evidence provided that the statutory indicators of reliability and integrity are satisfied, without insisting upon a formal certificate as a precondition to admissibility.

Eventually, the legal standards governing the admissibility of digital evidence in Mainland Tanzania are anchored in statutory principles of relevance, authenticity, integrity, reliability, evidential weight and lawful acquisition. Through section 64A of the Evidence Act and section 18 of the Electronic Transactions Act, Tanzanian law adopts a flexible, reliability-based

framework that empowers courts to evaluate electronic evidence on its merits rather than excluding it solely because of its digital nature. This framework promotes both technological neutrality and judicial discretion while safeguarding the integrity of the fact-finding process.

5. Tanzanian Judicial Approaches to Authentication and Reliability of Electronic Evidence: Critical Analysis of Key Cases

The judicial treatment of electronic evidence in Mainland Tanzania remains in its formative stage because Mainland Tanzania has very few reported decisions that directly analyze the authentication and reliability of electronic evidence under section 18 of the Electronic Transactions Act. Unlike jurisdictions such as India, Tanzania has not yet developed an extensive body of reported appellate decisions comprehensively interpreting the statutory requirements governing the authentication and reliability of digital evidence. Instead, Tanzanian courts have largely relied upon the statutory framework established by the Evidence Act,[26] particularly section 64A, read together with section 18 of the Electronic Transactions Act,[27] which requires courts to evaluate the reliability and integrity of electronic records before determining their admissibility and evidential weight.

5.1. *Jamii Media Co. Ltd v Attorney General*:[28] Recognition of Electronic Records

One of the earliest decisions touching upon electronic information is *Jamii Media Co. Ltd v Attorney General*.[29] Although the dispute primarily concerned the constitutionality of provisions of the Media Services Act,[30] the Court acknowledged the legal significance of online publications and electronic communications within the contemporary legal system. The significance of *Jamii Media* lies not in establishing evidentiary rules but in demonstrating judicial recognition that electronic records constitute legally cognizable documents capable of producing legal consequences. However, the Court did not analyze the statutory requirements for authentication under section 18 of the Electronic Transactions Act. Consequently, the decision offers only indirect guidance on the admissibility of digital evidence and leaves unanswered important questions regarding integrity, metadata, chain of custody and forensic preservation.

[26] Cap. 6 R.E. 2022.
[27] Cap. 442 R.E. 2023
[28] Miscellaneous Civil Cause No. 5 of 2016 (High Court of Tanzania, Main Registry)
[29] Ibid.
[30] Cap. 229 R.E. 2023.

5.2. *Republic v Mark Wilson Chacha*:[31] Judicial Acceptance of Mobile Phone Evidence

In *Republic v Mark Wilson Chacha*,[32] the High Court considered electronic communications and mobile telephone evidence as part of the prosecution's case. The Court admitted the electronic evidence after considering its relevance alongside the surrounding evidence. The decision reflects the practical willingness of Tanzanian courts to receive electronic evidence where it forms part of the evidentiary matrix. However, the judgment contains little detailed discussion of the statutory factors prescribed under section 18 of the Electronic Transactions Act. The Court did not undertake a structured analysis of the reliability of the computer system; preservation of electronic data; metadata; chain of custody; forensic acquisition; or possible alteration of the electronic records. Consequently, although the case demonstrates judicial acceptance of electronic evidence, it contributes relatively little to the development of legal principles governing authentication.

5.3. Statutory Preference for Reliability Rather than Technical Formalism

The most significant guidance regarding authentication is derived not from judicial decisions but from the statutory framework itself. Section 64A of the Evidence Act provides that electronic evidence is admissible in legal proceedings, while section 18 of the Electronic Transactions Act directs courts to determine admissibility and evidential weight by considering the reliability of the manner in which the electronic record was generated; the reliability of storage; preservation of integrity; identification of the originator; reliability of the communication system; and any other relevant circumstances. These statutory provisions demonstrate that Tanzania has adopted a functional reliability test, rather than imposing rigid procedural requirements comparable to the certification requirement formerly contained in section 65B(4) of the Indian Evidence Act, 1872.

The flexibility of the Tanzanian approach enables courts to admit electronic evidence without excluding otherwise reliable material because of technical procedural defects. Nevertheless, the absence of detailed judicial interpretation has created uncertainty concerning what constitutes sufficient proof of authenticity; acceptable methods of preserving chain of custody; admissibility of screenshots and social media evidence; treatment of cloud-based evidence; and standards governing expert digital forensic testimony. Accordingly, considerable discretion is

[31] [2020] TZHC 386
[32] Ibid.

left to trial judges, which may result in inconsistent approaches among different courts.

5.4. Emerging Judicial Trends

Despite the limited number of reported authorities as already intimated above, several trends can be identified. First, Tanzanian courts no longer reject evidence merely because it is electronic in nature. Secondly, admissibility is increasingly determined by statutory considerations relating to reliability and authenticity rather than by adherence to rigid technical formalities. Thirdly, electronic evidence is ordinarily evaluated together with other evidence rather than in isolation. Finally, the courts have yet to develop comprehensive principles governing digital forensic procedures, metadata, encryption, blockchain evidence, artificial intelligence-generated evidence or cloud computing. These trends indicate that Tanzanian jurisprudence remains predominantly statute-driven rather than precedent-driven. Unlike the position in India, where the Supreme Court has clarified authentication requirements through decisions such as *Anvar P.V. v P.K. Basheer*,[33] *Shafhi Mohammad v State of Himachal Pradesh*,[34] and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*,[35] Tanzanian courts have yet to articulate similarly comprehensive evidentiary principles. This presents both a challenge and an opportunity for future judicial development.

Therefore, the judicial approach to authentication and reliability of electronic evidence in Mainland Tanzania is characterized by limited but growing jurisprudence anchored in sections 64A of the Evidence Act and 18 of the Electronic Transactions Act. The available reported decisions demonstrate judicial acceptance of electronic evidence but provide only modest guidance on the practical application of statutory reliability criteria. As a result, the legislative framework remains the principal source of legal standards, while future appellate decisions will be essential in clarifying issues such as chain of custody, forensic integrity, metadata analysis, expert evidence, and the authentication of emerging forms of digital evidence.

6. India's Judicial Experience and Approaches to Digital Evidence: Authentication and Reliability

India has developed one of the most sophisticated bodies of judicial jurisprudence on the admissibility, authentication and reliability of digital evidence within the common law world.

[33] (2014) 10 SCC 473 (SC).
[34] (2018) 2 SCC 801 (SC).
[35] (2020) 7 SCC 1 (SC).

Unlike many jurisdictions where legislative provisions alone govern electronic evidence, Indian courts have played a decisive role in interpreting the statutory requirements under the Indian Evidence Act of 1872,[36] which is now substantially reenacted in the Bharatiya Sakshya Adhiniyam, 2023.[37] Through a series of landmark decisions, the Supreme Court has clarified the principles governing authentication of electronic records, the role of certificates under section 65B, and the distinction between primary and secondary electronic evidence. The evolution of this jurisprudence reflects a movement from uncertainty to doctrinal clarity, with increasing emphasis on preserving the authenticity, integrity and reliability of electronic records while safeguarding the fairness of criminal proceedings.

6.1. Statutory Foundation

The Information Technology Act,[38] amended the Indian Evidence Act by introducing sections 65A and 65B, creating a special evidentiary regime for electronic records. Section 65A provides that electronic records shall be proved in accordance with section 65B, while section 65B prescribes the conditions under which computer-generated electronic records are admissible. The purpose of these provisions is to ensure that electronic records admitted in court possess sufficient guarantees of authenticity, integrity and reliability despite their susceptibility to manipulation.

The statutory framework recognizes two broad categories of electronic evidence, which are primary electronic evidence, i.e., where the original electronic device itself is produced before the court; and secondary electronic evidence, i.e., where copies, printouts, CDs, DVDs, pen drives or other reproductions are tendered. The distinction between these two categories became central to subsequent judicial interpretation.

6.2. *Anvar P.V. v P.K. Basheer*:[39] Establishing the Authentication Rule

The dispute arose from an election petition in which the appellant sought to rely upon electronic evidence in the form of CDs containing speeches allegedly made during an election campaign. The principal question was whether such electronic evidence could be admitted without complying with section 65B. The Supreme Court departed from its earlier decision in *State*

[36] Act No. 1 of 1872
[37] Act No 47 of 2023, ss 62–63.
[38] Act No. 21 of 2000
[39] (2014) 10 SCC 473 (SC).

(NCT of Delhi) v Navjot Sandhu[40] by holding that sections 65A and 65B constitute a complete code governing electronic evidence.[41] Justice Kurian Joseph observed that "any documentary evidence by way of an electronic record… can be proved only in accordance with the procedure prescribed under Section 65B."[42] The Court held that where secondary electronic evidence is produced, compliance with section 65B(4) through a proper certificate is mandatory.

The judgment fundamentally changed Indian evidence law. Its strengths include enhancing authenticity; protecting against fabrication; ensuring traceability; and preserving chain of custody. However, scholars criticized the decision because parties often lack control over third-party servers; obtaining certificates from service providers may be impossible; rigid exclusion risks preventing reliable evidence from reaching the court. Despite these criticisms, *Anvar* remains the foundation of Indian digital evidence jurisprudence.

6.3. *Shafhi Mohammad v State of Himachal Pradesh*:[43] Introducing Flexibility

In *Shafhi Mohammad v State of Himachal Pradesh*,[44] the Supreme Court reconsidered the practical implications of *Anvar*. The Court recognized that parties frequently rely upon electronic evidence generated by third parties, including mobile service providers; internet companies; banks; and CCTV operators. Where the party seeking to produce the evidence lacks possession or control of the original device, strict insistence upon a section 65B certificate could produce injustice. Accordingly, the Court held that the certificate requirement should not be regarded as mandatory where the party cannot reasonably obtain it.[45] The decision promoted substantive justice and reduced procedural rigidity. Nevertheless, it generated considerable uncertainty because it conflicted with the three-judge decision in *Anvar*; lower courts became divided; and inconsistent evidentiary standards emerged.

Although *Shafhi Mohammad v State of Himachal Pradesh* was decided by a two-judge Bench, it could not legally overrule the earlier decision of a three-judge Bench in *Anvar P.V. v P.K. Basheer*.[46] Under the doctrine of precedent, a smaller Bench of the Supreme Court is bound by

[40] (2005) 11 SCC 600 (SC).
[41] *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473 (SC) paras 14–24.
[42] Ibid paras 22–27.
[43] (2018) 2 SCC 801 (SC).
[44] Ibid.
[45] Ibid., paras 22–27.
[46] *Central Board of Dawoodi Bohra Community v State of Maharashtra* (2005) 2 SCC 673 (SC) paras 12–14, where the Supreme Court affirmed that a Bench of lesser strength cannot disagree with or overrule a decision of a larger Bench and must refer the matter for reconsideration; *National Insurance Co Ltd v Pranay Sethi* (2017)

the decision of a larger Bench unless the matter is referred to a Bench of equal or greater strength for reconsideration. Consequently, the differing interpretations of section 65B created uncertainty in the law governing electronic evidence until the three-judge Bench in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[47] resolved the conflict by reaffirming *Anvar* and holding that *Shafhi Mohammad* was not correctly decided to the extent that it relaxed the mandatory certificate requirement.[48]

6.4. *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020):[49] Restoring Certainty

The uncertainty was finally resolved in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal.*[50] A three-judge Bench comprehensively reviewed the entire jurisprudence on electronic evidence. The Court held that *Anvar* correctly interpreted section 65B; *Shafhi Mohammad* was wrongly decided; the certificate requirement remains mandatory for secondary electronic evidence; and primary electronic evidence requires no certificate because the original device itself is produced.[51] Justice R.F. Nariman reaffirmed that the certificate under section 65B(4) is "a condition precedent" for admissibility of secondary electronic evidence.[52] The Court nevertheless introduced practical safeguards that where the certificate is unavailable because the electronic device belongs to another person, the trial court may summon the certificate; compel production; or issue appropriate procedural directions. Thus, procedural fairness was preserved without abandoning statutory requirements.

The decision restored legal certainty and so its principal contributions include reaffirming authentication safeguards; preserving integrity of electronic records; clarifying primary versus secondary electronic evidence; and protecting against fabricated digital material. Its principal weakness remains the practical difficulty of obtaining certificates from foreign companies or unwilling service providers.

16 SCC 680 (SC) para 30; *Union of India v Raghubir Singh* (1989) 2 SCC 754 (SC) 765, explaining the binding force of precedent and the importance of consistency in judicial decision-making.
[47] (2020) 7 SCC 1 (SC).
[48] Paras 45–73.
[49] (2020) 7 SCC 1 (SC).
[50] Ibid.
[51] Ibid., paras 52–74.
[52] ibid paras 62–63, 73.

6.5. Subsequent Judicial Developments

Subsequent Supreme Court decisions have consistently applied *Arjun Panditrao*. In *Ravinder Singh alias Kaku v State of Punjab*,[53] the Supreme Court reiterated that electronic records produced as secondary evidence must comply with section 65B unless the original device itself is produced. The Court confirmed that *Arjun Panditrao* settled the law governing authentication of electronic evidence. Similarly, *Sonu @ Amar v State of Haryana*[54] addressed objections to the absence of a section 65B certificate, holding that such objections should ordinarily be raised at the stage when the evidence is tendered rather than after the trial has concluded.

India's judicial experience illustrates the central role of appellate courts in developing coherent standards for the authentication and reliability of digital evidence. Through *Anvar P.V.*, *Shafhi Mohammad*, and *Arjun Panditrao*, the Supreme Court transformed an uncertain statutory framework into a structured doctrine that distinguishes between primary and secondary electronic evidence, prescribes authentication requirements, and reinforces the integrity of digital proof. For jurisdictions such as Tanzania, where reported jurisprudence remains comparatively limited, the Indian experience offers persuasive guidance on balancing technological realities with the fundamental objectives of evidentiary reliability and fairness.

7. Lessons for Tanzania from Indian Judicial Developments

From the account above, it is explicit that India provides a useful comparative experience because its courts have developed detailed jurisprudence on authentication, integrity, reliability and procedural safeguards governing electronic evidence. Through decisions such as *State (NCT of Delhi) v Navjot Sandhu*,[55] *Anvar P.V. v P.K. Basheer*,[56] *Shafhi Mohammad v State of Himachal Pradesh*,[57] and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*,[58] the Indian Supreme Court has addressed the challenges of admitting electronic records while maintaining safeguards against manipulation and fabrication. These developments provide important lessons for Tanzania in strengthening judicial approaches to digital evidence.

[53] (2022) 7 SCC 581.
[54] (2017) 8 SCC 570.
[55] (2005) 11 SCC 600 (SC).
[56] (2014) 10 SCC 473 (SC).
[57] (2018) 2 SCC 801 (SC).
[58] (2020) 7 SCC 1 (SC).

7.1. Development of Clear Judicial Standards on Authentication

One of the principal lessons from India is the importance of developing clear judicial standards for authentication of electronic evidence. In *Anvar P.V. v P.K. Basheer*,[59] the Indian Supreme Court held that electronic records require special safeguards because digital information can be easily altered, copied or manipulated. The Court interpreted sections 65A and 65B of the Indian Evidence Act, 1872 as creating a complete code for proving electronic records and required compliance with section 65B (4) where secondary electronic evidence was produced.[60] It emphasized that authentication serves several purposes such as establishing the source of the electronic record; confirming that the record has not been altered; identifying the person responsible for creating or transmitting it; and ensuring confidence in the integrity of the evidence.

Although Tanzania has adopted a more flexible reliability-based approach under section 18 of the Electronic Transactions Act, Tanzanian courts have not yet developed detailed judicial criteria explaining what constitutes sufficient authentication. The Indian experience demonstrates the need for Tanzanian courts to articulate practical guidelines addressing proof of ownership or control of electronic devices; methods of verifying digital communications; preservation of metadata; forensic extraction procedures; and chain of custody requirements. Such judicial guidance would promote consistency among trial courts and reduce uncertainty regarding admissibility.

7.2. Balancing Reliability with Flexibility

A second lesson from India is the importance of balancing procedural safeguards with practical realities. The strict approach adopted in *Anvar* generated concerns because parties often rely on electronic evidence controlled by third parties such as telecommunications companies; social media platforms; banks; and cloud service providers. In *Shafhi Mohammad v State of Himachal Pradesh*,[61] the Supreme Court attempted to address these difficulties by holding that the requirement of a section 65B certificate could be relaxed where the party producing the evidence lacked control over the electronic device.[62] However, this approach created uncertainty because a smaller Bench had departed from the earlier three-judge Bench decision

[59] (2014) 10 SCC 473 (SC).
[60] *Anvar P.V. v P.K. Basheer* (2014) 10 SCC 473 (SC) paras 14–24.
[61] (2018) 2 SCC 801 (SC).
[62] *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801 (SC) paras 22–27.

in *Anvar*. The conflict was resolved in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*,[63] where the Supreme Court reaffirmed *Anvar* but recognized practical difficulties by allowing courts to compel production of certificates through procedural powers.[64]

The Tanzanian framework already provides greater flexibility because section 18 of the Electronic Transactions Act focuses on reliability rather than mandatory certification. Nevertheless, Tanzanian courts should learn from the Indian experience by avoiding two extremes excessive technical rigidity, which may exclude reliable evidence; and excessive flexibility, which may permit unreliable digital material to influence judicial decisions. A balanced approach would require courts to assess reliability while developing procedural mechanisms for obtaining evidence from third-party electronic systems.

7.3. Recognition of the Importance of Digital Forensic Integrity

Indian jurisprudence demonstrates that authentication is closely connected to digital forensic integrity. Electronic evidence differs from traditional documentary evidence because digital information can be modified without obvious physical signs. Therefore, courts must examine how the evidence was collected; who collected it; whether the original data was preserved; whether forensic tools were reliable; and whether the chain of custody remained intact. In *Arjun Panditrao*, the Supreme Court recognized that electronic evidence requires safeguards because technological processes may affect the reliability of digital records.[65]

Tanzania should develop stronger judicial engagement with digital forensic principles. Courts should increasingly require parties relying on digital evidence to demonstrate proper acquisition methods; preservation of original devices; use of recognized forensic procedures; documentation of handling history; and expert explanation where technical issues arise. This is particularly important in criminal cases involving mobile phones, electronic financial transactions, CCTV footage and social media evidence.

7.4. Need for Appellate Guidance and Consistent Interpretation

A major feature of Indian experience is the role of appellate courts in clarifying uncertainty.

[63] (2020) 7 SCC 1 (SC).
[64] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 (SC) paras 52–73.
[65] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 (SC) paras 62–73.

Before *Arjun Panditrao*, Indian courts experienced inconsistent approaches because of conflicting interpretations between *Navjot Sandhu*, *Anvar* and *Shafhi Mohammad*. The Supreme Court eventually provided authoritative guidance by establishing a consistent framework.[66] Tanzanian courts face a similar challenge because reported decisions dealing specifically with digital evidence remain limited. The absence of appellate guidance may result in different approaches among trial courts concerning authentication requirements; admissibility of screenshots; mobile phone extraction reports; CCTV evidence; electronic banking records; and social media communications. The Tanzanian Court of Appeal may therefore play an important role in developing principles that clarify the application of section 18 of the Electronic Transactions Act.

7.5. Development of Rules Concerning Emerging Forms of Digital Evidence

Indian jurisprudence also demonstrates the need for courts to adapt evidentiary principles to emerging technologies. Digital evidence today extends beyond traditional computer records to include encrypted communications; artificial intelligence-generated material; blockchain records; cloud storage; Internet of Things devices; and digital financial platforms. Although Indian courts have not yet developed comprehensive rules for all emerging technologies, their jurisprudence demonstrates the importance of maintaining technologically neutral principles centered on authenticity and reliability. Tanzania should ensure that judicial interpretation of section 18 of the Electronic Transactions Act remains sufficiently flexible to address future technologies. Courts should avoid interpreting digital evidence narrowly and instead focus on whether the evidence provides reliable information capable of assisting the determination of facts in issue.

7.6. Institutional and Procedural Reforms

India's experience also demonstrates that effective regulation of digital evidence requires more than legislation. It requires trained judges; specialized prosecutors; competent digital forensic laboratories; clear investigative procedures; and technical expertise within the justice system. The admissibility of electronic evidence depends not only on legal rules but also on the ability of institutions to preserve and explain digital information. Tanzania should consider judicial training on digital evidence; development of digital evidence practice directions; strengthening

[66] *Central Board of Dawoodi Bohra Community v State of Maharashtra* (2005) 2 SCC 673 (SC) paras 12–14 (on judicial discipline and binding precedent).

forensic capacity within law enforcement agencies; adopting internationally recognized forensic standards; and encouraging expert testimony where technical issues arise.

Therefore, India's judicial experience provides valuable lessons for Tanzania in developing a coherent approach to the admissibility of digital evidence. The Indian Supreme Court's movement from uncertainty in *Navjot Sandhu*, through the strict authentication approach in *Anvar*, the attempted flexibility in *Shafhi Mohammad*, and the clarification provided by *Arjun Panditrao*, demonstrates the importance of balancing evidentiary reliability with practical accessibility. For Tanzania, the key lesson is that statutory recognition of electronic evidence under section 64A of the Evidence Act and section 18 of the Electronic Transactions Act is only the first step. Sustainable development requires judicial interpretation that clarifies authentication standards, preserves digital integrity, promotes consistency, and ensures that technological advancement does not undermine the fairness and reliability of judicial proceedings.

8. Feasible Recommendations and the Way Forward

The experience of India demonstrates that effective regulation of digital evidence requires more than statutory recognition. It requires consistent judicial interpretation, specialized procedural rules, institutional capacity and continuous judicial training.[67] Drawing from the Indian experience and international best practices, the following recommendations are proposed.

8.1. Develop Comprehensive Judicial Guidelines on Digital Evidence

The first recommendation is that the Judiciary of Tanzania, preferably through the Chief Justice or the Judicial Administration Department, should develop comprehensive judicial practice directions governing the admissibility and evaluation of digital evidence. Although section 64A of the Evidence Act recognizes the admissibility of electronic evidence and section 18 of the Electronic Transactions Act provides general criteria for determining admissibility and evidential weight, the legislation does not explain how courts should practically evaluate authenticity, metadata, chain of custody, forensic acquisition or cloud-based evidence. Consequently, judicial officers often exercise broad discretion without uniform standards.

The Indian experience illustrates the importance of judicial guidance. Following the

[67] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1 (SC) paras 52–74.

uncertainty created by *State (NCT of Delhi) v Navjot Sandhu*,[68] *Anvar P.V. v P.K. Basheer*,[69] and *Shafhi Mohammad v State of Himachal Pradesh*,[70] the Supreme Court in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[71] clarified the applicable principles governing electronic evidence and restored certainty in judicial practice.

Judicial practice directions in Tanzania should address authentication of electronic records; preservation of metadata; chain of custody; admissibility of screenshots and social media evidence; electronic banking records; CCTV recordings; digital forensic reports; treatment of cloud-based evidence; and expert testimony in digital investigations. Such guidance would enhance consistency, predictability and public confidence in judicial decision-making.

8.2. Strengthen Judicial Capacity Through Continuous Training

The rapid evolution of technology requires judicial officers to possess specialized knowledge concerning digital evidence. Judges increasingly encounter electronic communications, encrypted data, cryptocurrency transactions, cloud storage, artificial intelligence-generated material and digital forensic reports. The Judicial Training Institute (Lushoto) should therefore institutionalize specialized training programs on principles of digital forensics; electronic evidence; cybercrime investigations; metadata analysis; blockchain technology; artificial intelligence and evidence; electronic discovery; and international best practices.

The United Nations Office on Drugs and Crime (UNODC) has observed that judicial competence in digital evidence is essential to ensuring fairness and effective criminal justice responses to cyber-enabled offences.[72] Similarly, the Council of Europe Convention on Cybercrime (Budapest Convention) highlights the importance of specialized capacity-building in the investigation and prosecution of offences involving electronic evidence.[73] Training would reduce inconsistent approaches among courts and improve judicial confidence in evaluating complex digital evidence.

[68] (2005) 11 SCC 600 (SC).
[69] (2014) 10 SCC 473 (SC).
[70] (2018) 2 SCC 807 (SC).
[71] (2020) 7 SCC 1 (SC).
[72] United Nations Office on Drugs and Crime, *Practical Guide for Requesting Electronic Evidence Across Borders,* 2023, pp. 7–14.
[73] Council of Europe, *Convention on Cybercrime* (ETS No 185, 2001), arts. 14–21.

8.3. Develop National Digital Forensic Standards

The admissibility of electronic evidence depends significantly on the integrity of forensic processes. Courts can only attach weight to digital evidence where investigators demonstrate that electronic records have been collected, preserved and analyzed using scientifically reliable methods. Tanzania should adopt national digital forensic standards consistent with ISO/IEC 27037:2012,[74] which provides internationally recognized guidelines for the identification, collection, acquisition and preservation of digital evidence. National standards should regulate seizure of electronic devices; forensic imaging; preservation of original data; documentation of chain of custody; storage of digital exhibits; forensic reporting; and expert witness certification. Such standards would minimize disputes concerning authenticity and improve judicial confidence in electronic evidence.

8.4. Clarify the Law through Appellate Jurisprudence

Unlike India, where the Supreme Court has developed detailed jurisprudence on electronic evidence, Tanzanian appellate courts have issued relatively few reported decisions interpreting section 64A of the Evidence Act and section 18 of the Electronic Transactions Act. The Court of Appeal of Tanzania should take opportunities presented by appropriate cases to clarify standards of authentication; reliability of electronic records; admissibility of social media evidence; admissibility of screenshots; admissibility of cloud-based evidence; standards governing expert digital forensic testimony; treatment of encrypted communications; and evidential weight of computer-generated records. The Indian experience demonstrates that appellate guidance promotes consistency and legal certainty.[75]

8.5. Preserve Tanzania's Flexible Reliability-Based Approach

One of the principal strengths of the Tanzanian legal framework is that section 18 of the Electronic Transactions Act adopts a reliability-centered approach rather than imposing a mandatory certification requirement comparable to the former section 65B(4) of the Indian Evidence Act. This flexibility should be maintained. The Indian experience illustrates that rigid procedural requirements may unintentionally exclude reliable evidence where certificates

[74] ISO/IEC 27037:2012, *Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*.
[75] *Arjun Panditrao Khotkar*, ibid., paras 52–74; *Central Board of Dawoodi Bohra Community v State of Maharashtra* (2005) 2 SCC 673 (SC) paras 12–14.

cannot reasonably be obtained from telecommunications companies, internet service providers or foreign technology companies.[76] However, flexibility should not undermine evidentiary reliability. Tanzanian courts should continue to evaluate authenticity; integrity; reliability; relevance; provenance; and lawfulness of acquisition. This balanced approach is better suited to rapidly evolving technologies.

8.6. Promote Legislative Review to Address Emerging Technologies

Although the current statutory framework provides a sound foundation, technological developments have outpaced existing legislation. Parliament should consider periodic review of the Evidence Act, the Electronic Transactions Act and the Cybercrimes Act to address emerging issues, including artificial intelligence-generated evidence; blockchain technology; cryptocurrency transactions; Internet of Things (IoT) devices; cloud computing; deepfakes and synthetic media; digital identity verification; and cross-border access to electronic evidence. Comparative experience demonstrates that legislation governing digital evidence must remain technologically neutral while being sufficiently adaptable to new forms of electronic information.[77]

8.7. Enhance Regional and International Cooperation

Digital evidence frequently transcends national borders because electronic communications, cloud storage and online platforms are often hosted outside Tanzania. Effective investigation and prosecution therefore require international cooperation. Tanzania should strengthen mutual legal assistance arrangements, participate in regional judicial cooperation initiatives and align domestic procedures with internationally accepted standards for obtaining and preserving electronic evidence from foreign jurisdictions. Such cooperation would improve the availability and admissibility of cross-border digital evidence while respecting sovereignty and due process.[78]

[76] *Anvar P.V.,* ibid., paras 14–24; *Arjun Panditrao Khotkar,* ibid., paras 62–73.
[77] United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce* (1996) arts 5–9; United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime,* 2013, pp. 193–201.
[78] United Nations Office on Drugs and Crime, *Practical Guide for Requesting Electronic Evidence Across Borders* (2023); Council of Europe, *Convention on Cybercrime* (ETS No 185, 2001).

8.8. Encourage Academic and Judicial Research

The limited body of Tanzanian jurisprudence on digital evidence underscores the need for continued research. Universities, the Judiciary, the Tanganyika Law Society, the Office of the Director of Public Prosecutions and the Law Reform Commission should collaborate on empirical studies examining judicial treatment of electronic evidence, challenges encountered by courts and comparative best practices. Such research would provide an evidence-based foundation for future legislative and judicial reforms.

Eventually, Mainland Tanzania has established a progressive statutory framework for the admissibility of digital evidence through the Evidence Act and the Electronic Transactions Act. Nevertheless, legislation alone cannot ensure consistent and effective judicial practice. The Indian experience demonstrates that clear appellate guidance, specialized judicial training, robust forensic standards and procedural certainty are essential for maintaining the authenticity, integrity and reliability of electronic evidence.

The most appropriate way forward for Tanzania is **not** to replicate India's former mandatory certification regime, but rather to refine its existing reliability-based approach through judicial interpretation, institutional capacity-building and targeted legislative reform. By combining statutory flexibility with clearer judicial standards and internationally recognized forensic practices, Tanzania can develop a modern, coherent and technologically responsive legal framework capable of addressing the evidentiary challenges posed by the digital age.

9. Conclusion

The increasing reliance on digital technologies in criminal investigations and prosecutions has made the admissibility of electronic evidence a central issue in the administration of justice. This article has demonstrated that while Mainland Tanzania has established a sound statutory framework through the Evidence Act and the Electronic Transactions Act, judicial interpretation of the principles governing the admissibility, authentication and reliability of digital evidence remains comparatively underdeveloped. The limited body of reported case law leaves significant questions concerning the application of statutory standards to emerging forms of electronic evidence. In contrast, Indian criminal jurisprudence illustrates the critical role of the judiciary in developing coherent evidentiary principles. The decisions in *Anvar P.V.*

v P.K. Basheer,[79] *Shafhi Mohammad v State of Himachal Pradesh*,[80] and *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[81] demonstrate the evolution of judicial thinking on the authentication and admissibility of electronic records, balancing evidentiary reliability with the practical realities of obtaining and presenting digital evidence. Although the Indian requirement of certification under section 65B should not be transplanted wholesale into the Tanzanian legal system, the underlying principles of authenticity, integrity, reliability, and judicial consistency provide valuable guidance.

The article argues that Tanzania should build upon its existing reliability-based statutory framework by promoting clearer appellate jurisprudence, adopting judicial practice directions, strengthening digital forensic capacity, and enhancing the technical competence of judges, prosecutors and investigators. Such reforms would improve the consistency and predictability of judicial decision-making while preserving the flexibility necessary to respond to rapidly evolving technologies. Ultimately, the admissibility of digital evidence should not depend on rigid technical formalities, nor should it compromise the integrity of the judicial process. Rather, courts should strive to ensure that electronic evidence admitted in criminal proceedings is authentic, reliable, lawfully obtained and capable of assisting the court in the fair determination of facts. By drawing appropriate lessons from Indian criminal jurisprudence while remaining responsive to its own legal and institutional context, Mainland Tanzania can develop a modern, coherent and technologically responsive jurisprudence on digital evidence that enhances both the administration of justice and public confidence in the criminal justice system.

[79] (2014) 10 SCC 473 (SC).
[80] (2018) 2 SCC 807 (SC).
[81] (2020) 7 SCC 1 (SC).