Journal for Social Science Archives

Online ISSN: 3006-3310
Print ISSN: 3006-3302
Volume 4, Number 1, 2026, Pages 2553 – 2570
Journal Home Page
https://jssarchives.com/index.php/Journal/about

Rethinking the Authentication of AI-Generated Evidence under Article 164 of the Qanun-e-Shahadat Order, 1984: Reforming Pakistan's Evidentiary Framework

Muhammad Kashan Shahzad[1], Amna Imdad[2] & Naheed Sultana[3]

[1]*LL.B (Hons), Faculty of Law, The University of Faisalabad (TUF), Pakistan, Email: ch.kashan014@gmail.com*
[2]*Lecturer, Faculty of Law, The University of Faisalabad (TUF), Pakistan, Email: amnaimdad.law@tuf.edu.pk*
[3]*Lecturer, Faculty of Law, The University of Faisalabad (TUF), Pakistan, Email: naheedsultana.law@tuf.edu.pk*

ARTICLE INFO

Article History:

Received:	*February*	*06, 2026*
Revised:	*March*	*04, 2026*
Accepted:	*March*	*16, 2026*
Available Online:	*March*	*30, 2026*

Keywords:

Artificial Intelligence, AI-Generated Evidence, Article 164, Qanun-e-Shahadat Order, Digital Evidence Authentication

Corresponding Author:
Amna Imdad
Email:
amnaimdad.law@tuf.edu.pk

ABSTRACT

Artificial intelligence (AI) is transforming the administration of justice by generating digital content that is increasingly presented as evidence in judicial proceedings. While AI-generated text, images, videos, audio recordings, and analytical outputs offer significant evidentiary value, they also create complex challenges regarding authenticity, reliability, integrity, and admissibility. In Pakistan, Article 164 of the Qanun-e-Shahadat Order, 1984 provides courts with the discretion to admit evidence produced through modern devices and scientific techniques; however, it was enacted before the emergence of sophisticated AI technologies and does not establish specific standards for authenticating AI-generated evidence. This article critically examines the adequacy of Article 164 in addressing contemporary evidentiary challenges posed by artificial intelligence. Employing a qualitative doctrinal and comparative legal research methodology, the study analyzes Pakistan's evidentiary framework alongside selected international jurisdictions to identify legislative and procedural shortcomings. The research argues that the absence of AI-specific authentication standards may undermine judicial confidence, procedural fairness, and the integrity of digital evidence. It proposes legislative amendments, technical authentication protocols, judicial capacity building, and institutional reforms to modernize Pakistan's evidentiary regime and ensure that AI-generated evidence is admitted through transparent, reliable, and legally sound mechanisms.

1. Introduction

1.1 Background of the Study

Artificial intelligence (AI) has rapidly transformed numerous sectors, including healthcare, finance, education, governance, and the administration of justice. The increasing sophistication of AI systems has enabled the generation of digital content that closely resembles human-created materials, including written documents, photographs, videos, voice recordings, and predictive analytical reports. These developments have significantly expanded the role of digital evidence in judicial proceedings while simultaneously creating unprecedented challenges regarding authenticity, reliability, and admissibility. Unlike conventional electronic evidence, AI-generated evidence may be produced, modified, or manipulated with minimal human intervention, making it increasingly difficult for courts to distinguish genuine evidence from fabricated or altered digital content. The emergence of deepfakes, synthetic media, and generative AI has therefore raised serious concerns about the integrity of judicial processes and the preservation of fair trial guarantees (Xu et al., 2026).

Pakistan's evidentiary regime primarily governs modern scientific evidence through Article 164 of the Qanun-e-Shahadat Order, 1984, which empowers courts to admit evidence produced by modern devices or techniques whenever deemed appropriate. Although this provision was progressive at the time of its enactment, it was drafted long before the development of advanced artificial intelligence technologies capable of autonomously generating highly convincing digital material. Consequently, the existing legal framework provides broad judicial discretion but lacks clear statutory standards for verifying the authenticity, reliability, provenance, and integrity of AI-generated evidence. As AI technologies continue to evolve and become increasingly accessible, the absence of comprehensive authentication mechanisms exposes Pakistan's justice system to potential evidentiary abuse, inconsistent judicial practices, and challenges to procedural fairness. These developments necessitate a critical re-evaluation of Article 164 to determine whether it remains capable of addressing the evidentiary demands of the digital age (Israel & Amer, 2023).

1.2 Research Gap

Although considerable scholarship has examined electronic evidence, cybercrime, and digital forensics within Pakistan, limited attention has been devoted specifically to the authentication of AI-generated evidence under Article 164 of the Qanun-e-Shahadat Order, 1984. Existing studies generally focus on the admissibility of electronic records without addressing the distinctive characteristics of AI-generated content, including algorithmic decision-making, deepfakes, synthetic media, explainability, and the verification of machine-generated outputs. Moreover, there remains a lack of comprehensive comparative legal analysis assessing whether Pakistan's evidentiary framework is capable of responding to emerging AI technologies. This study seeks to bridge this gap by providing a doctrinal and comparative examination of Article 164 in light of recent technological developments and by proposing a coherent legal framework for the authentication of AI-generated evidence in Pakistan.

1.3 Research Objectives

i. To critically examine the adequacy of Article 164 of the Qanun-e-Shahadat Order, 1984 in governing the authentication of AI-generated evidence in Pakistan.
ii. To identify the legal, technical, and procedural challenges associated with authenticating AI-generated evidence before Pakistani courts.

iii. To comparatively analyze the legal frameworks and authentication standards governing AI-generated evidence in selected foreign jurisdictions.
iv. To evaluate the compatibility of Pakistan's existing evidentiary framework with emerging international best practices on AI-generated evidence.
v. To propose legislative, judicial, and technical reforms for strengthening the authentication of AI-generated evidence under Article 164 of the Qanun-e-Shahadat Order, 1984.

1.4 Research Questions

i. To what extent is Article 164 of the Qanun-e-Shahadat Order, 1984 adequate for governing the authentication of AI-generated evidence in Pakistan?
ii. What legal, technical, and procedural challenges arise in authenticating AI-generated evidence before Pakistani courts?
iii. How do selected foreign jurisdictions regulate and authenticate AI-generated evidence within their evidentiary frameworks?
iv. To what extent is Pakistan's existing evidentiary framework compatible with emerging international best practices on AI-generated evidence?
v. What legislative, judicial, and technical reforms are required to strengthen the authentication of AI-generated evidence under Article 164 of the Qanun-e-Shahadat Order, 1984?

1.5 Significance of the Study

This study is significant because it addresses one of the most pressing legal challenges arising from the integration of artificial intelligence into judicial proceedings. As AI-generated evidence becomes increasingly common in civil, criminal, and commercial litigation, courts require a clear legal framework that balances technological innovation with the protection of due process and the integrity of the justice system. The research contributes to legal scholarship by examining the intersection of artificial intelligence, digital evidence, and evidentiary law within the Pakistani context, where limited academic attention has been devoted to AI-specific authentication requirements. It also provides practical value for judges, legal practitioners, policymakers, digital forensic experts, and legislators by identifying deficiencies in the current evidentiary framework and proposing reforms that enhance judicial certainty and public confidence. Furthermore, the study supports Pakistan's broader efforts to modernize its legal institutions in response to rapidly evolving digital technologies and aligns domestic evidentiary practices with emerging international standards governing AI and digital evidence (Cheng, 2025).

1.6 Research Methodology

This research adopts a qualitative doctrinal legal research methodology supported by comparative legal analysis. The study relies exclusively on secondary sources, including the Qanun-e-Shahadat Order, 1984, the Constitution of Pakistan, the Electronic Transactions Ordinance, 2002, the Prevention of Electronic Crimes Act, 2016, judicial decisions of Pakistani superior courts, foreign legislation, international AI governance instruments, law commission reports, academic books, peer-reviewed journal articles, and policy documents. Through doctrinal analysis, the research critically examines the interpretation and application of Article 164 concerning AI-generated evidence, while the comparative approach evaluates legal frameworks adopted in jurisdictions such as the United Kingdom, the United States, the European Union, and Singapore. The collected material is analyzed analytically and comparatively to identify deficiencies in Pakistan's existing evidentiary framework and to formulate practical recommendations for legislative reform, judicial guidance, and institutional capacity building aimed at strengthening the authentication of AI-generated evidence in the age of artificial intelligence.

2. Legal Framework Governing AI-Generated Evidence in Pakistan

2.1 Concept and Nature of AI-Generated Evidence

Artificial intelligence (AI) has fundamentally altered the manner in which digital information is created, processed, and presented in legal proceedings. AI-generated evidence refers to any form of evidence that is produced, analyzed, enhanced, or authenticated through artificial intelligence systems rather than exclusively through direct human intervention. Such evidence may include AI-generated text, images, videos, audio recordings, facial recognition outputs, predictive analytics, automated reports, biometric identification results, and other forms of machine-generated digital content. Unlike conventional electronic evidence, which merely records human activities, AI-generated evidence may involve autonomous decision-making, content generation, or analytical processes based on sophisticated algorithms and machine learning models (Irfan et al., 2025). This distinctive characteristic introduces unique evidentiary concerns regarding authenticity, reliability, transparency, explainability, and accountability. The increasing sophistication of generative AI technologies has also facilitated the creation of highly realistic synthetic media, including deepfake videos and cloned voices, making it increasingly difficult to distinguish genuine evidence from manipulated or fabricated content. Consequently, traditional evidentiary principles developed for conventional documents and electronic records may not adequately address the legal complexities associated with AI-generated evidence, thereby necessitating more specialized authentication mechanisms capable of ensuring evidentiary integrity and judicial confidence (Cong-Lem, 2025).

2.2 Article 164 of the Qanun-e-Shahadat Order, 1984

Article 164 of the Qanun-e-Shahadat Order, 1984 serves as the principal statutory provision governing the admissibility of evidence produced through modern devices and scientific techniques in Pakistan. The provision grants courts broad discretionary authority to admit evidence obtained through technological means whenever such evidence is considered appropriate for the administration of justice. Its flexible wording enables courts to accommodate scientific and technological advancements without requiring frequent legislative amendments. However, the provision was enacted during a period when artificial intelligence and sophisticated digital technologies had not yet emerged as integral components of judicial proceedings. As a result, Article 164 neither defines AI-generated evidence nor establishes statutory procedures for verifying its authenticity, integrity, reliability, or provenance. The absence of explicit authentication requirements creates uncertainty regarding the evidentiary value of machine-generated outputs and leaves judges to determine admissibility on a case-by-case basis. While judicial discretion promotes flexibility, excessive reliance on discretionary standards may produce inconsistent decisions and varying evidentiary thresholds across different courts. Therefore, although Article 164 provides a legal foundation for admitting technologically generated evidence, its existing framework requires reconsideration to address the distinctive challenges posed by artificial intelligence (Lee et al., 2025).

2.3 Other Relevant Pakistani Laws

The legal regulation of AI-generated evidence in Pakistan extends beyond Article 164 and is supported by several statutes governing electronic records, cybercrime, and digital transactions. The Electronic Transactions Ordinance, 2002 recognizes the legal validity of electronic documents, digital signatures, and electronic communications, thereby facilitating the admissibility of digital records in legal proceedings. Similarly, the Prevention of Electronic Crimes Act, 2016 establishes criminal offences relating to unauthorized access, cyber fraud, identity theft, digital forgery, and other cyber-related misconduct, thereby indirectly contributing to the protection of digital evidence

from unlawful manipulation (Z. Li et al., 2025). Constitutional guarantees, particularly the right to a fair trial and due process, also influence the assessment of AI-generated evidence by requiring that evidence admitted before courts be reliable, lawfully obtained, and capable of meaningful judicial scrutiny. In addition, digital forensic procedures adopted by law enforcement agencies provide technical mechanisms for preserving electronic evidence through secure collection, storage, and analysis. Nevertheless, these legal instruments primarily regulate conventional electronic evidence and cyber offences rather than the unique characteristics of AI-generated outputs. They do not establish standardized protocols for verifying algorithmic decision-making, identifying synthetic media, or determining the reliability of generative AI systems. Consequently, significant legislative gaps remain concerning the authentication and evaluation of AI-generated evidence (Kickbusch et al., 2025).

2.4 Existing Judicial Approach toward Electronic and Digital Evidence

Pakistani courts have increasingly acknowledged the evidentiary importance of electronic and digital evidence in both civil and criminal litigation. Judicial decisions have generally adopted a progressive interpretation of Article 164 by permitting the admission of electronic records where their authenticity, relevance, and integrity can be reasonably established. Courts have recognized various forms of digital evidence, including electronic documents, mobile phone records, emails, surveillance footage, computer-generated records, and digital communications, while emphasizing the importance of maintaining an unbroken chain of custody and ensuring the reliability of forensic examination. However, the judicial approach remains largely focused on conventional electronic evidence created through human activity rather than content autonomously generated by artificial intelligence (Ajunwa & Chang, 2025). Existing judicial standards provide limited guidance for evaluating algorithmic outputs, detecting AI-generated manipulation, assessing the transparency of machine learning systems, or determining the evidentiary weight of synthetic media. As AI technologies become increasingly prevalent, courts may encounter substantial difficulties in distinguishing authentic digital evidence from fabricated AI-generated content without specialized technical expertise or statutory guidance. The absence of uniform judicial standards therefore creates uncertainty in evidentiary assessment and may undermine consistency, fairness, and public confidence in judicial decision-making. These challenges highlight the urgent need to modernize Pakistan's evidentiary framework by incorporating AI-specific authentication standards, technical verification protocols, and judicial guidelines capable of addressing the evolving realities of digital justice (Zhang, 2025).

3. Challenges in Authenticating AI-Generated Evidence

3.1 Reliability and Accuracy Issues

The authentication of AI-generated evidence presents significant challenges concerning reliability and accuracy, as artificial intelligence systems are not inherently infallible. Unlike traditional documentary or electronic evidence that generally reflects human actions or recorded events, AI-generated outputs are produced through algorithms trained on extensive datasets that may contain inaccuracies, inconsistencies, or outdated information. Generative AI systems are capable of producing convincing but factually incorrect content, commonly referred to as hallucinations, where fabricated information is presented with apparent credibility. Similarly, machine learning models may generate different outputs when presented with similar inputs, raising concerns regarding consistency and reproducibility. These characteristics complicate the judicial assessment of authenticity because courts must determine not only whether the evidence is genuine but also whether the underlying AI system produced reliable and accurate results. Without standardized verification procedures and independent technical validation, AI-generated evidence may

compromise the accuracy of judicial fact-finding and increase the likelihood of erroneous legal outcomes (Grossman & Grimm, 2025).

3.2 Deepfakes and Synthetic Media

One of the most significant challenges associated with AI-generated evidence is the emergence of deepfakes and other forms of synthetic media. Modern generative AI technologies can create highly realistic images, videos, and audio recordings that are virtually indistinguishable from authentic digital content. These technologies can replicate an individual's appearance, voice, facial expressions, and mannerisms with remarkable precision, enabling malicious actors to fabricate evidence capable of misleading investigators, litigants, and courts. Deepfake technology poses serious threats to the integrity of judicial proceedings because manipulated visual or audio evidence may falsely implicate innocent individuals or undermine credible evidence presented during litigation (E. C.-Y. Li & Pang, 2024). Conventional methods of examining digital evidence are often insufficient to detect sophisticated AI-generated manipulations, particularly when advanced editing techniques remove visible traces of alteration. Consequently, courts require specialized forensic tools and technical expertise capable of identifying synthetic media and verifying its authenticity before assigning evidentiary value. Failure to develop effective authentication mechanisms may significantly weaken public confidence in digital evidence and the administration of justice.

3.3 Bias, Transparency, and Explainability

AI-generated evidence also raises concerns relating to algorithmic bias, transparency, and explainability. Artificial intelligence systems learn patterns from training data, and where such data contain historical biases, incomplete information, or discriminatory assumptions, the resulting outputs may perpetuate unfair or inaccurate conclusions. Biased AI-generated evidence may disproportionately affect certain individuals or groups, thereby undermining the principles of equality, impartiality, and fairness that are fundamental to judicial proceedings. Furthermore, many advanced AI systems operate as "black boxes," making it difficult for users, legal practitioners, and judges to understand how particular conclusions or outputs were generated. The absence of explainability limits the ability of courts to evaluate the credibility of AI-generated evidence or to effectively challenge its accuracy during adversarial proceedings. Since judicial decision-making requires transparent reasoning and verifiable evidence, reliance on opaque AI systems without adequate explanations may conflict with procedural fairness and due process. Developing explainable AI models and transparent verification standards therefore represents an essential prerequisite for the responsible admission of AI-generated evidence (Bongurala et al., 2024).

3.4 Chain of Custody and Digital Integrity

Maintaining the chain of custody and ensuring digital integrity constitute essential requirements for authenticating AI-generated evidence. The chain of custody refers to the documented process through which evidence is collected, preserved, transferred, analyzed, and presented before the court without unauthorized alteration. AI-generated evidence introduces additional complexities because digital files may be easily copied, modified, compressed, or regenerated without leaving immediately visible indications of manipulation. The use of cloud computing, automated processing systems, and distributed digital platforms further complicates the preservation of evidentiary integrity. Consequently, courts must ensure that AI-generated evidence retains its original characteristics throughout the investigative and judicial process. Technical measures such as metadata preservation, cryptographic hash verification, secure digital storage, audit trails, and forensic imaging play a vital role in protecting the integrity of digital evidence. However, Pakistan

currently lacks comprehensive statutory procedures specifically addressing the preservation and authentication of AI-generated content, creating uncertainty regarding evidentiary reliability and increasing the possibility of disputes over authenticity (Alhur, 2024).

3.5 Burden of Proof and Evidentiary Weight

The emergence of AI-generated evidence also creates uncertainty regarding the burden of proof and the evidentiary weight assigned to such material during judicial proceedings. Traditional rules of evidence generally require the party relying on evidence to establish its authenticity before it can be admitted or relied upon by the court. However, AI-generated evidence introduces additional questions concerning who should bear responsibility for demonstrating the reliability of the AI system, the validity of its underlying algorithms, the integrity of its training data, and the absence of manipulation. Courts must also determine the appropriate evidentiary weight to assign to AI-generated outputs in comparison with human testimony, documentary evidence, and expert opinions. In the absence of statutory guidance, different courts may adopt inconsistent standards when evaluating AI-generated evidence, resulting in legal uncertainty and unequal treatment of litigants. Establishing clear authentication requirements and standardized evidentiary thresholds is therefore essential to ensuring consistency, fairness, and judicial confidence in AI-assisted litigation (Abubakar et al., 2024).

3.6 Privacy, Data Protection, and Ethical Concerns

The authentication of AI-generated evidence further raises important privacy, data protection, and ethical concerns. AI systems frequently rely on extensive datasets containing personal, financial, biometric, or sensitive information to generate analytical outputs or digital content. The collection, processing, and use of such information may infringe individual privacy rights if conducted without lawful authority, informed consent, or appropriate safeguards. Moreover, AI-generated evidence may expose confidential personal information beyond what is necessary for judicial proceedings, thereby creating risks of unauthorized disclosure and misuse (Porcile et al., 2024). Ethical concerns also arise regarding accountability for AI-generated outputs, particularly where automated systems produce inaccurate or discriminatory results that influence judicial decisions. Questions concerning responsibility for algorithmic errors, transparency in AI development, and respect for fundamental human rights require careful legal consideration. As Pakistan continues to integrate emerging technologies into its justice system, balancing technological innovation with privacy protection, ethical governance, and procedural fairness will remain essential for maintaining public trust in the authenticity and legitimacy of AI-generated evidence.

4. Comparative Legal Analysis

4.1 United Kingdom

The United Kingdom has adopted a pragmatic and technology-neutral approach to the admissibility and authentication of digital evidence, enabling its legal system to respond more effectively to emerging artificial intelligence technologies. Rather than introducing AI-specific evidentiary legislation, the United Kingdom relies on established principles of evidence law, judicial discretion, and procedural safeguards to evaluate the authenticity and reliability of electronically generated evidence. Courts generally require parties to demonstrate the provenance, integrity, and relevance of digital material through appropriate forensic verification and expert testimony where necessary. As the use of generative AI and synthetic media has expanded, judicial authorities and legal institutions have increasingly emphasized transparency, disclosure obligations, and the responsible use of AI in litigation (Azhar et al., 2025). Courts also recognize

the importance of digital forensic examination in detecting manipulated content, including deepfakes and altered electronic records. This flexible yet structured approach allows the legal system to accommodate technological developments while maintaining procedural fairness and judicial confidence. Although AI-specific statutory authentication standards are still evolving, the United Kingdom provides an important example of integrating technological innovation within an established evidentiary framework through judicial oversight and technical expertise.

4.2 United States

The United States has developed one of the most advanced legal frameworks for evaluating electronically generated evidence through its well-established rules governing authentication, expert testimony, and scientific evidence. Courts generally require parties to establish that digital evidence is what it purports to be before it may be admitted during judicial proceedings. Authentication often involves digital forensic analysis, metadata examination, witness testimony, and expert verification to establish reliability and integrity. The rapid emergence of generative artificial intelligence has prompted American courts and legal organizations to develop additional safeguards addressing AI-generated documents, images, audio recordings, and videos (Shami, Ashraf, et al., 2025). Several courts have introduced procedural requirements encouraging disclosure when AI tools assist in legal drafting or evidence preparation, while judicial authorities have emphasized the importance of verifying AI-generated material before relying upon it in litigation. The American approach reflects a combination of technological adaptability and rigorous evidentiary standards, ensuring that AI-generated evidence undergoes meaningful judicial scrutiny before influencing legal decisions. This emphasis on authentication, expert evaluation, and procedural accountability provides valuable guidance for jurisdictions seeking to regulate AI-generated evidence without compromising fairness or due process (Shami, Asghar, et al., 2025).

4.3 European Union

The European Union has adopted a comprehensive regulatory strategy that prioritizes trustworthy artificial intelligence, transparency, accountability, and the protection of fundamental rights. Rather than focusing exclusively on evidentiary rules, the European approach regulates the development, deployment, and use of AI systems through risk-based governance mechanisms that classify AI applications according to their potential impact on individuals and society. High-risk AI systems are generally subject to strict requirements relating to documentation, transparency, human oversight, accuracy, and technical robustness. These regulatory principles indirectly strengthen the authentication of AI-generated evidence by promoting traceability, explainability, and accountability throughout the lifecycle of AI systems (Manzoor et al., 2025). The European legal framework also places considerable emphasis on privacy protection, data governance, and human rights, ensuring that AI-generated evidence does not undermine procedural fairness or individual liberties. By combining technological regulation with evidentiary safeguards, the European Union seeks to create an environment in which courts can rely on AI-generated information while minimizing the risks associated with manipulation, algorithmic bias, and unreliable automated decision-making. This integrated regulatory model offers useful insights for countries seeking comprehensive legal reforms in response to emerging AI technologies (Ashraf et al., 2024).

4.4 Singapore

Singapore has emerged as a regional leader in artificial intelligence governance by adopting a forward-looking legal and institutional framework that encourages technological innovation while maintaining strong regulatory oversight. Its legal system emphasizes responsible AI development, transparent governance, and effective digital evidence management within judicial proceedings.

Courts increasingly recognize the growing importance of digital evidence and rely on modern forensic methodologies to establish authenticity, integrity, and reliability. Singapore has also invested significantly in digital infrastructure, judicial modernization, and professional training to strengthen institutional capacity in handling technologically complex disputes (S. Zafar, Asghar, et al., 2024). AI governance policies promote explainability, accountability, and risk management, encouraging organizations to maintain adequate documentation regarding AI systems and their outputs. These measures facilitate the verification of AI-generated evidence by enabling judges and forensic experts to evaluate how machine-generated conclusions were produced. Singapore's experience demonstrates that successful regulation of AI-generated evidence requires not only legislative reform but also continuous judicial education, technical expertise, and coordinated institutional development capable of responding to rapidly evolving digital technologies (S. Zafar, Zaib, et al., 2024).

4.5 Comparative Lessons for Pakistan

The comparative experiences of the United Kingdom, the United States, the European Union, and Singapore demonstrate that effective regulation of AI-generated evidence depends upon a balanced combination of legislative clarity, judicial oversight, technical expertise, and institutional preparedness. Although each jurisdiction has adopted different legal strategies, several common principles emerge. These include the necessity of establishing standardized authentication procedures, strengthening digital forensic capabilities, promoting transparency and explainability in AI systems, preserving the chain of custody for digital evidence, and ensuring meaningful judicial scrutiny through expert testimony and reliable technical verification (M. U. Zafar, Baig, et al., 2024). Comparative analysis further illustrates that broad judicial discretion alone is insufficient for addressing the complex evidentiary issues created by generative artificial intelligence. Instead, modern legal systems increasingly supplement judicial discretion with statutory guidance, technical standards, ethical governance principles, and specialized institutional support. Pakistan can draw important lessons from these jurisdictions by modernizing Article 164 of the Qanun-e-Shahadat Order, 1984 through AI-specific authentication provisions, standardized forensic protocols, judicial training programs, and institutional mechanisms for verifying synthetic media and machine-generated evidence. Such reforms would strengthen legal certainty, improve consistency in judicial decision-making, and enhance public confidence in the admissibility and reliability of AI-generated evidence within Pakistan's evolving digital justice system (M. U. Zafar, Asghar, et al., 2024).

5. Critical Evaluation of Article 164 in the Age of Artificial Intelligence

5.1 Adequacy of the Existing Legal Framework

Article 164 of the Qanun-e-Shahadat Order, 1984 has long served as the principal legal basis for admitting evidence obtained through modern devices and scientific techniques in Pakistan. The provision was intentionally drafted in broad and flexible terms to enable courts to accommodate technological advancements without requiring frequent legislative amendments. This flexibility has allowed Pakistani courts to recognize various forms of electronic and digital evidence, including computer records, mobile phone data, surveillance footage, and other electronically stored information (Manzoor et al., 2024a). However, the rapid emergence of artificial intelligence has fundamentally transformed the nature of digital evidence. Unlike conventional electronic evidence, AI-generated evidence may be autonomously created, modified, or synthesized through complex algorithms that often operate without direct human intervention. Consequently, Article 164 no longer provides a sufficiently comprehensive legal framework for addressing the unique evidentiary issues associated with artificial intelligence. Although its technology-neutral language

remains valuable, the provision lacks specific guidance regarding the authentication, verification, reliability, and evidentiary assessment of AI-generated content. As AI technologies become increasingly integrated into legal processes, the existing framework appears inadequate to ensure consistency, transparency, and judicial confidence in the admission of such evidence (Adnan & Asghar, 2024).

5.2 Gaps in Authentication Standards

One of the most significant weaknesses of Article 164 is the absence of clearly defined authentication standards specifically applicable to AI-generated evidence. While the provision authorizes courts to admit evidence produced through modern devices, it does not prescribe objective criteria for establishing the authenticity or integrity of machine-generated outputs. There are no statutory requirements concerning algorithm verification, metadata analysis, provenance documentation, digital watermarking, cryptographic validation, or the disclosure of AI system characteristics (Ali et al., 2024). Furthermore, the law provides little guidance regarding the identification of manipulated content such as deepfakes, synthetic media, or AI-generated documents. Without standardized authentication procedures, courts may apply inconsistent evidentiary standards depending on the individual judge's interpretation of Article 164. Such inconsistency creates legal uncertainty, increases litigation risks, and may undermine public confidence in judicial outcomes. The absence of detailed procedural safeguards also places considerable reliance upon expert witnesses whose methodologies may differ significantly, thereby producing conflicting opinions concerning the reliability of AI-generated evidence. These shortcomings demonstrate the urgent need for comprehensive statutory standards that ensure uniformity, predictability, and evidentiary integrity (Manzoor et al., 2024b).

5.3 Judicial Discretion versus Statutory Certainty

The discretionary nature of Article 164 has historically enabled Pakistani courts to adapt evidentiary rules to emerging technologies. Judicial discretion allows courts to evaluate the relevance, authenticity, and reliability of modern evidence according to the specific circumstances of each case. While such flexibility remains beneficial in responding to technological innovation, excessive dependence upon judicial discretion becomes problematic when confronting the complex technical characteristics of artificial intelligence. Judges may possess varying degrees of technological knowledge, leading to inconsistent interpretations of AI-generated evidence across different courts (Kanwel, Asghar, et al., 2024b). In the absence of statutory standards, similar forms of AI-generated evidence may receive different evidentiary treatment depending upon individual judicial preferences or the quality of expert testimony presented by litigating parties. Such inconsistency may compromise legal certainty and reduce public confidence in the fairness of judicial proceedings. A balanced evidentiary framework should therefore preserve reasonable judicial discretion while simultaneously establishing clear legislative guidelines that define minimum authentication requirements, procedural safeguards, and technical verification standards applicable to AI-generated evidence (Chaudhary et al., 2024).

5.4 Digital Forensic Capacity in Pakistan

The effectiveness of authenticating AI-generated evidence depends not only upon legislative provisions but also upon the availability of adequate digital forensic infrastructure and technical expertise. Pakistan has made gradual progress in developing digital forensic capabilities through specialized investigative agencies and forensic laboratories. However, existing institutional capacity remains primarily designed to examine conventional electronic evidence rather than sophisticated AI-generated content. Detecting deepfakes, synthetic media, manipulated metadata,

and algorithmically generated documents requires advanced forensic software, highly trained experts, and continuously updated technological resources (Kanwel, Khan, et al., 2024b). Many investigative agencies and judicial institutions continue to face shortages of specialized personnel, technical equipment, standardized operating procedures, and professional training in emerging AI technologies. Furthermore, coordination among law enforcement agencies, forensic laboratories, prosecutors, and courts requires significant improvement to ensure consistent evidentiary handling and authentication practices. Without substantial investment in digital forensic infrastructure and institutional capacity building, legislative reforms alone will be insufficient to address the practical challenges associated with verifying AI-generated evidence in judicial proceedings (Kanwel, Khan, et al., 2024a).

5.5 Compatibility with International Best Practices

International legal developments demonstrate a growing consensus that AI-generated evidence should be regulated through transparent authentication procedures, technical accountability, and human oversight. Comparative jurisdictions increasingly emphasize explainability, traceability, algorithmic transparency, secure chain of custody, and independent forensic verification as essential components of trustworthy AI governance. Many legal systems are moving toward risk-based regulatory models that impose additional safeguards on high-risk AI applications capable of influencing judicial decision-making (Altaf, 2023). In contrast, Pakistan's evidentiary framework remains largely dependent upon the general language of Article 164 without incorporating internationally recognized principles governing AI authentication and digital integrity. Although Article 164 possesses sufficient flexibility to accommodate technological developments, its current formulation does not adequately reflect contemporary international standards concerning responsible AI governance, digital evidence verification, or procedural transparency. Aligning Pakistan's evidentiary framework with internationally accepted best practices would strengthen cross-border legal cooperation, facilitate mutual recognition of digital evidence, and improve confidence in Pakistan's judicial system within an increasingly interconnected digital environment (Kanwel, Asghar, et al., 2024a).

5.6 Need for Legislative Reform

The foregoing analysis demonstrates that Article 164 requires comprehensive legislative reform to address the evidentiary realities of artificial intelligence. Rather than replacing the existing provision, legislative reform should build upon its flexible foundation by introducing AI-specific authentication requirements and procedural safeguards. Future amendments should provide statutory definitions of AI-generated evidence, establish standardized authentication protocols, prescribe requirements for preserving digital integrity, regulate the admissibility of synthetic media, and specify the circumstances in which expert testimony and forensic verification become mandatory (Kanwel, Khan, et al., 2024c). Legislative reforms should also encourage the adoption of technical standards for algorithm transparency, digital watermarking, metadata preservation, and secure chain-of-custody documentation. In addition, specialized judicial guidelines, professional training programs, accredited forensic laboratories, and interdisciplinary cooperation between legal and technological experts should complement statutory amendments to ensure effective implementation. A modernized evidentiary framework would preserve judicial flexibility while promoting greater legal certainty, consistency, transparency, and fairness in the authentication of AI-generated evidence. Such reforms are essential to safeguarding the integrity of Pakistan's justice system and ensuring that evidentiary law remains capable of responding to the continuing evolution of artificial intelligence and digital technologies (Ch et al., 2024).

6. Legal Framework Governing the Authentication of AI-Generated Evidence under Article 164 of the Qanun-e-Shahadat Order, 1984

The admissibility and authentication of AI-generated evidence in Pakistan must be understood within the broader legal principles governing electronic and digital evidence. Although the Qanun-e-Shahadat Order, 1984 was enacted before the emergence of artificial intelligence, its provisions—particularly Article 164—have enabled courts to admit evidence generated through modern devices and scientific techniques. Pakistani superior courts have consistently interpreted this provision as sufficiently flexible to accommodate technological developments while ensuring that the authenticity, reliability, and integrity of evidence remain subject to judicial scrutiny. Judicial precedents have emphasized that technological evidence is admissible only when its source, relevance, and credibility are satisfactorily established before the court.

Article 164 grants courts discretionary authority to admit evidence produced through modern devices or scientific techniques whenever such evidence is considered appropriate for resolving disputes. This provision has served as the statutory foundation for recognizing electronic records, digital communications, surveillance footage, forensic reports, mobile phone data, and Call Detail Records (CDRs). The Supreme Court has repeatedly acknowledged that modern technology plays an increasingly significant role in criminal investigation and judicial fact-finding. Decisions reported as **2016 SCMR 274**, **2021 SCMR 522**, **2021 SCMR 873**, and **2023 SCMR 383** demonstrate the judiciary's willingness to rely upon electronically generated evidence where its authenticity is independently established. Likewise, **PLD 2019 SC 175** and **PLD 2021 SC 362** reaffirm that electronic evidence cannot be accepted mechanically; rather, courts must carefully examine its reliability, relevance, and procedural compliance before assigning evidentiary weight.

The legal treatment of electronic evidence has further evolved through numerous judgments of the superior judiciary. Earlier decisions such as **PLD 2001 SC 384** and **PLD 1976 SC 452** established important evidentiary principles concerning proof, authenticity, and judicial evaluation that continue to influence the assessment of modern digital evidence. Although these decisions predate artificial intelligence, the principles they establish regarding credibility and evidentiary reliability remain equally applicable to AI-generated materials. The gradual judicial recognition of electronic evidence has therefore created a doctrinal foundation upon which future regulation of AI-generated evidence may be constructed.

Lower courts have also contributed to the development of evidentiary jurisprudence concerning digital evidence. Decisions reported as **2022 PCrLJ 59**, **2024 PCrLJ 1**, **PLJ 2023 Cr.C. 371 (F.B.)**, **PLJ 2009 Cr.C. 271**, **2022 YLR 1822**, **1999 MLD 2989**, **2008 MLD 1442**, and **PLD 2016 Lahore 467** collectively illustrate that electronic records, including mobile phone data and CDRs, are generally admissible when supported by proper authentication and corroborative evidence. These judgments consistently emphasize that the evidentiary value of digital material depends upon maintaining an unbroken chain of custody, preserving the integrity of electronic records, and establishing their connection with the facts in issue. Courts have repeatedly cautioned that electronic evidence should not be treated as conclusive merely because it is generated through technological means; rather, it must satisfy the same standards of authenticity and reliability applicable to other forms of evidence.

The emergence of artificial intelligence has, however, introduced challenges that extend beyond conventional electronic evidence. AI-generated documents, synthetic images, deepfake videos, cloned voices, and machine-generated analytical reports may be created without direct human involvement and may closely resemble authentic digital content. Unlike traditional electronic

records, AI-generated evidence presents additional concerns regarding algorithmic transparency, explainability, automated manipulation, and the identification of synthetic media. Existing judicial precedents governing CDRs and conventional electronic evidence provide valuable guidance but do not comprehensively address these new technological complexities. Consequently, while Article 164 and the existing case law establish an important legal foundation for admitting digital evidence, they remain insufficient to regulate the authentication of AI-generated evidence comprehensively. Legislative clarification, standardized authentication protocols, advanced forensic verification mechanisms, and specialized judicial guidelines are therefore essential to ensure that Pakistan's evidentiary framework remains capable of preserving fairness, reliability, and judicial confidence in the era of artificial intelligence.

7. Recommendations

7.1 Legislative Amendments

Pakistan's evidentiary framework requires comprehensive legislative reform to effectively address the challenges posed by AI-generated evidence. Article 164 of the Qanun-e-Shahadat Order, 1984 should be amended to expressly recognize AI-generated evidence as a distinct category of digital evidence and to establish clear statutory standards for its authentication and admissibility. The amended provision should define the essential requirements for proving the authenticity, integrity, provenance, and reliability of AI-generated content before it is admitted in judicial proceedings. The legislation should also require parties relying on AI-generated evidence to disclose the nature of the AI system used, the method through which the evidence was generated, and any relevant technical information necessary for judicial evaluation. Furthermore, statutory provisions should prescribe mandatory authentication procedures for high-risk AI-generated materials such as deepfake videos, synthetic audio recordings, and machine-generated documents by requiring independent forensic verification before they are relied upon by courts. Standardized legislative definitions and authentication requirements would significantly reduce uncertainty, promote consistency in judicial decision-making, and strengthen public confidence in the administration of justice.

7.2 Judicial and Institutional Reforms

Legislative amendments alone cannot ensure the effective authentication of AI-generated evidence without corresponding judicial and institutional reforms. Continuous judicial education should be introduced to enhance judges' understanding of artificial intelligence, digital evidence, algorithmic systems, and emerging forensic technologies. Specialized training programs should enable judges to evaluate expert testimony, identify potential AI-related risks, and apply uniform evidentiary standards in technologically complex cases. Similar capacity-building initiatives should be extended to prosecutors, legal practitioners, investigators, and law enforcement officials to ensure consistent handling of AI-generated evidence throughout the criminal and civil justice process. Institutional reforms should also include the establishment of accredited digital forensic laboratories equipped with advanced technologies capable of detecting manipulated digital content, verifying metadata, examining algorithmic outputs, and identifying synthetic media. In addition, standardized judicial practice directions and evidentiary guidelines should be developed to assist courts in determining the admissibility and evidentiary weight of AI-generated material. Strengthening institutional coordination among courts, forensic experts, investigative agencies, and regulatory authorities will improve procedural consistency and ensure the reliable authentication of digital evidence across Pakistan's legal system.

7.3 Technical and Regulatory Reforms

Effective regulation of AI-generated evidence requires the adoption of robust technical standards alongside legal reforms. Pakistan should develop nationally recognized technical protocols governing the preservation, authentication, storage, and verification of AI-generated evidence throughout the evidentiary lifecycle. Standard operating procedures should require secure chain-of-custody documentation, metadata preservation, cryptographic hash verification, digital watermarking, audit trails, and secure digital repositories to prevent unauthorized alteration of electronic evidence. Regulatory authorities should establish certification mechanisms for AI systems intended to generate or process evidence used in judicial proceedings, ensuring compliance with minimum standards of transparency, accuracy, explainability, and reliability. AI developers and service providers should also be encouraged to maintain detailed documentation regarding algorithm design, training datasets, model updates, and system limitations to facilitate judicial scrutiny whenever AI-generated outputs are challenged. Furthermore, interdisciplinary cooperation between legal professionals, computer scientists, digital forensic experts, and cybersecurity specialists should be institutionalized to ensure that authentication protocols remain responsive to rapidly evolving technological developments. Such technical and regulatory reforms would substantially strengthen the credibility and integrity of AI-generated evidence presented before Pakistani courts.

7.4 Future Research and Policy Development

Given the rapid evolution of artificial intelligence technologies, legal reform should be accompanied by continuous research and evidence-based policy development. Academic institutions, research organizations, and government agencies should undertake interdisciplinary studies examining the legal, technological, ethical, and societal implications of AI-generated evidence within Pakistan's justice system. Future research should explore emerging technologies such as generative AI, autonomous decision-making systems, blockchain-based evidence preservation, explainable artificial intelligence, and advanced forensic verification techniques to determine their implications for evidentiary law. Policymakers should establish a permanent multidisciplinary advisory body comprising legal scholars, judges, technology experts, digital forensic professionals, and cybersecurity specialists to monitor international developments and recommend periodic updates to Pakistan's evidentiary framework. National AI governance policies should also incorporate judicial perspectives to ensure that technological innovation remains consistent with constitutional guarantees of due process, fairness, privacy, and access to justice. Additionally, Pakistan should strengthen international cooperation with foreign regulatory authorities, judicial institutions, and global standard-setting organizations to exchange expertise and adopt internationally recognized best practices concerning AI governance and digital evidence authentication. Through sustained legislative review, institutional learning, and policy innovation, Pakistan can develop a modern evidentiary framework capable of maintaining judicial integrity while effectively responding to the opportunities and challenges presented by artificial intelligence.

8. Conclusion

8.1 Summary of Major Findings

This study critically examined the authentication of AI-generated evidence under Article 164 of the Qanun-e-Shahadat Order, 1984 and assessed whether Pakistan's existing evidentiary framework is capable of responding to the legal challenges created by rapidly advancing artificial intelligence technologies. The analysis demonstrated that AI-generated evidence, including machine-generated text, images, videos, audio recordings, and analytical outputs, differs fundamentally from

conventional electronic evidence due to its capacity for autonomous generation, sophisticated manipulation, and algorithmic decision-making. While Article 164 provides a broad legal basis for admitting evidence produced through modern devices and scientific techniques, it does not specifically address the distinctive authentication requirements associated with artificial intelligence. The study further identified significant legal and procedural challenges, including concerns relating to reliability, deepfakes, synthetic media, algorithmic bias, lack of transparency, chain of custody, digital integrity, evidentiary weight, privacy, and ethical governance. Comparative analysis of selected jurisdictions demonstrated that many legal systems are moving toward comprehensive regulatory approaches that combine legislative guidance, technical standards, judicial oversight, and digital forensic expertise to ensure the trustworthy authentication of AI-generated evidence. These findings collectively indicate that Pakistan's existing legal framework requires modernization to maintain the integrity of judicial proceedings in the digital era.

8.2 Evaluation of Article 164

The evaluation of Article 164 reveals that although the provision has successfully facilitated the admissibility of modern scientific and electronic evidence for several decades, it no longer sufficiently addresses the complexities introduced by artificial intelligence. Its technology-neutral wording has allowed courts considerable flexibility in adapting evidentiary principles to emerging technologies, thereby avoiding unnecessary legislative rigidity. However, this flexibility is accompanied by significant uncertainty because the provision lacks statutory definitions, standardized authentication procedures, and objective criteria specifically applicable to AI-generated evidence. As a result, courts remain heavily dependent upon judicial discretion and expert testimony when determining the admissibility and evidentiary value of machine-generated material. Such reliance may produce inconsistent judicial outcomes and varying standards of authentication across different cases. Moreover, the current legal framework provides limited guidance concerning algorithmic transparency, explainability, forensic verification, metadata preservation, or the detection of sophisticated AI-generated manipulation such as deepfakes and synthetic media. The absence of specialized institutional mechanisms and technical standards further weakens the practical implementation of evidentiary safeguards. Consequently, while Article 164 continues to provide an important legal foundation for technological evidence, it requires comprehensive legislative refinement supported by institutional and technical reforms to ensure legal certainty, procedural fairness, and judicial consistency in the authentication of AI-generated evidence.

8.3 Future Outlook

The increasing integration of artificial intelligence into commercial transactions, public administration, criminal investigations, and judicial proceedings ensures that AI-generated evidence will become an increasingly common feature of future litigation. As AI systems continue to evolve in sophistication, legal frameworks governing evidence must also evolve to preserve the integrity of judicial decision-making while encouraging responsible technological innovation. Pakistan has an important opportunity to modernize its evidentiary regime by introducing AI-specific authentication standards that combine legislative clarity with technological flexibility. Future reforms should establish standardized procedures for verifying AI-generated evidence, strengthen digital forensic infrastructure, promote algorithmic transparency and explainability, and provide continuous professional training for judges, investigators, prosecutors, and legal practitioners. At the policy level, interdisciplinary collaboration among lawmakers, technology experts, academic institutions, forensic specialists, and judicial authorities will be essential for

developing responsive legal solutions capable of adapting to rapidly changing technological environments. International cooperation and alignment with emerging global standards governing trustworthy artificial intelligence will further enhance Pakistan's ability to manage cross-border digital evidence and strengthen confidence in its legal system. Ultimately, reforming Article 164 should not merely focus on accommodating new technologies but should seek to establish a balanced evidentiary framework that safeguards constitutional guarantees of fairness, due process, transparency, and judicial accountability. By adopting proactive legislative, institutional, and technical reforms, Pakistan can create a modern evidentiary system capable of ensuring that AI-generated evidence is authenticated through reliable, transparent, and legally robust mechanisms, thereby preserving the credibility and effectiveness of the administration of justice in the age of artificial intelligence.

References

1. Abubakar, U., Falade, A. A., & Ibrahim, H. A. (2024). Redefining student assessment in Nigerian tertiary institutions: The impact of AI technologies on academic performance and developing countermeasures. Advances in Mobile Learning Educational Research, 4(2), 1149–1159.
2. Adnan, S. M., & Asghar, U. (2024). A critical examination of investor protection under the Securities and Exchange Commission of Pakistan about investment policies in Pakistan. Southern Journal of Social Sciences, 2(02), 41–52.
3. Ajunwa, I., & Chang, C. K. (2025). Provenance. Available at SSRN 5707362.
4. Alhur, A. (2024). Redefining healthcare with artificial intelligence (AI): the contributions of ChatGPT, Gemini, and Co-pilot. Cureus, 16(4), e57795.
5. Ali, S. M., Ch, S. N., & Asghar, U. (2024). A HISTORICAL JURISPRUDENTIAL PERSPECTIVE ON THE EAST INDIA COMPANY'S IMPACT ON THE SUB-CONTINENTAL JUDICIAL SYSTEM AND ITS PERSISTENCE IN MODERN PAKISTANI LAW. PAKISTAN ISLAMICUS (An International Journal of Islamic & Social Sciences), 4(02), 119–126.
6. Altaf, S. (2023). Impact of Cyber Harassment on the Self-Esteem and Academic Achievements of Pakistani Adolescents: In Gender Perspective. Zenodo (CERN European Organization for Nuclear Research).
7. Ashraf, C., Asghar, U., & Khan, I. A. (2024). SOLITARY CONFINEMENT IN UK POLICE CUSTODY: MISCARRIAGES OF JUSTICE AND CONFESSIONS BROUGHT ON BY THE ACCUSED'S PSYCHOLOGICAL COLLAPSE AND SUFFERING. International Journal of Social Sciences Bulletin, 2(4), 2324–2337.
8. Azhar, S., Rizvi, S. A. A., & Asghar, U. (2025). Criminal procedure code in Pakistan: Evaluating the process and challenges in investigating crimes. The Critical Review of Social Sciences Studies, 3(2), 789–799.
9. Bongurala, A. R., Save, D., Virmani, A., & Kashyap, R. (2024). Transforming health care with artificial intelligence: redefining medical documentation. Mayo Clinic Proceedings: Digital Health, 2(3), 342–347.
10. Ch, S. N., Abbas, R., & Asghar, U. (2024). Socio-Economic Implications of Delayed Justice: An investigation in to the recent practices in Pakistan. Pakistan Journal of Criminal Justice, 4(1), 121–133.
11. Chaudhary, S. I., Asghar, U., & Afzal, M. (2024). Examining restorative justice: Different approaches in Islamic customary law and international practices. PAKISTAN ISLAMICUS (An International Journal of Islamic & Social Sciences), 4(02), 41–54.

12. Cheng, E. K. (2025). Deepfakes, Photographs, and Trust in Evidence. Virginia Law Review Online.
13. Cong-Lem, N. (2025). Rethinking evidence-informed policy and practice in the age of generative artificial intelligence. London Review of Education, 23(1), 1–8.
14. Grossman, M., & Grimm, P. (2025). Judicial approaches to acknowledged and unacknowledged AI-generated evidence. Science and Technology Law Review, 26(2).
15. Irfan, M., Bennett, O., & Müller, A. (2025). Synthetic Evidence and Procedural Fairness: Admissibility Standards for AI-Generated Outputs in Civil and Criminal Courts. International Journal of Law, Policy and Scientific Research, 1(1), 60–73.
16. Israel, M. J., & Amer, A. (2023). Rethinking data infrastructure and its ethical implications in the face of automated digital content generation. AI and Ethics, 3(2), 427–439.
17. Kanwel, S., Asghar, U., & Khan, M. I. (2024a). Beyond Punishment: Human Rights Perspectives on Crime Prevention. Pakistan JL Analysis & Wisdom, 3, 14.
18. Kanwel, S., Asghar, U., & Khan, M. I. (2024b). From Violation to Vindication: Human Rights in the Aftermath of Crime. International Journal of Social Science Archives (IJSSA), 7(2).
19. Kanwel, S., Khan, M. I., & Asghar, U. (2024a). Crimes and Consequences: A Human Rights-Based Approach to Criminal Justice. International Journal of Human and Society, 4(01), 1073–2024.
20. Kanwel, S., Khan, M. I., & Asghar, U. (2024b). Human rights at the crossroads: Navigating criminal justice challenges. PAKISTAN ISLAMICUS (An International Journal of Islamic & Social Sciences), 4(01), 139–149.
21. Kanwel, S., Khan, M. I., & Asghar, U. (2024c). In the Shadow of Justice: Human Rights Implications of Criminal Acts. Journal of Asian Development Studies, 13(1), 578–585.
22. Kickbusch, S., Ashford-Rowe, K., Kemp, A., Boreland, J., & Huijser, H. (2025). Beyond detection: Redesigning authentic assessment in an AI-mediated world. Education Sciences, 15(11), 1537.
23. Lee, T., Lee, S., & Kim, S. (2025). Beyond Static Scoring: Enhancing Assessment Validity via AI-Generated Interactive Verification. ArXiv Preprint ArXiv:2512.12592.
24. Li, E. C.-Y., & Pang, K.-W. (2024). Fandom meets artificial intelligence: Rethinking participatory culture as human–community–machine interactions. European Journal of Cultural Studies, 27(4), 778–787.
25. Li, Z., Yi, W., & Chen, J. (2025). Beyond Accuracy: Rethinking Hallucination and Regulatory Response in Generative AI. ArXiv Preprint ArXiv:2509.13345.
26. Manzoor, B., Asghar, U., Ch, S. N., & Sarwar, S. (2025). Revisiting the jus ad bellum: a critical analysis of the right of self-defense and the prohibition on the use of force under international law. ASSAJ, 3(01), 54–64.
27. Manzoor, B., Asghar, U., & Fatima, M. (2024a). Investigating the Effects of Poverty on Pakistani Youth and Methods for Reaching the Sustainable Development Goals. Qlantic Journal of Social Sciences, 5(2), 337–347.
28. Manzoor, B., Asghar, U., & Fatima, M. (2024b). Investigating the Effects of Poverty on Pakistani Youth and Methods for Reaching the Sustainable Development Goals. Qlantic Journal of Social Sciences, 5(2), 337–347.
29. Porcile, G. J. A., Gindi, J., Mundra, S., Verbus, J. R., & Farid, H. (2024). Finding AI-generated faces in the wild. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 4297–4305.
30. Shami, A. Z. A., Asghar, U., & Ashraf, C. (2025). Data Protection and Cyber Security Laws in Pakistan: Addressing Digital Privacy in E-Commerce and Consumer Data. Dialogue Social Science Review (DSSR), 3(3), 524–536.

31. Shami, A. Z. A., Ashraf, C., & Asghar, U. (2025). International Arbitration in Energy Disputes: Lessons from UNCITRAL Case Laws. ACADEMIA International Journal for Social Sciences, 4(1), 175–184.
32. Xu, Z., Zhang, X., Xu, Y., Huang, Q., Chen, S., Yao, T., Ding, S., & Zhang, J. (2026). Genshield: Unified detection and artifact correction for ai-generated images. ArXiv Preprint ArXiv:2605.16122.
33. Zafar, M. U., Asghar, U., & Fatima, M. (2024). Social Economic and Administrative Hurdles to Health and Wellbeing: Evidence from Punjab, Pakistan's growing immunization program. Competitive Research Journal Archive, 2(04), 1–14.
34. Zafar, M. U., Baig, K., & Asghar, U. (2024). Ecological, Societal and Executive Management Leadership Development for Long-Term Sustainability in Academic Institutions. Pakistan Journal of Humanities and Social Sciences, 12(2), 1795–1803.
35. Zafar, S., Asghar, U., & Zaib, M. S. (2024). Exploring Crimes against Humanity and War Crimes: The Role of International Criminal Law in Addressing Atrocities. The Journal of Research Review, 1(04), 185–197.
36. Zafar, S., Zaib, M. S., & Asghar, U. (2024). The progression of forensics and transitional justice within the framework of technological advancements in the justice system. The Critical Review of Social Sciences Studies, 2(2), 725–751.
37. Zhang, H. (2025). The Evidentiary Value of AI-Generated Data: A Framework for Reliability and Admissibility. Education and Social Work, 2(2), 34–41.