JOURNAL OF ACADEMIC RESEARCH FOR HUMANITIES
ISSN 2663-192x

ORCID of JARH: https://orcid.org/0009-0000-0723-9485
DOI Number of the Paper: https://zenodo.org/records/17067016
Edition Link: Journal of Academic Research for Humanities JARH, 5(2) Apr-Jun 2025
Link of the Paper: https://jar.bwo-researches.com/index.php/jarh/article/view/558
HJRS Link: Journal of Academic Research for Humanities JARH (HEC-Recognized for 2024-2025)

DIGITAL EVIDENCE IN SOUTH ASIA: A COMPARATIVE LEGAL STUDY OF PAKISTAN, INDIA, AND BANGLADESH

Corresponding & Author 1:	**MUBASHIR HASSAN,** Student, Department of Law, Hazara University Mansehra, Pakistan. Email: mubashir6517@gmail.com
Author 2:	**ABDULLAH MUNAWAR**, Student, Department of Law, Hazara University Mansehra, Pakistan. Email: tanoliabdullah676@gmail.com
Author 3:	**FAREED AHMED,** Student, Department of Law, Hazara University Mansehra, Pakistan. Email: fareedS561@gmail.com
Author 4:	**IBRAR HAMEED,** Student, Department of Law, Hazara University Mansehra, Pakistan, Email: ibrarhameed658@gmail.com
Author 5:	**WASEEM AKRAM,** Student, Gillani Law College, Bahauddin Zakariya University, Multan, Pakistan, Email: Waseem.akrambalti08@gmail.com

Paper Information

Citation of the paper:
(Jarh) Hassan M., Munawar A., Ahmed F., Hameed I., and Akram W. (2025). Digital evidence in South Asia: a comparative legal study of Pakistan, India, and Bangladesh. In *Journal of Academic Research for Humanities*, 5(*3*), 68–76B.

Subject Areas for JARH:
1 Social Sciences
2 Law

Timeline of the Paper at JARH:
Received on: 06-05-2025.
Reviews Completed on: 28-05-2025.
Accepted on: 03-06-2025.
Online on: 30-06-2025.

Recognized for BWO-R:
HJRS HEC Journal Recognition System

Published by BWO Researches INTL..
BWO RESEARCHES (PVT) LTD INTERNATIONAL

DOI Image of the paper:
DOI 10.5281/zenodo.15420758

QR Code for the Paper:

Abstract

The dawn of the notion of digital evidence has raised new feuds of admissibility and reliability of evidence in the legal realm, due to their fragility, manipulation risks, and compatibility with traditional evidence rules. This study comparatively analyses the legal approaches of the three South Asian countries - Pakistan, India, and Bangladesh - in addressing the challenge of digital evidence admissibility. Despite the common evidentiary legal framework origin, each of them governs the admissibility of digital evidence with a distinct legislative framework. Pakistan introduced the Electronic Transactions Ordinance 2002 earlier and now deals with it via the Prevention of Electronic Crimes Act (PECA) 2016. Similarly, India amended the Evidence Act 1872 by inserting Sections 65A & 65B via the Information Technology Act 2000. Bangladesh has also been trying to come up with a challenge through the Information and Communication Technology Act 2006 and the Digital Security Act 2018. This study, on the one hand, examines important convergences between these countries' legal frameworks, such as difficulties with technical complexity, certification requirements, and lack of judicial capacity, by using qualitative legal analysis of statutes, landmark court decisions, and other secondary data. On the other hand, divergences between these legal frameworks have also been highlighted, which are mainly structural and methodological in nature. The findings highlight a common need for ongoing legislative reforms, enhanced forensic infrastructure, and specialized judicial training, so that it could harmonize legal standards not only in South Asia but also across the globe.

Keywords: Digital Evidence. Admissibility. Section 65B. PECA. DSA.

Introduction

The technological breakthroughs have not only changed human activities but also reshaped the outlook of legal frameworks and proceedings throughout the world (Obamanu, 2023). This is due to the debate over the role of digital or forensic evidence in the administration of justice. To avert the risk of making irrational conclusions during legal proceedings, it is essential to thoroughly assess the reliability and quality of any evidence. Concerns about the correctness of digital evidence, which is a relatively new science (Reith, 2002), have existed for a long time and are still under debate (Arshad, 2018). According to the International Organization for Computer Evidence, any information created, sent, or saved via electronic media that is utilized in court cases, internal cybersecurity investigations, malware analysis, etc., is referred to as digital evidence. Or "any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred (Casey, 2011). It can simply be duplicated and sent, easily changed and erased, and tainted by fresh information (Angel, 2024). Similarly, the term cyber forensics is used to describe the study of acquiring, storing, and recording evidence from digital electronic storage devices, including computers, digital cameras, smartphones, and other memory storage devices. It involves searching for, finding, and analyzing possible evidence as well as applying methodical investigative procedures in an automated setting. It is the process of looking into and analyzing data that is kept on or recovered from an electronic data storage medium in order to present it before a court of law (Pillai, 2016).

Several international legal frameworks have been established to govern the collection and application of digital evidence. To prevent crimes involving computers and the internet, the Budapest Convention on Cybercrime (2001) was created by the Council of Europe. It was the first international agreement aimed at containing such nature of crimes. It provides a legal framework for cooperation between signatory countries, enabling them to harmonize cybercrime and the sharing of digital evidence (Khan M. A., 2024). The global community is welcoming this digital equipment and techniques (Saeed A. A., 2022). By providing new and updated laws for electronic evidence, legislative bodies around the world are praising the new cyber revolution (Abbasi H. &., 2020). For example, to address the necessity for locating latent evidence on a computer, the Scientific Working Group Digital Evidence (SWGDE) was established by the directors of the Federal Crime Laboratory in Washington, DC. On March 2, 1998, the idea of digital evidence was presented to the directors of federal laboratories. Additionally, the first book on digital forensics, "Best Practices for Computer Forensics," was published in 2002 by the Scientific Working Group on Digital Evidence (SWGDE) (Barua A. E., 2022).

In South Asia, the handling of digital evidence and its monitoring poses unique challenges. In order to counter the growing threat of cybercrime, several nations in the area, particularly India, Pakistan, and Bangladesh, have passed and updated cybersecurity laws and made significant investments in monitoring technologies (Khan M. A., 2024). The parent statute in all three is the Evidence Act 1872, which primarily does not accept digital documents as evidence (Barua A. E., 2022). Yet, significant amendments have been made in the Parental Act to accommodate electronic evidence. Until 1984, the Evidence Act 1872 was the main law for evidence in Pakistan. In 1984, it was renamed as Qanun-e-Shahadat Order 1984, with minor changes from the previous. These changes were made only in articles 3 to 6 (which are concerned with Hudood), with the addition of article 44 and the proviso of article 42 (Abbasi H. R., 2021). As far as the law regarding the admissibility of digital evidence is concerned, no law existed before 2002 in Pakistan. However, the widespread availability of digital evidence and information made the legislature recognize the importance of digital evidence, which eventually resulted in the promulgation of the Electronic Transaction

Ordinance, 2002 (ETO). Historically, Pakistani courts have not always given much weight to digital evidence. But the ordinance significantly revised the established rules for evidence in criminal and civil trials (Khan M. S., 2023). A few provisions in the Qanun-e-Shahadat Order, 1984 (QSO), were also modified by this ordinance. Up until 2016, though the provisions of this ordinance were applied to a wide range of cybercrimes, it was insufficient to cover many areas of cybercrimes, including digital evidence. Hence, the power of law enforcement agencies was strengthened through the Prevention of Electronic Crimes Act, 2016 (PECA) (Usman, 2022).

For India, the impacts of information technology and the expansion of computers on the one hand, and the ability to collect and save information in digital forms, all made it necessary to change the law and add legal provisions that could encompass digital evidence (Dubey V. , 2017). In India, the main laws controlling the admissibility of digital evidence are the Indian Evidence Act of 1872 and the Information Technology Act of 2000. The Information Technology Act of 2000 was passed along with the necessary amendments to the Indian Penal Code, 1860, the Banker's Book Evidence Act, 1891, and the Indian Evidence Act, 1872, in order to bring modern IT into compliance with the law (Khudhair, 2021). The basis for digital records, their legitimacy, applicability, and acceptability are established by these statutes. The Indian Evidence Act 1872 has been amended to incorporate provisions about electronic records. Section 65B is one of the most prominent provisions of the Act that is related to electronic records, and it is specifically concerned with the admissibility of electronic records as evidence in courts (Bharati R. K., 2024). Section 65B of the Evidence Act governs the admissibility of electronic evidence. Section 65B (4) mandates the required certification of electronic evidence, while Section 65B (2) outlines the requirements for its admission in a court of law (Khudhair, 2021). The use of digital evidence in court is allowed by the Information Technology Act, which was passed in 2000 and subsequently updated. This act specifies how digital certificates and signatures should be handled and acknowledges electronic documents and digital signatures as legitimate legal documents.

In Bangladesh, cybercrimes are primarily addressed by the Information and Communication Technology Act of 2006. The Act's main provisions include materials about digital signatures, electronic records, types of offences, and the establishment and jurisdiction of the cybercrime and cyber appellate tribunals in Bangladesh (Ali B. G., 2018). Another important piece of legislation is the Digital Security Act, 2018. Both laws have been significantly amended (Ali B. G., 2018).

This study aims to conduct a comparative analysis of the legal frameworks and practical realities governing the admissibility of digital evidence in Pakistan, India, and Bangladesh. On the one hand, it will explore the major legal statutes enacted in each country concerning digital evidence and critically examine the landmark decisions by the courts of each country which played an important role in interpreting these laws; on the other it systematically analyzes major differences and similarities in the framework of these countries, concerning electronic evidence admissibility. The ultimate goal of the study is to evaluate the efficacy of these legal frameworks in securing reliable evidence for the delivery of justice in the contexts of these three major South Asian nations. Additionally, it will contribute to the larger international discussion of standardizing legal requirements for digital evidence in a globalized world.

Literature Review

Existing literature on the admissibility of digital evidence reveals that such evidence is becoming more and more important over time, but still underdeveloped in many criminal justice systems. In Pakistan, Saddique et al. (2024) assert, there are still major institutional and practical obstacles, even though Article 164 of the Qanun-e-Shahadat Order 1984 officially

acknowledges evidence from modern devices. According to the study, forensic infrastructure is unevenly developed, with most of the regions of Pakistan struggling with outdated equipment and a lack of standardized processes. Only a limited number of areas and forums, like the Punjab Forensic Science Agency (PFSA), have advanced capabilities. The admissibility of electronic evidence is directly hampered by the fact that judges and advocates mostly lack the necessary preparation and understanding of forensic science. Similarly, Bharati et al. (2024), while outlining Indian digital evidence legal frameworks, state that the admissibility of such evidence depends on rigorous adherence to Section 65B of the Indian Evidence Act. This section stresses that the evidence must be "authentic, reliable, and of integrity".

Zahoor et al. (2022) thinks that the Qanun-e-Shahadat Order 1984 (Article 164), which expressly allows evidence derived from modern devices, and the Electronic Transaction Ordinance 2002 (ETO), whose preamble requires courts not to reject digital evidence "merely on the ground that it is not in substantive and tangible form", are two important pieces of legislation that form the basis of Pakistan's legal framework for the admissibility of digital evidence. He wonders that despite the acknowledgement of digital evidence's admissibility by these statutes, judges routinely look for other evidence that is presented to corroborate the digital evidence, demonstrating a continued dependence on corroborative evidence. Important rulings such as Yasir Ayyaz and others vs the State uphold the admissibility of digital contents (audio/video) and devices where forensic analysis demonstrates authenticity.

Saeed et al (2022) highlight landmark rulings of Pakistani courts, specifically highlighting the Salman Akram Raja v. Government of Punjab case, which established that DNA evidence now provides "a reliable method for the judicial system to use in determining the identities of those responsible for a crime", though it was previously considered untrustworthy. Yet he also argues that though Pakistani courts are progressively acknowledging the admissibility of digital evidence, there exist persistent operational issues because of the insufficient technical skill and required capacity. Landmark cases like Anvar P.K. vs. P.K. Basheer also mandate Section 65B in India, a certificate to prove authenticity. It mentions major constraints regarding their admissibility, like the potential for manipulation, challenges in maintaining the chain of custody, and the lack of a uniform process. On the same footing, Vedwal A. (2023) also renders Section 65B of the Indian Evidence Act (IEA) as the pillar of India's legal framework for digital evidence. In the ***Arjun v. Kailash*** case, the Supreme Court made it compulsory to satisfy section 65B's requirement and specifically mentioned certification of the device accuracy and integrity by an authorized official. However, difficulties still exist because of the "very nature" of digital evidence, which includes its vulnerability to "tampering and alteration" and the crucial requirement for an uninterrupted chain of custody.

Correspondingly, Dubey (2017) observes, technological limitations and judicial inconsistencies pose serious problems for India's electronic evidence legal framework. Due to technological incompetence, lower courts frequently avoid specialized processes, as the trial judges are 'vastly inept and technologically unsound'. This led to conflicting decisions and uncertainty. For instance, in State v. Navjot Sandhu (2005), the Supreme Court allowed secondary evidence without complying with Section 65B. Furthermore, without strict controls, electronic records are "more susceptible to tampering, alteration, transposition, excision, etc".

As far as the admissibility of digital evidence under the legal framework of Bangladesh is concerned, Tanbir K. (2021) asserts that the Bangladesh Evidence Act 1872 still has not recognized digital records as evidence; nevertheless, the society has been significantly digitalized. He renders the 'legislative

inattention' as the prime cause of this legal gap. However, judicial decisions are endeavouring to fill this gap by broadening the meaning of the word 'document' and including electronic evidence within the term 'matter' under section 3 of the Evidence Act. For example, the famous Khaleda Akhter v. State (1985) case supported this approach, which ruled that video cassettes are admissible because "'matter' is a term of widest amplitude". Based on the same challenges, Barua (2022) urges amending section 3 of the Evidence Act to expressly recognize digital evidence in the courts as admissible evidence, following the Indian approach of encompassing these as evidence. Similarly, Ali (2018) states that there is a deficiency of any sort of comprehensive legal framework and guidelines regarding digital evidence in Bangladesh. He recommends a conceptual framework for cyber crimes in Bangladesh, which could encompass the "Collection and Preservation" and "Quality Management" of data.

Examination of the existing literature on electronic evidence reveals that there exists legal homework in each of Pakistan, India, and Bangladesh. However, there is also a significant gap in systematic comparative legal research. This study aims to fulfill this gap in comparative legal analysis between these three countries, regarding the admissibility of electronic evidence.

Objectives of the Research

The main objectives of this study are as follows:

- To compare and analyze the legislative frameworks governing digital evidence admissibility in Pakistan, India, and Bangladesh by identifying the major similarities and differences in their legislative approaches.
- To evaluate the role of landmark judicial interpretations in the evolution of digital evidence admissibility.
- To identify and assess the major contemporary challenges impacting the efficacy.

Research Questions

1. How do the legislative frameworks for digital evidence admissibility in Pakistan, India, and Bangladesh overlap or differ in their core admissibility conditions, procedural mechanisms, and approaches?
2. To what extent do the mandatory certifications help in determining evidence integrity while potentially restricting the admissibility of relevant evidence in specific cases?
3. What are the strengths and weaknesses of the institutional infrastructures established for digital evidence in each country?
4. What are the major common and specific jurisdiction challenges?

Novelty of the research

This study is an endeavour to bridge the research gap of comparing the jurisdiction of the three big South Asian nations through its rare tri-jurisdictional analysis of digital evidence frameworks. It explores in depth the legal reforms, institutional mechanisms, and judicial interpretations regarding the admissibility of digital evidence held in each country. It also identifies systemic hurdles and recommends solutions for enhancing evidentiary integrity. Its ultimate goal is to strengthen fair trials worldwide by advancing reliable digital evidence practices.

Research Methodology

To examine the admissibility frameworks of digital evidence in Pakistan, India, and Bangladesh, a qualitative method of study has been adopted in this study, which primarily focuses on comparative legal analysis. It uses primary as well as secondary sources for data and refers to landmark judicial precedents and amendments to foundational evidence laws of these countries. Secondary sources like existing academic literature on the topic have also been consulted.

The study starts with a preliminary review of the legal and historical development of digital evidence admissibility in these three jurisdictions, after which a comparative analytical framework is employed to evaluate procedural requirements, the institutional

arrangements, and structural variations in each country's legal framework. The study, in its core, identifies the convergences and divergences across the three legal systems. It also considers the wider ramifications for legal reforms, evidentiary integrity, and the administration of justice in the digital era by using descriptive, critical, and evaluative methodologies. It ultimately seeks to contribute to the growing international conversation on harmonizing standards for digital evidence.

The rationale behind the selection of these three jurisdictions was not only due to their shared colonial legal heritage but also due to their divergent legislative responses to the contemporary digital evidence challenges. As neighbouring countries with high digital adoption rates and similar cybercrime challenges, their comparative analysis will provide critical insights into how common law systems adapt to technological change.

Limitations

This study relies primarily on statutory analysis and case laws, though it acknowledges the absence of empirical field data. Dependence on secondary data may introduce interpretive biases or overlook ground-level procedural nuances. Furthermore, rapidly evolving cyber legislation in these jurisdictions means some analyses may become outdated, necessitating ongoing research to capture dynamic legal developments. These limitations underscore the need for future socio-legal studies.

Major Legal Documents Governing Digital Evidence Admissibility

This section elaborates on the legal framework regarding digital evidence in each country, encompassing the scope, structure, essentials and inherent challenges in these frameworks.

Legal framework in Pakistan

1. The Electronic Transactions Ordinance (ETO), 2002

The Electronic Transactions Ordinance (ETO), 2002, was the first-ever statute in Pakistan that dealt with the recognition and regulation of electronic evidence in the legal framework of the country. It creates some important equivalencies: if electronic papers are available for reference, they are considered to meet the legislative "writing" criteria (Section 4). Similarly, electronic documents maintain their legal integrity as "originals" provided they are consistently maintained (Section 5), and they also satisfy formal signing requirements (Section 7).

The ETO also made landmark amendments in the Qanun-e-Shahadat Order 1984, to insert provisions regarding digital evidence within the core evidence law of the country. It established relevancy for automated system records (Article 46A) and presumptions of authenticity for advanced electronic signatures (Section 9). In order to contain vulnerabilities like tampering, the Ordinance also requires technical safeguards, such as requiring security procedures to ensure data integrity (Section 2(x)). It also establishes the Electronic Certification Accreditation Council, which has to oversee the accredited certification service providers (Sections 18–24). The ETO's evidentiary requirements are still essential for confirming digital evidence in civil and business contexts, even though it has been superseded by PECA 2016.

2. Pakistan's Prevention of Electronic Crimes Act (PECA), 2016

Pakistan's Prevention of Electronic Crimes Act (PECA), 2016, directly addresses the issues of reliability and procedural integrity by establishing a thorough framework for the regulation and admissibility of digital evidence. PECA overcomes the traditional reluctance of courts to admit digital evidence by specifically acknowledging data, traffic data, content data, and information systems as legally viable evidence (Sections 2(xiii), 2(xviii), and 2(xx)).

Importantly, Section 164 stipulates that electronic evidence must meet requirements guaranteeing authenticity to be admitted. To meet the requirement of this authenticity and the "best evidence" requirement under Article 84 of the Qanun-e-Shahadat Order, a certificate under Section 164(4) is necessary, which must

describe the device's functionality, data processing, and integrity safeguards.

This act creates an agency, namely the National Cyber Crime Investigation Agency (NCCIA), for 'inquiry into, investigation and prosecution of the offences specified under the Act' (Section 29). This agency has exclusive powers for cybercrimes. It provides provisions of strict protocols for data preservation, search, seizure, and forensic imaging (sections 31–36). The technical complexities of evidence acquisition are tried to be addressed by the requirements for expedited preservation orders (Section 31), search and seizure warrants (Section 33), and specific protocols for handling seized data (Section 36). Furthermore, it mandates the establishment of an independent forensic laboratory (section 40).

An important ruling regarding the admissibility of digital evidence in Pakistan was made in the historic case of Ishtiaq Ahmed Mirza v. Federation of Pakistan. In this case, the Supreme Court held that if electronic evidence is shown to be genuine, trustworthy, and relevant, it may be admitted, including audio and video recordings. The Court emphasized how crucial it is to abide by the Electronic Transactions Ordinance of 2002 and Article 164 of the Qanun-e-Shahadat Order of 1984. It also emphasized that in order to prove the integrity of digital evidence, professional judgment and appropriate certification are required. Pakistan's legislative framework for managing electronic records in court proceedings was greatly updated by this case.

Legal framework in India

The Indian Evidence Act, 1872 (IEA), is the foundational evidence law in India. Its basic provisions were created for paper-based evidence, just like those of Bangladesh and Pakistan. However, the Information Technology Act, 2000 (IT Act) is the key piece of legislation that amended the IEA, and inserted Sections 65A & 65B, which expressly regulate electronic records. In addition, landmark court rulings, like State of Maharashtra v. Dr. Praful, endorsed the inclusion of electronic records in the definition of "document" (Section 3 IEA).

Section 65A simply declares that the "contents of electronic records may be proved in accordance with the provisions of section 65 B." Section 65 B deals with the requirements for the admissibility of digital evidence. It declares electronic records admissible (section 65B(1)) if they fulfill the following four mandatory conditions (section 65B (2)):

1. Information contained in the electronic record must have been produced by the computer during the time frame for which the computer was regularly used to store or process information for any activities that the person with legal control over the computer's use.
2. During the aforementioned time frame, the data was routinely fed into the computer as part of routine tasks.
3. During the said period, the computer was functioning properly, or if it wasn't, any issues didn't compromise the integrity or accuracy of the record.
4. The data in the record is a reproduction of or a derivation of data entered into the computer during routine operations.

The section also makes it compulsory that all these conditions must be "proved by a certificate". This certificate must fulfill the following criteria (section 65B(4)):

- Determine the electronic record and elaborate on the manner of the record's production.
- Explain the essentials of the relevant device.
- Fulfill the requirements of subsection 2.
- Must have the signature of a "responsible official position" who is operating or managing the device.

In Anvar P.V. v. P.K. Basheer case, the Supreme Court held that section 65B is a 'complete code', and no electronic evidence can be proven under any other provision of the Indian Evidence Act. It overruled the earlier view in State v. Navjot Sandhu (2005), which had allowed secondary evidence without strict compliance. In Shafhi Mohammad v. State of

Himachal Pradesh (2018), the court again relaxed its stringent stance and suggested that if the person having the evidence is not the party who relies on that evidence, he can seek the court's approval for the production of such evidence. However, in Arjun v. Kailash (2020), the court finally overruled the Shafhi Mohammad v. State of Himachal Pradesh (2018) decision and ruled that the 'sole' way to prove the contents of electronic evidence is section 65B. The court also reaffirmed the necessity of the certificate for admissibility; however, it also mentioned the exceptions to this.

Legal framework in Bangladesh

1. Information and Communication Technology Act, 2006 (ICT Act)

In Bangladesh, the Evidence Act, 1872 (EAB), which originally closely reflects the Indian Act (similar to Pakistan and India), is the foundational evidence legislation. The same outdated issues affect its definitions, best evidence rule, and documentary evidence provisions. The breakthrough in the digital evidence framework of Bangladesh was the Information and Communication Technology Act, 2006 (ICT Act). By granting electronic records the same legal standing as written documents (Section 6), it establishes that electronic evidence is legally admissible. Similarly, it recognizes digital (section 7) and validates electronic retention of records (section 9).

Integrity measures are required under the Act to ensure the credibility of the evidence. For instance, it renders the digital signatures as legitimate only when they are uniquely connected to and controlled by the signatory (section 16), and holds electronic records as "secure" if verifiable security protocols were followed (Section 17). The act also amends the Penal Code and Evidence to explicitly include electronic records within the definition of "document", while maintaining consistency with existing evidence frameworks (section 87).

2. Digital Security Act, 2018 (DSA)

In order to cope with new cyber threats and address the shortcomings of the ICT Act 2006, the Digital Security Act 2018 (DSA) has been introduced. This act aims at solidifying the framework of electronic evidence. It explicitly overrides the Evidence Act, 1872, by stating that, "any forensic evidence obtained or collected under this Act shall be admitted as evidence in a trial" (section 58). The act lays the foundations of the institutional framework by establishing digital forensic labs under the Digital Security Agency (section 10). On the other hand, it ensures quality control standards for these labs, so that they can meet the prescribed technical reliability criteria (Sections 11). On the same footing, the investigators have the authority to confiscate devices and traffic data that are essential to the chain of evidence, and the courts are mandated to preserve digital material for a maximum of 180 days (Section 44).

Similarly, Khaleda Akhter vs. State is a landmark decision by the Supreme Court of Bangladesh that addresses the admissibility of digital evidence. The court ruled that a video cassette that was created by recording something (like television program footage) qualifies as a "document" under Section 3 of the Evidence Act, 1872, and is therefore admissible as evidence in trial proceedings. This effectively expands the Act's scope to include audio and video recordings as documentary evidence. The court further clarified that the technological medium (such as magnetic tape) does not limit the admissibility of its contents as documentary evidence, and that the word "matter" in the statutory definition should be read in its "widest amplitude".

Discussion

An interesting interaction of common historical basis, divergent legislative approaches, and similar contemporary challenges may be expressly visible in the comparative study of the legal frameworks controlling the admissibility of digital evidence in Pakistan, India and Bangladesh. The common law historical background and the fundamental principles of the Indian Evidence Act, 1872, which was essentially created for a paper-based world, were passed down to all the said

countries. Due to this common paper-based legal origin, all three countries have to face the issue of incompatibility of traditional evidentiary procedures like the "best evidence rule" and the definition of "document". As a result, the main legislative motivation in each of the nations has been to fulfill this evidence gap, though each in a different way and with differing levels of procedural strictness.

Jurisprudential Convergences in the Legal Frameworks

There are numerous significant similarities between the legal frameworks of these three countries. The most significant among these is the common origin of these evidence law frameworks. All three have the Evidence Act 1872 at their base, and the latter acts as the foundation of evidence law in each country. However, to explicitly include the notion of digital evidence within the evidence law framework, significant legislative amendments have taken place in this core law in each of the countries. In addition, these amendments have been interpreted, admissibility requirements have been clarified, and practical application has been shaped by landmark judicial interpretations in each country. Last, but not least, all three are contemporarily facing the enduring challenges of technical complexity and crucially require judicial education to assess digital evidence and comprehend the nuances of forensic and certification procedures.

Critical divergences in the three legal frameworks

Despite having significant similarities, there are also major structural and methodological variances among these three countries. The biggest variation can be found in the degree of procedural rigidity. In this regard, perhaps the strictest framework is that of Section 65B of India, as construed by the Supreme Court. The certificate is necessarily required; failure to comply makes the evidence inadmissible, and fulfilling the four conditions can be difficult. Contrary to this strictness, in Pakistan, the framework supported by PECA's broader definitions, the establishment of the NCCIA, and mandated forensic labs, may provide a more integrated investigative and evidentiary structure.

Similar to Pakistan's Electronic Transactions Ordinance 2002, the ICT Act of Bangladesh created integrity safeguards for electronic documents and signatures (Sections 16, 17) on the one hand and gave digital signatures and electronic records the same legal standing as their paper equivalents (Sections 6, 7) on the other. Additionally, it amended the Penal Code and the Evidence Act of 1872 to define "document" in such a way that it could encompass electronic information. Furthermore, Bangladesh passed the Digital Security Act (DSA), 2018, after realizing the ICT Act's shortcomings in light of evolving cyber threats. By specifically superseding the Evidence Act about forensic evidence gathered under its provisions (Section 58), the DSA marks a significant shift in the context of electronic evidence admissibility. This act creates an institutional framework with Digital Forensic Laboratories under a Digital Security Agency (Sections 10, 11) and gives investigators the authority to seize devices and preserve data (Section 44).

Secondly, these legal frameworks differ in the institutional infrastructure. The PECA Act in Pakistan establishes the National Cyber Crime Investigation Agency (NCCIA) and mandates forensic labs. Similarly, specialized organizations and labs have been established in Bangladesh, including the Digital Security Agency and the Digital Forensic Labs under DSA. Although India also has specialized police units (such as Cyber Crime Cells), it does not have a single, comprehensive federal cyber investigation agency with an exclusive mandate like Pakistan's NCCIA, and the principal evidence statute does not require forensic lab accreditation uniformly mandated across the country.

The third major variation among the three is the presumption of integrity. By designating digital components as evidence and demanding a certificate that emphasizes functionality and

safeguards, PECA subtly promotes admissibility. For digitally collected evidence, the DSA circumvents conventional evidence rules. However, Admissibility may be more difficult under the Indian framework (IEA S.65B), which places the full burden of demonstrating system integrity and proper operation on the party seeking admission. There are no statutory presumptions in the normal course of business.

Contemporary Challenges and Systemic Hurdles

Assessing the effectiveness of these frameworks reveals common contemporary challenges to them. The certification requirement is a major procedural hurdle in each of the three nations, though it is necessary for establishing the integrity of the digital record. PECA is responsible for some restrictions regarding the conflict between privacy rights, investigative requirements, and the real-world difficulties of digital evidence. Due to this strict requirement, relevant evidence may be excluded if a technically sound certificate (India), one that fulfills Section 164(4) requirements (Pakistan), or one that relies on possibly uncertified techniques outside the DSA (Bangladesh) is not obtained. Secondly, there exists a technological gap. The judges and lawyers generally lack the expertise necessary to assess digital evidence critically or comprehend the complexities of forensic reports and certifications, which results in over-reliance or unwarranted skepticism.

This situation is due to the limited resources in establishing and running adequately equipped and staffed forensic laboratories, especially at the lower court levels in all jurisdictions. Furthermore, there is also a growing concern regarding the potential misuse of wide powers, particularly under laws like Bangladesh's DSA and Pakistan's PECA (such as real-time data collecting), and their impact on privacy rights. India's strict certificate requirement under S.65B runs the risk of injustice if important evidence is excluded because of technical non-compliance. This problem is less clearly stated but may also exist in the actual implementation of certification in Pakistan. The major divergences regarding the admissibility of digital evidence in the legal framework of the three countries are shown in Table 01.

Features	Pakistan (PECA 2016 Focus)	India (IT Act + IEA 165B)	Bangladesh (ICT Act + DSA)
Core Approach	Reliability & Integrity Focus (Judicial Discretion)	Formal Certificate Mandate (Rigid Procedure)	Reliability & Integrity Focus (Judicial Discretion)
Primary Statute	Prevention of Electronic Crimes Act, 2016	IT Act, 2000, which introduced Section 65 B in IEA 1872	ICT Act, 2006 + DSA, 2018 + Evidence Act, 1872
Admissibility Gateway	Article 164 QSO + PECA:	Sec 65B (1) IT Act/IEA: Admissible only if Sec 65B (2) conditions met	ICT Act + DSA: Admissible, court to give "due regard" to factors
Key Conditions	Reliability of generation/storage, integrity safeguards, originator ID, and other factors	Sec 65B (2) IT Act/IEA: Regular use, regular info feed, proper operation, info derived from feed	Same conditions as Pakistan
Certificate	An affidavit *can* prove conditions	Sec 65B (4) IT Act/IEA: Mandatory Certificate required (narrow exceptions)	No mandatory certificate
Major Challenges	Judicial expertise, forensic capacity	Rigidity of certificate, technical understanding	Fragmentation of laws, capacity gaps, and privacy concerns

Table 01: Major differences in the legal framework of the three countries
Source: Designed by the Author

These findings highlight the global challenge for aligning domestic digital evidence These

findings underscore the global challenge of aligning domestic digital evidence frameworks with international standards like the Budapest Convention. While all three jurisdictions reflect the Convention's emphasis on integrity and admissibility, procedural fragmentation and certification hurdles reveal gaps in harmonization. This study underscores the need for greater technical cooperation and shared protocols to fill the gap and establish digital evidentiary systems.

Conclusion

In conclusion, Pakistan, India and Bangladesh have all developed distinctive legal frameworks to handle the admissibility of digital evidence. These frameworks are based on their common historical origin of evidence law, but are influenced by particular legislative priorities and judicial interpretation. The shared issues of rigidity in admitting digital evidence, technical complexities, lack of resources, need for improving judicial capabilities, and the tussle between privacy rights and investigative effectiveness highlight the need for change and evolution in the legal frameworks of all three jurisdictions. To guarantee that these frameworks successfully fulfill their ultimate goal of securing reliable digital evidence, continuous legislative review, improved judicial and prosecutorial training in digital forensics, investments in forensic infrastructure, and nuanced judicial application of admissibility rules are highly needed. This comparative analysis contributes to understanding these evolving dynamics and highlights potential areas for cross-jurisdictional learning among these three South Asian Nations and the broader global discourse on digital evidence standards.

References

Abbasi, H. &. (2020). Admissibility of Electronic Evidence in Islamic Law and US Law-Need for a New Corroboration Theory. *MEI*, 19(1).

Abbasi, H. R. (2021). *Critical Analysis of Pakistani Law of Electronic Evidence from the Perspective of Sharī'ah and English Law-Recommendations for Pakistan,* Tahdhib-al-Afkar, 33-50

Ali, B. G. (2018). Digital evidence–an approach to safeguard from cybercrime in Bangladesh. *NDC E-JOURNAL*, 17(1), 23-41.

Angel, O. M. (2024). Digital evidence as a means of proof in criminal proceedings. *Revista de Gestão Social e Ambiental,*, 18(4), 04585-04585.

Anvar P.V. v. P.K. Basheer & Ors., 10 473. (SCC 2014).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal. (2020). *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 1. (7), 1*. SCC.

Barua, A. E. (2022). *Digital Evidence and Its Character as the Best Evidence Rule in the Law of Evidence in Bangladesh.* Doctoral dissertation, East West University.

Bharati, R. K. (2024). Forensic Bytes: Admissibility and Challenges of Digital Evidence in Legal Proceedings. *Int J Sci Res Sci & Technol*, 11(16), 24-35.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet.* Academic Press.

Digital Security Act (DSA) (2018).

Dubey, V. (2017). Admissibility of electronic evidence: an Indian perspective. *Forensic Research and Criminology International Journal*, 4(2), 58-63.

Information and Communication Technology Act. (2006).

Ishtiaq Ahmed Mirza v. Federation of Pakistan. (2019). PLD SC 675.

Khaleda Akhtar V. State, 37 (HCD 1985).

Khan, M. A. (2024). Digital Evidence, Surveillance Technology and Cybercrime: Analyzing the Impact on Criminal Law Policies in Bangladesh. *Department of Law and Justice.*

Khan, M. S. (2023). Digital Evidence and Pakistani Criminal Justice System: A Review Article. *Journal of Social Sciences Review*, 3(1), 489-498.

Khudhair, N. S. (2021). Revisiting the admissibility of electronic evidence: Indian jurisdictions and notes from other countries. *Psychology and Education*, 58(5), 1135-1148.

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

Order, Q.-e.-S. (1984).

Reith, M. C. (2002). An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3), 1-12.

Saddique, A. A. (2024). Role of Forensic Evidence in the Criminal Trials: A Legal Analysis from a Pakistan Perspective. *Research Journal of Psychology*, 2(3), 261-278.

Saeed, A. A. (2022). APPROACH OF PAKISTANI COURTS REGARDING ADMISSIBILITY OF MODERN DEVICES OR TECHNIQUES IN EVIDENCE. *Pakistan Journal of International Affairs*, 5(3).

Salman Akram Raja v. Government of Punjab, 203 (SCMR 2013).

Shafhi Mohammad v. State of Himachal Pradesh. (2018). *2*, 801. SCC.

State of Maharashtra v. Dr. Praful B. Desai. (2003). SCC 601.

State v. Navjot Sandhu, 11 SCC 600. (NCT of Delhi 2005).

Tanbir, K. (2021). Admissibility of Digital Evidence in Bangladesh. *SSRN 4274024*.

The Electronic Transactions Ordinance (ETO). (2002).

Usman, M. (2022). DIGITAL EVIDENCE: TESTIMONY OF EXPERT WITNESS in Pakistani Law. *Majallah-e-Talim o Tahqiq*, 4(1).

Vedwal, A. (2023). Admissibility of digital evidence for cybercrime investigation. *SSRN 4443356.*

Yasir Ayyaz and others v The State, 366 (LHR 2019).

Zahoor, R. A. (2022). Digital Evidence and Its Admissibility under Pakistani Law. *Journal of Development and Social Sciences*, 3(4), 51-60.