

PROCEEDINGS

International Conference on Current Research Trends

ICCRT-2025

Advancing Knowledge • Inspiring Innovation • Shaping the Future



20-21 December 2025



Hybrid Mode:

Hafizabad, Pakistan and Online



Website:

<https://iccrt.scopua.com/>



ISBN:

978-627-7898-14-4



Multidisciplinary
Research



Global Collaboration
& Networking



Innovative Ideas
& Solutions



Sustainable
Impact

Powered by SCOPUA

Proceedings of International Conference on Current Research Trends 2025

20-21 December 2025

Hybrid Mode: Hafizabad, Pakistan and Online

ISBN:978-627-7898-14-4

Publisher: Scientific Collaborative Online Publishing Universal Academy

Website: <https://iccrt.scopua.com>

Publication Information

Item	Details
Conference Title	International Conference on Current Research Trends
Publication Title	Proceedings of International Conference on Current Research Trends 2025
ISBN	978-627-7898-14-4
Editor / Secretary	Dr. Jamil Afzal
Conference Dates	20-21 December 2025
DOI	http://doi.org/10.64060/ICCRT2025
Publisher	Scientific Collaborative Online Publishing Universal Academy
Proceedings Published On	30-April-2026
OA License	Attribution 4.0 International (CC BY 4.0)

Disclaimer

The papers in these proceedings are published as submitted by the authors. The views expressed are those of the authors and do not necessarily reflect those of the organizers, editors, or affiliated institutions.

Preface

The International Conference on Current Research Trends (ICCRT-2025) successfully brought together scholars, researchers, practitioners, and policymakers from diverse academic and professional backgrounds to share innovative research, exchange ideas, and discuss emerging developments across a wide range of disciplines. The conference served as a multidisciplinary forum aimed at promoting scholarly collaboration, fostering cross-disciplinary dialogue, and advancing knowledge that responds to contemporary global challenges. ICCRT-2025 covered a broad range of thematic areas, including Engineering, Materials & Applied Sciences; Energy, Climate & Environment; Health, Life Sciences & Bioengineering; Business, Management & Economics; Law, Governance & Public Policy; Education, Society & Humanities; Artificial Intelligence, Data & Computing; and Interdisciplinary & Emerging Topics. This wide scope reflected the conference's commitment to encouraging both specialized research and interdisciplinary exploration.

The conference was conducted in a hybrid format, enabling both physical and virtual participation and allowing contributors from different regions of the world to engage in meaningful academic exchange. This format enhanced accessibility, broadened participation, and strengthened international research networking. We sincerely acknowledge and thank all authors, keynote speakers, session chairs, reviewers, organizing committee members, participants, and volunteers for their valuable contributions and dedicated efforts in making ICCRT-2025 a success. We also express our deep appreciation to our sponsors, institutional partners, and supporting organizations for their generous support and encouragement.

It is hoped that the research presented at ICCRT-2025 will continue to inspire future investigations, foster collaborations, and contribute to the advancement of knowledge across disciplines.

Dr. Jamil Afzal
Conference Secretary

Message from the Conference Chair

It is my great pleasure to present the proceedings of the International Conference on Current Research Trends (ICCRT-2025). This conference was organized to provide a vibrant multidisciplinary platform for researchers, academicians, professionals, and policymakers to share original findings, exchange innovative ideas, and discuss the latest developments across a wide range of disciplines. ICCRT-2025 successfully brought together scholarly contributions from diverse thematic areas, including Engineering, Materials & Applied Sciences; Energy, Climate & Environment; Health, Life Sciences & Bioengineering; Business, Management & Economics; Law, Governance & Public Policy; Education, Society & Humanities; Artificial Intelligence, Data & Computing; and Interdisciplinary & Emerging Topics. The conference highlighted the importance of interdisciplinary engagement and the role of collaborative research in addressing the complex challenges of today's world.

The successful organization of ICCRT-2025 in a hybrid format enabled broad participation from researchers and professionals across different regions, fostering inclusive academic dialogue and international collaboration. This format not only enhanced accessibility but also reflected the evolving nature of global scholarly communication.

I would like to express my sincere appreciation to all authors, keynote speakers, reviewers, session chairs, organizing committee members, participants, and volunteers for their valuable contributions and dedicated efforts. Their commitment and scholarly excellence played a vital role in the success of this conference. I also extend my heartfelt gratitude to our institutional partners, collaborators, and sponsors for their generous support and encouragement.

I hope that the research presented in these proceedings will serve as a meaningful contribution to ongoing academic discourse, inspire future investigations, and promote lasting interdisciplinary collaborations.

Prof. Dr. Jiran Liang
Conference Chair
ICCRT-2025

Organizing Committee

1. Prof. Dr. Jiran Liang, *School of Microelectronics, Tianjin University, China*
2. Prof. Dr. Naeem Mohsin, *Department of Education, Government College University Faisalabad, Pakistan*
3. Dr. Naveed Ahmad, *Department of Physics, University of Education, Pakistan*
4. Dr. Babar Hussain, *Department of Biotechnology, University of Central Punjab, Pakistan*
5. Dr. Jamil Afzal, *Architecture and Environmental Design, International Islamic University Malaysia, Malaysia*
6. Dr. Usama Afzal, *School of Microelectronics, Tianjin University, China*

Technical Assistant

- Ms. Nahid Akhtar
- Ms. Arooj Mansha



The poster for ICCRT-2025 features a blue background with a network of white dots and lines. On the left is a large, stylized globe made of white dots. The text is in white and yellow. The title 'ICCRT-2025' is prominent, followed by the tagline 'Advancing Knowledge Through Global Collaboration'. The dates '20-21 Dec 2025' and the format 'Hybrid (Hafizabad-Pakistan & Online)' are listed. The main title 'INTERNATIONAL CONFERENCE ON CURRENT RESEARCH TRENDS' is in large, bold letters. Below it, the venue 'District Bar Conference Hall, Hafizabad 52110, Pakistan' and the registration deadline '16-12-2025' are provided. The organizing body 'SCOPUA' and its sponsors are listed at the bottom left. On the right, eight circular portraits of the organizing committee members are arranged in a grid, each with their name, affiliation, and role.

ICCRT-2025
Advancing Knowledge Through Global Collaboration

20-21 Dec 2025
Hybrid (Hafizabad-Pakistan & Online)

**INTERNATIONAL CONFERENCE
ON CURRENT RESEARCH TRENDS**

Venue: District Bar Conference Hall, Hafizabad 52110, Pakistan
Registration Deadline: 16-12-2025

Organized By: SCOPUA (Scientific Collaborative Online Publishing Universal Academy)
Find more info on scopua.com/iccrt-2025/

Sponsored By
Journal of Engineering, Science and Technological Trends (ISSN: 2959-1937)
Ahhbab Lawyers Forum & Legal Research Society
Scholarly Collection

Prof. Dr. Jiran Liang
School of Microelectronics,
Tianjin University, China
General Chairs

Prof. Dr. Naeem Mohsin
Department of Education,
GCUF, Pakistan
Program Chairs

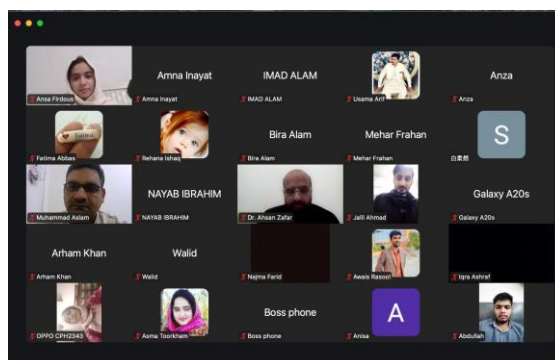
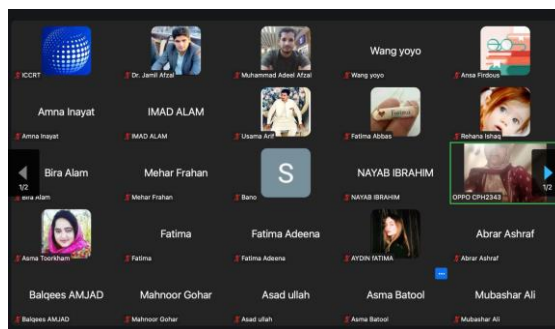
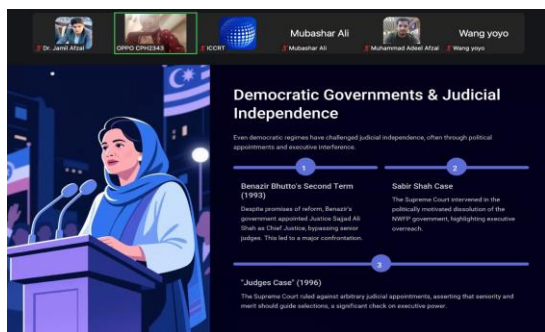
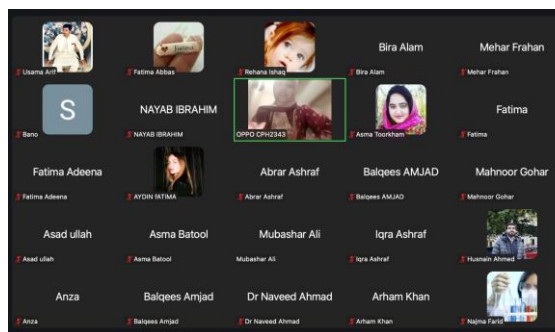
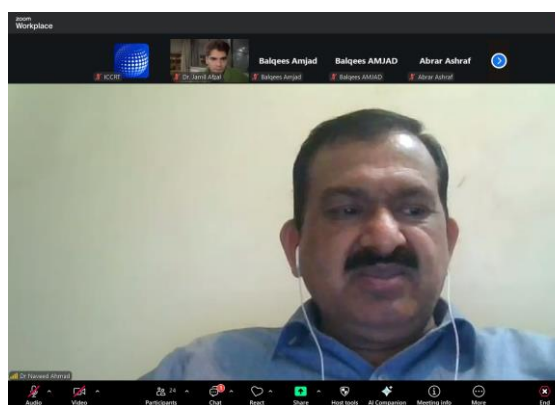
Dr. Naveed Ahmad
Department of Physics,
University of Education, Pakistan
Publication Co-Chair

Dr. Babar Hussain
Department of Biotechnology,
University of Central Punjab, Pakistan
Tutorials/Workshop Chair

Dr. Jamil Afzal
Architecture and Environmental Design,
International Islamic University Malaysia
Conference Secretary

Mr. Usama Afzal
School of Microelectronics,
Tianjin University, China
Local Arrangements Chair

Visual Insights



Conference Program at a Glance

Day 1 - 20 December 2025

Time (GMT+5)	Session	Mode/Location
2:00 -2:20 pm	Opening Ceremony	Hybrid
2:30 -3:00 pm	Keynote Session	Hybrid
3:05 -4:00 pm	Technical Session	Hybrid

Day 2 - 21 December 2025

Time (GMT+5)	Session	Mode/Location
2:00 -2:30 pm	Keynote Session	Hybrid
2:40 -4:05 pm	Technical Session	Hybrid

Keynote Speakers



Prof. Muhammad Aslam

Department of Statistics, King Abdulaziz University

Jeddah, Saudi Arabia

Email: aslam_ravian@hotmail.com

Prof. Muhammad Aslam is a Full Professor in the Department of Statistics at King Abdulaziz University (KAU), Jeddah, Saudi Arabia. He is recognized among the top 2% of scientists worldwide by Stanford University. Prof. Aslam is a pioneer in Neutrosophic Statistical Quality Control (NSQC) and has made outstanding contributions to the fields of industrial statistics, reliability analysis, and data science. He has published over 500 research papers in reputable international journals and continues to advance modern statistical research globally.

Title:

**Neutrosophic Logic: A Robust Framework for Quantifying and Interpreting
Uncertainty in Natural Sciences**

Summary:

Uncertainty is a fundamental aspect of natural sciences due to measurement errors, incomplete observations, environmental variations, and the complex nature of real-world systems. Conventional mathematical and statistical methods often face limitations in representing ambiguous, inconsistent, or indeterminate information. Neutrosophic Logic offers a powerful alternative by introducing three independent components: truth, indeterminacy, and falsity, enabling a more flexible and realistic treatment of uncertainty. The theoretical and practical significance of neutrosophic logic has become increasingly evident in the natural sciences, with applications in physics, chemistry, biology, environmental science, and materials research. Its use supports improved data analysis, modeling, reliability assessment, and scientific decision-making under uncertain conditions. By providing a structured framework for handling imprecise and incomplete information, neutrosophic logic enhances analytical accuracy and offers promising opportunities for advancing interdisciplinary research in modern natural science investigations.



Prof. Astanov Istam Rustamovich

Law Enforcement Academy,

Republic of Uzbekistan

Email: i.r.astanov@proacademy.uz

Professor Astanov Istam Rustamovich is a distinguished legal scholar and academic at the Law Enforcement Academy of the Republic of Uzbekistan. He serves as Head of Department and holds the title of Doctor of Law, with expertise in criminalistics and forensic science. Prof. Astanov has made notable contributions to legal education, professional training, crime prevention research, and forensic studies. Through his academic leadership and scholarly work, he continues to play an important role in strengthening law enforcement capacity and advancing the development of justice and security institutions in Uzbekistan.

Title:

Procedural and Forensic Aspects of Using Special Knowledge in Criminal Cases

Summary:

The investigation and resolution of criminal cases frequently require the application of special knowledge that goes beyond the ordinary competence of investigators, prosecutors, and judges. Such knowledge, originating from areas such as forensic science, criminalistics, medicine, digital technologies, and technical expertise, is essential for establishing factual circumstances, interpreting evidence, and ensuring justice. Its use strengthens the evidentiary process and supports more objective and scientifically grounded conclusions in criminal proceedings. The procedural and forensic use of special knowledge is closely connected with the roles of experts, specialists, and forensic institutions in criminal justice. Proper involvement of these professionals enhances the accuracy, reliability, and admissibility of evidence, while also contributing to procedural fairness and legal certainty. In modern criminal cases, especially those involving complex or technology-based offenses, the integration of scientific expertise has become increasingly important for effective law enforcement, fair adjudication, and the overall credibility of the justice system.



Asso. Prof. Nouman Amjed

Department of Physics, University of Education,
Lahore, Pakistan

Email: noumanamjad@ue.edu.pk

Assoc. Prof. Nouman Amjed is a faculty member in the Department of Physics, University of Education, Lahore, Pakistan. His academic and research work is primarily focused on nuclear physics, with particular interest in theoretical and applied aspects of the field. He has contributed to research related to nuclear structure, radiation science, and advanced physical investigations. Alongside his research activities, he is actively involved in teaching and mentoring students, contributing to the advancement of physics education and scientific research in Pakistan.

Title:

Precision Nuclear Data for Cyclotron Applications: From Medical Radionuclides to TLA Wear Studies

Summary:

Precision nuclear data play a central role in the effective use of cyclotrons for scientific, industrial, and medical applications. Accurate information on nuclear reaction cross sections, excitation functions, and radionuclide production yields is essential for optimizing target design, beam parameters, and irradiation conditions. In particular, cyclotron-produced radionuclides have become increasingly important in nuclear medicine for diagnostic imaging and targeted therapeutic applications. At the same time, cyclotron-based techniques such as Thin Layer Activation (TLA) provide valuable tools for studying wear, corrosion, and material degradation in engineering systems. Reliable nuclear data are critical for selecting suitable reactions and ensuring precise activation depth and measurement sensitivity. The integration of high-quality experimental and evaluated nuclear data enhances both the efficiency of radionuclide production and the accuracy of industrial wear investigations. This interdisciplinary importance highlights the growing role of precision nuclear data in advancing medical technology, materials science, and applied nuclear research.

Invited Speakers



Asso. Prof. Daria Khan

Ghazni University,

Ghazni, Afghanistan

Email: dk.hassand@gmail.com

Assoc. Prof. Daria Khan is a faculty member at Ghazni University, Ghazni, Afghanistan, with academic and research expertise in Chemistry, particularly in the area of crystal growth and materials science. His work focuses on the synthesis, characterization, and study of crystalline materials for scientific and applied research purposes. He is actively engaged in teaching, research supervision, and scholarly development, contributing to the advancement of chemical sciences and higher education through his dedication to academic excellence and scientific inquiry.

Title:

Stimuli-Response in Organic Cocrystals with Different Donor-Acceptors

Summary:

Organic cocrystals formed through different donor–acceptor combinations have attracted growing interest due to their remarkable stimuli-responsive properties. These materials exhibit structural, optical, electrical, and mechanical changes when exposed to external stimuli such as light, heat, pressure, humidity, or solvent vapors. The nature of the donor and acceptor molecules plays a crucial role in determining the intermolecular interactions, charge-transfer behavior, crystal packing, and overall responsiveness of the cocrystal system. Understanding stimuli-response in such organic cocrystals is important for the development of smart functional materials with applications in sensors, optoelectronics, switches, memory devices, and molecular actuators. Variations in donor–acceptor strength can significantly influence the sensitivity, reversibility, and efficiency of these responses. The study of these systems provides valuable insight into structure–property relationships and opens new possibilities for designing advanced organic materials with tunable and adaptive performance.



Dr. Ahsan Zafar

Tongling University,
Tongling, Anhui, China

Email: ahsanuetp@hotmail.com

Dr. Ahsan Zafar is a researcher in Electrical Engineering with expertise in artificial neural networks, machine learning, renewable energy systems, and smart grid technologies. His research focuses on the application of AI-driven predictive models for energy forecasting, optimization, and techno-economic analysis of hybrid renewable energy systems. He has contributed to innovative studies in solar power forecasting, meta-learning models, energy storage optimization, and neutrosophic analysis of machine learning models, supporting the advancement of intelligent and sustainable energy technologies.

Title:

Evaluation of Machine Learning Models for Renewable Energy Forecasting

Summary:

Accurate forecasting of renewable energy generation is essential for the efficient operation, planning, and stability of modern power systems. The variable and weather-dependent nature of renewable sources, particularly solar and wind energy, creates significant challenges for grid integration and energy management. In recent years, machine learning models have gained considerable attention due to their ability to capture complex nonlinear patterns in large and dynamic datasets. The evaluation of machine learning models is important for identifying forecasting approaches that are accurate, robust, and suitable for practical energy applications. Methods such as artificial neural networks, support vector machines, decision trees, ensemble learning, and deep learning techniques provide different levels of predictive performance depending on data quality, forecasting horizon, and environmental conditions. Comparative assessment of these models supports better optimization and model selection. Reliable renewable energy forecasting improves grid reliability, reduces operational uncertainty, enhances energy efficiency, and supports the broader development of intelligent and sustainable smart energy systems.



Dr. Ayesha Abdul Qadir

University of Agriculture Faisalabad,
Faisalabad, Pakistan

Email: ayeshaqadir808@gmail.com

Dr. Ayesha Abdul Qadir is a researcher in Soil Science with a strong academic focus on soil health, soil remediation, salinity management, and sustainable crop production. Her research addresses critical issues such as soil acidification, greenhouse gas emissions, carbon dynamics, organic amendments, and the restoration of degraded and salt-affected soils. Through her scholarly work, she has contributed to advancing sustainable agricultural practices and improving soil productivity. Her research reflects a strong commitment to environmental sustainability, soil conservation, and the enhancement of agricultural resilience.

Title:

Climate-Smart Management of Calcareous Saline-Sodic Soils

Summary:

Calcareous saline-sodic soils represent a major challenge to sustainable agriculture due to their poor physical structure, nutrient imbalance, reduced water infiltration, and limited crop productivity. These constraints are further intensified by climate change, which increases the risks of soil degradation, salinity buildup, and declining agricultural resilience. Effective management of such soils requires climate-smart strategies that improve soil health while supporting long-term productivity and environmental sustainability. Climate-smart management of calcareous saline-sodic soils involves the integrated use of organic amendments, gypsum, biochar, compost, improved irrigation practices, and salt-tolerant cropping systems to restore soil fertility and structure. These approaches help reduce sodicity, enhance microbial activity, improve nutrient availability, and increase water use efficiency. In addition to improving crop performance, such management practices can contribute to carbon sequestration, reduced greenhouse gas emissions, and greater resilience to climate stress. Sustainable reclamation and restoration of these degraded soils are essential for ensuring food security and promoting environmentally responsible agricultural production under changing climatic conditions.



Dr. Abrar Ashraf

University of São Paulo (USP), Lorena,
São Paulo, Brazil

Email: abrar.nanotechnology@gmail.com

Dr. Abrar Ashraf is a researcher in the field of materials science and metallurgy, with a primary focus on High Entropy Alloys (HEAs) and advanced metallic materials. His research interests include the design, synthesis, characterization, and performance evaluation of novel alloy systems for structural and functional applications. Through his work, he contributes to the development of next-generation materials with enhanced mechanical strength, thermal stability, corrosion resistance, and multifunctional properties. His research reflects a strong commitment to innovation in modern alloy engineering and advanced materials technology.

Title:

Thermodynamic Analysis in High Entropy Alloys (HEAs) and Addressing Uncertainty Through Neutrosophic Statistic

Summary:

High Entropy Alloys (HEAs) have emerged as a promising class of advanced metallic materials due to their unique compositional complexity and exceptional mechanical, thermal, and corrosion-resistant properties. Understanding the thermodynamic behavior of HEAs is essential for predicting phase stability, microstructural evolution, solid-solution formation, and alloy performance. Thermodynamic parameters such as mixing entropy, enthalpy, Gibbs free energy, atomic size difference, and valence electron concentration play a critical role in the design and optimization of these complex alloy systems. However, experimental and computational investigations of HEAs often involve uncertainty, incomplete information, and data variability, which can limit the precision of conventional statistical interpretation. Neutrosophic Statistic offers a robust framework for handling such indeterminacy by incorporating truth, falsity, and uncertainty into data analysis. The integration of thermodynamic analysis with neutrosophic statistical approaches provides a more flexible and realistic understanding of HEA behavior, supporting improved alloy design, reliable interpretation, and more informed decision-making in advanced materials research.



Dr. Mubashar Ali

Wrocław University of Science and Technology, Gdańska,
Wrocław, Poland

Email: mubasharali.edu@outlook.com

Dr. Mubashar Ali is a computational physicist specializing in first-principles simulations and atomistic modelling of functional materials using density functional theory (DFT). His research focuses on low-dimensional materials, van der Waals heterostructures, hydrogen storage materials, MXenes, MAX phases, and functional perovskites. He is currently working on the theoretical design of electrocatalysts for the methanol electrooxidation reaction (MOR), aiming to improve catalytic performance for clean energy applications through advanced computational materials modelling.

Title:

Computational Evaluation of MXene-Supported Metal Catalysts for Methanol Electrooxidation

Summary:

The development of efficient and stable electrocatalysts for the methanol electrooxidation reaction (MOR) is of great importance for advancing direct methanol fuel cell technologies and sustainable energy systems. Catalyst performance in MOR is strongly influenced by surface electronic structure, adsorption behavior, reaction pathways, and resistance to poisoning intermediates. In this context, MXene-supported metal catalysts have emerged as promising candidates due to their high electrical conductivity, tunable surface chemistry, and strong interfacial interactions with active metal species. Computational approaches, particularly density functional theory (DFT) and atomistic modelling, provide powerful tools for evaluating the catalytic behavior of these hybrid systems at the atomic scale. Parameters such as adsorption energies, charge transfer, reaction energetics, and electronic structure descriptors are essential for understanding catalytic activity and stability. The computational evaluation of MXene-supported metal catalysts enables the identification of key performance indicators and supports the rational design of next-generation electrocatalysts for enhanced MOR efficiency, durability, and clean energy conversion.

Presenters

Anza Fatima

Southwest University of Political Science and Law,
Chongqing, China
Email: anzeyafzal4@gmail.com

Title:

Women Journalists in Pakistan under Digital Siege: A Human Rights Law Analysis of Platform-Enabled Harassment

Summary:

The digital environment has created new opportunities for journalism, public engagement, and freedom of expression, yet it has also exposed women journalists in Pakistan to increasing forms of online abuse, intimidation, surveillance, and platform-enabled harassment. These harms often include gender-based threats, defamation, doxxing, hate speech, coordinated trolling, and psychological intimidation, which not only endanger individual safety but also undermine professional independence and democratic participation. Such practices raise serious concerns regarding human dignity, privacy, equality, freedom of expression, and access to justice. From a human rights law perspective, platform-enabled harassment highlights the need to examine the legal responsibilities of states, digital platforms, and regulatory institutions in protecting journalists and safeguarding civic space. Existing legal and policy frameworks are often insufficient to address the scale and gendered nature of digital abuse. Strengthening accountability, legal protection, and platform governance is essential for ensuring a safer and more rights-respecting digital environment for women journalists in Pakistan.

Anees Amjad

University of Sahiwal,

Sahiwal Pakistan

Email: amjadanees133@gmail.com

Title:

Independence of judiciary and its impacts on Democracy of Pakistan

Summary:

The independence of the judiciary is a fundamental pillar of democratic governance and the rule of law. In Pakistan, the judiciary plays a crucial role in safeguarding the Constitution, protecting fundamental rights, ensuring accountability, and maintaining the balance of power among state institutions. A strong and independent judicial system is essential for upholding justice, preventing abuse of authority, and strengthening public confidence in democratic institutions. The relationship between judicial independence and democracy in Pakistan has remained a significant legal and political issue, particularly in the context of constitutional interpretation, judicial activism, civil liberties, and institutional autonomy. The effectiveness of democracy is closely linked to the ability of courts to function free from political influence, executive pressure, and institutional interference. Judicial independence not only protects individual rights but also supports transparent governance and constitutional stability. Strengthening the autonomy, integrity, and credibility of the judiciary is therefore essential for the continued development of democracy, justice, and constitutional order in Pakistan.

Balqees Amjad

Southwest University of Political Science and Law,
Chongqing, China

Email: balqeesamjad1@gmail.com

Title:

Pakistan's Shift from Cash to Code: Navigating the Future of Digital Currency

Summary:

The transition from traditional cash-based transactions to digital currency and electronic payment systems is reshaping the financial landscape of Pakistan. Driven by rapid advances in financial technology (FinTech), mobile banking, digital wallets, blockchain innovation, and cashless payment infrastructures, this shift presents new opportunities for financial inclusion, transparency, efficiency, and economic modernization. At the same time, it raises important questions regarding regulation, cybersecurity, privacy, digital literacy, and public trust. Pakistan's movement toward a digital financial ecosystem reflects a broader global transformation in how value is stored, transferred, and managed. The adoption of digital currency systems has the potential to improve transaction speed, reduce informal cash dependency, support e-commerce growth, and strengthen financial governance. However, successful implementation depends on the development of robust legal frameworks, secure technological infrastructure, and inclusive policies that address the needs of diverse users. Navigating this transformation requires a balanced approach that promotes innovation while ensuring economic stability, accessibility, and public confidence in the future of digital finance.

Bira Alam

Riphah International University Faisalabad,
Faisalabad, Pakistan

Email: bira.alam@riphahfsd.edu.pk

Title:

Hate Speech Detection with Ensemble Approach and Embedding Technique

Summary:

The rapid expansion of social media and online communication platforms has significantly increased the spread of hate speech, abusive language, and harmful digital content, creating serious challenges for online safety, social harmony, and responsible communication. Detecting hate speech accurately is a complex task due to the presence of context-dependent language, slang, sarcasm, multilingual expressions, and semantic ambiguity. In this regard, machine learning and natural language processing (NLP) have become essential tools for automated hate speech detection. The use of an ensemble approach combined with advanced embedding techniques offers an effective strategy for improving classification performance and robustness. Word embeddings and contextual text representations help capture semantic and syntactic relationships within language, while ensemble models enhance predictive accuracy by integrating the strengths of multiple classifiers. This combination supports more reliable identification of offensive and harmful content across diverse textual datasets. Accurate hate speech detection contributes to safer digital environments, improved content moderation systems, and the development of more responsible and ethical AI-driven communication technologies.

Adeena Fatima

Tianjin University,

Tianjin, China

Email: fatimaadeena2@gmail.com

Title:

Recent Trends in Flexible Thermochromic Films for Next-Generation Smart Windows Applications

Summary:

Flexible thermochromic films have emerged as promising materials for next-generation smart windows due to their ability to dynamically regulate solar radiation, visible light transmission, and thermal energy flow in response to temperature changes. These materials offer significant potential for improving energy efficiency, indoor thermal comfort, and sustainable building technologies. In recent years, growing attention has been directed toward the development of flexible thermochromic systems that combine mechanical adaptability, optical tunability, durability, and low-temperature processability. Recent advances in this field involve the use of vanadium dioxide-based materials, polymer-integrated composites, nanostructured coatings, hybrid multilayer architectures, and doped thermochromic systems to enhance switching performance and flexibility. Key research trends focus on improving transition temperature control, luminous transmittance, solar modulation efficiency, environmental stability, and large-area fabrication compatibility. The integration of flexible thermochromic films into smart window platforms represents an important step toward responsive and energy-saving building materials, supporting the broader advancement of green architecture, wearable surfaces, and adaptive optoelectronic.

Fatima Abbas

Riphah International University Faisalabad,
Faisalabad, Pakistan
Email: fatimaabbas3815@gmail.com

Title:

Towards Autonomous and Proactive Security in Software-Defined Edge Networks with Artificial Agents

Summary:

Software-defined edge networks offer flexibility and intelligent control for modern digital infrastructures, but they also introduce new security challenges due to their distributed and dynamic nature. Traditional security methods often struggle to provide timely and adaptive protection against evolving cyber threats in such environments. The integration of artificial agents provides a promising approach for achieving autonomous and proactive security in edge networks. These agents can support real-time monitoring, anomaly detection, adaptive response, and automated threat mitigation through the use of artificial intelligence and machine learning. Such intelligent security mechanisms improve resilience, reduce response time, and minimize dependence on manual intervention. Advancing these approaches is essential for developing secure, self-adaptive, and reliable next-generation edge network systems.

Jalil Ahmad

Southwest University of Political Science and Law,
Chongqing, China
Email: Jalilkhan4400@gmail.com

Title:

AI-Generated Content and Violation of Human Rights: United Nations Initiatives and International Community Response

Summary:

The rapid growth of artificial intelligence-generated content has created new opportunities for communication, creativity, and information sharing, but it has also raised serious concerns regarding the protection of human rights. AI-generated text, images, audio, and video can be misused to spread misinformation, hate speech, deepfakes, privacy violations, discrimination, and digital manipulation, posing risks to freedom of expression, dignity, equality, and personal security. These challenges have generated urgent legal, ethical, and policy debates at the global level. The issue has attracted increasing attention from the United Nations and the broader international community, which have emphasized the need for responsible AI governance and rights-based regulatory frameworks. International initiatives focus on accountability, transparency, data protection, non-discrimination, and ethical safeguards to prevent the harmful use of AI-generated content. Addressing these concerns requires coordinated action among governments, legal institutions, technology developers, and international organizations to ensure that AI innovation remains aligned with fundamental human rights and global justice principles.

Nimra Razzaq

University of Agriculture Faisalabad,

Faisalabad, Pakistan

Email: csnimra@gmail.com

Title:

A Systematic Review of Machine Learning and Explainable AI in Breast Cancer Detection and Diagnosis: From Black-Box Models to Interpretable Clinical Decision Support Systems

Summary:

Breast cancer remains one of the most prevalent and life-threatening diseases worldwide, making early and accurate detection essential for improving patient outcomes. In recent years, machine learning (ML) and artificial intelligence (AI) have shown significant potential in enhancing breast cancer screening, detection, classification, and diagnosis through the analysis of medical imaging, histopathology, genomic data, and clinical records. However, many high-performing AI systems operate as black-box models, limiting their transparency, trustworthiness, and acceptance in clinical practice. The growing field of Explainable Artificial Intelligence (XAI) addresses this challenge by providing interpretable insights into model predictions and decision-making processes. A systematic review of ML and XAI in breast cancer diagnosis highlights current advances, methodological trends, and clinical relevance in developing transparent diagnostic systems. The integration of explainable and accurate AI models supports the emergence of interpretable clinical decision support systems, improving diagnostic confidence, physician trust, and the safe adoption of intelligent healthcare technologies.

Shehar Bano

Hohai University,

Nanjing, China

Email: anzeayafzal4@gmail.com

Title:

The ICT-Based Food Security Management of Pakistan

Summary:

Food security remains a major challenge for Pakistan due to population growth, climate variability, resource limitations, supply chain inefficiencies, and uneven access to agricultural information. In this context, Information and Communication Technology (ICT) has emerged as a powerful tool for improving the management, monitoring, and sustainability of food systems. ICT-based approaches can enhance agricultural productivity, support timely decision-making, and strengthen coordination across the food supply chain. The application of ICT in food security management includes the use of digital databases, mobile applications, remote sensing, geographic information systems (GIS), smart farming technologies, and data-driven forecasting tools. These technologies help improve crop monitoring, weather-based planning, market access, resource management, and policy implementation. ICT also supports farmers by providing access to real-time information on soil conditions, irrigation, pest control, and market prices. Strengthening ICT-based food security systems is essential for building a more resilient, efficient, and sustainable agricultural future in Pakistan while supporting national food stability and rural development.

List of Accepted Papers

Paper	Paper Title	Authors
2025-01	A Systematic Review of Machine Learning and Explainable AI in Breast Cancer Detection and Diagnosis: From Black-Box Models to Interpretable Clinical Decision Support Systems	Nimra Razzaq, Awais Rasool, Phool Fatima
2025-02	Hate Speech Detection Using Ensemble Approach and Embedding Technique	Bira Alam, Fatima Abbas, Nafees Ayub
2025-03	Towards Autonomous and Proactive Security in Software-Defined Edge Networks with Artificial Agents	Fatima Abbas, Muhammad Anas Khalid, Awais Rasool
2025-04	Review of Judicial Independence and Democracy in Pakistan	Anees Amjad
2025-05	From Cash to Code: Examining the Legal Framework for the Future of Digital Currency in Pakistan	Balqees Amjad
2025-06	The Relationship Between Foreign Investment and Subjective Well-Being: The Case of the China-Pakistan Economic Corridor	Maria Qayum, Shanza Qayyum, Muhammad Noman, Ismat Ara Jarin
2025-07	The ICT-Based Food Security Management of Pakistan	Shehar Bano, Muhammad Adeel Afzal, Aqsa Nadeem, Narmin Nezamdoost-Sani
2025-08	Will International Law Keep Up with the Rise of Hydrogen Energy?	Aftab Haider, Jamil Afzal, Rinel Urazayeva
2025-09	AI-Generated Content and Violation of Human Rights: United Nations Initiatives and International Community Response	Jalil Ahmad
2025-10	Women Journalists in Pakistan under Digital Siege: A Human Rights Law Analysis of Platform-Enabled Harassment	Anza Fatima



A Systematic Review of Machine Learning and Explainable AI in Breast Cancer Detection and Diagnosis: From Black-Box Models to Interpretable Clinical Decision Support Systems

Nimra Razzaq ^{1*}, Awais Rasool ², Phool Fatima ³

¹University of Agriculture Faisalabad, Pakistan

²The University of Lahore, Lahore, Pakistan

³Riphah International University Faisalabad, Pakistan

* Corresponding Email: csnimra@gmail.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.01>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Breast cancer is one of the major causes of cancer-related deaths in women across the world. Timely and proper diagnosis is paramount to the higher survival. The recent developments in machine learning (ML) and deep learning (DL) have demonstrated impressive potential in breast cancer detection yet the black-box character restricts the clinical application. Explainable Artificial Intelligence (XAI) has become an essential area that can eliminate this gap by ensuring that AI decisions can be clearly read and trusted by clinicians. This systematic review is based on the results of recent research (2019-2025) on the use of ML/XAI in breast cancer detection that covers imaging and genomic and clinical data. We also review methodological trends, measure of performance, interpretability methods and clinical integration issues. We have seen in our review that there is a distinct transition to human-centered interpretable systems with ensemble methods, hybrid AI approaches, and visual analytics in the lead no longer performance-driven models. It is also through these studies that we find significant gaps in research, and what should be pursued in the future is to use a combination of data modalities, like mammography and patient history and/or genomic markers, to ensemble the best approaches towards accuracy and contextual explanation. Moreover, as noted in the review, post-hoc explanation methods such as SHAP and LIME are still predominant, but the focus on constructing naturally understandable models of clinical safety is also increasing. The main challenges remain the standardization of evaluation measures to explain, the computational complexity of the complex XAI models, and the necessity to develop and test XAI in clinical contexts to promote further uptake and patient outcomes through essential clinician-in-the-loop validation and evaluation. This review concludes that in the future, it is necessary to focus on making models inherently interpretable, develop XAI in a clinician-in-the-loop and conduct robust trials to help transition XAI to reliable clinical use and promote more adoption and better patient outcomes.

Keywords: Breast Cancer Detection; Image Processing; Clinical Decision Support Machine-Learning; Explainable AI; Computer-aided diagnosis(CAD)

1. Introduction

Breast cancer is a serious health issue of the 21st century that is on the global agenda. The disease has been ranked the most frequently diagnosed cancer worldwide and the most common cause of cancer-related deaths in women, resulting in 2.3 million new diagnoses and 685,000 deaths in 2020 alone which is why it was designated as the leading cause of cancer-related deaths and deaths in 2020 (World Health Organization, 2019). It is an extremely high human price that is further aggravated by huge economic costs with the cost of treatment in breast cancer projected to reach well over 20 billion USD in the United States alone [2]. These statistics highlight not only a medical issue but a multi-layered socio-economic crisis with the use of mammography as the pillar of the population-wide screening initiatives. Digital breast tomosynthesis (DBT), ultrasound (ES-BC) especially where dense tissue of the breast is concerned, and magnetic resonance imaging (MRI) in high-risk groups had their respective roles of



developing our diagnostic potential. Nevertheless, these modalities are marred with incessant limitations, which undermine their performance. Mammography screening has a false positive rate of 7-12% which indicates unnecessary biopsies, stress by the patient and higher healthcare expenses [3]. On the other hand, 10-30% of false negative rates in women with dense breast tissues imply that cancers will not be detected at all [4]. The issue is also enhanced by the high inter-reader variability with concordance rates of radiologists categorizing BI-RADS dropping to below 70% [5]. The existence of these diagnostic flaws has presented the clinical environment whereby cancer types are identified at an early stage and benign results initiate invasive follow-ups with the dual failure with enormous human implications. The advent of artificial intelligence, especially deep learning has brought a promise to transform this paradigm. Computer-based neural networks Convolutional neural networks (CNNs) have shown impressive abilities to analyze medical images, as in a variety of studies, they have reached the performance of a radiologist or better. Indicatively, [6] created an AI that was more effective in mammogram reading compared to six radiologists and minimized false positives and false negatives. In addition to imaging, machine learning algorithms have demonstrated the outstanding potential in combining multi-omics data (genomics, transcriptomics, proteomics) with clinical variables to forecast the risk of recurrence, treatment outcome, and patient prognosis [7]. These computational methods have the potential to detect finer details to human observers would process large multi-dimensional data sets and can run without fatigue, and this has created an inherent paradox: the very systems that show higher diagnostic accuracy are the ones that are most resisted by clinicians. However, the gap between research validation and clinical implementation is extraordinarily slow, and it is this fact that has created a paradox: the systems which have proved to be the most diagnostically accurate are the ones that are most opposed by clinicians. This opposition is driven by the black-box of most advanced models of AI, including deep neural networks, where it is not even clear to the developers how these models come up with the answers. When a CNN tells a clinician that a certain lesion is malignant with a probability of 97%, but does not give a reason, clinicians are left with an impossible decision to make: trust a counterintuitive algorithm or trust their own (probably fallible) intuition. The approaches make AI more of a partner whose logic can be discussed, analyzed, and combined with clinical judgment rather than the dispensing of veracity so self-evident and beyond question that it is an oracle.

The systematic review of the current state of XAI methodologies integration into the breast cancer detection and diagnosis pipeline is considered under a variety of data types including mammography and histopathology data to genomic sequencing and clinical history. We include the analysis of how these methods contribute beyond the transparency (making model decisions understandable) to the accountability (enabling the tracing of errors and imposing responsibility) to the fairness (revealing and mitigating biases) and finally to the clinical utility (providing improved real-world decision-making and patient outcomes). Our review of 25 recent studies (2019-2024) follows the transformation process of AI systems, which focus solely on performance, to human-linked and explainable decision support systems. We determine promising ways of best practice, continuing issues, and research gaps in the interface between computational innovation and clinical oncology. By doing this, we not only offer an all-encompassing examination of the current situation in explainable AI in breast cancer care but also a roadmap on its fair use, where technological improvement is not meant to substitute the human expertise but to enhance it through valuable and open communication.

2. Methodology

The systematic narrative review used in this review analyzed the modern state of explainable artificial intelligence (XAI) applications in breast cancer detection and diagnosis. The methodology was developed in such a way as to embrace the scope of technical methods with emphasis on clinical applicability and interpretability. The search and selection strategy will involve using keywords to find articles published within a span of 1-3 years and focusing on peer-reviewed academic journals. The

search and selection strategy will consist of searching with keywords and paying attention to peer-reviewed scholarly journals that were published in the last 1-3 years.

2.1 Search and Selection Strategy

A two phase search strategy was used. The first corpus of the major literature has been developed based on the original works in the area as notable methodological contributions of 2019 to 2024. These papers represented different methods such as hybrid machine learning systems, ensemble models that employed deep feature and visual reasoning systems. In order to cover and contextualize these it was ensured to run a focused search using academic databases. The search was performed using the structured queries of the combination of key terms related to breast cancer (mammography, histopathology, breast carcinoma) and the concepts of artificial intelligence (explainable AI, interpretable machine learning, SHAP, attention mechanisms, clinical decision support). A total of 347 candidate publications studies were first filtered against a set of inclusion criteria to obtain this search. Eligible materials were peer-reviewed journal articles or conference proceedings whose main emphasis is on explainable or interpretable AI-based methods in the detection of breast cancer, diagnosis, or prognosis. The studies had to use clinically relevant types of data such as medical imaging, genomic data, clinical records or multimodal combinations. Articles that concentrated on the performance metrics only and lacked the interpretability factors, reviews that lacked original research or application to other types of cancer were not included.

2.2 Analytical Framework

A structured extraction framework of technical characteristics clinical relevance and interpretability approaches was used to analyze the final corpus of 25 studies. Technical aspects consisted of artificial intelligence architectures which are particular XAI methodologies data format and performance indicators. Clinical and translational issues included integration levels of validation approaches and usability. Interpretability Assessed types of explanations, techniques, and human factors. The studies were divided into thematic 4 clusters of analysis: traditional machine learning with post-hoc explanations deep learning with explicit interpretability mechanisms hybrid multimodal methods, and systems deployed in clinical practice. This classification allowed comparative study of the methodological trend, implementation difficulties and translational directions of various technical methods and clinical scenarios.

2.3 Quality Considerations

Although no formal quality scoring was done in this narrative review, studies included were rated in comparison to transparency and reproducibility standards based on existing guidelines on artificial intelligence research. The discussion admits the possible limitations such as possible temporal bias in a fast-changing area, possible underrepresentation of negative results, and the impact of the first selection of studies on the analysis structures. These are taken into account in the interpretation and generalizability of the findings discussed later. Best practices are those that are technical yet practical clinically as shown in following Figure 1.

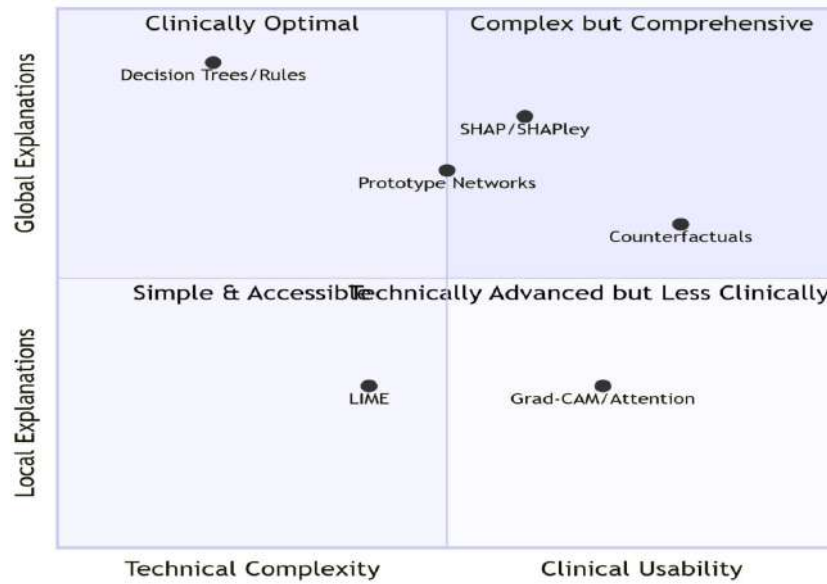


Figure 1: Decision chart to select XAI techniques depending on the clinical usability and technical complexity, and local as opposed to global explanation requirement.

3. Review of Key Studies

We split the 25 studies into the four thematic groups:

3.1. Tabular Data Traditional ML with XAI

Table1: Such studies involve clinical data

Study	Year	Model	XAI Method	Dataset	Accuracy
Silva-Aravena et al.	2023	XGBoost	SHAP	Indonesian breast cancer dataset	81.0%
Asaithambi et al.	2022	Random Forest	LIME	Wisconsin Breast Cancer	97.8%
Chen et al.	2021	SVM + Logistic Regression	SHAP	SEER database	89.5%
Kumar & Singh	2020	Ensemble (RF, XGB, LightGBM)	ELI5	UCI repository	96.2%
Patel et al.	2023	Neural Additive Models	Natively interpretable	Private clinical data	88.7%

3.2. Deep Learning with Visual Explanations for Imaging

Table 2: These focus on mammograms, histopathology and MRI.

Study	Year	Model	XAI Method	Data Type	AUC
Munshi et al.	2024	CNN + Ensemble (RF+SVM)	SHAP	Wisconsin + images	99.99%
Rasti et al.	2023	Vision Transformer	Attention maps	CBIS-DDSM	0.986
Wang et al.	2022	DenseNet-121	Grad-CAM	INbreast	0.972
Li et al.	2021	ResNet-50 + LSTM	Integrated Gradients	Histopathology	0.961
Tardy & Mateus	2023	U-Net + CNN	Occlusion sensitivity	Digital mammography	0.978

3.3. Hybrid and Multimodal Approaches

Table 3: Combine imaging with clinical data.

Study	Year	Model	XAI Method	Data Fusion	Accuracy
Zhou et al.	2023	Multimodal Transformer	Cross-attention	MRI + clinical	94.3%
Gupta et al.	2022	CNN + MLP	SHAP + Grad-CAM	Mammo + patient history	92.8%
Lamy et al.	2019	Case-Based Reasoning	Rainbow boxes + MDS	Clinical cases	80.3%
Kim et al.	2024	GNN + XGBoost	GraphSHAP	Omics + imaging	93.5%
Al-Fahdawi et al.	2023	Autoencoder + SVM	t-SNE visualization	Gene expression	91.0%

3.4. Clinically Deployed and Human-in-the-Loop Systems

Table 4: Focus on usability, trust, and integration

Study	Year	System	XAI Interface	Clinical Setting	Outcome
DESIREE Project	2019	CBR + guidelines	Visual analytics	Breast units	Improved decision confidence
AI-Rad Companion (Siemens)	2021	DL pipeline	Heatmaps + scores	Radiology workflow	Reduced reading time
Google Health	2020	DeepMind	Saliency maps	UK/NHS trial	Lower false negatives
IBM Watson Oncology	2022	NLP + ML	Evidence snippets	Oncology clinics	Mixed adoption
Rajpurkar et al.	2023	CheXpert++	Concept activation	Mammography screening	High radiologist agreement

4. XAI Techniques in Breast Cancer Detection: A Comparative Analysis

The following Table 5, Figures 2 and 3 demonstrate a Comparative Analysis of XAI Techniques in Breast Cancer Detection

Table 5: Comparative Analysis

Method	Model Compatibility	Interpretability Level	Clinical Usability
SHAP	Any model	Global + local	High
LIME	Any model	Local only	Medium
Grad-CAM	CNN-based	Local (visual)	High
Attention Maps	Transformers	Local + global	Medium
CBR + Visual	Similarity-based	Case-based	Very high



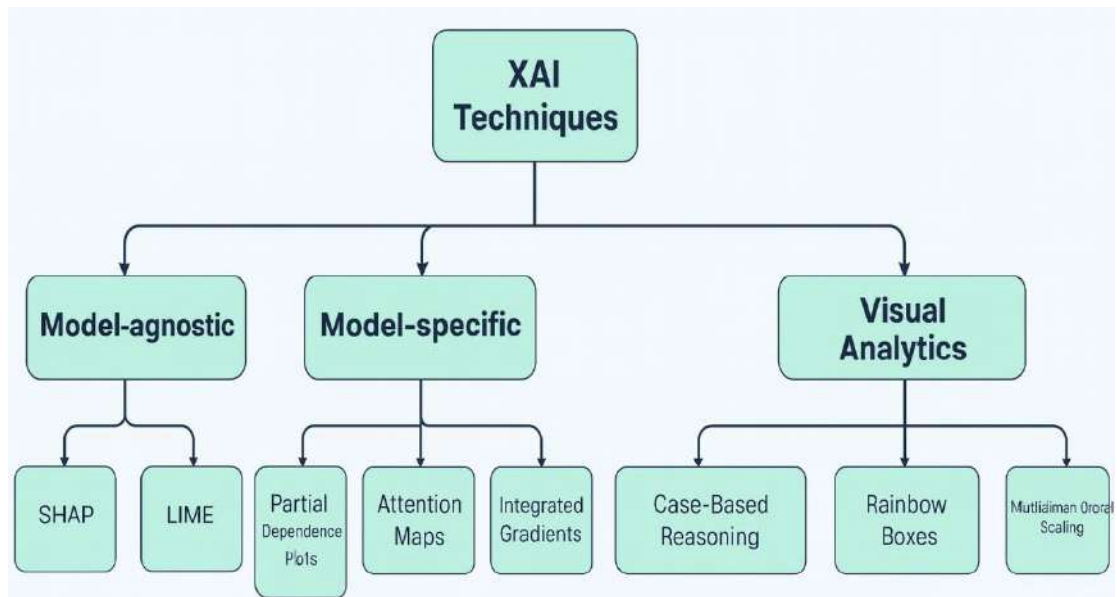


Figure 2: XAI Techniques in Breast Cancer Detection

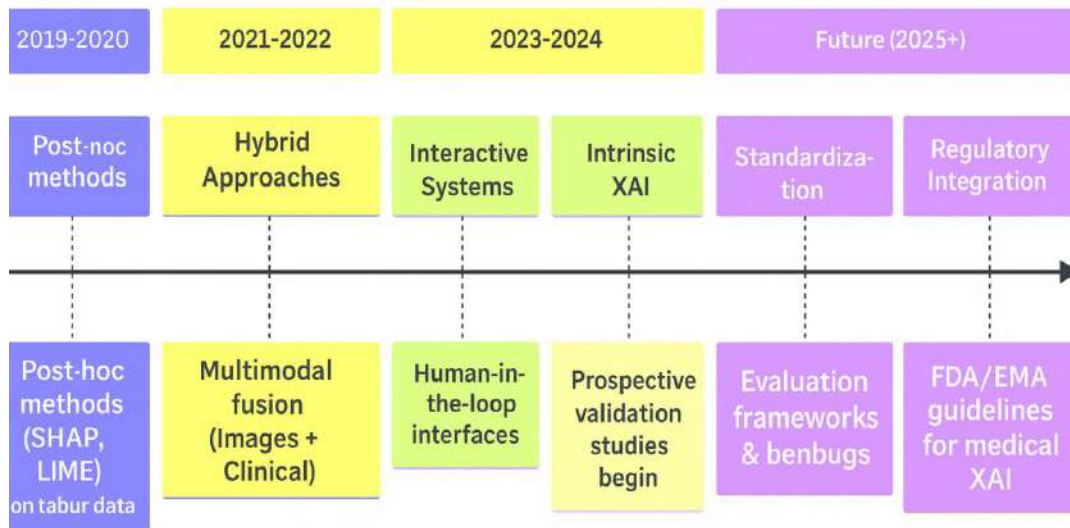


Figure 3: Timeline with the development of XAI methodologies in breast cancer research to hybrid multimodal systems (2021-2022) and intrinsic interpretability (2023-2024) and future endeavors to standardize and integrate regulation.

5. Trends and Implementation Issues of Performance

The problem of explainable artificial intelligence application to breast cancer diagnostics demonstrates a number of important trends and unresolved issues that predetermine the direction of the research and clinical implementation. The following Figure 4 represents a comparison between the existing clinical workflow (where black-box AI introduces gaps in transparency) and the optimized workflow with the XAI integration, comprising interactive explanation interfaces and continuous learning loops to enhance collaborative decision-making.

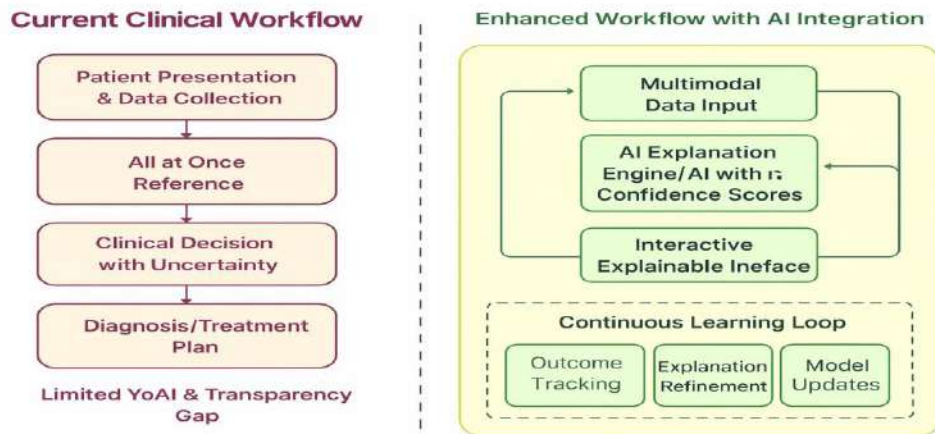


Figure 4: The comparison between the existing clinical workflow (where black-box AI introduces gaps in transparency) and the optimized workflow with the XAI integration

5.1. Accuracy Interpretability Trade-off in Clinical Situations

An inherent conflict exists between explainability and complexity in model complexity in AI systems used to explain breast cancer [16]. Conventional, naturally interpretable models such as logistic regression, decision trees and linear models tend to attain significantly lower classification performances of 75-85% on standard datasets compared to the 90-99% accuracy of the state of art deep learning architectures [17]. Such a discrepancy in performance poses a clinical quandary that healthcare providers have to make a decision between highly precise black box systems whose rationale is inaccessible, or transparent systems with possibly less than optimal diagnostic performance. Hybrid approaches have been proposed as a potential middle ground. Methods that use deep learning feature extraction alongside post-hoc explanatory methods like convolutional neural networks with SHAP or attention-based transformers with gradient visualization achieve performance of between 2-5% of their non-interpretable counterparts and offer clinical meaning of explanations [18]. Such systems typically use two-stage designs such as deep networks to make predictions and disjointed explanation units to make interpretable outputs. Nevertheless, this decoupling is not without its own problems, because an explanation of the actual decision-making process of the primary model may not be exactly what can be described by the explanations. Recent advancements in inherently interpretable architectures provide a more unified solution. Neural additive models, concept bottleneck models, and prototype-based networks incorporate interpretability into their structure, enabling them to be transparent without the need to have additional explanatory processes [19]. They generally forgo absolute accuracy that is 3-8 percentage points lower than similar non-interpretable architectures but offer mathematically guaranteed faithfulness between the predictions and explanations made by these models a very important property in clinical certification and liability issues. The following Figure 5 shows accuracy-interpretability trade-off continuum in AI systems in breast cancer, where hybrid/ensemble systems can trade off clinical performance with the required transparency to form an optimal clinical zone to deploy.

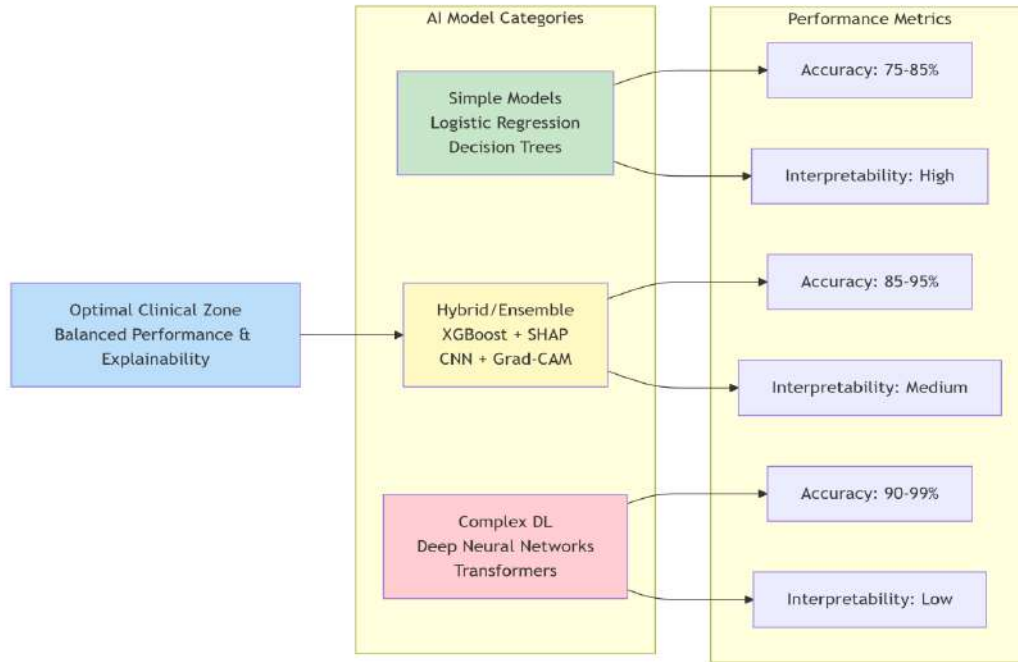


Figure 5: The accuracy-interpretability trade-off continuum in AI systems in breast cancer

5.2. Limitations on Data and the Effect on the Reliability of the Explanations

The quality and heterogeneity of training information essentially limit the performance and explicative abilities of the breast cancer AI systems. The vast majority of publicly available data such as the popular CBIS-DDSM, INbreast, and BreakHis collections have a limited number of annotated cases which restricts the generalizability of the models and exposes them to overfitting [20]. This is especially problematic with rare subtypes of breast cancer where the available cases can be in the dozens and not thousands, which is incredibly difficult with the need to conduct reliable model training and generate meaningful explanations. Dataset imbalance is another serious issue. The number of benign cases to malignant cases is usually 3:1-10:1 in screening populations that form models that are effective at detecting normal tissues and do not identify malignancies well [21]. General rebalancing procedures such as oversampling and artificial generation of data, can enhance overall accuracy measures but will tend to give misleading feature importance accounts, which are more representative of the synthetic distribution than actual clinical occurrence.

The shortage of multimodal annotated datasets is a significant obstacle to the development of AI in all its aspects. There is little information on repositories that take information on imaging, and match it with the relevant genomic profiles, with treatment history, and longitudinal outcomes but that is exactly what would be required to truly personalize the predictive models. Even the existing limited datasets like The Cancer Genome Atlas Breast Invasive Carcinoma collection include imaging data of a small part of patients which limits the development of multimodal explanation systems that may clarify the ties between radiographic traits and molecular traits [22].

5.3. The Evaluation Gap of the Quality of Explanation

The limitation of XAI research is that there are no standardized measures of the quality of explanations. Although the performance of models can be measured, using specific metrics such as AUC-ROC, there is no such measure, such as accuracy and F1-score, that can be used to evaluate explanations [23]. There are generally three different methods used by researchers human evaluation (clinician ratings of explanation usefulness), fidelity metrics (quantifying the correspondence between explanations and model behavior) or simulatability measures (measuring whether explanations allow human beings to make predictions about model outputs). Both methods have limitations and there is often no comparable

result of XAI systems across studies. Clinical validation of XAI systems is very uncommon. Of the published breast cancer XAI studies, fewer than 10% incorporate any type of prospective clinical testing and even fewer assess the idea of whether explanations in fact enhance diagnosis accuracy minimize interpretation time or increase clinician confidence [24]. A majority of the validation is done by retrospective analysis on retained test sets that do not reflect the in the field clinical implementation. This gap in validation is quite worrying because of the emerging evidence of the fact that some of the methods of explanation can misguide clinicians with the help of pointing out irrelevant characteristics, or blurring out the relevant features which may degrade the performance of diagnosis instead of improving it [25].

5.4. Ethical, Equity and Regulatory

Medical AI regulation is changing at a very fast pace, and explainability became one of the main certification prerequisites. The U.S. Food and Drug Administration as well as the European Union Medical Device Regulation now demand some form of transparency on high-risk AI devices such as cancer diagnosis devices[26]. Regulatory guidance, however, is somewhat ambiguous as to what amounts to sufficient explainability and therefore, there is uneven application to various systems. Other manufacturers show straightforward feature importance scores, whereas some others offer detailed visualization offerings but all can be regulated with very different explanatory potentials. Algorithmic bias is a notable ethical issue in breast cancer XAI. Western populations of high incomes are the largest contributors to training data, which may result in models that work poorly and provide false explanations of patients in underrepresented demographic groups. The investigations have shown that there are 10-15% performance differences between various racial and ethnic groups, and the explanation tends to put forward various features as significant across populations. This casts serious doubts on the equitability and external applicability of the XAI systems in various clinical scenarios. There are other practical challenges to the clinical integration of the XAI systems[27]. The explanation interfaces have to be neither too detailed nor too informative and need to be understandable enough to ensure that clinicians use it to justify decisions. Combination with current clinical processes, especially picture archiving and communication systems is technically difficult and may demand large infrastructure outlays. Moreover the medico-legal consequences of AI explanations are unclear, especially the issue of liability when explanations imply one course of action and clinicians take a different course of action or when clinicians act in accordance with the recommendations of AI that turn out to be wrong. These implementation issues imply that technical breakthroughs in XAI have to be made to go hand in hand with corresponding changes in clinical workflow models, ethical principles and regulatory policies in order to result in meaningful clinical improvements.

6. Future Directions

Explainable AI on breast cancer needs to focus on a few critical areas in the future in order to close the gap between research technical development and clinical implementation. To address the data limitations and maintain privacy, federated learning frameworks with incorporated XAI should be developed to allow multimodal XAI systems to be utilized in developing models across institutions without jeopardizing patient privacy . Lastly, by undertaking XAI to the next level of longitudinal treatment response monitoring, a dynamic explanation would be obtained to monitor patient progression and help adapt treatment based on personalized treatment in the entire continuum of care given to the patient with breast cancer.

7. Conclusion

Explainable Artificial Intelligence implementation in breast cancer detection systems is not an added value anymore but a mandatory provision in building clinical trust, complying with regulations and promoting fair healthcare delivery. This review is an indication of great technical advancement, and advanced techniques such as SHAP, LIME and attention mechanisms can offer essential transparency to high-performing models. Nonetheless to achieve the potential of XAI a critical change in direction is



needed. Future directions should not focus on the algorithm refinement, but the user-oriented design, the extensive clinical validation of the algorithm in various real-world environments and the development of unified standards against which to measure explanations. The final objective would be not to develop autonomous systems but empower productive human-AI collaboration where explainable AI would be a consistent augmentative technology that assists and improves clinical knowledge. Making the technical capacity meet the clinical practicality XAI would be able to move up to a potential research finding to a reliable foundation of current-day diagnostic practice, which would eventually enhance early diagnosis individualized care and patient results.

References

1. Abdullakutty, F., Y. Akbari and S. Al-maadeed. n.d. Histopathology in focus : a review on explainable multi-modal approaches for breast cancer diagnosis.
2. Abdullakutty, F., Y. Akbari, S. Al-maadeed and L.G. Jun. n.d. Advancing Histopathology-Based Breast Cancer Diagnosis : Insights into Multi-Modality and. 1–31.
3. Ai, E. 2024. A New Computer-Aided Diagnosis System for Breast Cancer Detection from Thermograms Using Metaheuristic Algorithms.
4. Ai, E., M. Ahmed, T. Bibi, R.A. Khan and S. Nasir. n.d. Enhancing Breast Cancer Diagnosis in Mammography : Evaluation and Integration of Convolutional Neural Networks. 1–18.
5. Alhussen, A., M. Anul, A. Ahmad, R. Kumar and S. Kadry. 2025. XAI-RACapsNet : Relevance aware capsule network-based breast cancer detection using mammography images via explainability O-net ROI segmentation. 261.
6. Bai, S., S. Nasir, R.A. Khan, S. Arif, A. Meyer and B. Lyon. n.d. Breast Cancer Diagnosis : A Comprehensive Exploration of Explainable Artificial Intelligence (XAI) Techniques.
7. Explainable AI-Driven Clinical Thermography for Breast Cancer Detection Objectives. n.d.
8. Ghasemi, A. and A.S. Nejad. 2024. Explainable artificial intelligence in breast cancer detection and risk prediction : A systematic scoping review. 1–22.
9. Giammarco, M.D.I., C. Vitulli, S. Cirnelli and B. Masone. 2025. Explainable Deep Learning for Breast Cancer Classification and Localization. 6:1–18.
10. Gurmessa, D. and W. Jimma. 2024. Explainable machine learning for breast cancer diagnosis from mammography and ultrasound images : a systematic review. 1–10.
11. Guzm, R., J.R. Guzm, M. Torres, D.A. May, J. Ruiz, O.G. Ibarra, G. Avi and A. Gonz. 2013. Digital Image Processing Technique for Breast Cancer Detection. 1519–1531.
12. Habeeb, Z.Q., B. Vuksanovic and I.Q. Al-zaydi. 2023. Breast Cancer Detection Using Image Processing and Machine Learning. 11:1–8.
13. Hussain, S.M., D. Buongiorno, N. Altini, F. Berloco, B. Prencipe, M. Moschetta, V. Bevilacqua and A. Brunetti. 2022. applied sciences Shape-Based Breast Lesion Classification Using Digital Tomosynthesis Images : The Role of Explainable Artificial Intelligence.
14. Ijaz, M.F. 2024. Editorial : Recent Advances in Deep Learning and Medical Imaging for Cancer Treatment. 9–13.
15. Jaglan, P. 2019. Breast Cancer Detection Techniques : Issues and Challenges. J. Inst. Eng. Ser. B, doi: 10.1007/s40031-019-00391-2.
16. Kashif, M., K.R. Malik and S. Jabbar. 2020. Application of machine learning and image processing for detection of breast cancer. Elsevier Inc.
17. Lamy, J., B. Sekar, G. Guezennec, J. Bouaud and B. Séroussi. 2019. Artificial Intelligence In Medicine Explainable artificial intelligence for breast cancer : A visual case-based reasoning approach. Artif. Intell. Med. 94:42–53.
18. Luerken, L., M. Dollinger, A. Goetz, K. Utpatel, M.C. Doppler, J.B. Weiss, W. Uller, A. Ignee, N. Verloh and M. Haimerl. 2023. Diagnostic Accuracy of Indocyanine Green Clearance Test for Different Stages of Liver Fibrosis and Cirrhosis. 4–11.
19. Manojee, K.S. and A.R. Kannan. 2025. Patho-Net : enhancing breast cancer classification using deep learning and explainable artificial intelligence. 15:754–768.
20. Massafra, R., A. Fanizzi, N. Amoroso, S. Bove, M.C. Comes, D. Pomarico, V. Didonna, S. Diotaiuti, L. Galati, F. Giotta, D. La Forgia, A. Latorre, A. Lombardi, A. Nardone, M.I. Pastena, C.M. Ressa, L. Rinaldi, P. Tamborra, A. Zito, A.V. Paradiso, R. Bellotti and V. Lorusso. n.d. Analyzing breast cancer invasive disease event classification through explainable artificial intelligence.
21. Mehdy, M.M., P.Y. Ng, E.F. Shair, N.I. Saleh and C. Gomes. 2017. Artificial Neural Networks in Image Processing for Early Detection of Breast Cancer. 2017.



22. Munshi, R.M., L. Cascone, N. Alturki, O. Saidani, A. Alshardan and M. Umer. 2024. A novel approach for breast cancer detection using optimized ensemble learning framework and XAI. *Image Vis. Comput.* 142:104910.
23. Oztekin, P.S., O. Katar, T. Omma and S. Erel. 2024. Comparison of Explainable Artificial Intelligence Model and Radiologist Review Performances to Detect. 2051–2068.
24. Papanastasopoulos, Z., R.K. Samala, H. Chan, L. Hadjiiski, M.A. Helvie and C.H. Neal. 2020. Explainable AI for medical imaging : deep-learning CNN ensemble for classification of estrogen receptor status from breast MRI. 11314:1–8.
25. Prodan, M. and E. Paraschiv. 2023. *applied sciences* Applying Deep Learning Methods for Mammography Analysis and Breast Cancer Detection.
26. Rashi, A. 2022. Minimum relevant features to obtain AI explainable system for predicting breast cancer in WDBC. 6:1312–1326.
27. Rezaei, Z. 2021. A review on image-based approaches for breast cancer detection , segmentation , and classification. *Expert Syst. Appl.* 182:115204.
28. Sadoughi, F., Z. Kazemy, F. Hamedan, L. Owji and T.T. Azadboni. 2018. Artificial intelligence methods for the diagnosis of breast cancer by image processing : a review Artificial intelligence methods for the diagnosis of breast cancer by image processing : a review. , doi: 10.2147/BCTT.S175311.
29. Saeidnia, H.R. 2025. Conceptual Model for Breast Cancer Diagnosis Using Machine Learning on Mammogram Data.
30. Sahni, P. and N. Mittal. n.d. *Breast Cancer Detection Using Image Processing Techniques*. Springer Singapore.

Declaration

Conflict of Study: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contribution Statement: All authors contributed equally.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable

Declaration of AI Use: Not Applicable

Author(s) Bio / Authors' Note

Nimra Razzaq from the University of Agriculture, Faisalabad, Pakistan. Email: csnimra@gmail.com

Awais Rasool from the University of Lahore, Pakistan. Email: awaisrasool373@gmail.com

Phool Fatima from Riphah International University, Faisalabad, Pakistan. Email: phool.fatima@riphafsd.edu.pk





Hate Speech Detection Using Ensemble Approach and Embedding Technique

Bira Alam ^{1*}, Fatima Abbas ¹, Nafees Ayub ²

¹Riphah International University Faisalabad, Pakistan

²Government College University Faisalabad, Pakistan

* Corresponding Email: bira.alam@riphahfsd.edu.pk

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.02>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

The rising trend of hate speech on the internet is being major concern to the internet security and societal coexistence, which will requires efficient automated detection tools. As much as different machine learning strategies have been suggested, the issue of the high accuracy using limited data still remains a challenge. This paper introduces a collective detecting frame of hate speech that was tested on the Ethos Binary dataset. Various machine learning classifiers such as K-Nearest Neighbor, Naive Bayes, Logistic Regression, and Decision Tree are used with pre-trained GloVe word embeddings in order to extract semantic representations of textual data. The models are also trained and tested in various hyperparameter configurations, to be robust. The experimental findings indicate that Decision Tree classifier is much better than other models, with a precision of 87, recall of 93, F1-score of 90 and an overall accuracy of 91. The results have shown that an ensemble learning approach with embedding techniques has the potential to greatly increase the performance of hate speech detection. This work helps to enhance viable and scalable solutions to the content of moderating dangerous content online.

Keywords: Hate Speech Detection; Ensemble Learning; Word Embeddings; GloV; Ethos Dataset; Machine Learning

1. Introduction

The high presence of social media sites had been greatly contributed to the spread of user-created information, including hate speech would discriminates against the user or any group of people based on factors like race, religion, gender, and ethnicity. The definition of hate speech is consistently an aggressive, abusive, or offensive language that is directed to the covered groups, and is usually aimed at talking down and causing hostility [1]. This kind of content does not only undermine online conversation, but also adds to the psychological damage, social rejection, and, in the worst scenario, real-life aggression.

Hate speech has been increased in the digital environment because of the speed with which it is shared on social networks like Facebook, Twitter, Instagram, and YouTube. The hate speech can be very tricky to pick up because it is usually propagated using misconceptions and inflammatory stories as noted in [2]. In addition, hate speech may be expressed not only in explicit ways, direct threats and slurs, but also in implicit ways, including sarcasm, coded language, and contextual abuse, which are more difficult to reveal by the conventional rule-based methods. [3] further pointed out that hate speech differs according to the categories of the target such as race, religion, gender and sexual orientation, which prevents the necessity of strong automated detection models.

Machine learning has become a viable option to overcome the flaws of the manual moderation and rule-based filtering. The classical machine learning algorithms are especially applicable to smaller datasets, on which the deep learning algorithms may be affected by overfitting and expensive computations. The above models have been shown to work in the past, namely Naive Bayes, Logistic Regression, Decision Trees, and ensemble methods in text classification tasks [4]. However, feature representation to a significant extent defines performance and the ability of the models to encode semantic background.



This paper is devoted to the Ethos Binary dataset, which is a under-researched hate speech corpus of short user-created remarks that are classified as hateful or non-hateful[1]. The dataset is relatively small and thus poses a challenge in terms of good classification and thus is a good testbed in terms of testing ensemble-based methods. This study is motivated by the earlier studies that have focused on the development of strong machine learning systems[2]. The ensemble approach used in this study also involves several classical classifiers that have been trained using GloVe-based embedding. The voting mechanism is used to aggregate the ensemble predictions to enhance generalization and elimination of the bias of each model.

A number of recent research papers have investigated sophisticated ways of detecting hate speech. To combine learning of related abusive language tasks, [3] suggested a multi-task learning framework, which performed better. Transformer-based models like DistilBERT were proved to be rather effective, whereas ensemble classifiers like AdaBoost could be more effective than single models proved to be, as demonstrated at[4]. It has been proven that ensemble classifiers such as AdaBoost could perform better in single models [5]. A profound ensemble-based NLP framework was proposed by [6] and it was superior to the traditional methods. These methods are good in that they can get high results although they usually use large scales of data or complex structures. Conversely, the paper focuses on efficiency and effectiveness on a scarcely studied dataset based on classical models with improvements of ensemble learning and word embeddings.

The main goal of the study will be to enhance the accuracy and reliability of hate speech classification on the Ethos dataset with the aid of thorough text preprocessing, ready-to-use GloVe embeddings, and an ensemble-based classification system. This work can advance scalable and useful hate speech detection systems that can be used to provide safer and more inclusive online communities because it focuses on a relatively unexploited dataset.

2. Literature Review

The section will summarize the existing studies in hate speech detection in different languages and social media platforms, with a focus on the methodologies, data sets and performance metrics.

The past few years have seen research on various methods of detecting hate speech. A modular neural classifier in cross-lingual detection on English, Italian, and German, the proposal by [7] comprised LSTM, GRU, and Bi-LSTM, word vectors, n-grams, sentiment lexicon, emojis, and social network features. [8] trained CNN, RNN, and BERT-based models on Arabic tweets, and compared the hybrid and single architectures to find the best detection.

In low-resource languages[4] addressed Urdu tweets by combining sentiment analysis with SMOTE, dynamic stop words filtering, and feature selection techniques, evaluating SVM and Multinomial Naïve Bayes. In a similar way[5] used the LSTM and Bi-LSTM networks to detect hate speech on social media, utilizing preprocessing algorithms, including stemming, tokenization and one-hot encoding, and word representations.

The Roman Urdu Hate Speech corpus was created by [9] and the study used NB, LR, RF, SVM, and CNN among the supervised learning methods. Transformer based methods have become increasingly popular too. [10][11] have also identified the difficulties in identifying subtle hate speech, with BERT embeddings and neural networks or ensemble deep learning models. Some of the researches have been directed toward regional and low-resource languages.

Ensemble learning and hybrid architectures have been brought out to the forefront [12]. The article [13] exhibited stacked English tweet recordings utilizing SVM, LR, and XGBoost with word2vec and universal encoding.

The other studies pointed out difficulties in the accuracy of classification, interpretability, and cross-lingual applicability. Some promising results were obtained with methods that incorporate both traditional machine learning and deep learning, transformers, and attention mechanisms used on

languages, including Arabic, Urdu, Roman Urdu, Indonesian, and Dravidian code-mixed datasets. The following Table 1 shows a comparison of the literature.

Table 1: Suggested Comparison Table for Literature Review

Author(s)	Year	Language/Dataset	Methodology	Features	Key Findings
Corazza et al[6]	2020	English, German	Italian, LSTM, GRU, Bi-LSTM	Word vectors, n-grams, emojis, sentiment lexicon	Cross-lingual detection with modular classifier
Alshalan& Khalifa[11]	2020	Arabic	CNN, BERT	RNN, Word embeddings	Hybrid models improved detection accuracy
Paul& Bora[12]	2021	English	LSTM, Bi-LSTM	One-hot encoding, word embeddings	Sequence modeling effective for text sequences
Tița& Zubiaga[13]	2021	Multilingual	mBERT, RoBERTa	XLN-Transformer layers, dropout	Fine-tuned models improved class imbalance handling
Mahajan al.[14]	et 2024	Multilingual	CNN-LSTM, BiLSTM, BiGRU	GloVe embeddings	Hybrid ensemble model outperformed single models

3.Methodology

This paper has used Ethos Binary Dataset, which is a highly curated dataset that is used to do binary classification in the detection of hate speech. Two major columns make up the dataset: comments and isHate and are separated by semicolons to be easily processed as structured data. It comprises 998 comments out of which 433 ones have been classified as hate speech (1) and 565 as non-hate (0). Although the dataset is rather small, it is of good quality and structured to be referred to as a good resource to develop, test, and evaluate machine learning models. Its size can be easily preprocessed, extracted features, and tested on various model settings, which is adequate to the methodology used, although its weaknesses must be admitted.

3.1 Data Preprocessing

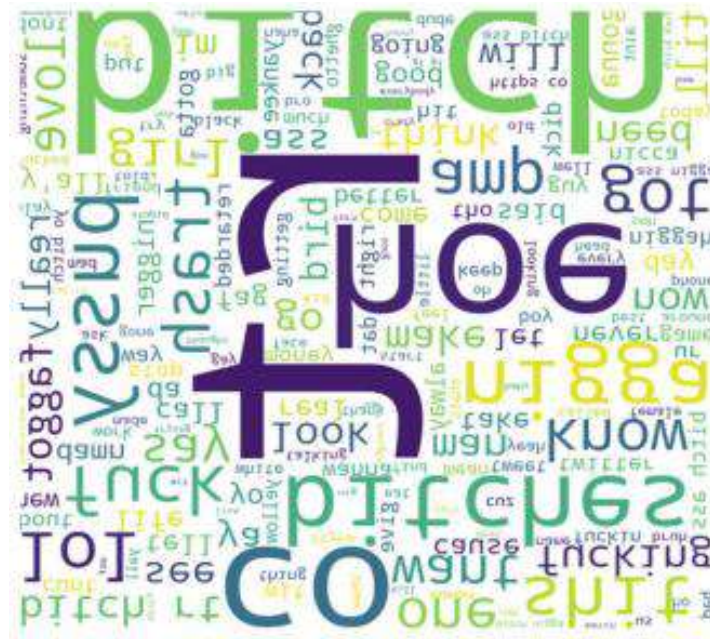
The raw textual data requires preprocessing so that this data can be converted into a uniform format that can be read by machine learning algorithms. In the case of Ethos data, the steps taken were:

Tokenization: The keras tokenizer was used to segment text data into individual tokens and each word was associated to a unique integer in terms of frequency. The process gave 3,885 different tokens.

Stopword Elimination: Instances of the most frequent word with minimal semantic value, including is, the, and, etc., were filtered out by list of NLTK stopwords with a customized filtering function and only informative words were extracted.

Stemming: The Porter Stemmer of NLTK was used to convert words to their root form, standardizing variations and enhancing the efficiency and consistency of the downstream feature representation.

The Figure 1 showcases the most common words in hateful messages of Ethos-based dataset, which underlines the use of offensive and discriminative words that trigger the necessity of automated hate speech recognition.



3.2 Data Splitting

The dataset was divided into two sections (training and testing) to facilitate the quality training and testing of the model. This will guarantee a proper trade-off between model learning and unbiased evaluation of performance, despite small dataset.

3.3 Embedding Technique

Pre-trained GloVe (Global Vectors for Word Representation) embeddings were used to get semantic word representations. The tokens were mapped to a semantical relationship and contextual meaning of a 100-dimensional dense vector space. By using the GloVe embeddings to supplement a small dataset, it is possible to overcome certain weaknesses of these small data sets to a certain extent and offer rich, context-sensitive feature representations.

3.4 Ensemble Learning

In order to improve predictive performance, ensemble learning technique was used, which involves the integration of various machine learning algorithms. The learning algorithms that are part of the ensemble have a different purpose of hate speech detection.

K-Nearest Neighbor classifier is an effective model to detect hateful content as it uses the similarity of text samples in the feature space to determine hateful words, thus an effective model to identify patterns in which hateful words resemble those previously encountered.

Naive bayes takes advantage of the fact that there are probabilistic associations between words and class labels, which enables it to identify those words that occur frequently as offensive or discriminatory.

The reasons for the use of Logistic Regression Logistic Regression is used to model a textual characteristic relationship to a label of a classification that has a linear decision boundary and provides stability and interpretability in classification decisions.

This is because the Decision Tree classifier will capture non-linear interactions of the features, which will allow it to identify the complex linguistic design and contextual patterns common with hate speech. The ensemble arrangement is complementary and strengthens the weaknesses of the individual classifiers by combining these strengths.

Every model was trained on Ethos and several cases with varied random seeds were pooled together using a soft Voting Classifier. This measure enhances prediction stability and accuracy which is especially desirable in light of a relatively small dataset.

3.5 Evaluation Metrics

Precision, recall, F1-score and accuracy were used as quantitative measures to evaluate model performance.

Precision: The ratio of correctly predicted hate comments of all the hate comments made.

Recall: Percentile of correct identification of actual hate comments.

F1-Score: Precision and recall in a given sample, weighted towards their harmonic mean, or balance between false negatives and positives.

Precision: The total percentage of correct comments.

All these metrics give a holistic analysis of the model performance to ensure high and interpretable results of the performance even with a small dataset. To give a summary of the hat speech detention framework to be proposed, Figure 2 illustrates the entire methodology workflow embraced in this study. The diagram gives an overview of the key steps of the strategy, such as preprocessing of data, feature extraction based on GloVe embeddings, training of an ensemble model, and evaluation.

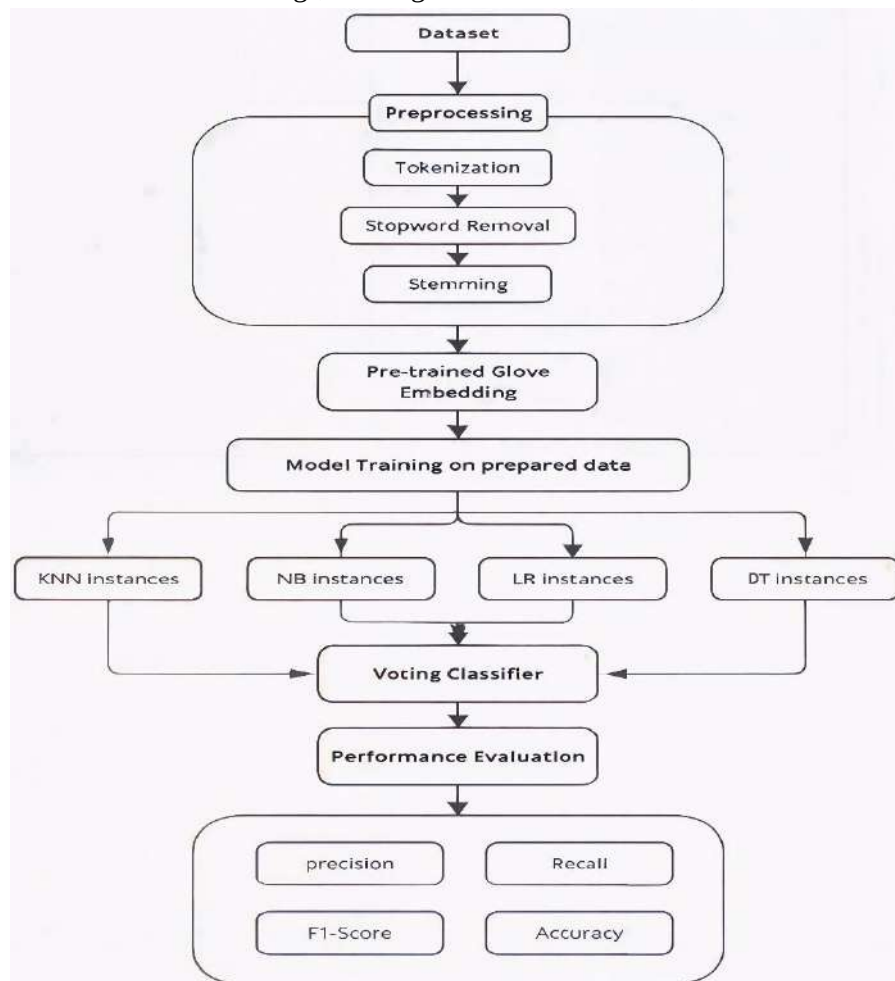


Figure.2 Methodology Diagram

3.6 Methodology Workflow

In Figure 2. It is initiated by Ethos data collection, then there is data preprocessing involving tokenizing, removing stopwords, and stemming. Pre-trained GloVe embeddings are subsequently used to transform usable texts into numerical feature vectors. Several machine learning models KNN, Naive Bayes, Logistic Regression, and Decision Tree are independently trained and assembled into an ensemble with the help of a soft Voting Classifier. Lastly, the precision, recall, F1-score and accuracy are used to assess the performance of hate speech detection with the ensemble model.

3.7 Limitations

The Ethos dataset (998 comments) is quite small in its size, which can limit its ability to be used to generalize to the larger or more heterogeneous online context. However, its structured design, accurate labelling, and representative response of hate and non-hate speech makes it sufficient to develop and test the offered machine learning model. GloVe embeddings and ensemble learning are also used to reduce the weaknesses of the dataset, increase robustness of the model, and predictive confidence.

4. Results

The current section states the results of the experiment conducted on the Ethos Binary Dataset. The effectiveness of four ensemble-based machine learning classifiers, K-Nearest Neighbor (KNN), Naive Bayes (NB), Logistic Regression (LR), and Decision Tree (DT), were determined with the help of the common metrics: precision, recall, F1-score, accuracy, and ROC-AUC. The conclusions are presented in a table form to be more understandable and easier to compare.

4.1 Performance Comparison

Table 2 is a report of the quantitative result of both models on the Ethos dataset. The Decision Tree ensemble performs better in all the evaluation metrics than the other classifiers.

Table 2: Performance Comparison of Machine Learning Models on the Ethos Dataset

Model	Precision (%)	Recall (%)	F1-score (%)	Accuracy (%)	ROC-AUC
K-Nearest Neighbor	70	74	72	75	0.87
Naive Bayes	67	67	67	73	0.76
Logistic Regression	66	64	65	71	0.76
Decision Tree	87	93	90	91	0.93

4.2 Discussion of Results

These findings prove that the Decision Tree ensemble model is the most accurate (91) and has the highest F1-score (90), which means that it is better able to detect instances of hate speech at the expense of false classification. Its high recall (93%) entails the fact that it has a high sensitivity in terms of identifying the hateful content, which is extremely crucial in hate speech detection work.

KNN has matched performance in terms of accuracy regarding precision and recall, but its accuracy is lower than that of the Decision Tree. Naive Bayes and Logistic Regression have relatively high lower performance, and perhaps this can be explained by the fact that they have stronger assumptions concerning the independence of features and the linear separability, respectively.

The large ROC-AUC (0.93) of the Decision Tree also supports this fact and proves that the decision tree is strong and classifies well on the Ethos data. These results imply that ensemble-based Decision Tree models that have been trained on semantic Glov embeddings are highly appropriate in detecting hate speech despite being trained on relatively small data sets.

5 Conclusion

This paper examined the usefulness of ensemble-based machine learning models in hate speech recognition with the Ethos Binary Dataset and pre-trained GloVe word embedding. There were four classifiers, namely Naive Bayes, K-Nearest Neighbor, Logistic Regression and Decision Tree, whose performance was tested on standard performance metrics.

The experimental outcomes show that Decision Tree ensemble model has the best results, having the highest accuracy at 91, precision at 87, recall at 93, and F1-score at 90. These results suggest that the Decision Trees, in combination with the semantic word representations, can be especially useful in doing the hate speech classification. KNN also demonstrated good performance whereas Naive Bayes and Logistic Regression performed with lower effectiveness.

Though the Ethos dataset is not that large, its systematic labeling and certain classification of hate and non-hate content show that it can be evaluated using specific methods. Pre-trained GloVe embeddings and ensemble learning were used, which contributed to the overcoming of data size constraints and the enhancement of the model robustness.

The research in the future can consider the investigation of bigger and more varied data to contribute to the generalization improvement further. Also, more complex ensemble strategies, deep neural networks, and imbalance-correcting methods might also enhance the accuracy of detection. On the whole, this paper has shown that well-developed ensemble techniques can give credible and understandable decisions to automated hate speech detection to help to make the internet a safer place.

References

- [1] S. Mukherjee and S. Das, “Application of Transformer-Based Language Models to Detect Hate Speech in Social Media,” vol. 2, no. December 2021, pp. 278–286, 2023, doi: 10.47852/bonviewJCCE2022010102.
- [2] F. Alkomah and X. Ma, “A Literature Review of Textual Hate Speech Detection Methods and Datasets,” *Inf.*, vol. 13, no. 6, pp. 1–22, 2022, doi: 10.3390/info13060273.
- [3] A. Haque, “Hate Speech Detection in Social Media Using the Ensemble Learning Technique Hate Speech Detection in Social Media Using the Ensemble Learning Technique,” 2023.
- [4] K. U. Wijaya and E. B. Setiawan, “Hate Speech Detection Using Convolutional Neural Network and Gated Recurrent Unit with FastText Feature Expansion on Twitter,” vol. 9, no. 3, pp. 619–631, 2023, doi: 10.26555/jiteki.v9i3.26532.
- [5] A. K. Das, A. Al Asif, A. Paul, and M. N. Hossain, “Bangla hate speech detection on social media using attention-based recurrent neural network,” *J. Intell. Syst.*, vol. 30, no. 1, pp. 578–591, 2021, doi: 10.1515/jisys-2020-0060.
- [6] F. E. Ayo, O. Folorunso, F. T. Ibharalu, I. A. Osinuga, and A. Abayomi-Alli, “A probabilistic clustering model for hate speech classification in twitter,” *Expert Syst. Appl.*, vol. 173, no. February, p. 114762, 2021, doi: 10.1016/j.eswa.2021.114762.
- [7] D. Mody, Y. D. Huang, and T. E. Alves de Oliveira, “A curated dataset for hate speech detection on social media text,” *Data Br.*, vol. 46, p. 108832, 2023, doi: 10.1016/j.dib.2022.108832.
- [8] M. Almaliki, A. M. Almars, I. Gad, and E. S. Atlam, “ABMM: Arabic BERT-Mini Model for Hate-Speech Detection on Social Media,” *Electron.*, vol. 12, no. 4, pp. 1–16, 2023, doi: 10.3390/electronics12041048.
- [9] R. T. Mutanga, N. Naicker, and O. O. Olugbara, “Detecting Hate Speech on Twitter Network using Ensemble Machine Learning,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 3, pp. 331–339, 2022, doi: 10.14569/IJACSA.2022.0130341.
- [10] Z. Al-Makhadmeh and A. Tolba, “Automatic hate speech detection using killer natural language processing optimizing ensemble deep learning approach,” *Computing*, vol. 102, no. 2, pp. 501–522, 2020, doi: 10.1007/s00607-019-00745-0.
- [11] R. Alshalan and H. Al-Khalifa, “A deep learning approach for automatic hate speech detection in the saudi twittersphere,” *Appl. Sci.*, vol. 10, no. 23, pp. 1–16, 2020, doi: 10.3390/app10238614.
- [12] C. Paul and P. Bora, “Detecting Hate Speech using Deep Learning Techniques,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 2, pp. 619–623, 2021, doi: 10.14569/IJACSA.2021.0120278.
- [13] T. Tița and A. Zubiaga, “Cross-lingual Hate Speech Detection using Transformer Models,” *arXiv Prepr. arXiv2111.00981*, 2021, [Online]. Available: <https://arxiv.org/abs/2111.00981>
- [14] E. Mahajan, H. Mahajan, and S. Kumar, “EnsMulHateCyb: Multilingual hate speech and cyberbully detection in online social media,” *Expert Syst. Appl.*, vol. 236, no. May 2023, p. 121228, 2024, doi: 10.1016/j.eswa.2023.121228.
- [15] A. Chhabra and D. K. Vishwakarma, “A Truncated SVD Framework for Online Hate Speech Detection on the ETHOS Dataset,” 2023 *Int. Conf. Innov. Trends Inf. Technol. ICITIIT 2023*, pp. 1–4, 2023, doi: 10.1109/ICITIIT57246.2023.10068574.

Declaration

Conflict of Study: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contribution Statement: All authors contributed equally.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable

Declaration of AI Use: Not Applicable

Author(s) Bio / Authors’ Note

Bira Alam from Riphah International University, Faisalabad, Pakistan. Email: bira.alam@riphahfsd.edu.pk



Fatima Abbas from Riphah International University, Faisalabad, Pakistan. Email: fatima.abbas@riphahfsd.edu.pk

Nafees Ayub from Government College University Faisalabad, Pakistan. Email: nafees.ayub@gcuf.edu.pk





RESEARCH PROPOSAL

Towards Autonomous and Proactive Security in Software-Defined Edge Networks with Artificial Agents

Fatima Abbas ^{1*}, Muhammad Anas Khalid ², Awais Rasool ³

¹Riphah International University Faisalabad, Pakistan

²University of Management & Technology Lahore, Pakistan

³University of Lahore, Lahore, Pakistan

* Corresponding Email: fatima.abbas@riphahfsd.edu.pk

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.03>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Edge computing is transforming latency-sensitive systems such as autonomous vehicles, Industrial IoT, and smart infrastructure. Yet, when managed by centralized Software-Defined Networking (SDN) controllers, these environments face complex security risks. Existing defenses are largely reactive, acting only after damage occurs. This research introduces a proactive, multi-agent AI security framework in which distributed agents monitor system status, detect anomalies, and recommend real-time policy adjustments. A novel coordination mechanism enables adaptive reconfiguration of SDN policies through programmable APIs. To address resource limitations at the edge, the framework employs federated learning and lightweight, self-optimizing models, delivering efficient and scalable security for resource-constrained environments. Prototyped on open-source platforms and tested against real-world attack scenarios, the framework will be evaluated for detection latency, resilience, and response efficiency. The evaluation should show that the framework provides a scalable, context-aware defense that strengthens the resilience of critical infrastructure in heterogeneous domains such as smart cities, healthcare, and energy.

Keywords: Proactive Security; Autonomous Security; Artificial Agents; Software-Defined Edge Networks

1. Motivation

Edge computing has brought processing closer to data sources, boosting responsiveness and reducing bandwidth use. Yet decentralization complicates efforts to maintain a unified and robust security posture, especially when dynamic reconfigurations are managed by SDN controllers. This architecture increases the attack surface, allowing adversaries to exploit controller vulnerabilities or compromise edge nodes. As cyberattacks targeting edge infrastructure, including ransomware, botnets, and distributed denial-of-service (DDoS) campaigns, become increasingly prevalent, security architectures must evolve to both defend against and proactively anticipate emerging security threats.

Most existing approaches to edge network security remain reactive, detecting threats only after damage occurs. This research proposes a proactive AI-driven framework that employs adaptive agents to detect anomalies and vulnerabilities, isolate malicious traffic, and dynamically reconfigure routing through SDN programmability. By integrating proactive mitigation strategies, the framework delivers scalable and adaptive protection tailored to the demands of secure and efficient edge environments.

2. State of the Art

This manuscript surveys the state of the art in securing SDN-enabled edge environments from eight complementary perspectives. It spans topics including architectural integration, the evolution of security threats, AI-driven intrusion detection, federated learning, and multi-agent defense systems. The review also explores lightweight frameworks for resource-constrained devices, programmable controller architectures, and trust management in distributed networks. Collectively, these themes trace the field's progression from initial capability scarcity toward *risk-aware resilience*, highlighting design principles that enable edge systems to be fast, adaptive, and inherently trustworthy.



2.1 Edge Computing and SDN Integration

Edge computing brings compute and storage closer to data sources, improving responsiveness and reducing backbone bandwidth. This shift is crucial for latency-sensitive applications such as autonomous systems, Industrial IoT, and augmented reality, where milliseconds matter. Surveys of mobile/edge computing document architectural patterns and deployment models aimed at real-time processing and tighter QoS compared with centralized cloud approaches [1] [2].

Integrating edge computing with Software-Defined Networking (SDN) adds network-wide programmability for traffic steering, policy enforcement, and resource optimization.

Programmable control can improve service delivery and resource allocation compared with static, distributed architectures, enabling dynamic adaptation to workload and context [3]. This convergence underpins low-latency paths, bandwidth efficiency, and rapid roll-outs of new services across heterogeneous edge sites.

SDN logically separates concerns into planes that interact via well-defined interfaces: the data plane forwards packets; the control plane computes and installs forwarding rules; and the management (or orchestration/application) plane monitors, configures, and coordinates services across the infrastructure [4] [5]. This separation increases flexibility and automates network management while exposing new dependencies between planes in resource-constrained edge settings. Figure 1 illustrates the SDN architecture across management, control, and data planes.

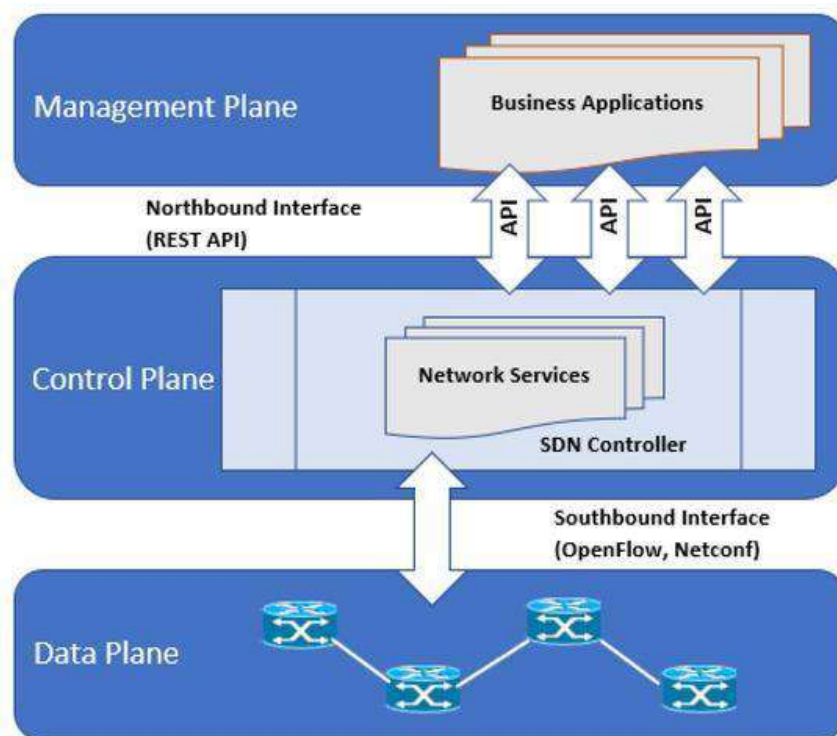


Figure 1. SDN architecture with management, control, and data planes. Reprinted from [5]

Several critical threats can affect the SDN-edge ecosystem, including man-in-the-middle attacks, interception of control plane traffic, and data poisoning of edge nodes [6]. These threats underscore the necessity for further development of security mechanisms tailored to the unique characteristics of Edge-SDN systems and may serve as the foundation for future research into artificial intelligence-based detection and mitigation strategies.

2.2 SDN Security Threats in Edge Environments

The security environment of SDN managing edge networks offers a very complicated combination of threats that are significantly diverse relative to conventional network security problems. The innovative architecture features of the centralized control complemented by the edge processing introduces new

attack vectors that need a specific security response. Awareness of such threats is key to creating robust security structures that will secure the edge infrastructures without interfering with their performance benefits. [3] provide the detailed taxonomy of known attacks on SDN controller in edge networks which comprise five main categories attackers use: controller hijacking, flow rule manipulation, topology poisoning, denial-of-service (DOS) against a controller, and northbound API misuse.

These categories are illustrated in Figure 2.1, which presents a visual taxonomy of common SDN controller attacks in edge environments. [7] Explain the flow rule manipulation attacks, which was capable of diverting traffic by using attacker-controlled nodes.

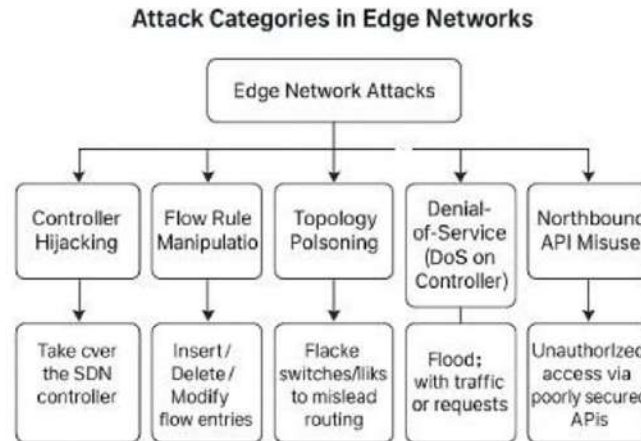


Figure 2: Taxonomy of SDN Controller Attack Categories in Edge Networks Adapted from [3] and [7]

It further facilitates cyber intelligence gathering by enabling the undetected interception and monitoring of data over a prolonged period. In [8], the authors examine topology poisoning attacks, which involve the injection of false information regarding the network's status. As a result, the controller is misled and may draw incorrect conclusions, leading to potentially hazardous routing decisions.

Conventional security facilities are insufficient when it comes to handling these types of SDN specific threats because edge environments are resource-constrained and time-sensitive. [9] Note that there is an essential shift in paradigm between reactive and proactive security models to the models in which anomalies could be detected and isolated until they cause damage to the system. They demonstrate that conventional security methods are not readily adaptable to the dynamic nature of edge networks managed by SDN, emphasizing the necessity of adaptive security mechanisms that operate effectively within the constraints of edge computing. Their proposed approach leverages AI-based security solutions to address these challenges.

3. Artificial Intelligence-Based Intrusion Detection Systems

The use of artificial intelligence as an intrusion detection tool in SDN-controlled edge networks represents a paradigm shift from traditional signature-based intrusion detection methods to intelligent, learning-based intrusion protection systems. The AI agents provide the potential to identify threats in real-time and with adaptive responses as well as constantly learning new patterns of attack activity in dynamic edge environments, where conventional security systems have been less successful.

Supervised learning techniques have been proved to be quite effective in detecting attack patterns that are already known. Other studies such as those by [10] evaluate supervised learning approaches systematically and show that performance of ensemble methods like those that include Random Forest and Support Vector Machine (SVM) can perform even better (detection rates above 95%). [11] Provide a review that shows that hybrid solutions that integrate Convolutional Neural Networks (CNNs) with Recurrent Neural Networks (RNNs) are more successful since they achieve more accurate detection and a lower number of false positives as compared to the traditional methods. Nonetheless, [12] highlight barriers to deployment, noting that increased data sharing is essential to facilitate a more seamless and effective implementation.

Integration of Federated Learning techniques helps to deal with both computational and privacy issues of edge security. [13] Illustrate how federated learning presents a potential solution of enabling collaborative threat detection at edge nodes with no centralized-data aggregation, offering an unbalancing yet effective trainer, with privacy and reduced communication overhead. [14] Address the issue of resource constraints by utilizing lightweight neural network architectures, including model pruning, quantization, and knowledge distillation, which makes it possible to process the AI-based detection on the resource-constrained devices. All of these developments pave the way in trying to realize distributed multi-agent systems, which can offer autonomous decision-making systems.

4. Federated Learning for Distributed Edge Security

Federated learning has developed into an extreme methodology of implementation of distributed security systems in the edge networks where they solve inherent problems in privacy preservation, bandwidth ratio, and dispersion of computational resources. The paradigm helps to achieve group learning

The use of the technology also allows network edge machines to process data securely without specializing network in data aggregation making it particularly suitable in applications where sensitivity of the data and efficiency of the network become critical.

The new trends have depicted that there has been a commendable improvement in terms of performance of the system in the detection as well as efficiency. The offered Bidirectional Encoder Representations from Transforms (BERT) based federated intrusion detection system in [15] appears to have better results over 94 percent detection accuracy and a guarantee of privacy since the training is done locally in the fifth generation (5G) ecosystems. The work by

[16] offering a federated structured framework that is specifically assigned to the IOT networks includes self-adaptive aggregation algorithms that can reduce the quantity of utilized bandwidth during a communication process up to 75%. Demonstrating that a zero-trust federated learning system may achieve a 99.5 detection accuracy even when 20 percent of the participants are malicious, [17] also reveal how to overcome this difficulty: by means of a zero-trust federated learning system, one may reach the reported 99.5 detection accuracy.

The issue of model personalization and security is done away with by innovative methods. An ensemble knowledge distillation based federated learning in heterogeneous IOT networks is introduced by [18], and Federated Multi Agent Deep Ensemble (FEDMADE) with dynamic aggregation techniques is proposed by [2]. The work of [19] presents the Secure Federated Deep Neural Network (SECFEDDNN) framework, which embeds differential privacy and profiles of Byzantine fault tolerance with little performance overhead. Development notwithstanding, convergence in heterogeneous environments and privacy versus threat intelligence sharing are issues of concern and multi-agent systems have been seen as potential players in an enhanced coordination.

5. Multi-Agent Systems for Autonomous Network Defense

Multi-agent systems constitute an advanced method to distributed network security that allows a highly decentralized, coordinated security mechanism throughout the complex edge computing environments. These systems use the principles associated with distributed artificial intelligence to form trust networks of intelligent agents that can be used to make independent decisions, collective solver of problems, and adaptive learning, which serves as a scalable, recoverable network protection architecture to manage edge control networks through SDN.

Modern implementations prove to be considerably more beneficial in comparison to centralized methods. The work by [7] introduces a novel, Multi-Agent Systems (MAS)-based firewall system in which the regulations of SDN controllers are dynamically updated by distributed, network-wide agents that decreases the response time to various threats by up to 60 percent and are also more resilient toward Advanced Persistent Threats APTs and insider attacks. [20] Propose Q-learning agents to enable colluding Distributed Denial-of-Service DDoS mitigation with attack success rates reduction and more

than 30% compared to static systems. [21] present auction-based systems of coordination that enhance the efficiency of the system via optimal task allocation by 45 percent.

More sophisticated coordination mechanisms are introduced, which includes swarm intelligence and reputation management. Rodriguez and [13] create collective swarm-based intrusion detection systems that are capable of managing the environmental scale of the edge environments. Respecting trust issues, [22] introduce the concept of blockchain based reputation systems which identify and isolate bad actors and reward the good ones, thereby encouraging the cooperative aspect of the interaction. Nevertheless, challenges persist due to the complex nature of coordination in dynamic environments and the trade-offs between autonomous decision-making and centralized control. These issues extend to policy enforcement and highlight the need for lightweight security solutions optimized for resource-constrained edge devices.

6. Lightweight Security Frameworks for Resource-Constrained Edge Devices

The lightweight security frameworks are quite hard to find out in an edge computing environment involving a very limited number of computational resources, power consumption, and memory space. Such limitations necessitate the development of new ways that provide high levels of security and operate on limited resources of edge devices such as IOT) sensors, embedded systems and mobile devices.

The solution that [3] and [23] address is the performance of the Edge Guard as an intrusion detection system that is edge-centered to detect as many as 90 percent of the detected attacks even with the limitation of 1GB RAM available.

[14] Introduce the concept of federated learning as an efficient mechanism to reduce the computational in-device requirements by up to 70 percent, which includes the compression of models, quantization of gradients, and asynchronous updates. [12] Propose end-to-end neural network optimisation which included model pruning, quantization, and knowledge distillation to enable advanced detection by designing to run on devices with limited resources.

The optimization of communication and energy efficiency is the most crucial thing when it comes to scenarios using devices with limited resources, including battery-assisted ones. The energy-efficient scheme makes it to the end of regulating the degree of detection dynamically to minimize energy use with the consideration of the remaining battery power level of the gadget and extrapolating it to give the device an additional working period of up to 40 per cent [16] create powerful communication procedures that reduce unnecessary processing and communication load by 60 percent, while maintaining the same level of message delivery assurance. Despite these advancements, challenges remain in maintaining effective security within the constraints of limited resources and an evolving threat landscape. This underscores the renewed relevance of SDN controller-based architectures, which can enable intelligent coordination and dynamic policy enforcement.

7. SDN Controller Architecture and Programmable Network Management

Programmability of networks is based on the SDN controller designs that form the basis of the network control in edge computing by programmability of networks in their entirety as well as providing the maximum flexibility by dynamic network configuration and deployment of network policies. The wide-ranging network topology, different application requirements, and sophisticated security guidelines in the distributed edge architecture are some of the factors that have led to the development of SDN controllers.

Newer SDN controllers have an architecture that is extensible and have open Application Programming Interfaces APIs that notify third party security applications. In a comprehensive comparative analysis of the most common controllers, [7] show that Open Network Operating System ONOS excels in the segment of scalability and developer ease of work since it can scale to over 1000 of the switches and registers sub-millisecond flow set up times. In transitioning to the new paradigm shift, the intent-based networking architectures, introduced by [20] have assisted to save the 80 percent

workload of policy configuration chores and since the translation of the security requirements of the high level into the network level configurations are automatic, it can be said that consistency is enhanced.

Sophisticated architectures address the edge requirements with distributed control planes and AI is a part of the latter. [4] provide hierarchical SDN plans that lead to the creation of new SDN control planes that have 70 per cent less latency because of local edge controllers as well as global coordination. The article suggests novelty in implementing a new AI-based controller and machine learning to gather controllers and optimize policy choice, as well as to learn optimal network policies, lowering errors made in the process by 30 percent and 60 percent, respectively[1]. However, there are still risks that security services may be penetrated, as well as issues with scale, and they have an interest in trust and reputation systems of distributed edge networks.

8. Trust and Reputation Management in Distributed Edge Networks

Trust and reputation management systems have become foundational in terms of providing reliable and secure operations of distributed edge networks, especially when multiple agents that are autonomously operating are required to cooperate without any centralized management. The systems enable quantifiability and control of uncertainty in distributed interactions, and the ability to make informed decisions regarding collaboration, resource sharing and information exchange in dynamic edge environments.

The study by [19] introduces a detailed blockchain-based trust system in SDN edge networks that keeps the immutable trust records and stops the malicious attack on the trust judgments. Their mechanism supports opaque audit records and decentralized agreement on levels of trust and is an effective way of discovering and quarantining malicious to maximize the level of collaboration in a group of legitimate interactors. [7] come up with lightweight equivalences that utilize reputation aggregation and cryptographic verification to combat the computational expenses and deliver an effective trust control technique that can assist in resource-limited settings.

Although some of the issues facing trust-based security mechanisms have been resolved, several problems still remain such as computational complexity of blockchain based systems in constrained settings, at the onset of trust inconsistencies in partitioned networks, and balancing trust accuracy with system very responsiveness.

An examination of existing literature has highlighted research gaps in self-organizing security systems whereby agents can self-learn how to protect systems in spite of changing network topologies and adversary tactics and strategies. A 2019 survey by Ismail and wazir khan confirms all of the above, but also strongly underlines the necessity of adopting proactive methods of threat prevention that concern itself with not only trust management but also real-time, adaptive defense mechanisms, and there is a related strong need to consider developing fabricated solutions that simultaneously apply multi-agent reasoning, federated learning, and lightweight trust management to the area of real-world network security.

9. Objectives

9.1 Primary Objective

Design, develop, and validate a proactive, intelligent, and distributed security framework for SDN-orchestrated edge networks. The framework will employ learning agents that adapt to evolving threats in real time while preserving latency, throughput, and overall network performance.

9.2 Main Objectives

1. Architecture design: Create a multi-agent proactive security architecture with agents deployed at strategic edge nodes to autonomously monitor traffic, detect anomalies, share insights, and recommend real-time policy updates to the SDN controller.
2. Learning-based detection: Embed lightweight machine learning within edge agents (e.g., federated



learning, LSTM, reinforcement learning) to enable real-time threat detection and behavior prediction with minimal computational overhead.

3. Dynamic policy adaptation: Develop mechanisms for agents to drive on-the-fly SDN flow reconfiguration via programmable northbound APIs, enabling flexible, automated, and context-aware responses.
4. Resilience and scalability: Engineer robustness against DDoS, topology poisoning, and insider threats, and ensure scalability across heterogeneous edge networks with negligible performance degradation.
5. Evaluation and validation: Use SDN controllers (e.g., Ryu) and emulators (e.g., Mininet) to assess detection accuracy, false-positive/false-negative rates, response time, added latency, throughput impact, resource overhead, and resilience under sustained attack.
6. Open science contribution: Release an open-source prototype and publish best-practice recommendations for deploying proactive, intelligent security in SDN-based edge environments.

These objectives support secure, adaptive, and self-healing edge infrastructures essential to smart cities, autonomous systems, telemedicine, and critical infrastructure management.

10. Research Questions

The proposed research aims to develop a secure, autonomous, and proactive architecture for managing cybersecurity threats in software-defined edge networks. To achieve this goal, the following research questions are formulated. These questions will guide the research process and will be addressed through the development, implementation, and evaluation of the proposed solutions during the PhD study:

- **RQ1: Agent design and deployment:** How can lightweight, autonomous artificial agents be designed and deployed at edge nodes to effectively detect and respond to cybersecurity threats in real-time, without breaching latency and resource constraints typical of edge environments?
- **RQ2: Learning for collaboration and adaptability:** What is the efficacy of integrating federated learning and reinforcement learning into multi-agent systems for enhancing intrusion detection accuracy, adaptability, automatic detection and remediation of system vulnerabilities, and collaborative decision-making in SDN-managed edge networks?
- **RQ3: Learned policy influence via SDN programmability:** To what extent can artificial agents dynamically influence and reconfigure Software-Defined Networking (SDN) controller policies through northbound APIs to enable context-aware, automated mitigation of network security threats?
- **RQ4: Scalability and resilience under attack:** How does a proactive, multi-agent security architecture scale across heterogeneous edge topologies, and how resilient is it against adversarial scenarios such as DDoS, flow-rule flooding, control-plane saturation, and rogue node injection?
- **RQ5: Evaluation metrics and trade-offs:** How scalable and resilient is a proactive, multi-agent security architecture across heterogeneous edge network topologies with eventual high-risk vulnerabilities subjected to diverse adversarial scenarios such as DDoS attacks, flow rule flooding, and rogue node injections?
- **RQ5: Evaluation metrics and trade-offs:** How scalable and resilient is a proactive, multi-agent security architecture across heterogeneous edge-network topologies when faced with eventual high-risk vulnerabilities and diverse adversarial scenarios — such as DDoS attacks, flow-rule flooding, and rogue-node injections — as assessed through quantifiable performance (throughput, latency), security (detection rate, false-positive rate), and adaptability (time-to-mitigation, recovery speed) metrics?

The table below summarizes the current proposal research questions.

11. Summary of Research Questions



RQ	Focus	Core Aim
RQ1	Agent Design & Deployment	Develop lightweight, autonomous agents for edge nodes that can detect and respond to threats in real time without breaching latency or resource limits.
RQ2	Learning Integration	Assess the benefits of combining federated learning and reinforcement learning in multi-agent systems to boost detection accuracy, adaptability, and collaboration.
RQ3	Dynamic Policy Adaptation	Explore how agents can safely and context-sensitively reconfigure SDN controller policies via northbound APIs for automated, low-latency threat mitigation.
RQ4	Scalability & Resilience	Evaluate system performance, scalability, and resilience under diverse topologies and adversarial scenarios (e.g., DDoS, flow-rule flooding, rogue nodes).
RQ5	Evaluation Metrics & Trade-offs	Define and analyze the metrics and trade-offs between detection performance, automatic remediation, overhead, false positives, and quality of service in realistic edge deployments.

12. Research Project Proposal

12.1 Basis for Work Development

The rise of edge computing and SDN as interdependent technologies has created new opportunities for optimizing resource allocation, network control, and service delivery at the edge. However, these advancements also introduce critical security risks, especially due to the centralization of control in SDN and the distributed, resource constrained nature of edge nodes. Research from 2020 to 2025 has demonstrated growing threats like SDN controller hijacking, data injection, botnets, and insider attacks in edge deployments [3] and [23].

While traditional security mechanisms focus on post-attack mitigation or static rule enforcement, recent trends highlight the need for autonomous, intelligent, and proactive systems. Multi-agent systems (MAS), integrated with machine learning (ML) and SDN programmability, offer a way to build adaptable security mechanisms that respond to threats dynamically while preserving edge performance [22] and [1].

This project is built on the premise that distributed artificial agents, equipped with learning capabilities and embedded within SDN-managed edge environments, can collectively detect, report, and respond to security anomalies in real time. These agents can learn from both local and shared experiences to continuously enhance the resilience of the edge network infrastructure.

12.2 Work Description

System Architecture

The proposed architecture will consist of:

- **Edge Nodes:** Embedded with lightweight agents that collect network and host level Operational status.
- **SDN Controller:** Receives agent alerts and dynamically updates routing rules or applies mitigation policies.
- **Agent Communication Layer:** Uses publish-subscribe messaging for efficient sharing of insights.
- **AI Engine:** Implements machine learning algorithms (e.g., federated learning, RL) for threat classification and adaptive defense.

The architecture will use the Ryu controller, Mininet for emulated topologies, and the framework like TensorFlow Lite or PyTorch Mobile to deploy ML models on the edge devices

Agent Design

- Each artificial agent will consist of the following components:
- Monitoring Module: Captures flow stats, packet anomalies, CPU usage, and system logs.
- Feature Extractor: Applies dimensionality reduction and normalization for lightweight inference.
- Detection Engine: Uses LSTM or hybrid CNN-RNN models for anomaly detection.
- Communication Module: Exchanges alerts with peer agents and controller over secure channels.
- Policy Recommender: Suggests policy actions such as rerouting, flow blocking, or quarantine.

Agent learning will be based on recent research in collaborative and federated learning [12], enabling decentralized model updates without transmitting raw data

Threat Scenarios and Response

- The system will be evaluated under multiple real-world inspired attack scenarios:
- DDoS against SDN Controller
- Flow Rule Flooding
- Rogue Edge Node Injection
- Botnet Communication (e.g., Mirai-based)
- Insider Data Leakage

Response strategies will include flow re-routing, dynamic reauthentication, agent based isolation, and policy reconfiguration using Ryu's REST API.

Experimental Setup

A simulation testbed will be built using:

- Mininet to emulate edge nodes and switches
- Ryu SDN controller for routing management
- Wireshark and sFlow for traffic analysis
- Scapy to generate attacks and traffic anomalies
- Python-based ML models for anomaly detection
- Docker for agent containerization
- Edge devices like Raspberry Pi (optional for hardware testing)

Experiments will be conducted across varied topologies (tree, mesh, hybrid) to test scalability, responsiveness, and detection accuracy.

Performance Evaluation Metrics

The system will be evaluated using the following metrics:

- Detection Accuracy: Percentage of true positives vs. false positives
- Threat Response Time: Time between anomaly detection and mitigation
- Network Throughput: Impact on data transmission during defense
- Latency Overhead: Added delay due to agent actions or controller response
- Agent Resource Utilization: CPU, RAM, and energy usage

Benchmark comparisons will be made against centralized IDS (e.g., Snort) and static Rule-based SDN defenses.

13. Key Contributions

This project will provide:

1. A novel multi-agent framework tailored for SDN-based edge environments.
2. Lightweight ML-based anomaly detection methods deployable on edge devices.



3. Real-time integration with SDN controllers for dynamic threat response.
4. Experimental validation through simulations and open-source prototype release.
5. Research publications, workshops, and conference presentations to share findings with the academic and professional community.

Expected Outcomes

The suggested study will provide theoretical and practical findings that will help in intelligent, secure, and autonomous edge networking. The results of these outcomes aim to reflect the literature gaps that have been determined and deliver solutions in real-time and can be scaled to the SDN-managed edge infrastructures.

- An intelligent, self-adaptive security model for SDN edge networks
- Reduced threat mitigation time without compromising performance
- Guidelines for scalable deployment of AI agents in constrained environments
- Increased trustworthiness of edge infrastructures in critical domains

Project Outputs

By the conclusion of the project, the following outcomes are expected, each explicitly addressing gaps in the existing literature:

- A modular, scalable multi-agent security framework for SDN-controlled edge networks

Although the former paradigms primarily focus on centralized, decision-making, this model allows distributed coordination and adaptable options, which enhances resistance and scalability to the changes of dynamic edge environments.

- AI-driven, lightweight intrusion detection agents suitable for real-world deployment

Our agents can be trained on tight edge nodes by leveraging compressed model representations and federated learning unlike traditional deep learning models, which are too resource intensive [3].

- A full-featured simulation testbed for edge security experimentation

The current assessments tend to be non-reproducible or lack emulation to the real world. Our testbed can address this gap since it simulates various topologies and types of attacks using tools such as Mininet and RYU.

- Open-source code repository, including setup instructions and model weights All implementation assets will be published to enhance the reproducibility and promote adoption and this is opposite to closed configurations of most academic prototypes.
- At least three peer-reviewed publications in high-impact venues. This will guarantee the sharing of innovative methods and benchmarks of performance, which will help in the overall discourse in SDN, edge computing, and AI-based cybersecurity.
- A defended and approved PhD dissertation, contributing to the academic and industrial edge security domains.

14. Answers to Research Questions

This section presents the expected answers to the defined research questions, based on the results obtained during the PhD research. These reflect the key contributions and outcomes of the work.

The outcomes of the PhD research are expected to provide well-substantiated answers to the research questions:

- **RQ1 Answer:** By developing a modular and lightweight agent framework optimized for edge resources, the research demonstrates that autonomous agents can be effectively deployed on edge nodes. Using containerization, rule-based threat detection, and distributed inference, the agents maintain real-time response capabilities while preserving latency and resource limits.
- **RQ2 Answer:** The integration of federated learning and reinforcement learning into multi-agent systems significantly enhances detection accuracy and system adaptability. Experimental results show improved responsiveness to novel threats, reduced false positives, and the emergence of cooperative



behaviors that support distributed defense mechanisms in SDN-managed environments.

- **RQ3 Answer:** The research confirms that agents equipped with policy reconfiguration capabilities via northbound APIs can dynamically adapt the SDN controller's behavior based on contextual threat intelligence. This enables automated and context-aware mitigation strategies, reducing administrative overhead and response time to evolving threats.
- **RQ4 Answer:** The proposed proactive, multi-agent security architecture scales across heterogeneous edge topologies and withstands varied adversarial scenarios — including DDoS attacks, flow-rule flooding, and rogue node injections. Both simulation and prototype testing should confirm the next aspects: i) consistent detection and mitigation under load; ii) quick recovery via collaborative reconfiguration and trust propagation; and
iii) sustained control-plane performance and service continuity.
- **RQ5 Answer:** The investigation establishes quantitative and qualitative benchmarks for evaluating security, adaptability, and system cost, including: (i) threat detection accuracy, precision, and recall; (ii) control-plane overhead and latency impact; (iii) the cost of false positives to service quality; and (iv) adaptability and recovery time under adversarial conditions. Prior research should suggest that a careful balance of these metrics can achieve high security assurance without imposing excessive demands on network resources.

15. Limitations and Mitigation Strategies

There are several potential shortcomings and risks during PhD work. The table below summarizes them alongside the corresponding mitigation actions.

Risk / Limitation	Mitigation Strategy
Real-world data scarcity	Integrate synthetic traffic generation, open resources (e.g., CICIDS2017 [24], TON IoT [25]), and regulated testbed emulation to generate plausible and heterogeneous training / validation data. Further, we should add some recent surveys: A survey of public IoT datasets in network security research [26], Network traffic classification: Techniques, datasets, and challenges , and others. Such datasets as UNSW HomeNet [27], may also supply realistic IoT traffic to edge security research activities.
Resource constraints at the edge	Use lightweight ML models, federated learning, and selective offloading of complex computation to SDN controllers to fit within CPU, memory, and energy limits.
Evolving threat landscape	Implement adaptive learning with online updates, periodic re-training, and continuous feedback loops between agents and controllers to keep pace with new attack vectors.
Agent coordination and trust issues	Deploy trust-aware mechanisms, fault-tolerant coordination protocols, and fallback policies to ensure graceful degradation during communication failures or malicious agent activity.
Evaluation complexity	Iteratively enhance the testbed and benchmark against state-of-the-art systems to approximate large-scale topologies and realistic adversarial conditions.

References

- [1] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Futur. Gener. Comput. Syst.*, vol. 97, pp. 219–235, 2019, doi: 10.1016/j.future.2019.02.050.
- [2] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, 2018, doi: 10.1109/JIOT.2017.2750180.
- [3] X. Zhang, C. Chen, Y. Xie, X. Chen, J. Zhang, and Y. Xiang, "A survey on privacy inference attacks and defenses in cloud-based Deep Neural Network," *Comput. Stand. Interfaces*, vol. 83, p. 103672, 2023, doi: <https://doi.org/10.1016/j.csi.2022.103672>.



- [4] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, 2015, doi: 10.1109/JPROC.2014.2371999.
- [5] A. Hamarshah, "An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning," *Appl. Sci.*, vol. 14, no. 11, 2024, doi: 10.3390/app14114530.
- [6] M. Raza, M. Jasim Saeed, M. B. Riaz, and M. Awais Sattar, "Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks," *IEEE Access*, vol. 12, no. May, pp. 69551–69567, 2024, doi: 10.1109/ACCESS.2024.3395997.
- [7] A. A. Okon, "A Blockchain-enabled SDN Framework for Multi-operator Networks," no. January, 2025.
- [8] J. Chen, Q. Li, H. Wang, and M. Deng, "A machine learning ensemble approach based on random forest and radial basis function neural network for risk evaluation of regional flood disaster: A case study of the yangtze river delta, China," *Int. J. Environ. Res. Public Health*, vol. 17, no. 1, pp. 1–21, 2020, doi: 10.3390/ijerph17010049.
- [9] A. Rahdari et al., "Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions," *Comput. Mater. Contin.*, vol. 80, no. 2, pp. 2511–2533, 2024, doi: 10.32604/cmc.2024.052994.
- [10] J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, "Security in SDN: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 159, no. November 2019, p. 102595, 2020, doi: 10.1016/j.jnca.2020.102595.
- [11] M. Abdallah, N. An Le Khac, H. Jahromi, and A. Delia Jurcut, "A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs," *ACM Int. Conf. Proceeding Ser.*, 2021, doi: 10.1145/3465481.3469190.
- [12] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018, doi: 10.1109/COMST.2018.2844341.
- [13] T. V. Phan, T. G. Nguyen, N. N. Dao, T. T. Huong, N. H. Thanh, and T. Bauschert, "DeepGuard: Efficient Anomaly Detection in SDN with Fine-Grained Traffic Flow Monitoring," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 3, pp. 1349–1362, 2020, doi: 10.1109/TNSM.2020.3004415.
- [14] S. Ismail, S. Dandan, and A. Qushou, "Intrusion Detection in IoT and IIoT: Comparing Lightweight Machine Learning Techniques Using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset Datasets," *IEEE Access*, vol. 13, no. February, pp. 73468–73485, 2025, doi: 10.1109/ACCESS.2025.3554083.
- [15] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash, and M. Shaheed, "SDN Security Review: Threat Taxonomy, Implications, and Open Challenges," *IEEE Access*, vol. 10, no. April, pp. 45820–45854, 2022, doi: 10.1109/ACCESS.2022.3168972.
- [16] K. M. Kokila M and S. R. K. Srinivasa Reddy Konda, "DeepSDN: Deep Learning Based Software Defined Network Model for Cyberthreat Detection in IoT Network," *ACM Trans. Internet Technol.*, 2025, doi: 10.1145/3737875.
- [17] Y. Tseng, F. Näit- Abdesselam, and A. Khokhar, "A comprehensive 3- dimensional security analysis of a controller in software- defined networking," *Secur. Priv.*, vol. 1, no. 2, 2018, doi: 10.1002/spy2.21.
- [18] A. Hirsi, L. Audah, A. Salh, M. A. Alhartomi, and S. Ahmed, "Detecting DDoS Threats Using Supervised Machine Learning for Traffic Classification in Software Defined Networking," *IEEE Access*, vol. 12, no. September, pp. 166675–166702, 2024, doi: 10.1109/ACCESS.2024.3486034.
- [19] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, "Intrusion Detection for Wireless Edge Networks Based on Federated Learning," *IEEE Access*, vol. 8, pp. 217463–217472, 2020, doi: 10.1109/ACCESS.2020.3041793.
- [20] A. John, I. F. Bin Isnin, S. H. H. Madni, and M. Faheem, "Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms," *Intell. Syst. with Appl.*, vol. 22, no. December 2023, p. 200381, 2024, doi: 10.1016/j.iswa.2024.200381.
- [21] I. Akbari, E. Tahoun, M. A. Salahuddin, N. Limam, and R. Boutaba, "ATMoS: Autonomous Threat Mitigation in SDN using Reinforcement Learning," *Proc. IEEE/IFIP Netw. Oper. Manag. Symp. 2020 Manag. Age Softwarization Artif. Intell. NOMS 2020*, 2020, doi: 10.1109/NOMS47738.2020.9110426.
- [22] S. Facchinetti, S. A. Osmetti, and C. Tarantola, "Network models for cyber attacks evaluation," *Socioecon. Plann. Sci.*, vol. 87, no. PB, p. 101584, 2023, doi: 10.1016/j.seps.2023.101584.
- [23] A. M. Sheikh, M. R. Islam, M. H. Habaebi, S. A. Zabidi, A. R. Bin Najeeb, and A. Kabbani, "A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies," *Futur. Internet*, vol. 17, no. 4, pp. 1–54, 2025, doi: 10.3390/fi17040175.

- [24] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “CICIDS2017: Intrusion Detection Evaluation Dataset,” pp. 1–11, 2017.
- [25] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “A Detailed Analysis of the CICIDS2017 Data Set BT - Information Systems Security and Privacy,” P. Mori, S. Furnell, and O. Camp, Eds., Cham: Springer International Publishing, 2019, pp. 172–188.
- [26] N. Moustafa, “A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets,” *Sustain. Cities Soc.*, vol. 72, p. 102994, 2021, doi: 10.1016/j.scs.2021.102994.
- [27] A. Azab, M. Khasawneh, S. Alrabace, K. K. R. Choo, and M. Sarsour, “Network traffic classification: Techniques, datasets, and challenges,” *Digit. Commun. Networks*, vol. 10, no. 3, pp. 676–692, 2024, doi: 10.1016/j.dcan.2022.09.009.

Declaration

Conflict of Study: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contribution Statement: All authors contributed equally.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable

Declaration of AI Use: Not Applicable

Author(s) Bio / Authors' Note

Fatima Abbas from Riphah International University, Faisalabad, Pakistan. Email: fatima.abbas@riphahfsd.edu.pk

Muhammad Anas Khalid from the University of Management & Technology, Lahore, Pakistan. Email: anaskhalid021@gmail.com

Awais Rasool from the University of Lahore, Pakistan. Email: awaisrasool373@gmail.com





Review of Judicial Independence and Democracy in Pakistan

Anees Amjad ^{1*}

¹Department of Law, University of Sahiwal, Pakistan

* Corresponding Email: amjadanees133@gmail.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.05>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Judicial independence is the backbone of constitutional democracy because it ensures that judges can decide cases without fear, pressure, or political bargaining. In Pakistan, however, this idea has developed in a turbulent constitutional environment shaped by repeated military takeovers, unstable civilian rule, and frequent constitutional disruption. This research examines how Pakistan's superior judiciary has alternated between complicity and resistance, and how that pattern has affected democratic governance and the rule of law. Using a doctrinal and contextual method, the study traces the historical roots of judicial compromise beginning with *Federation of Pakistan v. Maulvi Tamizuddin Khan* (PLD 1955 FC 240), where the dissolution of the Constituent Assembly was upheld on technical grounds, an early turning point that later nourished the Doctrine of Necessity. The research shows that necessity jurisprudence gradually became a recurring legal cover for extra-constitutional governance, especially during the regimes of Ayub Khan, Yahya Khan, Zia-ul-Haq, and Pervez Musharraf. In these periods, Provisional Constitutional Orders (PCOs), enforced oaths, and "validation judgments" reshaped courts from constitutional guardians into crisis managers. This study also highlights that threats to judicial independence are not only external. Internal controversies relating to accountability, politicized appointments, seniority disputes, and administrative influence have weakened institutional cohesion and public trust. Further, the research finds that democratic governments have often repeated executive interference through appointment manipulation, political pressure, and resistance to adverse rulings, proving that democratic legitimacy alone does not guarantee constitutional restraint. Finally, the study evaluates contemporary developments, including the Twenty-seventh Constitutional Amendment (2025) and debates around restructuring constitutional adjudication. It concludes that judicial independence is not merely a legal safeguard but a democratic necessity: where courts compromise, constitutional limits collapse. The research recommends transparent appointments, respect for seniority, institutional autonomy, and clear limits on executive interference to rebuild constitutionalism and democratic resilience in Pakistan.

Keywords: Judicial Independence; Doctrine of Necessity; Constitutionalism; Martial Law; Democratic Governance

1. Introduction

Judicial independence lies at the core of constitutional democracy and the rule of law [1]. The right to information in relation with Judicial independence is also one of major factor for democracy and the rule of law[2, 3]. It requires that judges decide cases free from political pressure, institutional interference, or private influence, thereby ensuring fair adjudication and maintaining public confidence in the legal system. In democratic settings, an independent judiciary functions as a safeguard against arbitrary power, protects fundamental rights, and upholds constitutional supremacy[4]. In Pakistan, however, the ideal of judicial independence has evolved within a contested political landscape marked by military interventions, fragile civilian rule, and recurring constitutional disruption[5]. Since independence in 1947, Pakistan's judiciary has played an ambivalent role, at times legitimizing authoritarian rule while at other moments resisting executive dominance and asserting constitutional limits. A critical early episode was *Federation of Pakistan v. Maulvi Tamizuddin Khan* (PLD 1955 FC 240), in which the Federal Court upheld the dissolution of the Constituent Assembly and laid the groundwork for the "doctrine of necessity"[6]. This doctrine, subsequently invoked in later crises, provided legal cover for extra-constitutional governance, including military coups, and severely compromised judicial autonomy. Under the regimes of General Ayub Khan, General Zia ul Haq, and General Pervez Musharraf, courts repeatedly validated military rule through pliant interpretations,



PCOs, and enforced oaths, even as pockets of resistance emerged around questions of constitutionalism and rights.

The suspension of *Chief Justice Iftikhar Muhammad Chaudhry* in 2007 and the ensuing lawyers' movement symbolized a turning point in the public and professional imagination of judicial independence in Pakistan[7]. Yet, the pressures on the judiciary have persisted under both military and civilian governments, including through politicized judicial appointments, manipulation of seniority, and attempts to influence high-profile litigation. In the contemporary context, assessments such as *Freedom in the World 2025* point to a formal electoral framework coexisting with entrenched military influence over political outcomes, media space, and policy direction, raising serious concerns about the quality of democratic governance. Recent constitutional developments have intensified these concerns. The Twenty-seventh Amendment to the Constitution of Pakistan (2025) restructures the judicial architecture by establishing a Federal Constitutional Court to assume primary responsibility for constitutional adjudication and by reshaping the appointment, transfer, and supervision of judges[8]. Critics, including international legal bodies such as the International Bar Association's Human Rights Institute and the International Commission of Jurists, argue that the amendment amounts to a "flagrant attack" on judicial independence, entrenching military dominance and weakening institutional checks and balances[9]. The reported resignations of senior Supreme Court judges in protest against these changes further underscore the depth of institutional unease and the perception that the superior judiciary's role in constitutional review is being systematically curtailed. Against this backdrop, the link between judicial independence and democracy in Pakistan is both institutional and normative. Judicial autonomy provides a crucial mechanism for ensuring that governmental action remains subject to constitutional constraints, that fundamental rights are meaningfully protected, and that the separation of powers is not reduced to a mere formal claim. Where courts are unable or unwilling to fulfill this role, whether due to overt coercion or more subtle forms of executive leverage, democratic accountability erodes, civil liberties weaken, and the constitutional order tilts toward managed or hybrid authoritarianism.

This article undertakes a doctrinal and contextual analysis of judicial independence in Pakistan, tracing its historical evolution, doctrinal foundations, and contemporary challenges. It examines landmark cases, including *Maulvi Tamizuddin Khan* and later jurisprudence under the doctrine of necessity, as well as key constitutional changes culminating in the Twenty-Seventh Amendment, to evaluate how courts have alternated between complicity and resistance in the face of executive and military power. Methodologically, the article employs a doctrinal [10] approach combined with historical and institutional analysis to assess the extent to which existing safeguards can still sustain a judiciary capable of acting as an effective guardian of the Constitution. In doing so, it seeks to contribute to broader debates on constitutionalism, separation of powers, and democratic resilience in Pakistan and comparable hybrid regimes.

2. The Doctrine of Necessity: Judicial Validation of Power and Democratic Fragility

The Doctrine of Necessity is a contentious legal principle used to justify actions taken outside the constitutional framework in the name of preserving the state or restoring order in exceptional circumstances[11]. In its classical formulation, drawn from medieval English law and later constitutional theory, it rests on the maxim that necessity may temporarily override ordinary legal rules where their strict application would imperil the community or the state itself. In principle, this doctrine is intended as a narrow, time-bound exception to protect the legal order, not to displace it. In Pakistan, however, the doctrine has acquired a very different and deeply problematic character. Rather than remaining a last-resort safeguard, it has evolved into a recurring judicial device used to validate unconstitutional seizures of power, particularly military coups and the dissolution of representative institutions. In country's constitutional history, the *Doctrine of Necessity* has been pivotal in enabling repeated constitutional breakdowns instead of preventing them[12]. Superior courts have frequently



invoked necessity not to preserve the Constitution, but to rationalize its suspension, abrogation, or radical alteration under extra-constitutional regimes. Military rulers and non-representative executives have relied on the judiciary's willingness to accept "state necessity" as a legal justification for emergency rule, PCOs, and the sidelining of elected institutions. Each time courts upheld these measures, plainly unconstitutional acts were transformed into legally sanctioned orders, granting de facto legitimacy to de jure illegality.

2.1 *Maulvi Tamizuddin Khan Case*

The case titled as *Federation of Pakistan v. Maulvi Tamizuddin Khan*, PLD 1955 FC 240, is widely regarded as the foundational moment in the judicial entrenchment of the *Doctrine of Necessity* in Pakistan[13]. The dispute arose when the Governor-General unilaterally dissolved the Constituent Assembly, which was engaged in drafting Pakistan's first Constitution. *Maulvi Tamizuddin Khan*, the President of the Assembly, challenged this dissolution, arguing that it was unconstitutional and violated the emerging democratic structure of the state[14]. The case thus posed a stark question: would the judiciary defend representative constitution-making, or endorse executive prerogative power? Initially, the Sindh Chief Court sided with *Maulvi Tamizuddin Khan*, holding that the Governor-General's action was unlawful and beyond his constitutional authority. This judgment affirmed the principle that even the highest executive officeholder remained bound by legal limits. However, the Federal Court, led by *Chief Justice Muhammad Munir*, overturned the decision, holding that the Constituent Assembly was not a fully lawful body because it had not been properly constituted under existing legal instruments. This reasoning allowed the Court to treat the Governor-General's dissolution as legally sustainable, effectively prioritizing formalistic technicalities over the substantive democratic function of the Assembly. Justice Munir's reasoning extended beyond narrow legal interpretation into an overt preference for "state necessity" and political stability. By emphasizing the need to avoid a constitutional vacuum and to preserve continuity of governance, the Court implicitly endorsed the idea that legality could yield to perceived necessity. Although the term "*Doctrine of Necessity*" was not yet fully articulated in the sophisticated form it would later assume, its core logic, sanctioning extra-constitutional actions in the name of state survival, was clearly embedded in the judgment. This decision thus supplied the intellectual and jurisprudential foundation upon which later courts would build when validating coups, martial law regimes, and emergency decrees.

2.2 *Impact of Constitutional Cases*

In the decades following the *Maulvi Tamizuddin Khan Decision*, the *Doctrine of Necessity* matured into a recurring judicial rationale in country's constitutional jurisprudence [15]. Superior courts repeatedly relied on necessity to validate extra-constitutional regimes, including the military coups of 1958, 1977, and 1999, as well as various emergency proclamations and PCOs. Instead of correcting the initial doctrinal misstep, the judiciary embedded it more deeply, transforming an extraordinary justification into a familiar legal instrument. Over time, necessity moved from the margins to the center of constitutional discourse, shaping how crises were interpreted and resolved. Through a series of landmark cases, courts affirmed the suspension or abrogation of constitutions, endorsed martial law authorities, and permitted the restructuring of state institutions without democratic mandate. Each judicial validation strengthened a dangerous pattern: once unconstitutional acts received judicial approval, they acquired a veneer of legality, blurring the line between lawful constitutional change and raw political power[16]. This blurred boundary did not only affect abstract doctrine; it also reshaped institutional behavior. Political actors came to expect that courts would eventually reconcile extra-constitutional interventions with constitutional language, thereby lowering the perceived cost of breaching constitutional norms. The democratic cost of this jurisprudential trajectory has been severe. Judicial endorsement of extra-constitutional actions weakened parliamentary sovereignty by allowing non-elected authorities to usurp legislative and constituent powers with legal blessing. Public trust in the judiciary's impartiality and courage eroded as courts were seen as partners, rather than checks, in

projects of authoritarian consolidation. The separation of powers became more formal than real, as executive and military actors repeatedly escaped meaningful judicial scrutiny in moments of greatest constitutional stress. Democracy in Pakistan thus suffered not only because constitutions were suspended or rewritten, but because the very institution tasked with defending the constitutional order repeatedly ratified its violation.

3. Martial Laws in Pakistan and Judicial Independence

The constitutional history of Pakistan is inseparable from the recurring influence of martial law[17]. Each military intervention has not only interrupted the democratic process but has also reshaped the judiciary's character and role within the state. The courts, often positioned as guardians of constitutional order, were repeatedly placed under political and institutional pressure to validate extraconstitutional actions. These judicial compromises eroded the foundations of democratic governance and constitutional supremacy. This analysis examines how successive martial law regimes, under *General Ayub Khan*, *General Yahya Khan*, *General Zia-ul-Haq*, and *General Pervez Musharraf*, systematically weakened judicial independence and transformed the nature of constitutional adjudication in Pakistan.

3.1 General Ayub Khan's Regime (1958–1969)

General Ayub Khan's military takeover in October 1958 marked the first major constitutional rupture in Pakistan's political history[18]. The 1956 Constitution was abrogated, national and provincial assemblies were dissolved, and the military consolidated executive and legislative powers. The judiciary, instead of resisting this unconstitutional seizure, legitimized it through judicial reasoning cloaked in the doctrine of "state necessity." The Supreme Court, in the landmark *State v. Dosso* (1958) case, validated Ayub Khan's actions, laying the groundwork for the subordination of the judiciary to military power. This reasoning shifted the judiciary's role from a protector of constitutional limits to a facilitator of executive dominance. The court justified its decision by suggesting that maintaining order and continuity outweighed adherence to constitutional forms a rationale that would haunt Pakistan's judicial system for decades. Following the abrogation, Ayub Khan introduced the 1962 Constitution, which placed significant restrictions on the judiciary's powers[19]. It institutionalized executive control over the courts, narrowing judicial review and blurring the separation of powers. Judges functioned in a climate where opposing the regime was not only risky but institutionally discouraged. The long-term impact of Ayub Khan's regime was devastating to judicial independence. By normalizing judicial validation of unconstitutional acts, the courts blunted the public's confidence in legal institutions. Democracy, stripped of judicial protection, became vulnerable to future takeovers. Ayub's era set the precedent that extraordinary rule could be judicially validated, embedding a culture of submission within the judiciary.

3.2 General Yahya Khan's Regime (1969–1971)

When General Yahya Khan assumed power in 1969, he deepened the constitutional instability left by his predecessor[20]. Unlike Ayub, Yahya Khan did not attempt to preserve even a façade of constitutional continuity; instead, he ruled directly through martial law regulations, effectively sidelining the judiciary altogether. During this period, the superior courts operated under severe constraints. Their jurisdiction was curtailed, and their ability to review military orders or protect individual rights was virtually nullified. The judiciary's silence in the face of these violations exposed deep institutional fragility, it became a bureaucratic appendage rather than an independent branch of government. The judiciary's failure to challenge *Yahya Khan's* abrogation of the Constitution had severe consequences. Without constitutional oversight, executive authority expanded unchecked, precipitating political repression and alienation. This vacuum of legality contributed to broader national disintegration, culminating in the *separation of East Pakistan* in 1971[21]. The *Yahya regime* highlights how the erosion of judicial independence can accelerate both political and territorial instability. When courts are silenced, the rule of law collapses, and constitutional order becomes irretrievable.



3.3 General Zia-ul-Haq's Regime (1977–1988)

General Zia-ul-Haq's takeover in 1977 presented a more sophisticated and entrenched form of militarized governance[22]. Rather than merely suspending the Constitution, Zia sought to re-engineer the legal and judicial framework to ensure long-term control[23]. His manipulation of constitutional provisions and introduction of ideological law served both political and authoritarian purposes. The Fifth and Sixth Amendments were central to this process. These amendments altered the terms of judicial retirement, shifted appointment powers, and expanded executive discretion in judicial administration. Judges became dependent on the regime for advancement, undermining both institutional autonomy and personal security. Zia also pursued a systematic Islamization of law, establishing Shariat benches and other parallel legal structures. While framed as religious reform, these measures functioned politically to align the judiciary with the regime's ideological narrative and to suppress independent judicial interpretation. Courts under Zia frequently validated his policies through judgments that prioritized "national stability" or "Islamic values" over constitutional legality. Instances of judicial resistance were swiftly punished through dismissal or marginalization. The resulting culture of compliance eroded public confidence and entrenched executive dominance. Even after Zia's death and the restoration of civilian rule, the judiciary struggled to reclaim its independence. The institutional legacies of constitutional manipulation and ideological control outlived the regime itself, leaving behind a cautious and often politically deferential judiciary. Zia's rule thus institutionalized judicial submission not through overt coercion, but through structural and psychological conditioning.

3.4 General Pervez Musharraf's Regime (1999–2008)

General Pervez Musharraf's coup in 1999 initiated a more legally nuanced era of military governance[24]. Learning from earlier regimes, Musharraf sought legitimacy through legal instruments rather than outright abolition of the Constitution[25]. The *Provisional Constitutional Order (PCO)* became the cornerstone of his strategy, compelling judges to swear allegiance to the new regime before resuming their duties[26]. This oath effectively divided the judiciary: those who refused were dismissed, while those who complied retained their positions. Judicial independence was replaced by conditional loyalty to executive power. The confrontation reached its peak in 2007 when Musharraf suspended *Chief Justice Iftikhar Muhammad Chaudhry*, triggering a constitutional crisis[27]. Unlike previous eras, this confrontation sparked resistance both within and beyond the legal community. The *Lawyers' Movement (2007–2008)* united thousands of legal professionals, civil society groups, and ordinary citizens demanding restoration of judicial independence. It was the first time in Pakistan's history that the judiciary, supported by public mobilization, became a symbol of constitutional defiance rather than submission. The reinstatement of the judiciary following Musharraf's resignation represented a partial victory for democratic resilience. Courts, emboldened by public support, began asserting their authority in subsequent years through judicial activism. Yet, structural vulnerabilities, such as executive influence in appointments and institutional politicization, remained unresolved. Musharraf's era therefore represents both continuity and transformation. It reaffirmed the persistent threat posed by military rule to judicial independence but also introduced a new chapter in which public and professional resistance revitalized hopes for constitutionalism.

The history of martial law in Pakistan reveals a recurring pattern: judicial complicity under pressure and constitutional compromise under coercion [28]. From Ayub Khan's initial abrogation to Musharraf's calculated manipulation of legality, the judiciary repeatedly prioritized stability over [29]. Each validation of military rule weakened the rule of law, eroded democratic structures, and conditioned the judiciary to accommodate executive encroachment [13]. However, Pakistan's judicial evolution also demonstrates a potential for renewal [30]. The Lawyers' Movement signaled that judicial independence can be reclaimed when anchored in public demand, professional solidarity, and constitutional conviction [31]. Yet, the legacy of martial law reminds us that institutional reforms are essential. Judicial appointments, tenures, and jurisdictions must be protected constitutionally, free from



military or executive interference [13]. True judicial independence in Pakistan can only be achieved through a firm constitutional culture, one that rejects the doctrine of necessity and affirms that no political crisis justifies the subversion of the rule of law [13]. The judiciary must reclaim its rightful place as the custodian of the Constitution, not its interpreter under duress. Only then can Pakistan break the cycle of constitutional collapse and ensure sustainable democratic governance [32].

4. Controversies Within the Apex Judiciary

Pakistan's Supreme Court, empowered by Articles 184 and 189 of the Constitution to protect fundamental rights and interpret the foundational law, faces its deepest challenges from within its own ranks rather than solely from external forces like military coups or executive overreach (Khan, 2015). Internal controversies ranging from doctrinal flip-flops and ethical scandals to politicized trials and administrative favoritism, have steadily eroded the Court's credibility, turning it from an impartial referee into a perceived player in power struggles. These self-inflicted wounds reveal a judiciary grappling with its core identity, where judges' divisions and compromises have fractured public trust and weakened constitutional guardianship [33].

The *Maulvi Tamizuddin Khan v. Federation of Pakistan* case (PLD 1955 FC 240) set this troubling pattern early [34]. In 1955, the Federal Court upheld Governor-General Ghulam Muhammad's dissolution of the Constituent Assembly based on a narrow procedural flaw under the Government of India Act, 1935, ignoring the democratic will of elected representatives [35]. Chief Justice Muhammad Munir's majority opinion prioritized "legal continuity" over popular sovereignty, laying the groundwork for the "doctrine of necessity" that later justified martial laws. Justice Sharif's dissent warned of the dangers, but the ruling trained courts to favor stability over democracy, priming the judiciary for decades of deference to extra-constitutional power. This internal vulnerability peaked in the *State v. Zulfikar Ali Bhutto* trial (PLD 1979 SC 38), where a divided 4-3 Supreme Court upheld the former prime minister's death sentence amid General Zia-ul-Haq's dictatorship [22]. The majority, led by Chief Justice Anwar-ul-Haq, accepted flawed evidence like coerced testimony and limited Bhutto's defense rights, breaching fair trial principles now enshrined in Article 10-A [36]. Dissenters exposed the political motivations, and international bodies like the International Commission of Jurists labeled it a "judicial murder". The split not only scarred the Court's reputation but also portrayed it as a tool for regime consolidation, amplifying perceptions of bias and forum-shopping [37].

More recently, the presidential reference against Justice Qazi Faez Isa under Article 209 (PLD 2021 SC 1) highlighted the tricky balance between accountability and independence. Triggered after Isa's critical rulings on military land allotments, the probe alleged hidden assets and was seen as executive retaliation. A 10-judge bench quashed it in 2021, insisting on solid evidence for misconduct claims and protecting judges from reprisals. This decision underscored a key tension: unchecked power breeds arrogance, but selective scrutiny stifles courage, calling for SJC reforms like transparent processes to prevent abuse. Justice Shaukat Aziz Siddiqui's 2018 removal by the Supreme Judicial Council further muddied accountability waters. After a speech alleging ISI interference in case assignments, the SJC deemed it misconduct under Article 209, prioritizing judicial silence overexposing systemic issues. Critics argued it punished whistleblowing, chilling honest critique, while supporters cited ethics codes. The case exposed how internal discipline can suppress reform, demanding rules that protect truth-tellers without chaos. The 2019 treason conviction of Pervez Musharraf under Article 6 (PLD 2019 Islamabad 1) offered a bold contrast, with a special court rejecting necessity defenses for his 2007 emergency. Yet, Supreme Court suspensions and his eventual exile diluted enforcement, revealing judicial hesitation against entrenched powers. This gap between strong words and weak action showed disunity's cost, undermining deterrence. Appointment controversies compound these fractures. Skipping senior judges for elevations, often via 18th or 26th Amendment tweaks, breeds cronyism accusations, violating Article 175(3)'s collegial spirit and fostering factions. Similarly, opaque registrar picks, who control

case lists and benches under Article 191, invite suspicions of backdoor influence, breaching equal access in Article 25.

These episodes, from early doctrinal dodges to modern ethics clashes, prove Pakistan's judicial crisis is as much homegrown as imposed. Doctrinal U-turns, trial stains, and admin games have blurred law and politics, sapping constitutional faith. Reforms like fixed seniority, insulated SJC, open administration, and dissent-friendly ethics are essential. Only by mending these internals can the Supreme Court reclaim its role as democracy's unyielding sentinel.

5. Democratic Government & Judicial Independence

5.1 Benazir Bhutto's Second Term: Acting Chief Justices and Executive Manipulation

The second democratic tenure of Benazir Bhutto (1993–1996) is often remembered as a missed opportunity for consolidating judicial independence [37]. Although the period marked a return to civilian rule after years of authoritarian dominance, executive conduct toward the judiciary reflected continuity rather than reform. One of the most controversial practices during this period was the frequent appointment of *Acting Chief Justices* instead of confirming senior-most judges. This tactic allowed the executive to exert indirect influence over judicial leadership by keeping top judicial offices temporary and uncertain [38]. Acting appointments weakened institutional confidence, discouraged judicial assertiveness, and signaled that tenure security depended on executive goodwill. From a constitutional perspective, this practice undermined the principle of separation of powers. Judicial independence does not merely depend on the absence of overt interference; it also requires structural stability. By manipulating appointments, the executive retained leverage over judicial administration, case allocation, and internal discipline. Importantly, these actions did not occur in a vacuum. They were shaped by historical patterns, where executives learned that judicial compliance could be achieved without overt coercion. Thus, even under democratic rule, the judiciary remained vulnerable, not because democracy was absent, but because democratic norms had not yet matured into constitutional restraint.

5.2 Pakistan Peoples Party's Rough Handling of Judges: Political Pressure and Institutional Weakening

Beyond appointments, the Pakistan Peoples Party's broader engagement with the judiciary during democratic rule reflected a confrontational approach that strained institutional boundaries [39]. Judges perceived as unfriendly to executive interests were subjected to political criticism, public delegitimization, and administrative sidelining [40]. Such "rough handling" manifested through pressure tactics rather than formal removal. Public statements questioning judicial motives, resistance to implementing court orders, and strategic delays collectively weakened judicial authority [41]. While civilian governments possess democratic legitimacy, constitutionalism demands restraint in how that power is exercised [42]. This period illustrates a critical paradox: democracy alone does not guarantee judicial independence. When political actors view courts as obstacles rather than partners in governance, judicial autonomy suffers. The judiciary, already institutionally fragile due to past authoritarian subordination, found itself navigating a democratic environment that reproduced many of the same pressures, albeit in subtler forms. Institutionally, these practices deepened mistrust between branches of government and discouraged judicial boldness. Judges became cautious, aware that assertiveness might invite political backlash. Consequently, judicial independence was compromised not through coups or emergency decrees, but through everyday political hostility [43].

5.3 Judgment in the Judges Case: Restoration Jurisprudence and Judicial Autonomy

The Judges Case represents a turning point in Pakistan's constitutional jurisprudence [44]. For the first time, the Supreme Court articulated a doctrine aimed explicitly at restoring judicial autonomy by limiting executive dominance over appointments. The Court emphasized that judicial independence is a *structural requirement* of the Constitution, not a privilege granted by the executive. It reaffirmed the seniority principle and restricted arbitrary discretion in judicial appointments [45]. This jurisprudence

marked a conscious effort to undo decades of executive encroachment documented in earlier chapters. However, the judgment's significance lies not only in its legal reasoning but also in its symbolic message: the judiciary was attempting institutional self-correction. By asserting control over its own composition, the Court sought to reclaim legitimacy eroded by earlier compromises. Yet, the restoration was incomplete. The judgment operated within a political environment still resistant to judicial autonomy. While it strengthened doctrinal foundations, implementation remained contested. Nevertheless, the Judges Case laid the groundwork for later constitutional reforms, demonstrating that jurisprudence could serve as a vehicle for democratic recalibration [46].

5.4 Judicial Crisis During the Zardari Government: Executive–Judiciary Confrontation and Appointments Controversy

The democratic government led by Asif Ali Zardari witnessed one of the most visible confrontations between the executive and the judiciary [47]. The refusal to immediately restore deposed judges following the Lawyers' Movement intensified institutional conflict and tested democratic commitment to constitutional supremacy. Appointments once again became a focal point of controversy. Allegations of favoritism, delays in confirmations, and resistance to court rulings reflected executive discomfort with an assertive judiciary [45]. The confrontation underscored unresolved tensions inherited from both authoritarian and earlier democratic periods. This crisis demonstrated that judicial independence, once asserted, invites resistance from political actors accustomed to judicial accommodation. The executive's reluctance to yield ground highlighted a broader structural issue: democratic legitimacy was being used to justify constitutional defiance. Ultimately, the judiciary's persistence during this period strengthened its public standing. Yet, the episode also exposed institutional fragility, judicial authority still depended heavily on political negotiation rather than unquestioned constitutional acceptance [48].

5.5 The Need for the 18th and 19th Constitutional Amendments: Balancing Independence and Accountability

The 18th Amendment and 19th Amendment emerged as structural responses to decades of judicial–executive conflict [49]. These amendments institutionalized a new appointment mechanism through the Judicial Commission and Parliamentary Committee [50]. The objective was balance: safeguarding judicial independence while ensuring democratic oversight. The Judicial Commission prioritized professional input, while the Parliamentary Committee introduced representative accountability. This hybrid model sought to prevent unilateral control by either branch. Critically, the amendments reflect lessons learned from earlier controversies. Absolute executive discretion had failed; unchecked judicial autonomy also risked elitism. The new framework attempted to reconcile independence with transparency [51]. While debates over effectiveness continue, the amendments represent a constitutional acknowledgment that judicial independence must be *systematically protected*, not episodically defended. They mark a shift from reactive jurisprudence to proactive constitutional design [52].

5.6 Vote of No Confidence and the Deputy Speaker's Ruling: Constitutional Breakdown and Judicial Intervention

The Deputy Speaker's ruling dismissing a vote of no confidence constituted a profound constitutional crisis. By bypassing explicit constitutional procedures, the ruling threatened parliamentary sovereignty and democratic continuity [53]. The judiciary's intervention restored constitutional order by reaffirming that political processes must operate within legal boundaries. This moment demonstrated the Court's willingness to confront executive overreach even in politically charged environments. Importantly, the intervention reflected institutional learning. Unlike earlier eras, the judiciary did not retreat into formalism or deference. Instead, it asserted its role as a constitutional referee, signaling maturity in democratic adjudication [54].

5.7 Supreme Court's Verdict: Hope for Democratic Consolidation

The Supreme Court's verdict on the no-confidence crisis stands as a hopeful marker for Pakistan's democratic future. By prioritizing constitutional text and democratic procedure over political expediency, the Court reaffirmed its commitment to constitutional supremacy. This assertiveness reflects an evolved judiciary, one shaped by past failures but willing to defend democratic norms. While challenges persist, the verdict suggests that judicial independence, though fragile, is no longer passive. It offers cautious optimism that democracy and constitutionalism can coexist through principled adjudication. Judicial independence in Pakistan emerges not as a static principle, but as an evolving struggle contested, corrected, and cautiously advancing.

6. Conclusion

This study examined judicial independence in Pakistan not as a theoretical constitutional promise, but as a practical institutional reality. As discussed, controversies relating to judicial conduct, accountability, appointments, and administration exposed deep institutional fragmentation. Once accommodation became normalized, the judiciary grew vulnerable to politicization, selective accountability, and erosion of moral authority. Internal divisions weakened the judiciary's ability to act collectively and independently. The return to democratic rule did not automatically restore judicial independence. Civilian governments, despite democratic legitimacy, often repeated patterns of executive dominance through manipulation of appointments, political pressure, and resistance to unfavorable judgments. This confirms a central conclusion of this study: democracy without constitutional restraint can undermine judicial independence just as severely as authoritarian rule. When courts validate unconstitutional actions or tolerate executive interference, constitutional limits on power weaken. This encourages both military and civilian executives to bypass democratic institutions.

References

1. Lamer, A., *The rule of law and judicial independence: protecting core values in times of change*. UNBLJ, 1996. 45: p. 3.
2. Afzal, J. and C. Yongmei, *Federal and provincial legislation regarding 'Right to Information' for good governance in Pakistan*. Discover Global Society, 2023. 1(1): p. 12.
3. Afzal, J., *Impact of Enactment of 'The Prevention of Electronic Crimes Act, 2016' as Legal Support in Pakistan*. Academy of Education and Social Sciences Review.
4. Tiwari, S., *The Role of the Judiciary in Upholding Democratic Principles*. Issue 6 Int'l JL Mgmt. & Human., 2024. 7: p. 539.
5. Nazir, J., Z. Jabeen, and S.U. Khan, *THE FUTURE OF CONSTITUTIONAL GOVERNANCE IN PAKISTAN: PROSPECTS AND CHALLENGES*. Journal of Religion and Society, 2024. 2(4): p. 126-141.
6. Akhtar, Z., *A Legal Paradox: Pakistan's Constitution, Martial Law and State Necessity*. Sri Lanka J. Int'l L., 2009. 21: p. 153.
7. Hussain, S., *Together without Consensus: Class, Emotions and the Politics of the Rule of Law in the Lawyers' Movement (2007-09) in Pakistan*. 2018: City University of New York.
8. Shafiq, H.M.S., et al., *Constitutional court appointments mechanism and judicial independence; a study of USA, Maldives, Canada, Germany, Egypt and Pakistan*. Pakistani Journal of International Affairs, 2022. 5(2).
9. Afzal, J., *Digital Law Enforcement Challenges and Improvement, in Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 47-78.
10. Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024: Springer.
11. Paulsen, M.S., *The constitution of necessity*. Notre Dame L. Rev., 2003. 79: p. 1257.
12. Stavsky, M.M., *The doctrine of state necessity in Pakistan*. Cornell Int'l LJ, 1983. 16: p. 341.
13. Wolf-Phillips, L., *Constitutional legitimacy: A study of the doctrine of necessity*. Third World Quarterly, 1979. 1(4): p. 97-133.
14. Siddique, O., *The jurisprudence of dissolutions: Presidential power to dissolve assemblies under the Pakistani constitution and its discontents*. Ariz. J. Int'l & Comp. L., 2005. 23: p. 615.
15. Choudhury, Z., *The Role of Judiciary in the Constitutional Development of Pakistan (1947-1971)*. Dhaka Univ. Stud. Part F, 1989. 1: p. 1.
16. Agresto, J., *The Supreme Court and constitutional democracy*. 1984: Cornell University Press.
17. Aziz, S., *The Constitution of Pakistan*. 2018.



18. Khan, A., M. Ahmad, and A. Waheed, *Pakistan's Journey to Civilian Rule (1958-70): An Analysis of Ayub Era*. Global Legal Studies Review, 2016. **1**(1): p. 1-8.
19. Gul, S., N.A. Khan, and S.S. Sulehri, *THE 1962 CONSTITUTION AND ITS IMPLICATIONS FOR PARTY POLITICS IN PAKISTAN: A STUDY OF CONTROLLED DEMOCRACY UNDER AYUB KHAN*. International Research Journal of Islamic Culture and Communication (IRJICC), 2025. **3**(3): p. 1-19.
20. Burki, S.J., *Rise to Power*, in *Pakistan Under Bhutto, 1971–1977*. 1980, Springer. p. 58-75.
21. Choudhury, Z.I., *Roots of Dictatorship in Pakistan, 1954-1971*.
22. Burki, S.J., *Pakistan under Zia, 1977-1988*. Asian Survey, 1988. **28**(10): p. 1082-1100.
23. Hussain, M.Z., *Islam in Pakistan under Bhutto and Zia-ul-Haq*, in *Islam, Muslims and the Modern State: Case-Studies of Muslims in Thirteen Countries*. 1994, Springer. p. 47-79.
24. Behuria, A.K., *How military dominates the political space in Pakistan: A study of Musharraf's rule (1999-2008)*. Journal of peace studies, 2009. **16**(1-2): p. 76-102.
25. Fatima, Z. and R. Shafique, *General Pervez Musharraf: The Political Strategies to Consolidate Power (1999-2008)*. ACADEMIA International Journal for Social Sciences, 2025. **4**(2): p. 1577-1588.
26. Ali, G., P.D.R. Musarrat, and M.S. Azhar, *Federalism in Pakistan During Musharraf Regime*. Journal of Public Administration and Governance, 2012. **2**(3): p. 171-188.
27. Ghias, S.A., *Miscarriage of chief justice: judicial power and the legal complex in Pakistan under Musharraf*. Law & Social Inquiry, 2010. **35**(4): p. 985-1022.
28. Ahmad, S.N., *From Martial Law to Martial Law: Politics in the Punjab, 1919-1958*. 2019: Routledge.
29. Kureshi, Y., *Seeking supremacy: The pursuit of judicial power in Pakistan*. 2022: Cambridge University Press.
30. Khan, M.S., *Genesis and evolution of public interest litigation in the supreme court of Pakistan: toward a dynamic theory of judicialization*. Temp. Int'l & Comp. LJ, 2014. **28**: p. 285.
31. Hussain, F., *The judicial system of Pakistan*. 2011: Supreme Court of Pakistan Pakistan.
32. Islam, N., *Democracy and governance in Pakistan's fragmented society*. International Journal of Public Administration, 2001. **24**(12): p. 1335-1355.
33. Zemans, F.K., *The accountable judge: guardian of judicial independence*. S. Cal. L. Rev., 1998. **72**: p. 625.
34. Khan, H., *Developing Liberal Jurisprudence in Pakistan: Role of Justice AR Cornelius*. Policy Perspectives, 2020. **17**(1): p. 129-139.
35. Abbas, N., *Constitutional crisis of Pakistan: A historical study*. Pakistan Journal of International Affairs, 2023. **6**(2).
36. Jamali, N.H., et al., *A Comparative Analysis of the Right to a Fair Trial in Pakistan in Context with ICCPR's Set out Standards*. Beijing L. Rev., 2024. **15**: p. 231.
37. Geyh, C.G., *To Legitimacy and Beyond: A Reform Agenda to Restore Public Confidence in the Federal Courts*. Law & Contemp. Probs., 2024. **87**: p. 1.
38. Panhwar, S.H., *Benazir Bhutto Selected Speeches 1989–2007*. 2009, Location unknown: Self Published.
39. Landau, D., *Political institutions and judicial role in comparative constitutional law*. Harv. Int'l LJ, 2010. **51**: p. 319.
40. King, J.A., *Institutional approaches to judicial restraint*. Oxford journal of legal studies, 2008. **28**(3): p. 409-441.
41. Fletcher, W.A., *The discretionary constitution: Institutional remedies and judicial legitimacy*. The Yale Law Journal, 1982. **91**(4): p. 635-697.
42. Cardozo, B.N., *The nature of the judicial process*. Vol. 21. 1921: Yale University Press.
43. Resnik, J., *Managerial judges*. Harv. L. Rev., 1982. **96**: p. 374.
44. Qaiser, M.N., A. Warraich, and M.S. Jamil, *THE ROLE OF THE JUDICIAL COMMISSION: JUDICIAL INDEPENDENCE IN PAKISTAN POST-26TH AMENDMENT*. International Journal of Social Sciences Bulletin, 2025. **3**(4): p. 684-696.
45. Munir, B., A.N. Khan, and D.N. Ahmed, *Judicial Activism, Selectivism, and Executive's Functional Space: A Critical Appreciation in the Context of Pakistan*. Journal of Research Society of Pakistan, 2021. **58**(1): p. 28-35.
46. Khan, A., I. Naseem, and M. Inamullah, *Constitutional Dynamics and Judicial Autonomy in South Asia: A Comparative Study of Pakistan and its Neighbors*. Al Manhal Research Journal, 2025. **5**(1).
47. Lee, H.P., *Judiciaries in Crisis—Some Comparative Perspectives*. Federal Law Review, 2010. **38**(3): p. 371-389.
48. Rosenthal, M., G. Barzilai, and A. Meydani, *Judicial review in a defective democracy: Judicial nominations and judicial review in constitutional courts*. Journal of Law and Courts, 2021. **9**(1): p. 137-157.
49. Collett, T.S., *Judicial independence and accountability in an age of unconstitutional constitutional amendments*. Loy. U. Chi. LJ, 2009. **41**: p. 327.

50. Shah, A., *Making federalism work: the 18th constitutional amendment*. 2012: World Bank, Washington, DC.
51. Geyh, C.G., *Judicial independence, judicial accountability, and the role of constitutional norms in congressional regulation of the courts*. Ind. LJ, 2003. **78**: p. 153.
52. Ali, R.N., *Independence of Judiciary in Pakistan: An analysis of 18th & 19th Constitutional Amendments*. Journal of Social Sciences Review, 2021. **1**(2): p. 1-12.
53. Bromo, F., *Early parliamentary dissolutions and judicial review: lessons from comparative cases*. Comparative Legal History, 2025: p. 1-21.
54. Kavelidze, E., *Vote of No-Confidence as the Form of Government's Political Responsibility*. J. Law, 2014: p. 52.

Declaration

Conflict of Study: The author declare that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable

Declaration of AI Use: The author declares that the AI tool "ChatGPT" was used to assist with drafting in the preparation of this manuscript. All content was critically reviewed, verified, and edited by the author, who take full responsibility for the accuracy and integrity of the work.



From Cash to Code: Examining the Legal Framework for the Future of Digital Currency in Pakistan

Balkees Amjad ^{1*}

¹School of International Law, Southwest University of Political Science and Law, China

* Corresponding Email: balkeesamjad1@gmail.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.07>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Pakistan's cash-heavy economy is rapidly moving toward digital finance, driven by fintech growth and the State Bank of Pakistan's Raast instant payment system, making it crucial to assess whether existing laws can support a future Digital Rupee or central bank digital currency (CBDC). This study evaluates how well Pakistan's current monetary and financial framework can accommodate CBDC, identifies regulatory and institutional gaps, and proposes reforms to protect monetary sovereignty, enhance financial inclusion, and maintain coherence across the financial system. This paper treats the shift "from physical cash to digital code" as a legal paradigm change that demands an updated understanding of legal tender, payments, and state-backed money in the digital age. Using doctrinal legal analysis, comparative case studies, and policy review, it examines whether Pakistan's existing rules can safely support CBDC design, issuance, and use. The study traces Pakistan's move from a predominantly cash-based economy to expanding digital rails, focusing on Raast and major private platforms such as Easypaisa, JazzCash, and licensed electronic money institutions (EMIs). It analyzes post-COVID-19 uptake of digital payments alongside persistent barriers such as low digital literacy and trust, especially among underserved groups. The paper also benchmarks Pakistan's emerging CBDC posture against international experiences, including China's e-CNY, the EU's Digital Euro, and Nigeria's eNaira, to highlight lessons on legal tender status, architecture, and inclusion. It then critically reviews key statutes i.e., the State Bank of Pakistan Act 1956, the Payment Systems and Electronic Funds Transfer Act 2007, the Foreign Exchange Regulation Act 1947, and the Prevention of Electronic Crimes Act 2016, showing that despite strong SBP authority, definitional gaps and overlapping mandates create legal uncertainty over digital assets, data protection, consumer redress, and cybersecurity. This study recommends targeted amendments to foundational monetary and payments legislation and the adoption of a dedicated "Digital Currency Act" that clearly defines the legal tender status of a Digital Rupee, allocates governance responsibilities, and embeds safeguards for privacy, cybersecurity, and user rights. It further argues that aligning Pakistan's framework with FATF, IMF, and BIS standards will allow the country to harness its growing digital infrastructure to foster inclusion, safeguard rights, and position itself as a regional leader in secure and equitable digital finance.

Keywords: Digital Currency; CBDC; Legal Framework; Pakistan; Financial Inclusion; FATF Compliance

1. Introduction

Over the past decade, Pakistan's financial landscape has undergone a remarkable transformation. A country once dominated by cash transactions is now witnessing a steady rise in [1]. What began as an experiment in financial technology has evolved into a nationwide movement toward digital finance [2]. This shift is not merely following a global trend but also it reflects Pakistan's need to expand financial inclusion, reduce transaction costs, strengthen transparency, and modernize its payment system [3]. However, the transition from physical cash to digital value is more than a technological upgrade; it is a fundamental legal and economic turning point [4]. It challenges long-held assumptions about what constitutes "money," who may issue it, and how it should be regulated. As digital platforms grow, so too do questions about the legal definition of tender, the authority to issue and control digital money, liability in cases of system failure or fraud, and data protection for users in an increasingly



interconnected ecosystem[5]. In short, Pakistan's financial transformation demands a parallel modernization of law and regulation [6].

For decades, Pakistan's reliance on cash has fueled a vast informal economy and deepened the divide between formal and informal finance [7]. Large segments of the population remain unbanked, hindered by limited access to banking services, social disparities, low financial literacy, and mistrust in institutions [8]. Recognizing these barriers, the State Bank of Pakistan (SBP) has taken decisive steps to promote digitalization through platforms like *Raast*, the country's instant payment system, and mobile money services such as Easypaisa and JazzCash [9] [10]. Yet, while these innovations promise inclusion and efficiency, they also expose critical legal uncertainties for regulators, service providers, and the public. These uncertainties become even more complex when digital payments evolve into digital currency. Around the world, digital currencies are reshaping legal and monetary boundaries [11]. Cryptocurrencies like Bitcoin operate beyond state control, while central bank digital currencies (CBDCs) represent state-backed digital money designed to coexist with traditional cash [12, 13]. Pakistan now stands at this crossroads. The SBP has expressed justified caution toward unregulated crypto-assets due to their potential for money laundering, fraud, and financial instability [14]. At the same time, growing interest in a possible "Digital Rupee" signals Pakistan's intent to innovate responsibly under a sovereign framework [15]. The central question is clear: How can the law encourage digital innovation without undermining monetary sovereignty, financial stability, and public trust? Existing legal frameworks, rooted in statutes such as the *State Bank of Pakistan Act 1956*, the *Foreign Exchange Regulation Act 1947*, the *Payment Systems and Electronic Funds Transfer Act 2007*, and the *Prevention of Electronic Crimes Act 2016*, provide a valuable foundation for currency and payment regulation [16]. Yet, these laws were conceived for a physical economy, not one where money might exist purely as digital code. Critical legal issues remain unresolved, including the definition of digital legal tender, issuance authority in the digital domain, treatment of digital tokens, and the delineation of regulatory responsibilities across banking, telecom, data, and cybersecurity regimes. A future Digital Rupee would, therefore, require more than incremental reform [17]. It demands a comprehensive legal architecture that clearly defines its legal tender status, governance mechanisms, convertibility, and distribution model [18, 19]. Such a framework must embed robust standards for consumer protection, dispute resolution, operational resilience, and cybersecurity [20, 21]. Comparative experience from other jurisdictions reveals that technological readiness alone is insufficient [22]; successful CBDC implementation must rest on strong legal certainty and cross-sector coordination [23, 24]. Any move toward a Digital Rupee must preserve monetary sovereignty and align with international obligations[25]. Currency issuance is a central act of state authority; its digital extension must be explicitly authorized in law and consistent with Pakistan's commitments under global AML/CFT and financial integrity standards. As cross-border payments accelerate, legal clarity and international compliance will be essential to maintaining trust and stability [26, 27].

So, this research examines;

- Whether Pakistan's current legal and institutional framework can effectively support the development of a Digital Rupee.
- Identifying the regulatory gaps, statutory limitations, and policy challenges that must be addressed to enable a secure and inclusive digital monetary system.
- How Pakistan's "cash-to-code" transition is not only an economic or technological evolution but a defining legal moment.

2. Evolution of Currency and Digital Transformation in Pakistan

Pakistan's shift from a cash-based to a digital financial ecosystem has been the result of a long historical and institutional journey shaped by economic realities, uneven access to banking, and rapid technological change. For decades, cash was the dominant means of exchange in Pakistan, valued not

only for its convenience but also for the trust and autonomy it provided in daily commerce. However, this reliance on physical currency reinforced a large informal economy, limited transaction documentation, and constrained the state's ability to broaden the tax base and extend formal financial services. The ongoing move "from cash to code" thus represents a structural shift in how money is used, regulated, and understood within the economy. Following independence in 1947, Pakistan initially relied on monetary institutions inherited from British India. With the establishment of the State Bank of Pakistan in 1948, the state began consolidating authority over currency issuance and monetary policy (SBP, 2023). Much of the twentieth century was defined by efforts to manage physical currency, maintain confidence in the Pakistani Rupee, control inflation, and foster monetary stability (World Bank, 2019). Despite expansion in formal banking, access remained concentrated in urban centers. In rural areas, limited infrastructure, low financial literacy, and mistrust in formal institutions kept large populations excluded from the regulated banking system, sustaining a heavy reliance on cash transactions[28].

The early 2000s marked a pivotal phase with the rise of mobile connectivity and affordable internet access. Technology began reshaping consumer behavior and introduced new possibilities for financial inclusion through digital channels[29]. Branchless banking emerged as a key innovation, driven by partnerships between banks, telecom operators, and microfinance institutions. Landmark services such as Easypaisa, launched in 2009, and JazzCash soon after, enabled millions of unbanked users to send and receive money, pay bills, and conduct essential transactions via mobile phones. This digitalization played a transformative role in expanding financial access and empowerment among previously excluded communities. Pakistan's digital payments landscape entered a more mature phase with the launch of Raast in 2021, an instant payment system spearheaded by the SBP to enable real-time, low-cost transactions across banks, fintechs, and government channels (SBP, 2021). Raast's integration with public payment programs has demonstrated how national payment infrastructure can foster inclusion, transparency, and efficiency (United Nations Capital Development Fund). Since its rollout, digital retail payments have increased significantly through mobile and internet banking platforms, establishing an operational backbone for potential innovations such as a central bank digital currency (CBDC)[30]. Concurrently, Pakistan's fintech sector has accelerated digital adoption by introducing user-friendly digital wallets, peer-to-peer platforms, and merchant payment tools. In response, the SBP introduced a licensing and regulatory framework for Electronic Money Institutions (EMIs), enabling non-bank entities to issue e-money under formal oversight (SBP, 2019). This framework has encouraged innovation while guiding the gradual transition toward a "cash-lite" economy. Nonetheless, digital growth raises governance challenges, including compliance with Know Your Customer (KYC) and anti-money laundering (AML) rules, and ensuring interoperability between banks, fintechs, and public payment systems (IMF, 2023).

Despite measurable progress, public adoption of digital payments remains uneven across regions and demographics. Urban youth have embraced cashless tools faster than rural or elderly populations, who continue facing barriers such as weak connectivity, lower digital literacy, and concerns about fraud[28, 31]. The COVID-19 pandemic temporarily accelerated digital payment adoption, yet long-term success hinges on consumer education, cybersecurity, and robust grievance redress mechanisms (World Bank, 2022). Current initiatives emphasizing digital literacy and women's participation underscore that financial transformation in Pakistan is as much a social challenge as it is technological[32]. Today, Pakistan's currency evolution stands at a critical threshold[33]. The nation possesses essential building blocks, branchless banking networks, EMI frameworks, and Raast infrastructure, but moving toward a sovereign digital currency will require more than technological readiness. Legal clarity, institutional coordination, and public trust are vital foundations for sustainable digital monetary transformation (SBP, 2023). Ultimately, Pakistan's journey from cash dependency toward digital enablement reflects a deeper evolution in governance, inclusion, and the very definition of money in a digital economy.

3. The Existing Legal and Regulatory Framework in Pakistan

The existing legal and regulatory framework in Pakistan provides a partial but incomplete foundation for governing digital finance and any future move toward a digital rupee [34]. Much of the core statutory architecture was designed for a cash-dominant, bank-centric system, and has been stretched through regulations and circulars to accommodate electronic payments rather than natively digital forms of money such as CBDCs or tokenized instruments. Within this framework, four statutes are particularly important: *the State Bank of Pakistan Act, 1956*; *the Payment Systems and Electronic Funds Transfer Act, 2007*; *the Foreign Exchange Regulation Act, 1947*; and *the Prevention of Electronic Crimes Act, 2016*, alongside the evolving regulatory role of the State Bank of Pakistan (SBP) itself.

The *State Bank of Pakistan Act, 1956* establishes SBP as the central bank and vests in it the core mandate of regulating the monetary and credit system, issuing currency, and securing monetary stability in Pakistan [35]. It gives SBP the exclusive authority to issue banknotes and defines the legal tender status of currency, framing the traditional architecture of sovereign money [36]. Over time, amendments have enhanced SBP's autonomy in monetary policy and its supervisory control over the banking sector, including powers over licensing, regulation, and oversight of banks and certain financial institutions [37]. This statute forms the constitutional backbone for any future digital currency, because questions such as who may issue a digital rupee, whether it is legal tender, and how it relates to existing forms of money are ultimately grounded in the SBP Act [38]. However, the Act was drafted long before digital currencies and does not explicitly define "digital currency" or "CBDC," leaving ambiguity over whether a digital rupee could be treated as a form of "currency" under the existing provisions or whether express legislative amendments would be required [39]. In practice, SBP has relied on its general powers to issue regulatory frameworks for payment systems and fintech, but those remain secondary legislation layered onto a statute built for physical cash and conventional deposits [40]. *The Payment Systems and Electronic Funds Transfer Act, 2007* (PS&EFT Act) is the central statute governing electronic payments and payment systems in Pakistan. It provides legal recognition and regulatory machinery for payment systems, payment instruments, and electronic funds transfers, empowering SBP to designate and supervise system operators and service providers [41]. Among other things, it allows SBP to prescribe standards for the safety, efficiency, and soundness of payment systems, and to oversee the operation of systems such as real-time gross settlement and retail payment schemes. The Act also embeds important consumer-protection features: it sets obligations on financial institutions regarding information disclosure, error resolution, and liability for unauthorized or incorrect electronic transfers, and it provides customers with civil remedies against service providers in cases of negligence or non-compliance. This framework has enabled the regulated roll-out of card networks, internet banking, mobile banking, and, more recently, instant payment platforms such as Raast, which rely on SBP's authority to designate and govern system operators and payment institutions [42]. Yet, the PS&EFT Act focuses on infrastructure, mechanisms, and responsibilities around electronic transfers, not on redefining what constitutes "money" itself [42]. It treats electronic funds transfer primarily as a means of moving existing monetary balances, typically deposits, rather than as a legal category of digital sovereign currency [43]. As a result, while the Act can readily be used to regulate wallets, payment switches, and digital payment schemes, it does not resolve core conceptual questions that would arise with a CBDC, such as whether digital units issued directly by SBP are to be treated as deposits, cash equivalents, or a distinct class of legal tender [44]. Nor does it directly address tokenized assets or smart-contract-based payment mechanisms, which are increasingly relevant for modern digital currency design [45]. The *Foreign Exchange Regulation Act, 1947* (FERA) is a pre-independence statute that Pakistan retained and applies to regulate dealings in foreign exchange, payments to and from non-residents, and the movement of currency and certain financial instruments across borders [46]. It empowers the federal government and SBP to impose licensing requirements, control foreign currency accounts, restrict certain cross-border payments, and regulate the import and export of currency and

bullion [47]. FERA is important in the digital context because any cross-border use of digital currency or interaction with foreign digital assets would intersect with Pakistan's exchange-control regime. However, FERA's language is rooted in traditional concepts of "currency," "securities," and "foreign exchange," and does not expressly accommodate digital tokens, crypto-assets, or cross-border digital wallets [48]. In practice, SBP has drawn on its powers under banking and foreign-exchange law to instruct banks and payment providers not to facilitate trading or settlement in cryptocurrencies and unregulated virtual assets, citing concerns around money laundering, capital flight, and consumer protection, but the statute itself does not spell out how such instruments should be classified or treated [49]. If Pakistan were to issue a CBDC with cross-border functionality, or to formally regulate stablecoins and other digital instruments linked to foreign currencies, FERA would likely require updating or interpretive clarification to ensure consistent treatment and effective AML/CFT control [50].

The Prevention of Electronic Crimes Act 2016, constitutes Pakistan's principal cyber-crime statute, criminalizing conduct such as unauthorized access to information systems, data interception, electronic fraud, electronic forgery, and offenses relating to identity and information misuse [51]. It provides law-enforcement agencies with powers to investigate, search, and seize electronic evidence and establishes penalties for a range of offenses that can target or exploit digital financial platforms, including online banking systems and payment infrastructure [52]. In the context of digital currency, PECA would be relevant to prosecuting hacking of CBDC wallets, manipulation of transaction records, phishing schemes targeting digital-wallet users, and other cyber-enabled financial crimes [53]. Its broad definitions of "information system" and "data" allow its application to financial platforms even though it is technology-neutral [54]. However, PECA is fundamentally a criminal-law instrument; it does not provide prudential standards or operational requirements for financial institutions, nor does it establish a sector-specific framework for incident reporting, resilience, or cyber-risk management in payment and currency systems [54]. Thus, while it complements financial regulation by providing sanctions against harmful conduct, it does not itself regulate how digital currency infrastructure must be designed or governed. Within this statutory landscape, the State Bank of Pakistan plays a central regulatory and policymaking role [55]. Under the SBP Act and related laws, it licenses and supervises banks, microfinance institutions, payment system operators, payment service providers, exchange companies, and, more recently, electronic money institutions (EMIs) and digital banks. SBP has issued a dedicated regulatory framework for EMIs, allowing non-bank entities to offer e-money and wallet services subject to capital, governance, and risk-management requirements. It has also published a licensing and regulatory framework for digital banks, aimed at fostering branchless, technology-driven banking models under strict prudential oversight. On the infrastructure side, SBP oversees key systems including the real-time gross settlement system and the instant payment system Raast, leveraging its PS&EFT powers to designate and regulate system operators and ensure interoperability, security, and efficiency [56]. Regarding virtual assets, SBP has taken a cautious, restrictive policy stance. Through circulars and public advisories, it has directed banks and regulated entities not to facilitate trading, custody, or settlement services for cryptocurrencies and related tokens, citing concerns over volatility, consumer risks, and potential misuse for money laundering and terrorism financing, as well as the absence of a formal legal framework for such assets. At the same time, SBP has participated in policy discussions about exploring a central bank digital currency, aligning with emerging international practice, and has signaled interest in studying CBDC models, including potential benefits for payments efficiency and financial inclusion [57]. This dual posture, promoting digitalization of regulated financial services while restricting unregulated private digital assets, reflects the tension between innovation and risk management that will shape any future legal framework for a digital rupee [58]. Despite these building blocks, the existing financial-law framework reveals several significant gaps and limitations when examined through the lens of a future digital currency system. One fundamental gap is the absence of

explicit legal definitions and categories for digital currency, CBDCs, and virtual assets in primary legislation. Neither the SBP Act nor the PS&EFT Act clearly specifies what constitutes digital legal tender, how it relates to physical currency and bank deposits, or what obligations public bodies and private parties would have to accept it in discharge of debts [59]. Without such clarity, a CBDC implementation would rely heavily on regulatory interpretation and could be vulnerable to legal challenges, especially regarding issues such as priority in insolvency, treatment under existing contract law, and interaction with tax and accounting rules. A second limitation concerns data governance, privacy, and surveillance. Large-scale digital currency systems, particularly retail CBDCs, generate granular transaction data that can be highly revealing of individuals' economic behavior. Pakistan currently lacks a comprehensive, enacted personal data protection law, although draft legislation has been proposed; existing statutes such as PECA focus on criminalizing unauthorized access or misuse rather than on proactive rules for collection, processing, retention, and sharing of financial data [60]. Any future digital currency framework will have to reconcile SBP's legitimate needs for oversight and AML/CFT compliance with constitutional and human-rights concerns about privacy and state surveillance, which are not yet fully articulated in financial legislation [61]. Third, the legal treatment of private digital assets and crypto-based instruments remains largely regulatory and policy-driven rather than statutory [62]. SBP's directions have effectively constrained the involvement of regulated entities with cryptocurrencies, but there is no specific statute that categorizes virtual assets, sets licensing requirements for virtual asset service providers, or defines their relationship to existing categories such as "securities" or "commodities." This can create legal uncertainty, especially in light of evolving international standards such as those issued by the FATF, which expect jurisdictions to establish clear regulatory regimes for virtual assets and associated service providers [63]. A fourth gap lies in the framework's limited adaptation to programmable money, smart contracts, and decentralized infrastructures. The PS&EFT Act contemplates centralized operators and service providers and assigns them responsibilities for ensuring accuracy, security, and reversals, but it does not expressly address complex arrangements where transactions are executed automatically based on code, or where decentralized validators share responsibility. Questions about liability allocation, dispute resolution, error correction, and legal finality of transactions in such environments would need more tailored statutory treatment if Pakistan were to adopt advanced digital currency features. Fifth, cross-border dimensions of digital currency are insufficiently captured by FERA's traditional categories. If Pakistani residents were to hold foreign CBDCs or stablecoins, or if a Pakistani CBDC were used abroad, complex questions would arise about exchange control, capital-account management, and cross-border AML/CFT supervision that FERA, in its current form, only partially addresses. Addressing these cross-border aspects is crucial not only for financial stability but also for maintaining correspondent-banking relationships and compliance with global standards. Finally, existing coordination mechanisms among SBP, SECP, FBR, and cyber-crime and data-protection authorities have not yet been fully re-engineered for a digital-currency environment that cuts across monetary law, securities regulation, cyber-security, taxation, and consumer protection [64]. Fragmented mandates may lead to regulatory overlaps, inconsistencies, or gaps when dealing with complex digital products that span payments, investment features, and data processing [65]. An effective legal framework for digital currency will require clearer allocation of responsibilities, formal coordination channels, and possibly new institutional arrangements or joint regulatory bodies. Overall, Pakistan's current legal and regulatory framework is robust enough to support incremental digitalization of payments and the growth of regulated digital financial services, but it remains incomplete for a fully fledged digital currency ecosystem. The move "from cash to code" will therefore demand a deliberate legislative agenda: clarifying the legal nature of digital sovereign money, updating exchange-control and payment laws, embedding privacy and data-governance safeguards, designing statutory regimes for virtual assets, and strengthening inter-agency coordination. Without these reforms, any CBDC or comprehensive digital

currency framework would rest on a legal foundation that is functional but not fully fit for purpose in the new monetary era [66].

4. Legal Challenges in the Digital Currency Ecosystem

Digital currency creates legal pressure because most financial laws were written for a world of physical cash, paper instruments, and bank-centred transactions [67]. Code-based money operates through apps, networks, and automated systems that do not fit neatly into older legal categories [68]. In Pakistan, the challenge is sharper because digital payments are growing fast, yet primary legislation has not fully caught up with CBDCs, private digital assets, and programmable payment tools. As a result, uncertainty appears at the points where law normally provides clarity: definitions, jurisdiction, privacy, consumer rights, and liability [69].

4.1 Ambiguities in legal definition and status

The first and most basic problem is definitional. Many legal systems, including Pakistan's, do not clearly define "digital currency," "virtual assets," or "CBDC" in primary statutes [70]. Monetary law still tends to describe "currency" and "legal tender" with reference to notes and coins, while electronic payment laws focus on moving balances rather than creating a new form of sovereign money. This creates uncertainty about how a future Digital Rupee would be treated in law: is it the same as cash, a new category of legal tender, or simply another electronic value instrument? These questions matter because legal status affects contracts, discharge of debts, insolvency priority, taxation, and accounting treatment. For private digital assets, the classification problem is even more complex [71]. A cryptocurrency or stablecoin may be treated as a commodity, a security, a payment instrument, or a sui generis asset, each label triggering different licensing duties, investor disclosures, and consumer safeguards. Where statutes are silent, regulators often rely on circulars or case-by-case decisions. That approach can discourage responsible innovation, while leaving enough "grey space" for unregulated actors to operate. It also places courts in a difficult position when disputes arise over ownership, collateral enforcement, fraud recovery, or the legal effect of smart-contract obligations [72].

4.2 Jurisdictional and enforcement challenges

Digital currency systems routinely operate across borders. Users may be in one country, service providers in another, and infrastructure (servers, nodes, cloud services) scattered globally. This reality complicates jurisdiction, applicable law, and enforcement [73]. Traditional conflict-of-laws tools, such as the place of contracting, performance, or location of assets, are harder to apply when assets exist as entries on ledgers accessible from anywhere. For regulators and law enforcement agencies, cross-border structure creates practical limits. A wallet provider or exchange may serve Pakistani users through an app without being locally licensed. Authorities may struggle to compel compliance, obtain records, freeze assets, or enforce sanctions. International cooperation mechanisms exist, but they often move slowly compared to the speed of digital transactions, and they are poorly suited to decentralized systems with no identifiable operator. This gap can be exploited for fraud, money laundering, or sanctions evasion through "jurisdiction shopping." Even in a CBDC context, cross-border use raises difficult questions. If non-residents can hold or transact in a Digital Rupee, Pakistan would need clear rules on court jurisdiction, regulatory cooperation, and exchange-control treatment, areas where traditional foreign exchange laws were not drafted with digital units in mind [74].

4.3 Data protection and privacy issues

Digital currency systems generate detailed transactional data that may be more granular than ordinary banking records. In a retail CBDC, particularly an account-based model, transaction trails can reveal personal patterns of spending, location, and lifestyle [75]. This creates a legal balancing task: enabling AML/CFT compliance and financial oversight without turning digital money into a tool of excessive surveillance. In many developing jurisdictions, including Pakistan, data protection regimes remain incomplete or unevenly enforced. Where clear rules are missing, individuals may not know who can

access their transaction data, for what purpose, and for how long. If the legal framework allows broad access without oversight, adoption may weaken due to fear of monitoring [76]. If privacy is designed too strongly without risk controls, it may conflict with FATF expectations and weaken AML/CFT enforcement. Another layer concerns data localization and cross-border data flows: when digital currency platforms use foreign cloud infrastructure, questions arise about which laws apply, how regulators can access data, and what remedies exist if data is misused or leaked. Without clear statutory safeguards, trust, the currency of digital finance can erode quickly [77].

4.4 Consumer rights and dispute resolution mechanisms

Digital currency ecosystems challenge consumer protection because users often interact with apps, wallets, and automated processes rather than traditional bank branches [77]. Funds may be stored in wallet structures instead of bank accounts, and transactions may involve multiple intermediaries like banks, EMIs, payment switches, technology vendors, and sometimes smart-contract code. When something goes wrong unauthorized transfers, system outages, mistaken payments, or fraud, the question becomes: who is legally responsible, and what remedy does the user have? Existing electronic transfer rules offer a starting point, but they were not drafted for complex digital value chains or self-executing transactions. Smart contracts create a particularly difficult problem: if a transfer occurs due to faulty code, an oracle error, or an automated trigger, the law may not clearly allocate loss between developer, platform, intermediary, and user. Cross-border services complicate matters further because platforms may be licensed under foreign standards or not effectively supervised at all. For a CBDC, policymakers must decide how far statutory protections will go, whether certain losses are guaranteed, how mistaken or fraudulent transfers will be handled, and which forum (courts, ombudsman, arbitration, specialized tribunals) will provide accessible and timely dispute resolution [78].

4.5 Cybersecurity threats and liability concerns

Because digital currency systems rely on information infrastructure, cybersecurity is not a side issue—it is a core legal risk. Threats include hacking of wallets, phishing and identity theft, malware targeting user devices, insider abuse, denial-of-service attacks, and vendor-chain vulnerabilities [79]. A major incident can undermine confidence in payments and, at worst, affect financial stability. Pakistan's cybercrime law provides tools to punish attackers, but criminal law alone does not create a prevention framework. It does not set minimum resilience standards, define institutional duties, or clearly allocate liability when breaches occur. This leaves urgent legal questions open: What cybersecurity standards must intermediaries meet? Who compensates users when losses result from weak safeguards or third-party failures? In a CBDC system, how will responsibility be shared between the SBP, banks, EMIs, and technology providers? If liability rules are weak, providers may underinvest in security; if rules are overly strict, they may avoid participation or innovation. A credible framework therefore needs clear standards for resilience, mandatory incident reporting, audit requirements, compensation rules where fault exists, and viable insurance or guarantee mechanisms, supported by cooperation with international best practices because cyber risks do not respect borders.

4.6 Overall implications

These challenges show that digital currency is not simply an “upgrade” of payments. It is a structural change that tests the boundaries of monetary law, private law, criminal enforcement, and data governance. If the legal system remains unclear on status, jurisdiction, privacy, consumer protection, and cybersecurity liability, digital currency initiatives may struggle to earn trust, withstand disputes, or deter misuse. For Pakistan, the solution cannot be purely reactive or circular-based. It requires proactive legislative reform, clear regulatory mandates, and coordinated institutional strategy so that the move from cash to code strengthens, rather than destabilizes, the legal order around money [80].

5. CBDC and Its Legal Implications



A CBDC sits at the centre of Pakistan's debate on how to modernize money while protecting monetary stability and legal certainty [81]. A Digital Rupee would not be merely a new payment service; it would be a new form of sovereign money issued under state authority. That makes it legally different from wallets, EMIs, or private tokens, and it means its legitimacy must be anchored in clear law [82]. If designed and governed properly, a Digital Rupee can strengthen inclusion and efficiency. If launched without statutory clarity and safeguards, it can trigger uncertainty, litigation, and loss of public confidence in the rupee itself. The policy case for a Digital Rupee typically rests on five connected objectives: expanding financial inclusion, improving payment efficiency, reducing cash handling costs and informality, strengthening monetary policy transmission, and responding strategically to private digital assets and foreign CBDCs. Pakistan still has a large unbanked and underbanked population, and a retail CBDC could offer a low-cost, risk-free payment option backed directly by the SBP, especially if designed with tiered wallets and simplified onboarding for low-risk users. A Digital Rupee could also support instant settlement at low cost, complementing national infrastructure such as Raast and strengthening e-commerce and government-to-person transfers [83]. Over time, digital money can reduce the fiscal burden of printing, transporting, and securing cash, while also curbing counterfeiting and improving transparency in financial flows, provided privacy safeguards are strong enough to sustain trust. A CBDC may further improve monetary policy monitoring by providing more timely aggregate data and, depending on design, potentially offering new tools for targeted interventions, though interest-bearing or programmable features raise sensitive legal and political questions. Finally, a Digital Rupee can protect monetary sovereignty by offering a regulated alternative if unregulated crypto-assets, stablecoins, or foreign CBDCs begin to substitute for the rupee in domestic transactions [84].

Because a CBDC changes the form of state money, it requires a firm legal foundation for issuance authority, legal tender status, and user rights. In Pakistan, this inevitably engages the SBP Act and the legal meaning of "legal tender." The law would need to expressly define the Digital Rupee as a central bank liability, clarify SBP's exclusive authority to issue and redeem it, and specify its relationship with physical rupees and bank deposits, including convertibility and redemption rights. Without explicit statutory backing, a Digital Rupee could face uncertainty in contractual disputes, insolvency scenarios, and questions about whether public or private actors must accept it as payment [85]. Clear legislation would also protect monetary sovereignty by affirming that rupee-denominated digital legal tender remains a state monopoly even when money becomes code. Legal implications also flow from governance choices. Pakistan would need to adopt a workable operating model: a direct CBDC (SBP provides wallets/accounts), an intermediated model (banks/EMIs distribute wallets under SBP oversight), or a hybrid model (SBP runs the core ledger while intermediaries provide customer-facing services). Intermediated or hybrid models are generally more consistent with maintaining the role of banks and avoiding sudden disintermediation [85]. Whatever model is chosen, the legal framework must allocate responsibilities and liabilities clearly across SBP, intermediaries, and technology providers, covering KYC/AML duties, cybersecurity standards, dispute handling, error correction, and operational resilience [86].

Cross-border functionality introduces further legal risk. If the Digital Rupee can be held by non-residents or used abroad, exchange control, capital flow management, and external stability concerns arise [87]. Pakistan's foreign exchange rules would need modernization to address offshore wallet use, conversion rules, holding limits, and reporting obligations [82]. Without such provisions, digital channels could increase capital flight risks or open enforcement gaps. Finally, CBDC design has constitutional and rights implications. The level of traceability and programmability determines how much the state can observe or influence private transactions. CBDC law must therefore balance legitimate oversight needs with privacy, due process, and property protections, supported by clear limits, oversight mechanisms, and remedies.

International experience reinforces these lessons. China's e-CNY shows the value of explicit statutory backing and centralized governance, while also raising warnings about surveillance if privacy safeguards are weak [88]. The EU's Digital Euro approach highlights the importance of rights-based design, institutional coordination, and legal safeguards to protect stability and avoid crowding out private payments [88]. Nigeria's eNaira demonstrates that even with a legal basis, adoption depends on public trust, clear communication, and smooth user experience especially in developing contexts [89]. Across models, the common thread is clear: CBDC works best when law and design move together, providing legal legitimacy, predictable governance, and enforceable protections.

6. International Regulatory Standards and Compliance

International standards shape Pakistan's choices because digital currencies move quickly across borders and can affect correspondent banking, market access, and reputational standing. Any credible Digital Rupee framework must align with FATF expectations, cross-border payments work led by BIS/CPMI and the IMF, and the emerging global principles on CBDC legal soundness and financial stability [34]. These standards do not remove Pakistan's policy discretion, but they set boundaries for what is internationally acceptable particularly on supervision, transparency, and risk controls.

6.1 FATF, AML/CFT, and data protection

FATF sets the global baseline for AML/CFT, including rules for virtual assets and virtual asset service providers (VASPs). Its guidance expects countries to identify risks, license or register relevant service providers, supervise them, and enforce core duties such as customer due diligence, recordkeeping, and suspicious transaction reporting [34]. FATF also emphasizes the "travel rule," requiring originator and beneficiary information to accompany transfers, and extends attention to stablecoins and peer-to-peer risks. Pakistan's exit from the FATF grey list reflects strengthened AML/CFT systems, but it also means Pakistan must ensure that digital currency design does not reopen risk channels, such as anonymous large-value transfers or weak intermediary controls [90]. Data protection is closely linked to AML/CFT because compliance requires processing sensitive identity and transaction information. International practice is moving toward a balance: enabling necessary monitoring while restricting access, limiting retention, strengthening security, and ensuring proportionality. For Pakistan, this requires clear rules on who can access CBDC transaction data, under what legal authority, and subject to which oversight and remedies, so that AML/CFT objectives are met without creating unchecked surveillance risks [91].

6.2 Cross-border payments, FX control, and CBDC

CBDCs are increasingly discussed in global work on improving cross-border payments, particularly under BIS/CPMI and IMF initiatives. These bodies note that CBDCs can reduce cost and settlement delays, but only if systems are designed for interoperability and backed by strong governance and legal coordination [92]. "Multi-CBDC" models ranging from compatible domestic systems to shared platforms, raise complex legal issues such as settlement finality, applicable law, access criteria, data sharing, and dispute resolution across jurisdictions. For Pakistan, cross-border design matters because remittances and trade flows are central to the economy. A Digital Rupee that can integrate safely into cross-border channels could improve speed and cost, but it would also require exchange-control modernization. Traditional statutes like the Foreign Exchange Regulation Act were not written for foreign CBDCs or offshore digital wallets. International guidance suggests that if non-residents can hold CBDC or cross-border transfers become frictionless, states must reassess capital flow tools, consider holding limits, and ensure consistent treatment of digital and traditional instruments for balance of payments and FX reporting. Without alignment, cross-border digital channels could undermine capital account policies or enable opaque outflows [93].

6.3 Alignment with IMF/BIS policy standards

The IMF and BIS stress that CBDCs must be legally sound, financially stable, and internationally cooperative. A clear legal foundation is treated as non-negotiable: the law must identify CBDC as a

central bank liability, clarify legal tender status where intended, and define the rights and duties of users and intermediaries [94]. These bodies also warn that poorly designed CBDCs can destabilize bank funding, accelerate run[95]s, or weaken monetary policy if users can move at speed from deposits into central bank money without safeguards. In cross-border contexts, IMF/BIS work emphasizes respect for monetary sovereignty and warnings against unintended currency substitution, particularly for smaller or developing economies. Legal frameworks are therefore expected to include tools such as tiered access, holding caps for non-residents, and cooperation agreements that specify applicable law, data sharing, and crisis protocols. For Pakistan, alignment implies designing the Digital Rupee within amended central banking and payments law, embedding stability protections, and handling cross-border use through structured agreements rather than unregulated market expansion [96].

6.4 Overall compliance implications for Pakistan

International standards create both discipline and opportunity [97]. FATF rules constrain anonymity and demand strong intermediary supervision; IMF/BIS principles require legal clarity and stability safeguards; cross-border payment standards push interoperability and governance. Pakistan's strengthened AML/CFT regime provides a strong base, but compliance will require translating standards into enforceable domestic rules. For a Digital Rupee, this means embedding FATF-consistent controls for intermediaries and any licensed VASPs, modernizing foreign exchange and payments legislation to cover digital flows, aligning data governance with privacy safeguards, and ensuring cross-border features comply with settlement finality and cooperation principles [98]. A Digital Rupee built on these standards is more likely to be trusted domestically and accepted internationally [95].

7. Ethical, Socio-Economic, and Inclusion Dimensions

Digital money changes not only how people pay, but also who can participate safely and effectively in the financial system. In Pakistan, where inequalities in income, gender, geography, and literacy already shape access to banking and technology, inclusion is not a side benefit, it is a core test of legitimacy. Digital finance has expanded access through mobile wallets and branchless banking, reducing travel costs and lowering barriers for small transactions [99]. A Digital Rupee could deepen this progress by offering low-cost state-backed value, integrating with social protection payments, and supporting tiered wallets that bring excluded users into formal channels. But without careful design, a “digital by default” approach can widen inequality and expose vulnerable groups to new risks. Gender remains a critical fault line. Women are less likely to own phones, control SIM registration, or hold independent accounts, and social norms can limit their digital autonomy. If digital currency assumes personal device ownership and independent credentials, women may be pushed into dependence on male relatives or informal intermediaries, reducing control over their own funds. Rural communities face similar structural barriers: weaker connectivity, fewer agents, limited merchant acceptance, and lower digital literacy. For these groups, cash may remain more practical unless legal and policy measures actively close access gaps. The risk is that the benefits of digitalization concentrate in cities while rural areas remain excluded or become dependent on informal “helpers” who charge fees and create exploitation risks [100].

Digital literacy is another determinant of fairness [101]. The shift from cash to code creates a divide between users who can navigate apps and protect credentials and those who cannot. Low literacy users, the elderly, people with disabilities, and remote communities face higher exposure to scams, coercion, and social engineering [102]. They also face practical barriers when disputes occur: where to complain, how to prove unauthorized transfers, and how to secure timely reversal or compensation. Economic inequality compounds these issues, as poorer users may share devices, switch off data to save costs, or rely heavily on agents, reducing privacy and increasing vulnerability [103]. These realities mean that digital currency does not automatically empower; empowerment depends on rights-based legal safeguards. Inclusive legal and policy approaches must therefore be built into the framework. Law should preserve meaningful choice, including continued cash use and non-smartphone access channels

during a long transition. Tiered KYC and risk-based onboarding should be legally supported so low-risk wallets can be opened more easily while higher tiers carry stronger AML/CFT controls. Consumer protection rules should be updated for wallet-based environments, requiring clear disclosures in plain language, fee transparency, accessible confirmations (SMS/voice), time-bound complaint handling, and compensation where provider fault exists. Privacy and data minimization principles should limit unnecessary collection and sharing, with special care for shared device contexts. Accessibility requirements should ensure interfaces work for disabilities and low-literacy users. Agent regulation is essential because agents remain the main access point in many areas; conduct rules, fee display obligations, and shared institutional liability are needed so users are not left without recourse. Finally, social protection integration should prioritize beneficiary control, especially for women, so that digital payments strengthen autonomy rather than enable capture by third parties [104]. Participation and oversight matter too: consultation with civil society and consumer groups, and independent ombudsman mechanisms, can improve trust and accountability. In Pakistan's case, inclusion is the bridge between technical feasibility and public legitimacy [105].

8. Policy Recommendations and Legal Reform Agenda

Pakistan requires a coherent reform agenda to move from incremental digitization toward a legally grounded digital currency regime [106]. The objective should be to integrate a future Digital Rupee into the monetary system without undermining stability, rights, or innovation, while closing the gaps that current statutes and regulatory practice leave exposed. Reform should focus on legal clarity, institutional capacity, and coordinated governance so that digital finance evolves within predictable, enforceable rules. A first pillar is targeted amendment of core monetary and payments laws. The State Bank of Pakistan Act should be updated to define the "Digital Rupee" as a central bank liability and, where intended, as legal tender alongside notes and coins [107]. It should clarify issuance and redemption authority, convertibility with physical rupees, and the state monopoly over rupee-denominated digital legal tender. The Payment Systems and Electronic Funds Transfer Act should be modernized to explicitly cover CBDC wallets, tokenized payment instruments, and smart-contract settlement features, while strengthening liability rules for multi-party digital value chains and automated errors. Foreign exchange law should be revised to address cross-border holdings and transfers of Digital Rupee units, foreign CBDCs, and stablecoins, including clear rules for non-resident access, offshore wallets, conversion, reporting, and capital flow limits. These changes would reduce uncertainty for remittances, trade, and cross-border fintech services while protecting external stability [108].

Beyond amendments, Pakistan would benefit from a dedicated Digital Currency and Virtual Assets Act to bring coherence and transparency to the regulation of both sovereign and private digital instruments. Such legislation could define categories (CBDC, stablecoins, other crypto-assets), set licensing and conduct rules for intermediaries and VASPs, establish prudential and governance requirements for digital currency infrastructure, and integrate consumer protection, AML/CFT duties, and cybersecurity obligations into a single statutory scheme rather than scattered circulars. This would move Pakistan from ad hoc restriction toward predictable, enforceable regulation that can deter misuse while enabling lawful innovation [109].

Legal reform must also strengthen institutions and coordination mechanisms [110]. Within the SBP, specialized capacity on digital currency, data governance, and cyber risk should be resourced with clear mandates [111]. Regulatory sandboxes and pilots should be formalized with explicit authority to admit firms, impose conditions, and grant time-bound waivers within defined limits [112]. CBDC pilots should have legally clear status, participant rights, and liability rules so that testing does not create confusion about whether pilot units are "real money." Inter-agency coordination should be institutionalized through a Digital Finance and Currency Coordination Council involving SBP, SECP, FBR, consumer and competition bodies, cybercrime agencies, and data protection authorities. Its role

should include harmonizing overlapping rules, sharing supervisory information, and coordinating systemic incident responses, with regular public reporting to build confidence. Judicial and professional capacity building is also necessary: courts will be asked to interpret new categories of money, resolve disputes involving smart contracts and wallets, and allocate liability after cyber incidents. Training programs, guidance materials, and potentially specialized benches or tribunals can improve consistency and competence in fintech dispute resolution [113].

To guide drafting, Pakistan can adopt clear legislative principles that translate into model clauses [114]. A legal certainty clause should declare the Digital Rupee as a form of currency issued by SBP and, where intended, legal tender equivalent in value to physical rupees. A state monopoly clause should prohibit any private actor from issuing rupee-denominated digital instruments claiming legal tender status, supported by penalties for counterfeit or unauthorized issuance. Intermediated distribution clauses should authorize SBP to designate licensed banks and EMIs as intermediaries and permit tiered wallet categories with proportionate KYC, balance caps, and risk-based functionality [115]. Data governance clauses should restrict CBDC data processing to necessary purposes, impose minimization and retention limits, and require oversight safeguards for access to detailed individual records. Consumer protection clauses should impose duties of fair treatment, transparent fees, accessible disclosures, time-bound complaint resolution, and compensation rules for unauthorized or erroneous transfers caused by provider fault or system failure. Cybersecurity and resilience clauses should mandate minimum standards, independent audits where appropriate, and incident reporting obligations, alongside clear sanctions for non-compliance. Cross-border clauses should empower SBP to permit or restrict non-resident access and cross-border use consistent with FX and capital flow policy. Finally, technology-neutral drafting should ensure the law does not lock Pakistan into a specific platform, while still requiring security, reliability, and verifiability standards. Taken together, these reforms provide a realistic legal pathway for Pakistan's transition from cash to code [116]. By updating foundational statutes, enacting focused digital currency legislation, strengthening institutions, and embedding rights-based safeguards, Pakistan can create a Digital Rupee framework that supports innovation and inclusion while protecting sovereignty and stability [117].

9. Conclusion

Pakistan's transition from cash to code is a defining change in its monetary and legal architecture. While existing laws support the digitization of payments, they do not yet provide a complete framework for CBDCs, digital legal tender, or the governance of virtual assets. Key legal risks, uncertain definitions, cross-border enforcement gaps, privacy and data governance weaknesses, consumer protection limitations, cybersecurity exposure, and incomplete alignment with international standards, must be addressed if Pakistan is to avoid regulatory fragmentation and loss of public trust. Global experience shows that successful digital currency projects are grounded in explicit statutory authority, credible governance, and rights-sensitive safeguards. A Digital Rupee can strengthen inclusion, reduce cash-handling costs, and enhance payment efficiency, but only if the SBP's issuance authority and the currency's legal status are clearly defined, intermediaries are properly regulated, and privacy and consumer rights are protected. With a coherent legislative agenda, structured pilots, and strong institutional coordination, Pakistan can build a hybrid regime where sovereign digital money coexists with regulated private innovation turning "cash to code" into a legally secure path toward inclusive growth and digital sovereignty.

References

1. Rizvi, S.K.A., B. Naqvi, and F. Tanveer, *Is Pakistan ready to embrace Fintech innovation?* 2018.
2. Siddik, M.N.A. and S. Kabiraj, *Digital finance for financial inclusion and inclusive growth*, in *Digital transformation in business and society: Theory and cases*. 2019, Springer. p. 155-168.
3. Javed, M. and W. Zhuquan, *Analysis of accounting reforms in the public sector of Pakistan and adoption of cash basis IPSAS*. Universal Journal of Accounting and Finance, 2018. 6(2): p. 47-53.



4. Garnaut, R., *Macro-economic implications of the turning point*. China Economic Journal, 2010. **3**(2): p. 181-190.
5. Afzal, J., *Exploring the New Horizons of International Law Concerning Globalization of Economy*. Springer Nature.
6. Hanif, M.N., *Restructuring of financial sector in Pakistan*. 2002.
7. Mughal, K.S. and F.G. Schneider, *How informal sector affects the formal economy in Pakistan? A lesson for developing countries*. South Asian Journal of Macroeconomics and Public Finance, 2020. **9**(1): p. 7-21.
8. Adelaja, A.O., et al., *Advancing financial inclusion through fintech: Solutions for unbanked and underbanked populations*. World Journal of Advanced Research and Reviews, 2024. **23**(01): p. 427-438.
9. Bokhari, H. *Digital financial inclusion of the informal sector: the case of Raast Platform in Pakistan*. in *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*. 2022.
10. Nesse, P.J., et al. *Growth of mobile financial services key learnings from literature, industry analysis and cases. in 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. 2017. IEEE.
11. Belke, A. and E. Beretta, *From cash to central bank digital currencies and cryptocurrencies: a balancing act between modernity and monetary stability*. Journal of Economic Studies, 2020. **47**(4): p. 911-938.
12. Dow, S., *Monetary reform, central banks, and digital currencies*. International Journal of Political Economy, 2019. **48**(2): p. 153-173.
13. Afzal, J., *Globalization of Economy and Regulatory Laws of Digital Currency*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 113-124.
14. Meighan, S.J., *The Regulation of Crypto-assets for Anti-Money Laundering*. 2024.
15. Ghauri, B.S.U., G.R. Nafees, and S.A. Anwer, *Navigating Socio Economic and Security Challenges: An exploration of Central Bank Digital Currency (CBDC) Implementation in Pakistan*. Journal of Indian Studies, 2024. **10**(1): p. 49-76.
16. Akhtar, S., *Assessing the Cybercrime Legislation in Pakistan: a Comparative Study of European Union and Pakistani Cybercrime Laws*. Available at SSRN 4555751, 2023.
17. Manzoor, R., et al., *Digital financial services in Pakistan: opportunities, challenges and suggestions*. J Financ Econ, 2021. **6**(2): p. 1-6.
18. Feichtner, I., *Public Law's Rationalization of the Legal Architecture of Money: What Might Legal Analysis of Money Become?* German Law Journal, 2016. **17**(5): p. 875-906.
19. Afzal, J., *Decentralized Currencies and Digital Economy: Stability and Implications of Digital Currency*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 97-112.
20. Ballaji, N., *Consumer Protection in the Era of Digital Payments: Legal Challenges and Solutions*. Beijing L. Rev., 2024. **15**: p. 1268.
21. Afzal, J., *Digital Security Legislation Trends to Facilitate Digital Economy*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 53-64.
22. Bruno, I., et al. *Technology readiness revisited: a proposal for extending the scope of impact assessment of European public services*. in *Proceedings of the 13th international conference on theory and practice of electronic governance*. 2020.
23. Rachmad, Y.E., *Global Regulations for CBDC: Bridging Uniformity in International Policy*. The United Nations and the Nobel Peace Prize Awards, 2025.
24. Afzal, J., *Potential of International Law and Digital Economy*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 147-166.
25. Afzal, J., *International Law and the Globalization of the Economy*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 1-18.
26. Zetsche, D.A., et al., *DLT-based enhancement of cross-border payment efficiency—a legal and regulatory perspective*. Law and Financial Markets Review, 2021. **15**(1-2): p. 70-115.
27. Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024: Springer.
28. Akbar, F., et al., *The Impact of Financial Scams on Consumer Trust in the Banking Sector: A Qualitative Analysis*. International Journal of Discovery in Social Sciences, 2025. **1**(1).
29. Gabor, D. and S. Brooks, *The digital revolution in financial inclusion: international development in the fintech era*, in *Material cultures of financialisation*. 2020, Routledge. p. 69-82.
30. Afzal, J., *International Law and Emerging Economic Issues*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 79-95.
31. Afzal, J., et al., *Review of various Aspects of Digital Violence*. Journal of Engineering, Science and Technological Trends, 2024. **1**(2).

32. Javed, A., M.Z. Ashraf, and S. Shahbaz, *Digital Transformation and Its Influence on Women's Economic Empowerment in Pakistan*. Sustainable Futures, 2025. **10**: p. 101092.
33. Jalil, A. and H. Hina, *Monetary Policy Crafting a Path for Pakistan's Economic Stability*. 2024: Pakistan Institute of Development Economics.
34. Khan, R.U., K. Ullah, and M. Atiq, *Regulatory constraints, responsibilities and consultation (CRC) for legal institutionalization of cryptocurrencies in Pakistan*. Qualitative Research in Financial Markets, 2024. **16**(4): p. 680-708.
35. Arby, M.F., *State Bank of Pakistan: Evolution, functions and organization*. 2004.
36. Huber, J., *Modern Money and Sovereign Currency*. Real-world Economics Review, 2014. **66**: p. 38-57.
37. Javed, S.A., *First Response to the SBP Amendment Act 2021*. 2021.
38. Alexander, K., *The european central bank and banking supervision: The regulatory limits of the single supervisory mechanism*. European Company and Financial Law Review, 2016. **13**(3): p. 467-494.
39. Dordevic, L., et al., *Strengthening bank regulation and supervision: National progress and gaps*. 2021, International Monetary Fund.
40. Chaudhuri, R. and Graber, *Central Bank Independence, Regulations, and Monetary Policy*. 2018: Springer.
41. Shahin, W. and E. El-Achkar, *Banking and monetary policies in a changing financial environment: A regulatory approach*. 2016: Routledge.
42. Hossain, A.A., *Central banking and monetary policy in the Asia-Pacific*, in *Central Banking and Monetary Policy in the Asia-Pacific*. 2009, Edward Elgar Publishing.
43. Ricks, M., *Money as infrastructure*. Colum. Bus. L. Rev., 2018: p. 757.
44. Goldfinger, C., *Intangible economy and electronic money*. The future of money, 2002: p. 87-122.
45. Helleiner, E., *Electronic money: a challenge to the sovereign state?* Journal of international affairs, 1998: p. 387-409.
46. Brunnermeier, M.K., H. James, and J.-P. Landau, *The digitalization of money*. 2019, National Bureau of Economic Research.
47. Caliskan, K., *Data money: The socio-technical infrastructure of cryptocurrency blockchains*. Economy and Society, 2020. **49**(4): p. 540-561.
48. Melecky, M., *Choosing The Currency Structure Of Foreign-Currency Debt: A Review Of Policy Approaches*. Journal of International Development, 2012. **24**(2): p. 133-151.
49. Eichengreen, B. and D.J. Mathieson, *The Currency Composition of Foreign Exchange Reserves Retrospect and Prospect*. 2000.
50. Thimann, C., *Global roles of currencies*. International Finance, 2008. **11**(3): p. 211-245.
51. Ahmad, W., U. Asghar, and M. Afzal, *An analysis of the effectiveness of FIA cyber crime laws in preventing and investigating online fraud in Pakistan: Challenges and recommendations*. Research Consortium Archive, 2025. **3**(2): p. 836-852.
52. Akhlaq, M., *Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan*. PCL Student Journal of Law, 2021. **5**(1): p. 30-66.
53. Arshad Khan, E., *The prevention of electronic crimes act 2016: An analysis*. LUMS LJ, 2018. **5**: p. 117.
54. Haq, I.U. and S.M. Zarkoon, *Cyber Stalking: A Critical Analysis of Prevention of Electronic Crimes Act-2016 and Its Effectiveness in Combating Cyber Crimes, A Perspective from Pakistan*. Pakistan's Multidisciplinary Journal for Arts & Science, 2023: p. 43-62-43-62.
55. Aleem, Y., M. Asif, and M.U. Ashraf, *The Prevention of Electronic Crimes Act 2016 And Shrinking Space for Online Expression in Pakistan*. Ilkogretim Online, 2021. **20**(2).
56. Mehmood, M., *The Role of Cyber Security in Promoting Digital Inclusion: A Case Study of Pakistan*. Annals of Human and Social Sciences, 2025. **6**(1): p. 35-44.
57. Aziz, B. and S.H. Bhatti, *Securing the Cyberspace for E-Commerce Industry of Pakistan: A Consumer Protection Perspective*. Journal of Law & Social Studies (JLSS), 2023. **5**(1): p. 30-41.
58. Fehr, C., C. LiCalzi, and T. Oates, *Computer crimes*. Am. Crim. L. Rev., 2016. **53**: p. 977.
59. CRIME, F.A.C. and C. LAW, *BORBA PROTIV CYBER KRIMINALA: KRIVIČNOPRAVNI I KRIMINALISTIČKI ASPEKT*.
60. Batool, S., et al., *Good governance via E-Governance: moving towards digitalization for a digital economy*. Review of applied management and social sciences, 2021. **4**(4): p. 823-836.
61. Taylor, N., *State surveillance and the right to privacy*. Surveillance & Society, 2002. **1**(1): p. 66-85.
62. Ferreira, A. and P. Sandner, *Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure*. Computer Law & Security Review, 2021. **43**: p. 105632.
63. Jovanić, T. *An overview of regulatory strategies on crypto-asset regulation-challenges for financial regulators in the Western Balkans*, in *Tatjana Jovanić, An Overview of Regulatory Strategies on Crypto-Asset Regulation-Challenges for Financial Regulators in the Western Balkans*, in: *EU Financial*

Regulation and Markets-Beyond Fragmentation and Differentiation (Eds. I. Bajakić, M. Božina Beroš), Conference Proceedings, Zagreb. 2020.

64. Iqbal, F., et al., *The dual impact of digital currencies on economy and environment: Insights into the role of monetary control*. International Journal of Business and Economic Affairs, 2024. **9**(4): p. 22-44.
65. Putrevu, J. and C. Mertzanis, *The adoption of digital payments in emerging economies: challenges and policy responses*. Digital Policy, Regulation and Governance, 2024. **26**(5): p. 476-500.
66. Matsuura, J.H., *Digital Currency: An International Legal and Regulatory Compliance Guide*. 2016: Bentham Science Publishers.
67. Monye, O.F., *Rethinking the legal and institutional framework for digital financial inclusion in Nigeria*. 2021.
68. Stracca, L., *Digitalization Comes to Money*, in *Redefining the Monetary Standard in the Digital Age: Digital Innovations and the Future of Monetary Policy*. 2025, Springer. p. 55-98.
69. Ganne, E., *Can Blockchain revolutionize international trade?* 2018: World Trade Organization Geneva.
70. Hrytsai, S., *The place of virtual assets in the structure of digital financial technology*. International Science Journal of Management, Economics & Finance, 2022. **1**(3): p. 34-48.
71. Wendehorst, C., *Proprietary rights in digital assets and the conflict of laws*, in *Blockchain and Private International Law*. 2023, Brill Nijhoff. p. 101-127.
72. Muradyan, S.V., *Digital assets: Legal regulation and estimation of risks*. Journal of Digital Technologies and Law, 2023. **1**(1).
73. Geva, B. and M. Muraj, *The Digitization of Money: Stablecoins and CBDC*. Banking & Finance Law Review, vol. 40, no. 1, 2024, pp. 115-141., 2023.
74. Zatti, F. and R.G. Barresi, *Digital assets and the law: Fiat money in the era of digital currency*. 2024: Taylor & Francis.
75. Gruschka, N., et al. *Privacy issues and data protection in big data: a case study analysis under GDPR*. in *2018 IEEE international conference on big data (big data)*. 2018. IEEE.
76. Changchit, C., *Data protection and privacy issue*. Journal of Information Privacy and security, 2008. **4**(3): p. 1-2.
77. Bygrave, L.A., *Privacy and data protection in an international perspective*. Scandinavian studies in law, 2010. **56**(8): p. 165-200.
78. Cortés, P., *Online dispute resolution for consumers in the European Union*. 2010: Taylor & Francis.
79. Shad, M.R., *Cyber threat landscape and readiness challenge of Pakistan*. Strategic Studies, 2019. **39**(1): p. 1-19.
80. Saleem, B., et al., *A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap*. International Cybersecurity Law Review, 2024. **5**(4): p. 533-561.
81. Mu, Y. and A. Mu, *CBDC: Concepts, benefits, risks, design, and implications*. Benefits, Risks, Design, and Implications (October 1, 2022), 2022.
82. Hassan, A., S.S. Rao, and B. Amjad, *Risk Factors of Criminal Recidivism into Criminal Activities*. Global Legal Studies Review, 2023. **8**(2): p. 117-123.
83. Handayani, F. and F. Yuliana, *Design and legal aspect of central bank digital currency: a literature review*. Journal of Central Banking Law and Institutions, 2022. **1**(3): p. 509-536.
84. Rachmad, Y.E., *Redefining Money: Implementation and Challenges of CBDC in the Digital Era*. The United Nations and the Nobel Peace Prize Awards, 2025.
85. Infante, S., et al., *The macroeconomic implications of CBDC: A review of the literature*. 2022.
86. Dupuis, D., K. Gleason, and Z. Wang, *Money laundering in a CBDC world: a game of cats and mice*. Journal of Financial Crime, 2022. **29**(1): p. 171-184.
87. Nosheen, M., T. Mumtaz, and B. Amjad, *Gendered Dynamics and Economic Influences in Transboundary Mountain Ecology: A Case Study of the Himalayan Region*. Journal of Asian Development Studies, 2024. **13**(4): p. 349-367.
88. Wang, H., *China meets digital currency: E-CNY and its implications for businesses*. The Law Gazette (November 2021 issue, Forthcoming), UNSW Law Research Paper, 2021(21-77).
89. Oluwaleke, E.A., D. Akhimie, and O. Olonade, *Awareness and Understanding of Enaira in Nigeria*. Acta Universitatis Danubius. Oeconomica, 2023. **19**(5).
90. Nosheen, M., K. Farooq, and B. Amjad, *The role of islamic finance in promoting entrepreneurship and economic growth*. International Journal of Social Sciences Bulletin, 2024. **2**(4): p. 2006-2014.
91. Khan, A., et al., *Regulatory strategies for combatting money laundering in the era of digital trade*. Journal of Money Laundering Control, 2025. **28**(2): p. 408-423.
92. He, D., *Digitalization of cross-border payments*. China Economic Journal, 2021. **14**(1): p. 26-38.
93. Bindseil, U. and G. Pantelopoulos, *Towards the holy grail of cross-border payments*. 2022: ECB Working Paper.

94. Wouters, J. and J. Odermatt, *Comparing the 'four pillars' of global economic governance: A critical analysis of the institutional design of the FSB, IMF, World Bank, and WTO*. Journal of International Economic Law, 2014. **17**(1): p. 49-76.
95. Bennett, D., S.A. Asjad Naqvi, and W.P. Schmidt, *Constraints on compliance and the impact of health information in rural Pakistan*. Health Economics, 2015. **24**(9): p. 1065-1081.
96. Walter, A., *Emerging Countries in Global Financial Regulatory Standard Setting: What Is to Be Done?* 2019.
97. Akhtar, S., H. Hussain, and R.Y. Hussain, *Contributing role of regulatory compliance and Islamic operations in bank risk: Evidence from Pakistan*. Nankai Business Review International, 2021. **12**(4): p. 618-635.
98. Amjad, B., et al., *Towards Automation and Digital Justice: A Review of Digital Twin Technology for Automation in Justice System*. Journal of Asian Development Studies, 2025. **14**(3): p. 49-62.
99. Paccoud, I., et al., *Socio-ethical challenges and opportunities for advancing diversity, equity, and inclusion in digital medicine*. Digital health, 2024. **10**: p. 20552076241277705.
100. Mordini, E., et al., *Ethics, e-inclusion and ageing*. Stud. Ethics L. & Tech., 2009. **3**: p. 1.
101. Celik, I., *Exploring the determinants of artificial intelligence (Ai) literacy: Digital divide, computational thinking, cognitive absorption*. Telematics and Informatics, 2023. **83**: p. 102026.
102. Amjad, B., A. Saeed, and A. Amjad, *Social responsibility of corporate sector: a comparative analysis between Pakistan and United Kingdom (UK)*. Pakistan Social Sciences Review, 2024. **8**(2): p. 01-16.
103. Aydin, M., *Does the digital divide matter? Factors and conditions that promote ICT literacy*. Telematics and Informatics, 2021. **58**: p. 101536.
104. Nasah, A., et al., *The digital literacy debate: An investigation of digital propensity and information and communication technology*. Educational Technology Research and Development, 2010. **58**(5): p. 531-555.
105. Anurogo, D., et al., *Digital Literacy 5.0 to enhance multicultural education*. Multicultural Islamic Education Review, 2023: p. 95-104.
106. Esposito, M., Y. Akbar, and F.X. Campbell, *Digitalization in Emerging Economies*. 2025: Cambridge University Press.
107. Ranjan, A. and I. Talbot, *Challenge, Continuity, and Change in Pakistan*. 2025: Taylor & Francis.
108. Aslam, A. and M.A. Shah, *Tec (h) tonic shifts: taxing the "digital economy"*. 2020: International Monetary Fund.
109. Jaswal, B.A., *Digitization of archival collections by libraries in Pakistan: Issues, strategies, challenges and opportunities*. Pakistan Journal of Information Management and Libraries, 2016. **17**: p. 97-108.
110. Pomaza-Ponomarenko, A., et al., *Legal reform and change: research on legal reform processes and their impact on society. Analysis of factors that facilitate or hinder legal change, including political, social, and economic factors*. Journal of Law and Sustainable Development, 2023. **11**(10): p. e1854-e1854.
111. Pomaza-Ponomarenko, A., et al., *Dynamics of legal transformatins: Assessment of impact on society and analysis of determinations of changes in the legislative sphere*. Multidisciplinary Reviews, 2024. **7**.
112. Richman, D., *Institutional Coordination and Sentencing Reform*. Tex. L. Rev., 2005. **84**: p. 2055.
113. Zainutdinova, E.V., *Models of legal regulation of digital rights and digital currency turnover*. Legal Issues Digit. Age, 2023. **4**: p. 93.
114. Yanto, S.E. and F. Santiago, *The Legal Vacuum in Law Enforcement of Digital Currency Crimes by the Police*. Journal of World Science, 2024. **3**(12): p. 1576-1586.
115. Pranevičienė, K., M. Sadzevičius, and N. Gaubienė, *Recovery of Digital Assets and Cryptocurrencies in Civil Enforcement Proceedings: Key Challenges*. Prawo i Więż, 2025. **55**(2).
116. Etuge, N., *Digital currency and the law: the way forward For a stable regulatory framework in Cameroon's monetary and financial system*. The Law Brigade (Publishing) Group, 2022.
117. Deryugina, T., *Problems of determining the legal nature of digital currency*. Perm U. Herald Jurid. Sci., 2024. **64**: p. 274.

Declaration

Conflict of Study: The author declare that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable



Declaration of AI Use: The author declares that the AI tool "ChatGPT" was used to assist with drafting in the preparation of this manuscript. All content was critically reviewed, verified, and edited by the author, who take full responsibility for the accuracy and integrity of the work.



The Relationship Between Foreign Investment and Subjective Well-Being: The Case of the China-Pakistan Economic Corridor

Maria Qayum ^{1*}, Shanza Qayyum ², Muhammad Noman ², Ismat Ara Jarin ³

¹School of Economics & Management, China Three Gorges University, Yichang City 443002, China

²School of Economics and Management, Zhengzhou University, China

³School of Basic Medical Sciences, China Three Gorges University, Yichang City 443002, China

* Corresponding Email: maria.qayyum1@yahoo.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.08>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

China and Pakistan have maintained significant bilateral commercial and mutually beneficial relationships throughout history. The China-Pakistan Economic Corridor (CPEC) is a multifaceted growth strategy that revolves around several unique initiatives. The Chinese government anticipates investing a significant amount in the CPEC on multiple projects in general. In today's globalized environment, CPEC is a strategy for ensuring economic prosperity for both countries and is seen as an important breakthrough in this area. To examine the CPEC operational scenario, its confines, difficulties, and advantages, the mutually beneficial economic connection between China and Pakistan was extensively studied in this paper. To compare the general public's opinion of it with intended public perceptions, an empirical approach was employed. To examine the general public's opinions of it with a focus on public perceptions of foreign investment, an empirical approach was used. A PLS-SEM analysis aimed at improving the community well-being of Pakistan. The findings of the PLS-SEM direct pathway testing showed that IV and DV have a direct association, supporting the accepted hypotheses H1–H6. We also weigh up the respondents' respective educational attainment together with gender as controlling variables; however, the results for both of these factors revealed no correlation in opposition to CPEC. This proves categorically that there is no relationship between the DV and either gender, education, or both. In this study, H1a, H2a, H4a, H5a, and H6a had significant associations in relation to age in the role of a moderator, although further moderators did not exhibit significant associations to some extent. Age substantially moderates the correlation between CPEC and IV, illustrating the moderating effect of age on the association. All factors in the present investigation are subject to a considerable relationship with one another; furthermore, a number of them have an intermediate to high correlation with one another. The research carried out demonstrated that CPEC has the potential for significant beneficial socioeconomic implications for the two nations, while the Pakistani public believes it will provide them with several opportunities for long-term social sustainability. The results of this research will aid decision-makers in formulating policies that are more efficient and support sustainable development.

Keywords: Foreign Investment; China-Pakistan economic corridor; Community wellbeing; social-wellbeing; public perceptions; PLS-SEM analysis

1. Introduction

Over the Government and administrators need the public's opinion since it serves as the most important factor in policy making, and lawmakers are required to appropriately assess the general public's perception in its entirety [1]. Through this, policymakers can prevent potentially adverse initiatives while rendering decisions that are in the best interests of the general population as a whole. Opinion among the general population has become a powerful tool for changing legislation and influencing the choices of elected representatives as a result of the convenience of having approach to social media platforms like social networking websites and social media channels[2].The fundamental objective of the people's viewpoint analysis is to determine how the general public perceives and makes decisions related to a particular issue, political coalition, rule, or leadership[3].Consequently, a widespread



misconception exists that it is more difficult to accurately forecast the opinions of the general people due to the diversity of viewpoints. Nevertheless, via democratic procedures, elected officials, in specifically, are required to have a full understanding of exactly how the general public perceives about issues with rule of law[4] and public policy. In the context of government officials as well as academic institutions the public's perception of studies indicates that Pakistan is in poor shape. Strong financial relationships, collaboration, and commerce have existed between Pakistan and the People Republic China for several decades. China is becoming one of Pakistan's closest partners in commerce as a supplier of both products and services. Despite the fact that Pakistan and China just agreed to their first bilateral long-term trade agreement in January 1963, there is evidence of bilateral economic and trade relationships throughout both nations (GOP, 2014). These two nations have recently begun a new phase of their economic corridor design as a result of the economic corridor concept's successful mutually beneficial execution[5]. The China-Pakistan Economic Corridor progressive initiative that is in its early stages of emerging for the coming century. It establishes an economic link on either side of the Asian continent and the Indian Ocean through extending the influence it entails to neighbouring East, Western, South, Central, and Asian regions. With the suggestion to construct a strategic industrial transportation system connecting Kashgar in the western Chinese province of Sinkiang alongside Gwadar near Balochistan, plans to strengthen China-Pakistan trade and investment regions underneath the initiative appear to have originally been formed in the middle of the 2000s[6]. \$46 billion has been invested heavily on this project. China-Pakistan economic corridor is a multifaceted strategy for growth that encompasses a number of unique initiatives. These foremost focus on the following initiatives: (a) linkages, which span a 3000 km road and the construction of a deep-sea port and airport together with a train route from Kashghar, Western China, to Gwadar, Pakistan; (b) the organization of an information infrastructure; and (c) an increase in Pakistan's electricity consumption by collaborative work; (d) the manufacturing sector; and (e) advancements in the agricultural sector. Protecting China's interests, such as making investments in Pakistan's power industry, the links in the entirety of these initiatives have lasting significance to China. As a result, both nations are interested in the proposed initiatives. The CPEC project has officially commenced, however it appears that both sides would go through several segments till 2030[7]. The establishing of two main corridors—one at Gwadar port, and the other connecting Gwadar and Kashgar via road transportation—was and continues to be a significant accomplishment. In the following three-year periods, the CPEC will increase the gross domestic product (GDP) level by 1.5%. Additionally, it will result in foreign investment reaching as much as 0.5% of the total GDP of Pakistan, improvements to ecological health and infrastructure, increased revenue potential, a prosperous economy, and the generation of electricity[8]. The total effect of the funding might range from early 2016 to and be greater than 6% annually[9].

Fortunately, the entirety of the venture's expectations is met, China-Pakistan economic corridor is anticipated having a significant positive influence on the financial system of Pakistan, shareholders, countless indigenous people, and the natural surroundings[10]. Pakistan will also greatly take advantage of this. A connection pathway might also grant China prospective route privileges by global regulations. CPEC is schedule to be built at a time of great need at the point where The Maritime Belt and the Road Belt come together. Sustaining a steady supply of electricity from Middle East and the Africa is very essential for China's growth in the upcoming time period, and this undertaking will make it possible to create and strengthen a stability in the Indian Ocean[11]. China sees neighbourhoods' integration during the time that must aimed at having a exert influence on the world. During a speech in 2014 to the Foreign Affairs Committee of the Communist Party, China's President Xi committed towards putting bordering nations' ties first[12]. Establishing connections between growing nations that rich in resources, particularly power, is another pillar of the strategy. It is going to promote Chinese merchandise as a third party. Nevertheless, there are still limitations to CPEC that ought to be considered[13]. The potential value of the property, the expense of relocating people, the geography,

the reality that a part of the corridor has previously existed, ecological difficulties, and safety hazards are a few of them[14]. According to a few academics, Pakistan and China are cooperating well on the CPEC initiatives, but there are additionally a variety of issues that are hazardous to them, including security situation in Pakistan, political instability, interference from outsiders, inequalities in administrative establishment, trade discrepancies between the two nations, environmental conditions associated with the corridors of infrastructure, and Pakistan's poor foreign investment situation[15, 16]. The only thing that the country of Pakistan might be competent to guarantee is that these initiatives are completed is indistinct. The most important factors for the growth of CPEC include Pakistan's resolve, the Chinese leadership's vision for the economic growth of the western area, and agreeable alliance between the two countries[17]. The approach known as empirical research was employed in the present analysis to measure the public's sentiment in Pakistan toward CPEC. Similar investigations have already been carried out in the field, as Huang Delin described in his earlier research, and while both China and Pakistan have encountered obstacles and restrictions to ensuring the effective execution of their respective corridors, public viewpoint remains a key building block for CPEC[18, 19]. Opinion among the general population is perceived differently by different individuals. For others as well, it is the culmination of individuals' diverse or opposing perspectives. The opinions of those who are subject to the influence of governmental entities and to which they must give extensive contemplation are realized to come within this group[20]. American sociologist Charles Horton Cooley asserts that the public's view is "a greater amount than a philosophical word." The community's constituents engage in an ongoing process of contributing to and collaboration. Each of the ideas, sentiments, and viewpoints on that have developed as a result of a team included of individuals working collectively[21]. Any individual is required to make available involvement and express a viewpoint concerning when it pertains to matters that involve public concern. It frequently lacks positivism, impartiality, and knowledge. Nevertheless, the reality that a lot of individuals have the exact same opinion gives it credence[22].

In the present research, the methodology known as PLS-SEM[23] was employed to find out public perceptions on Chinese investment for Pakistan, and the inside CPEC further more projections meant intended for both nations and areas were also desired objectives. Age may be able to decrease the variation impact between DV and IV. Two key socio-economic factors that might act as moderator are gender and educational achievement. In an instance, moderators improve the correlation that exists between the variables that are neither dependent nor independent. The association between SInt (H1a), SAcc (H2a), SCon (H3a), SAct (H4a), SCoh (H5a), and SAff (H6a) is thus thought to be significantly moderated by age. Using the information from our literature analysis, additionally, we formulated the following hypothesis (Fig.1).

- **H1;** Social integration is significantly correlated with China-Pakistan economic corridor (CPEC).
- **H1a;** Age and social integration are moderately correlated with the China-Pakistan Economic Corridor (CPEC).
- **H2;** Social acceptance is significantly correlated with China-Pakistan economic Corridor (CPEC).
- **H2a;** Age and social acceptance are moderately correlated with the China-Pakistan Economic Corridor (CPEC).
- **H3;** Social contribution is significantly correlated with China-Pakistan economic corridor (CPEC).

- **H3a;** Age and social contribution are moderately correlated with the China-Pakistan Economic Corridor (CPEC).
- **H4;** Social actualization is significantly correlated with China-Pakistan economic corridor (CPEC).
- **H4a;** Age and social actualization are moderately correlated with the China-Pakistan Economic Corridor (CPEC).
- **H5;** Social Coherence is significantly correlated with China-Pakistan economic corridor (CPEC).
- **H5a;** Age and social coherence are moderately correlated with the China-Pakistan Economic Corridor (CPEC).
- **H6;** Social Affiliation is significantly correlated with China-Pakistan economic corridor (CPEC).
- **H6a;** Age and social affiliation are moderately correlated with the China-Pakistan economic corridor (CPEC).

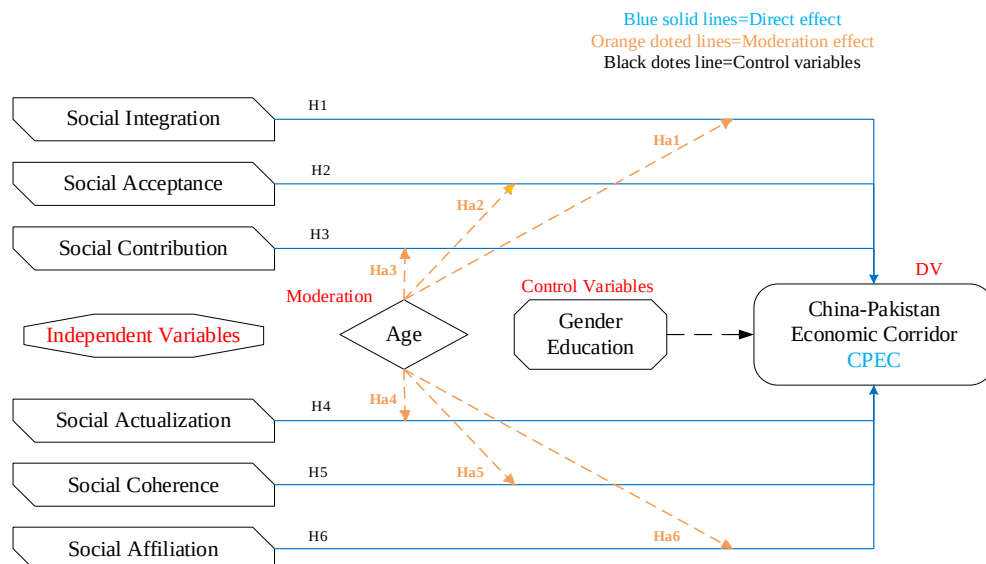


Figure 1: Theoretical framework of study

2. Materials and Methods

The basic statistics that formed the foundation of the present investigation; data was collected and evaluated during the course of the investigation's numerous analysis phases[24]. The proposed investigation focused on an empirical analysis of people perceptions of the China-Pakistan economic corridor. The public's viewpoint is obviously quite significant, particularly within a country with a democratic system, which is why the governing body consistently treats it with respect. It is believed that there are many avenues to convey our emotions and thoughts in the modern world, particularly through social media. Data on public opinion has been acquired for the present investigation using an empirical method and a questionnaire survey. With the assistance of experts in the field and published literature, an instrument was designed. The core data were collected by means of an online survey given to professionals and young people. 650 participants were incorporated into the research project's population. Participants that participated either directly or indirectly throughout this matter, such as faculty members of foreign affairs academics and, to a specific extent, certain pupils who actually did their own studies in this particular field of study, were somewhat the main subjects of the assessments[25]. All procedures performed in this study involving human participants were in accordance with the ethical standards of the institutional review board- China Three Gorges University

(IRB2021SP001). All participants were made aware that their responses would be kept anonymous and confidential and that the data would only be utilized for the purposes of the study. Considering the advantages, it provided and the ease of approaching participants in surveys, a convenience sampling method was employed to determine the investigation's population.

It additionally minimizes costs, time, and diligence. For the six following notions, the research employed a 5-point Likert scale in order to gather opinions from its participants. Social Integration, Social Acceptance, Social Contribution, Social Actualization, Social Coherence, Social Affiliation, and details regarding Pakistan's Economic Corridors made up the bulk of the survey questionnaire.

The design required us to translate the survey instrument into Urdu (the local language), check its validity, and mail it to the participants since that we employed an assortment of parameters that had been earlier designed by numerous investigators in the English language. In order to assess the instrument's effectiveness, its contents were originally distributed to 25 individuals. Smart PLS-4 and SPSS Version 25 were both utilized for analysing information obtained via the use of questionnaires and interviews. The descriptive statistics and probabilities were implemented to investigate the features that defined the participants and dataset. The School of Economics and Management Science at China Three Gorges University in China conducted the study. Every person who participated gave their free, informed permission. The School of Economics and Management Science's Academic Committee on Ethics approved the research being conducted-SEM is frequently employed to acquire research purposes to examine the correlations that exists between factors because this considered to be among the most effective methods to accurately forecast results[26]. This represents due to the fact that PLS-SEM is the technique that is often suggested for estimating and assessing explanatory variables for taking into account all conceivable variations.

Compared to other techniques, PLS-SEM facilitates a lower sample size despite nevertheless providing accurate findings. It additionally has the ability evaluate numerous frameworks simultaneously, both inside and outside[27]. Complicated pathway models may be examined by employing this kind of information collection. The growing acceptance of the PLS-SEM technique in the field of management sciences is possibly due to the benefits it provides, according to contemporary investigations in academia[28]. This implies the fact that the PLS-SEM method would be seen to represent the most suitable for the purposes of this study. The handling of non-linear relationships between accounts in the model makes the two-stage evaluation more productive. A PLS-based method of route modelling is put to the analyse twice to ensure accuracy as well as consistency of the build measurements. The validity and reliability of an outer model of structure are examined just before the construction of an inner model or interaction involving the latent variables[29].

3. Data Analysis

3.1. Measurement Model Assessment

The opinion and anticipation of the general population in the China-Pakistan Economic Corridor (CPEC) provided the attainable basis for the team to conduct the current investigation, during which we incorporated the factors that followed to determine exactly how individuals thought with respect to CPEC's social integration, social acceptance, social contribution, social actualization, social coherence, and social affiliation. To analyse the relationship that exists between DV, IV, and Moderation in future studies, 650 responses to questionnaires altogether have been collected. The procedure of forming public perceptions is challenging and tedious

as well. Instead of just a few months or a few weeks, perspective formation is an exhaustive procedure the following: generally, requires many ages. Consensus-based representation of existing problems or critically important legislative changes; public thinking, however, is at best sporadic.

Table 1: *Reliability and Validity Analysis*

Variables	Items	VIF	Loadings	T-Value	α	CR	AVE
Social Acceptance	SAcc1	1.327	0.599	7.682	0.703	0.777	0.501
	SAcc2	1.534	0.643	7.175			
	SAcc3	1.123	0.847	36.588			
	SAcc4	1.476	0.629	6.405			
Social Actualization	SAct1	1.327	0.599	19.129	0.787	0.841	0.571
	SAct2	1.534	0.643	18.678			
	SAct3	1.123	0.847	16.020			
	SAct4	1.476	0.629	79.248			
Social Affiliation	SAff1	1.913	0.825	34.138	0.783	0.919	0.741
	SAff2	2.653	0.875	46.737			
	SAff3	2.314	0.869	50.163			
	SAff4	2.418	0.871	60.491			
Social Coherence	SCoh1	2.186	0.846	52.427	0.882	0.919	0.738
	SCoh2	2.444	0.882	82.774			
	SCoh3	2.201	0.846	51.576			
	SCoh4	2.315	0.863	56.466			
Social Contribution	SCon1	1.916	0.741	32.713	0.827	0.884	0.659
	SCon2	2.026	0.745	16.893			
	SCon3	1.203	0.832	67.234			
	SCon4	1.763	0.701	41.489			
Social Integration	SInt1	1.509	0.707	18.812	0.731	0.827	0.544
	SInt2	1.527	0.707	19.115			
	SInt3	1.487	0.769	28.770			
	SInt4	1.249	0.767	30.469			
China Pakistan Economic Corridors	CPEC1	2.861	0.862	46.272	0.913	0.939	0.793
	CPEC2	3.519	0.903	91.381			
	CPEC3	2.943	0.868	76.728			
	CPEC4	4.142	0.928	135.962			

As consequently, social integration = 0.731; social acceptance = 0.703; social contribution = 0.827; social actualization = 0.787; social coherence = 0.882; social affiliation = 0.783; and China Pakistan economic corridors = 0.913 were found to be reliable and widely recognized examines for the accuracy of the data (Table 1, Fig 2). Furthermore, the average variance extracted (AVE), which is used to demonstrate the extent to which variance in variables is explained by the construct of latent variability, specifically, the composite reliability (often referred to as CR) and have been employed. The correct abbreviations, AVE and CR, were subsequently used to indicate these parameters. Overall latent factors with loading values that are resulting in are required to be considerably higher to be significant, consisted incorporated. The above findings imply that there is enough information in the obtained information to support further research. The PLS-SEM assessment comprehend is split down into numerous steps, with the structural model analysis making up the next stage. It is essential to consider a variety of factors while analysing the structural path model, For instance, multicollinearity, the empirical significance of the path coefficients, as well as the degree of confidence. The reliability of the structural path model also needs to be evaluated.

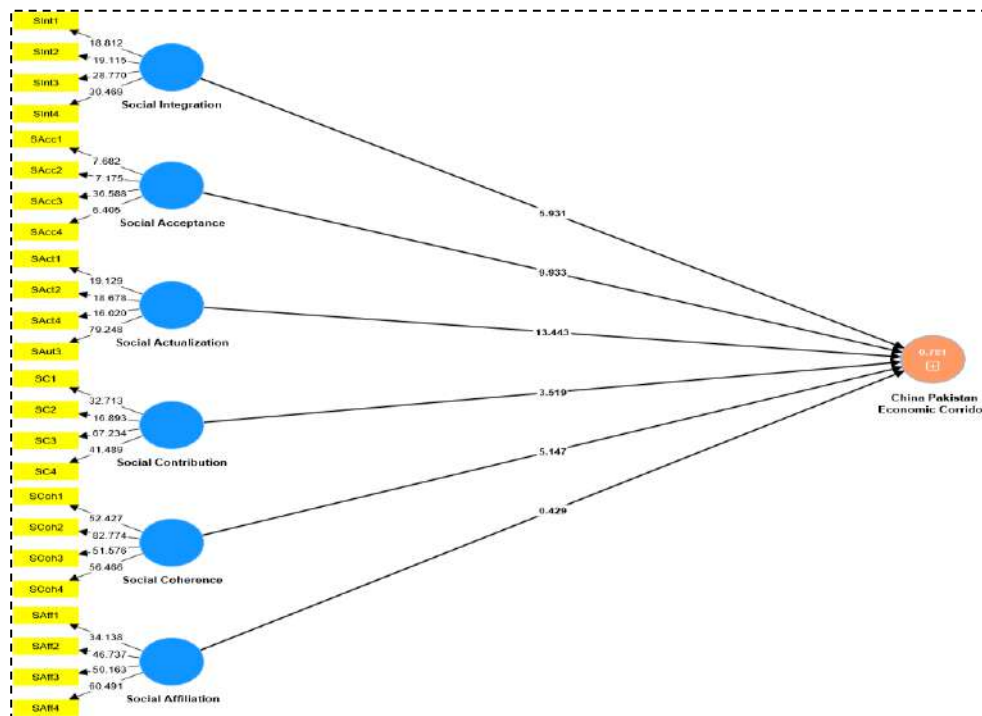


Figure 2: Measurement model, orange colour latent = DV, blue colour latent = IV

The current study, which used the guidelines given by Hair Jr. et al to analyze the structural model, evaluated a model to ascertain the precise impacts that various factors affect on CPEC in order to completely comprehend the results. A PLS-SEM path analysis's findings (Fig. 3) showed an R2 coefficient value of 0.781 and Q2 value of 0.620, demonstrating that the suggested model matched the data well (Table 4).

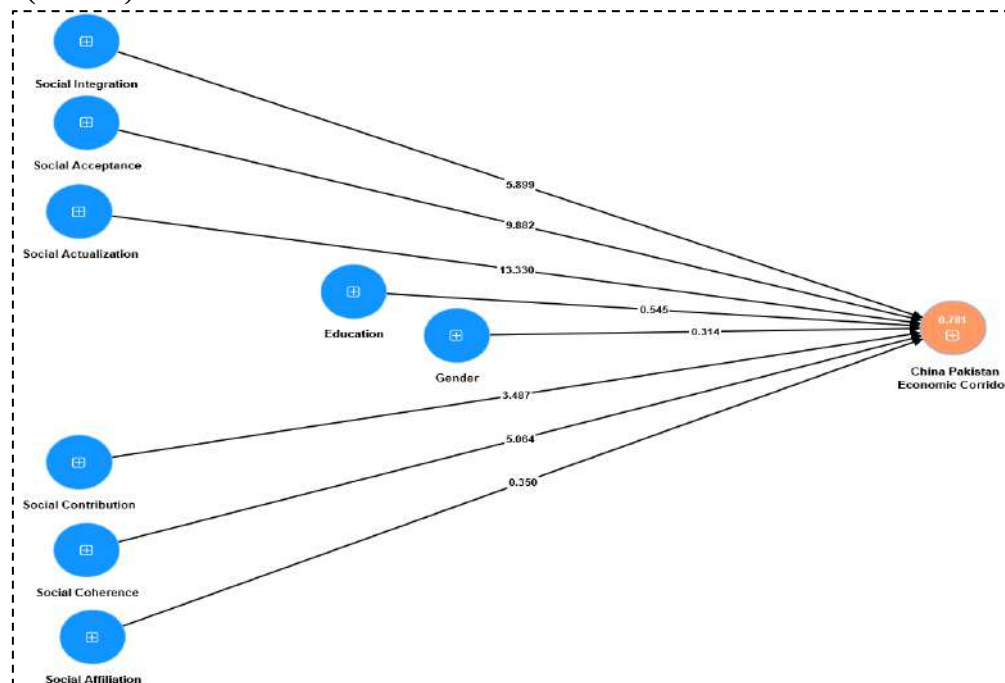


Figure 3: PLS-SEM Path Model, orange color latent = DV, blue color latent = IV

The suggested model's discriminant validity is examined using the Fornell-Larcker and HTMT ratios. As evidenced by the maximum significant correlation between the variables in each of the columns of Table 2, Fornell and Larcker criteria have been applied to validate discriminant validity. One alternate method for proving discriminant validity consisted of the HTMT ratio method. They asserted that each of the Fornell-Larcker criteria lacked the ability to distinguish between the existence and absence of

discriminant validity, although they were helpful in assessing discriminant validity. The HTMT is currently often employed to assess discriminant validity as a result of the method. Table 3 includes the HTMT values for each of the factors that were examined. PLS-SEM is frequently utilized for analysing data to examine the association that exists between indicators for the reason that it provides one of the best methods for result prediction. This may be determined by the simple fact that the recommended method for determining and evaluating an explicating variable in accordance to reason for the significant amount of change is PLS-SEM. In comparison to other techniques, PLS-SEM enables the use of a lower population size despite nevertheless providing good-quality findings. Additionally, it facilitates cross-model simultaneously internal as well as external computation. Investigating intricate pathway models is additionally doable employing this kind of data collecting. According to modern empirical findings, the PLS-SEM methodology's appeal in the field of management science is probably to some extent mainly due to its prospective benefits. So, it could be expected that the methodology known as the most appropriate solution for such an investigation may be PLS-SEM. Considering the approach takes non-linear relationships into account, a two-phase evaluation is preferable. To ensure the precision and homogeneity of the examined designs, two independent assessments using a PLS-based route modelling technique are carried out. To develop a proposed internal model or association that involves the latent factors, a operational model is examined after convergent validity has been established.

Table 2: Fornell-Larcker Criterion

Variables	S. D	Mean	CPEC	Social Acceptance	Social Actualization	Social Affiliation	Social Coherence	Social Contribution	Social Integration
CPEC	0.014	0.796	0.889						
Social Acceptance	0.036	0.159	0.551	0.858					
Social Actualization	0.026	0.126	0.549	0.365	0.739				
Social Affiliation	0.031	-0.107	0.331	0.636	0.276	0.812			
Social Coherence	0.039	0.485	0.845	0.546	0.517	0.409	0.685		
Social Contribution	0.024	-0.054	0.377	0.363	0.329	0.516	0.455	0.861	
Social Integration	0.031	0.342	0.806	0.496	0.479	0.393	0.816	0.498	0.757

Table 3: HTMT Ratio

Variables	CPEC	Education	Gender	Social Acceptance	Social Actualization	Social Affiliation	Social Coherence	Social Contribution	Social Integration
CPEC									
Education	0.061								
Gender	0.014	0.218							
Social Acceptance	0.837	0.075	0.037						
Social Actualization	0.777	0.098	0.081	0.863					
Social Affiliation	0.419	0.054	0.079	0.585	0.618				
Social Coherence	0.614	0.124	0.071	0.666	0.552	0.409			
Social Contribution	0.365	0.121	0.094	0.558	0.478	0.584	0.753		
Social Integration	0.639	0.029	0.067	0.622	0.528	0.393	0.436	0.329	

3.2. Structural Model Assessment

PLS-SEM was employed to examine the association between variables such as China-Pakistan economic corridor (CPEC) and social integration (SInt), social acceptance (SAcc), social contribution (SCon), social actualization (SAct), social coherence (SCoh), and social affiliation (SAff). By first looking at the documented links that exist between the various elements, we validate the proposed hypotheses. Then we further executed a bootstrapping analysis with 5,000 iterations to determine

whether the findings corroborated our predictions. Direct path analysis using PLS- SEM demonstrated; Sint-> CPEC ($\beta = 0.126$; $p < 0.000$), SAcc-> CPEC ($\beta = 0.486$; $p < 0.000$), SAct-> CPEC ($\beta = 0.346$; $p < 0.000$), SCon-> CPEC ($\beta = -0.112$ $p < 0.002$), SCoh-> CPEC ($\beta = 0.157$; $p < 0.000$), SAff -> CPEC ($\beta = -0.054$; $p < 0.029$) are significant. The foregoing findings support the previously established hypothesis H1–H6. We also looked at each participant's educational attainment and gender as potential additionally factors that might cause confusion. Gender ($\beta = 0.003$; $p < 0.932$) and Education level ($\beta = -0.008$; $p < 0.699$) indicated an insignificant association to the China-Pakistan Economic Corridor (CPEC). This suggests that neither educational attainment nor gender are predictors of dependent variable (Table 4 and Fig 3).

Table 4: Path Analysis (PLS-SEM)

Hypothesis	Statistical Paths	Beta (β)	Std. Dev	T-Value	P-Value	Decision
H1	Social Acceptance -> CPEC	0.486	0.037	9.882	0.000	Accepted
H2	Social Actualization -> CPEC	0.346	0.032	13.330	0.000	Accepted
H3	Social Affiliation -> CPEC	-0.054	0.024	2.203	0.029	Accepted
H4	Social Coherence -> CPEC	0.157	0.038	5.064	0.000	Accepted
H5	Social Contribution ->CPEC	-0.112	0.033	3.487	0.002	Accepted
H6	Social Integration ->CPES	0.126	0.027	0.350	0.000	Accepted
Control Variables						
	Gender -> CPEC	0.003	0.019	0.545	0.932	Insignificant
	Education ->CPEC	0.008	0.019	0.314	0.699	Insignificant
	R2			0.781		
	Adjusted R2			0.787		
	Q2			0.620		

The general public's viewpoint is commonly acknowledged to be essential to decision-making processes, particularly in governments[30]. Administrations, nevertheless take decisions first before informing the general public in countries like Pakistan during which public engagement is minimal and the majority of decisions are taken at the highest levels of government. Even on issues that are of public importance, the public's viewpoint has never been taken into consideration throughout the procedure for making decisions[31]. As a consequence, we only emphasize the factors that we think will have the most impact on the federal government's performance and overall well-being. As a consequence, the facts can be biased by either overplaying the benefits or underplaying the potential hazards and challenges; therefore, those who are against needs to bring attention to the shortcomings of the decision.

Table 5: Moderation Effect (Age)

Hypothesis	Statistical Paths	Beta (β)	Std. Dev	T-Value	P-Value	Decision
H1a	Age x Social Integration -> CPEC	0.025	0.028	0.905	0.365	Rejected
H2a	Age x Social Acceptance-> CPEC	-0.099	0.030	3.290	0.001	Accepted
H3a	Age x Social Contribution -> CPEC	0.029	0.030	0.981	0.327	Rejected
H4a	Age x Social Actualization -> CPEC	0.143	0.039	3.658	0.000	Accepted
H5a	Age x Social Coherence -> CPEC	-0.006	0.030	0.208	0.835	Rejected
H6a	Age x Social Affiliation-> CPEC	0.024	0.030	0.790	0.429	Rejected

In table Table.5 shown the PLS-SEM investigation's final phase involved assessing the degree of moderation between DV and IV. In PLS-SEM, categorically classified moderation is evaluated to ensure that we may look at hypotheses from H1a through H6a. Findings of the investigation showed a little moderating influence on the associations between both the independent and dependent variables of the subject under study. A brief description of the moderation analysis is exhibited in (Table.5; Figure.4)

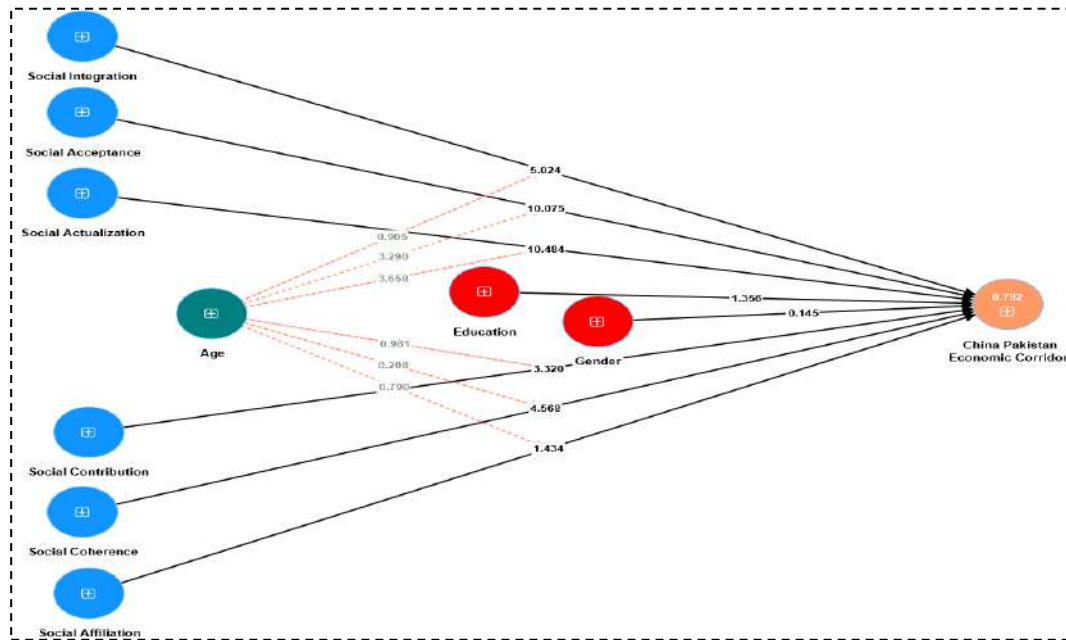


Figure 4: Moderator (Age); latent variables in red are controls; latent variables in green are moderators; latent variables in orange are significant moderators.

3.3. Moderation Effect of Variables (Slope for Slope Analysis)

Moderation effect is always tested on +1 sigma and -1 sigma to see its effect on the relationship between IDV and DV.

H1a; Age and social integration are moderately correlated with the China-Pakistan Economic Corridor (CPEC).

Here, moderation effect is insignificant, in case if it was insignificant, 1 standard deviation increase in age would cause $0.150 + (0.025)$ change in relationship between social integration to China Pakistan economic corridor. (Green colour line). Here moderation effect is significant. In case if it was insignificant, 1 standard deviation decreases in age would cause $0.150 - (0.025)$ change in relationship between social integration to China Pakistan economic corridor. (Red colour line). As P-Value (0.365) is insignificant we can say that Age not positively moderates the relationship between social integration and public perception about China Pakistan economic corridor (Fig 5).

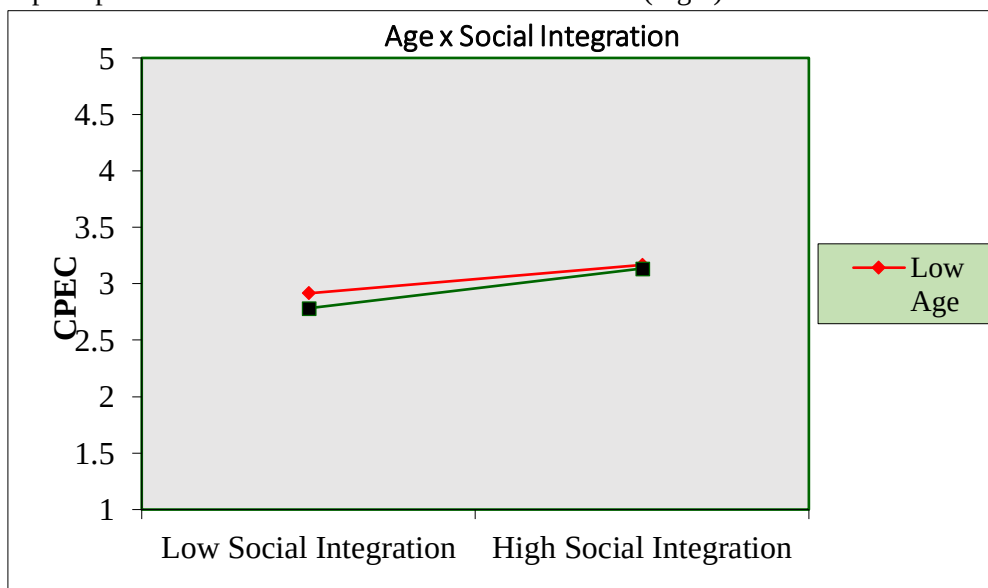


Figure 5: Age x Social Integration

H2a; Age and social acceptance are moderately correlated with the China-Pakistan Economic Corridor (CPEC).

Here, moderation effect is significant, in case if it was significant, 1 standard deviation increase in age would cause $0.404 + (-0.099)$ change in relationship between social acceptance to China Pakistan economic corridor. (Green colour line). Here moderation effect is significant. In case if it was significant, 1 standard deviation decreases in age would cause $0.404 - (-0.099)$ change in relationship between social acceptance to China Pakistan economic corridor. (Red colour line). As P-Value (0.001) is significant we can say that Age positively moderates the relationship between social acceptance and public perception about China Pakistan economic corridor (Fig 6).

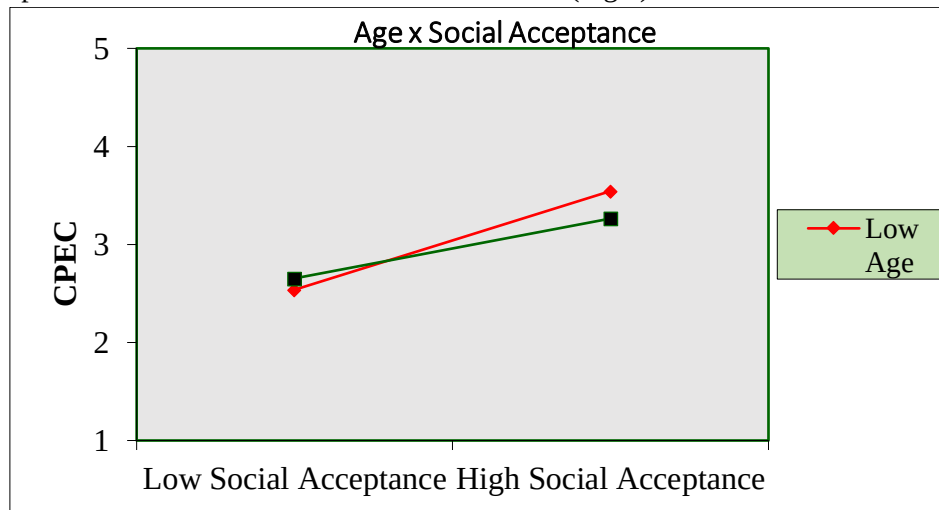


Figure 6: Age x Social Acceptance

H3a; Age and social contribution are moderately correlated with the China-Pakistan Economic Corridor (CPEC).

Here, moderation effect is insignificant, in case if it was insignificant, 1 standard deviation increase in age would cause $-0.110 + (0.029)$ change in relationship between social contribution to China Pakistan economic corridor. (Green colour line). Here moderation effect is insignificant. In case if it was insignificant, 1 standard deviation decreases in age would cause $-0.110 - (0.029)$ change in relationship between social contributions to China Pakistan economic corridor. (Red colour line). As P-Value (0.327) is insignificant we can say that Age not positively moderates the relationship between social contribution and public perception about China Pakistan economic corridor (Fig 7).



Figure 7: Age x Social Contribution

H4a; Age and social actualization are moderately correlated with the China-Pakistan Economic Corridor (CPEC).

Here, moderation effect is significant, in case if it was significant, 1 standard deviation increase in age would cause $0.384 + (0.143)$ change in relationship between social actualization to China Pakistan economic corridor. (Green colour line). Here moderation effect is significant. In case if it was significant, 1 standard deviation decreases in age would cause $0.384 - (0.143)$ change in relationship between social actualization to China Pakistan economic corridor. (Red colour line). As P-Value (0.000) is significant we can say that Age positively moderates the relationship between social actualization and public perception about China Pakistan economic corridor (Fig 8).

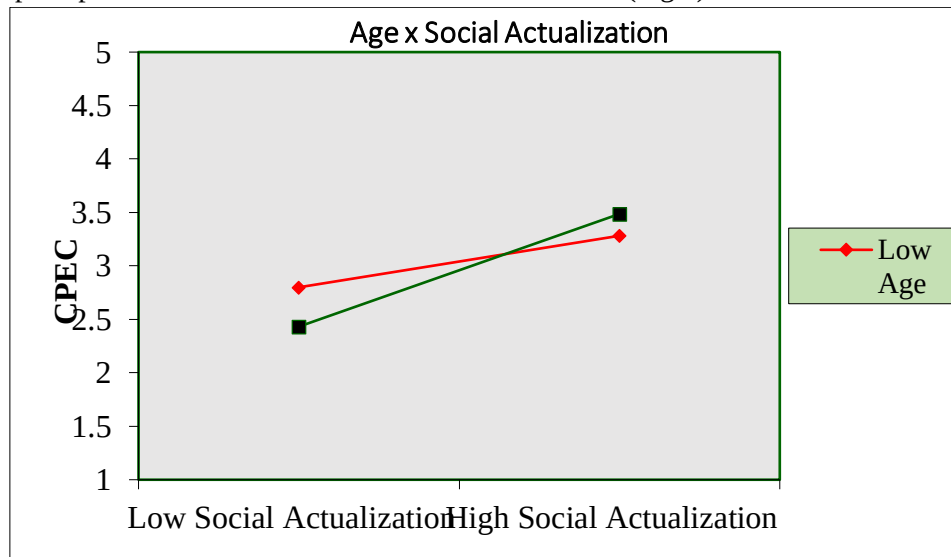


Figure 8: Age x Social Actualization

H5a; Age and social coherence are moderately correlated with the China-Pakistan Economic Corridor (CPEC).

Here, moderation effect is insignificant, in case if it was insignificant, 1 standard deviation increase in age would cause $0.181 + (-0.006)$ change in relationship between social coherence to China Pakistan economic corridor. (Green colour line). Here moderation effect is insignificant. In case if it was insignificant, 1 standard deviation decreases in age would cause $0.181 - (-0.006)$ change in relationship between social coherence to China Pakistan economic corridor. (Red colour line). As P-Value (0.835) is insignificant we can say that Age not positively moderates the relationship between social coherence and public perception about China Pakistan economic corridor (Fig 9).

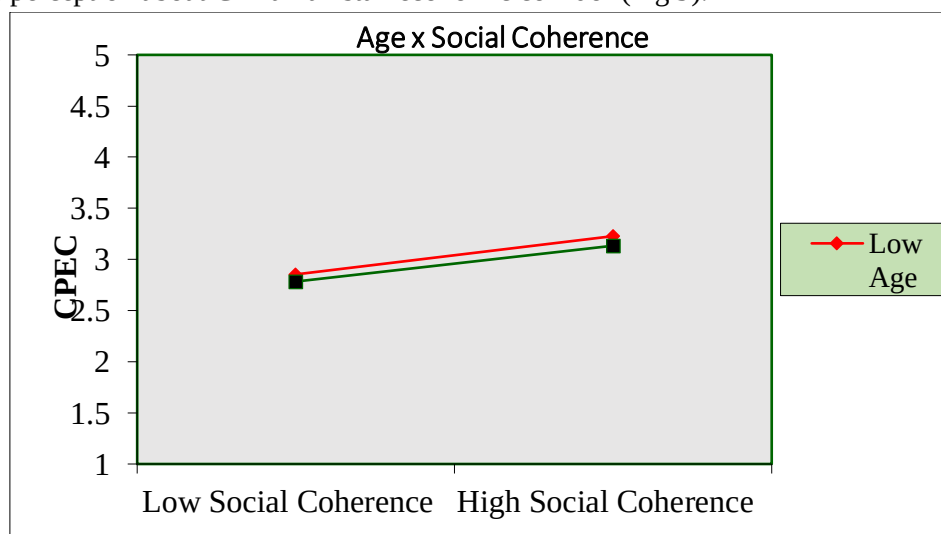


Figure 9: Age x Social Coherence

H6a; Age and social affiliation are moderately correlated with the China-Pakistan Economic Corridor (CPEC).

Here, moderation effect is insignificant, in case if it was insignificant, 1 standard deviation increase in age would cause $-0.036 + (0.024)$ change in relationship between social affiliations to China Pakistan economic corridor. (Green colour line). Here moderation effect is insignificant. In case if it was insignificant, 1 standard deviation decreases in age would cause $-0.036 - (0.024)$ change in relationship between social affiliations to China Pakistan economic corridor. (Red colour line). As P-Value (0.429) is insignificant we can say that Age not positively moderates the relationship between social affiliation and public perception about China Pakistan economic corridor (Fig 10).

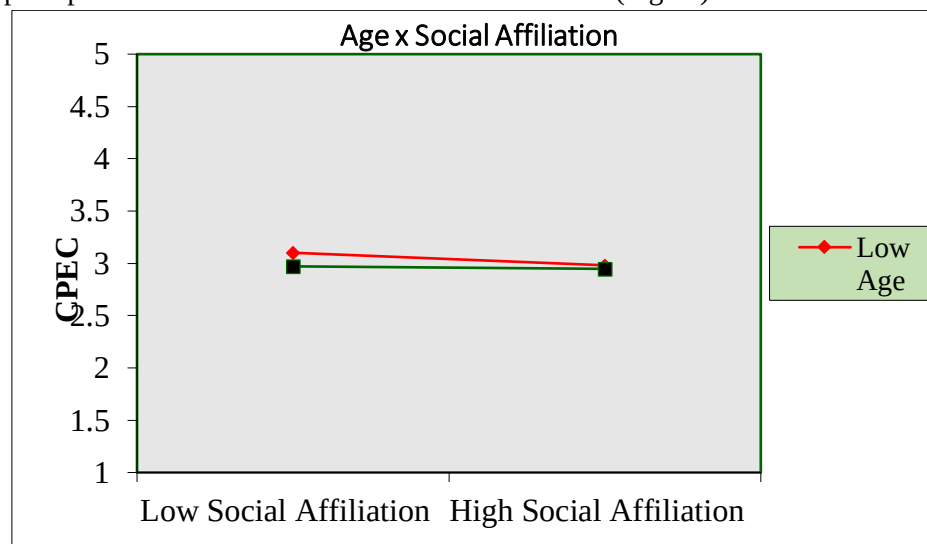


Figure 10: Age x Social Affiliation

Table 6. Correlation among Variables

Variables	Age	CPEC	Social Coherence	Education	Social Integration	Social Acceptance	Gender	Social Contribution	Social Actualization	Social Affiliation
Age	1.000									
CPEC	-0.16	1.000								
Social Coherence	-0.053	0.554	1.000							
Education	0.196	-0.061	0.120	1.000						
Social Integration	-0.005	0.552	0.368	0.01	1.000					
Social Acceptance	-0.050	0.332	0.639	0.114	0.275	1.000				
Gender	-0.208	0.016	-0.069	-0.22	-0.034	-0.089	1.000			
Social Contribution	-0.192	0.848	0.549	-0.09	0.516	0.409	0.015	1.000		
Social Actualization	0.087	0.38	0.366	-0.05	0.331	0.516	0.077	0.455	1.000	
Social Affiliation	-0.156	0.809	0.499	-0.101	0.479	0.393	0.049	0.819	0.498	1.000

For quantitative representations to depict an appropriate relationship between variables, correlations were utilized. In addition to providing an approach for understanding the nature of association among every single one of the distinct attributes, this investigation also offers an estimating technique. The highlighted numbers display the findings of a Pearson's correlation analysis on multivariate parameters. It is clear that there is a considerable to somewhat positive connection between all of the traits. Table 4 shows the statistical characteristics and correlation coefficient values based on gender, education level, and age as well as the China-Pakistan Economic Corridors (CPEC), social integration (SInt), social acceptance (SAcc), social contribution (SCon), social actualization (SAct), social coherence (SCoh), and social affiliation (SAff). A technique for determining the link between any numbers of variables is correlated. The Pearson correlation coefficients should fall between +1.0 and -1.00. The strength of the connection depends on the size of the number, where 1 is the largest. In that particular investigation,

there is a strong association between every single factor with one another, and several of them have a good to excellent relationship. All of the factors studied showed relevance for each other by having an insignificant moderately significant connection (Table 6).

4. Discussion of Results

All nations must make difficult decisions; thus, it shouldn't be left to the abilities of just one institution. The use of social networking sites has made it easier and quicker to share information dissemination. By spreading the word, every individual is going to become aware of your incredible journey[32]. In order to regulate and counter-manage the perceptions of the general public, members of society as a whole, the military forces that are and other civilian organizations must collaborate[33]. At each stage of the development and execution of the numerous CPEC-related undertakings, the public must be constantly informed. The projected economic corridor will be very helpful to China's objective of expanding up and strengthening its western provinces because of its close connection to these regions. As the economic integration between regions keeps growing, the CPEC could assist. China forges closer connections with the countries of southern, central, and western Asia and collaborates for breakthroughs. The transport of Middle Eastern oil to China's western and central regions is going to be replaced by a natural gas pipeline which runs across the Karakoram Mountain range connecting Gwadar to China. Currently, nearly all of China's petroleum imports pass through the Strait of Malacca, an international route which is susceptible to obstruction and uncertain geographical conditions.

The planned Economic Corridor may be advantageous for Pakistan's economy; hence it has to be carefully considered. Pakistan has experienced a steep fall in recent foreign direct investment (FDI) as a result of the nation's severe energy difficulties, and the manufacturing industry is currently operating considerably below its capacity. The country's energy shortages are expected to be alleviated by the proposed natural gas and petroleum pipelines connecting Iran through Gwadar to Kashgar via Pakistan. Pakistan's unique excellent placement at the centre of the Middle East's intersections, Central Asia, and China's large consuming and supplying markets makes the planned corridor potentially extremely profitable from a transit perspective, potentially reinventing Pakistani society, economic trajectory. Pakistan may become an international commercial operations hub and electricity transit corridor with China's financial support for the infrastructure development. Each of these factors is expected to have a significant effect on Pakistan's business establishments, agricultural, and industrial expansion. Being the world's biggest exporting nation and the second-biggest importer in the global economy, China's status is only increasing. Across Africa, the region known as the Middle East, and the remaining regions of Asia, and America are among its many trading partners.

The two neighbouring countries, China and Pakistan, are close friends and work together in a variety of areas. China is capitalising and as a result of the establishment of the China-Pakistan Economic Corridor (CPEC), Pakistan has received an immense amount of revenue. to construct new roads, power plants, railways, hospitals, airports, educational facilities, and other facilities that will either directly or indirectly enhance both urban and rural life in Pakistan. China may contribute a whole lot more for Pakistan's progress for the reason it is an emerging economy with a lower GDP rate than China. At the moment, Pakistan is likewise dealing with a population that is growing rapidly rate of growth, but also with many challenges associated with growing urbanization, including traffic congestion, a lack for healthcare facilities, unemployment rates[34], and shortcomings with water and land.

In this study, we sought to learn the general public's opinions about CPEC and what they thought of it[35]. Every single one of our hypotheses is supported by the research's findings. It is crucial to understand how the general people feel about how the CPEC will affect their access to education and employment prospects. The country's tourist business is of the utmost importance and has a significant beneficial influence on its GDP. Pakistanis believe that these developments will increase the number of possibilities for both countries to go to one another. From the perspective of the people, certain additional metrics also demonstrated substantial connections with CPEC[36]. As previously stated, the

Gwadar complex is a significant initiative for the China-Pakistan economic corridor (CPEC), a worldwide effort that benefits both China and Pakistan[37]. According to professionals' predictions, Pakistan's financial system and yearly gross domestic product (GDP) will reap the rewards from this special economic zone. Economic conditions in the Gwadar region are expected to shift and it is certain that both the economic situation and the community's standard of life will significantly improve. More and more individuals will find employment in both nations thanks to these developments, which will create jobs. It will also provide a large number of job possibilities for high-tech technicians and talented people across China's 10 provinces. Additionally, it will enhance China's transportation sector.

5. Policy Implication & Suggestions

A few of the few studies that look into the link between six factors and the idea of facts and the public attitude of CPEC Statistics on social integration, acceptance, contribution, actualization, coherence, and affiliation in society[38]. In addition to being Pakistan's next-door neighbour, China has been a close ally all across their respective histories. China has recently made significant financial investments in Pakistan for the CPEC, which will undoubtedly transform the landscape for both nations. Asia's Southern, central region and Western economies alongside China will collaborate more closely as a result of the CPEC, which would additionally improve the integration of their respective economic systems. This research evaluated a few projects associated with CPEC and their effects on the growth of social wellbeing of Pakistan[38]. Here are a few possibilities for policymakers on the need to maintain openness and responsibility in each project. All of these business operations' earnings need to be distributed wisely across all industries and geographical areas.

The implementation of such strategies and programs that are needed for betterment might be ensured through surveillance structures for urban development. Pakistan has to maintain stability in politics in the area to the best of its abilities and overcome threats to security if it wants to draw in additional foreign capital to the Pak-China corridor. In accordance with the Pak-China cooperation, the CPEC must provide significant possibilities to native investors, and all urban revitalization efforts in other cities, including those involving infrastructure, well-being, and educational opportunities, should be equally beneficial to Pakistan and China. The predicted surge of inexpensive items might have an impact on our sector. The destiny of numerous communities and Pakistan as a whole would be determined by the strategies that the industrialized administration is going to put into place. Pakistan might additionally be open to Chinese companies operating in the fields of management of water resources, the filtration of drinking water, the solid waste management, surveillance of the quality of water, and development of land. They could invest funding in such regions, which would benefit Chinese enterprises by showing their ability to can generate money and would also help Pakistan rehabilitate these parts of the country[39-41].

Pakistan is a growing nation that strives for growth in all spheres of life. Being in a prosperous and welcoming nation is a gift[42]. Both nations stand to gain from the economic corridors between China and Pakistan and can forge close connections. China has a sizable economy, and numerous countries depend on it for a variety of factors. An extensive network of transit and roadways will be built as part of these initiatives, which would enable Pakistan's local economy to have strong ties with China. A lot of students may travel under these schemes to China for further education, and vice versa, so it's not just concerning commercial connections. Development advantages have resulted from China and Pakistan's cooperation on a variety of projects, including roads, trains, energy initiatives, and the opening of the Gwadar port, airport, and medical facilities. This particular fruit will benefit both nations and assist in resolving the energy situation, raising the GDP of both nations, and improving infrastructure. These corridors will allow China to shorten its path to the Persian Gulf and save time and energy.

China can now travel the 45-day trek from Kashgar to Gwadar in only ten days. The geostrategic situation of the two nations will significantly improve in terms of local connection and condensed trade

channels[43]. Without a doubt, CPEC will result in the construction of a project of remarkable scope. These projects are expected to be a sign of good regional, domestic, and economic modifications, and by doing so, Pakistan and China's relationship will advance beyond the realization of our destiny. In both countries, there is relatively little interpersonal interaction. To guarantee the CPEC's a successful outcome, similar to how the original Silk Road operated, civilisation conversation (through culture exchange, partnerships between technology and education), and the dissemination of Silk Road history and a significant contribution will be played by tourism. The management of both transportation and infrastructure projects should be founded on the common desires that emerge from these discussions, which in turn foster an environment of recognizing, open discussion, and collaborative ambitions.

6. Conclusion

In this study, we evaluated how the general public felt about the CPEC's social integration, social acceptance, social contribution, social actualization, social coherence, social affiliation, and economic corridors between China and Pakistan using the following criteria. This investigation focused on what the general population thought of and anticipation of Chinese investment in Pakistan (CPEC). In order to investigate the association between DV, IV, and Moderator in subsequent investigations, an aggregate of 650 validated survey responses was gathered. Following an analysis of the collected information employing PLS-SEM and SPSS, recommendations and findings were drawn from the study. The results of the investigation show that there were significant connections between Sint and CPEC as well as SAcc, SAct, SCon, SCoh, and SAff. Under this study, the range H1–H6 is acceptable. Additionally, almost every factor has low to moderate relationships with one another. The investigation demonstrated that CPEC is going to have significant positive effects on the social welfare of both nations, but certain obstacles and obligations must additionally be taken into account when fictionalizing these projects. It also demonstrated that the Pakistani public is very satisfied and happy with these projects and continues to look to the future of Pakistan's stable political environment and its accomplishment of the aforementioned initiatives. The present investigation has specific constraints, such as the possibility of collecting more data and the need for more interviews with foreign policy decision-makers and CPEC-related personnel. All the restrictions and issues were left to be discussed in greater depth.

References

1. Mobasher, M.B., *Understanding ethnic-electoral dynamics: how ethnic politics affect electoral laws and election outcomes in Afghanistan*. Gonz. L. Rev., 2015. **51**: p. 355.
2. Valenzuela, S., N. Park, and K.F. Kee. *Lessons from Facebook: The effect of social network sites on college students' social capital*. in *9th International Symposium on Online Journalism*. 2008.
3. McKelvey, B. and H. Aldrich, *Populations, natural selection, and applied organizational science*. Administrative Science Quarterly, 1983: p. 101-128.
4. Yongmei, C. and J. Afzal, *Impact of Enactment of 'The Prevention of Electronic Crimes Act, 2016' as Legal Support in Pakistan*. Academy of Education and Social Sciences Review, 2023. **3**(2): p. 203-212.
5. Wolf, S.O. *China-Pakistan economic corridor, civil-military relations and democracy in Pakistan*. 2016. SADF Working Paper Series, South Asia Democratic Forum (SADF), WP.
6. Karrar, H.H., *In the shadow of the Silk Road: Border regimes and economic corridor development through an unremarkable Pakistan-China border market*. Comparative Studies of South Asia, Africa and the Middle East, 2019. **39**(3): p. 389-406.
7. Hussain, E., *China–Pakistan economic corridor: will it sustain itself?* Fudan Journal of the Humanities and Social Sciences, 2017. **10**: p. 145-159.
8. Sanchez-Triana, E., et al., *Revitalizing industrial growth in Pakistan: Trade, infrastructure, and environmental performance*. 2014: World Bank Publications.
9. Awais, M., et al., *Impact of financial literacy and investment experience on risk tolerance and investment decisions: Empirical evidence from Pakistan*. International Journal of Economics and Financial Issues, 2016. **6**(1): p. 73-79.
10. Chan, M.H.T., *The belt and road initiative—the new silk road: a research agenda*. Journal of Contemporary East Asia Studies, 2018. **7**(2): p. 104-123.
11. Djankov, S. and S. Miner, *China's Belt and Road Initiative: motives, scope, and challenges*. 2016: Peterson Institute for International Economics.



12. Abid, M. and A. Ashfaq, *CPEC: Challenges and opportunities for Pakistan*. Journal of Pakistan Vision, 2015. **16**(2): p. 142-169.
13. Kumar, J., et al., *Cross border project in China-Pakistan economic corridor and its influence on women empowerment perspectives*. Plos one, 2022. **17**(6): p. e0269025.
14. uddin Ahmed, S., et al., *China Pakistan Economic Corridor and Pakistan's energy security: A meta-analytic review*. Energy policy, 2019. **127**: p. 147-154.
15. Wolf, S.O., *China-Pakistan Economic Corridor of the Belt and Road Initiative*. 2021: Springer.
16. Afzal, J., et al., *Statistical Analysis of Foreign Investment Using Neutrosophic Interval Based Approach*. Neutrosophic Sets and Systems, 2025. **79**(1): p. 14.
17. Bhattacharjee, D., *China Pakistan economic corridor*. Available at SSRN 2608927, 2015.
18. Hussain, F. and M. Hussain, *China-Pak economic corridor (CPEC) and its geopolitical paradigms*. International Journal of Social Sciences, Humanities and Education, 2017. **1**(2): p. 79-95.
19. Afzal, J., M.A. Afzal, and Z. Nishtar, *Completion of the ten years of the China-Pakistan Economic Corridor (CPEC) and its economical goals*. Inverge Journal of Social Sciences, 2023. **2**(4): p. 23-29.
20. Ruggie, J., *Protect, respect and remedy: A framework for business and human rights*. Innovations: Technology, Governance, Globalization, 2008. **3**(2): p. 189-212.
21. Johnson, D.W. and R.T. Johnson, *Making cooperative learning work*. Theory into practice, 1999. **38**(2): p. 67-73.
22. Fivush, R., *Accuracy, authority, and voice: Feminist perspectives on autobiographical memory*. Toward a feminist developmental psychology, 2000: p. 85-105.
23. Afzal, J. and G. Anwar, *AN EMPIRICAL STUDY ON ACADEMIC SUSTAINABILITY OF MOBILE LEARNING AT UNIVERSITY LEVEL*. Pakistan Journal of Educational Research, 2023. **6**(2).
24. Tellis, W., *Introduction to case study*. The qualitative report, 1997. **3**(2): p. 1-14.
25. Afzal, J., W. Lumeng, and M. Aslam, *Assessment of tolerance, harmony and coexistence: a study on university students in Government College University, Faisalabad*. Siazga Research Journal, 2022. **1**(1): p. 06-10.
26. Hair Jr, J.F., M.C. Howard, and C. Nitzl, *Assessing measurement model quality in PLS-SEM using confirmatory composite analysis*. Journal of Business Research, 2020. **109**: p. 101-110.
27. Lowry, P.B. and J. Gaskin, *Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it*. IEEE transactions on professional communication, 2014. **57**(2): p. 123-146.
28. Legate, A.E., et al., *PLS-SEM: Prediction-oriented solutions for HRD researchers*. Human Resource Development Quarterly, 2023. **34**(1): p. 91-109.
29. Wong, K.K.-K., *Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS*. Marketing Bulletin, 2013. **24**(1): p. 1-32.
30. Hall, C.M. and J. Jenkins, *Tourism and public policy*. A companion to tourism, 2004: p. 523-540.
31. Litva, A., et al., *'The public is too subjective': public involvement at different levels of health-care decision making*. Social science & medicine, 2002. **54**(12): p. 1825-1837.
32. Lieb, R., *Content marketing: Think like a publisher-How to use content to market online and in social media*. 2012: Que Publishing.
33. Wang, J., *Shock troops, Bulls**t, and Captain America: the US Marines' Decoding of Generation Kill and the Marine identity from the grunt's perspective*. 2022.
34. Afzal, J., et al., *Relationship between Organizational Silence and Commitment of Employees at University Level*. Siazga Research Journal, 2023. **2**(1): p. 58-65.
35. Rizvi, H.A., *The China-Pakistan Economic Corridor*. Strategic Studies, 2014. **34**: p. 1-17.
36. Xu, Z., et al., *China-Pakistan Cultural Exchanges and Cooperation under Belt & Road Initiative*. Siazga Research Journal, 2023. **2**(3): p. 186-191.
37. Ahmad, R., H. Mi, and L.W. Fernald, *Revisiting the potential security threats linked with the China-Pakistan Economic Corridor (CPEC)*. Journal of the International council for small business, 2020. **1**(1): p. 64-80.
38. Ahmar, M., *Strategic meaning of the China-Pakistan economic corridor*. Strategic Studies, 2014. **34**: p. 35-49.
39. Starr, S.F.S.S.F., *A 'Greater Central Asia A 'Greater Central Asia Partnership' for Afghanistan and Its Neighbors Its Neighbors*. Central Asia-Caucasus Institute & Silk Road Studies Program, 2005.
40. Afzal, M.A., et al., *Empirical Evidence on Corporate Social Responsibility: A Case Study of Chinese Companies in Pakistan*. International Journal of Trends and Innovations in Business & Social Sciences, 2024. **2**(3): p. 367-374.
41. Afzal, J., H. Khatoon, and G. Anwar, *A Comprehensive Study on Sales of Chinese Books and Literature in Pakistan*. Siazga Research Journal, 2023. **2**(4): p. 310-318.

42. Nussbaum, M.C., *Creating capabilities: The human development approach and its implementation*. Hypatia, 2009. **24**(3): p. 211-215.
43. ZBaig, Z., M. Nilofar, and U. Meena, *The Impact Of Inwards FDI on domestic management practices in Pakistan*. Webology (ISSN: 1735-188X), 2022. **19**(2).

Declaration

Conflict of Study: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contribution Statement: All authors contributed equally.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: The paper and additional data include the research's distinctive findings; for more information, contact the article's corresponding author(s).

Acknowledgement: The author is thankful to the editor and reviewers for their valuable suggestions to improve the quality and presentation of the paper.

Declaration of AI Use: Not Applicable

Ethical Statement: The human research ethics committee of the University approved this study (Ref. Number: IRB/2024/MAR003). This study has been performed in accordance with the Declaration of Helsinki.

Informed Consent: Written informed consent for participation was obtained from respondents who participated in the survey. No data was collected from anyone under 18 years old.

Author(s) Bio / Authors' Note

Maria Qayum from the School of Economics & Management, China Three Gorges University, Yichang City 443002, China. Email: maria.qayyum1@yahoo.com

Shanza Qayyum from the School of Economics and Management, Zhengzhou University, China. Email: shanzaqayyum5@gmail.com

Muhammad Noman from the School of Economics and Management, Zhengzhou University, China. Email: mr.nomanqureshi92@gmail.com

Ismat Ara Jarin from School of Basic Medical Sciences, China Three Gorges University, Yichang City 443002, China. Email: jarinismatara@gmail.com





The ICT-Based Food Security Management of Pakistan

Shehar Bano ¹, Muhammad Adeel Afzal ², Aqsa Nadeem ^{3*}, Narmin Nezamdoost-Sani ⁴

¹School of Geography and Remote Sensing, Hohai University, Nanjing, China

²College of Economics & Management Science, China Three Gorges University, China

³Department of Microbiology, University of Karachi, Pakistan

⁴Department of Food Science and Technology, Faculty of Agriculture, Urmia University, Urmia, Iran

* Corresponding Email: aqsanadeem434@gmail.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.09>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Food security remains a critical development challenge for Pakistan, exacerbated by population pressures, climate vulnerabilities, and systemic inefficiencies within its agrarian economy. In the current research, there is a research question that examines the use of Information and Communication Technology (ICT) as a game changer in terms of advancing food security, other vital determinants such as the agri-food system, greenhouse gas emission, GDP per capita, drinking water provision, and population growth. It is affirmed using the annual data from 2001 to 2023, and with the development of a model of Autoregressive Distributed Lag (ARDL), as a result of the assessment showed that there is indeed a stable long-run co-integrating relationship between the variables. The findings prove that ICT, the agri-food system, and GDP per capita have great positive impacts on long-run food security, and gas emissions are also positively correlated as well, which indicates that there is a complex association between them and agricultural output. The first one is that in the short run, when the error-correction mechanism is efficient, it implies that the adjustment to the equilibrium following a shock is fast. The results highlight the need to have a strategic approach to digital innovation, an effective food value chain, and sustainable economic policies in order to develop a resilient food system. The paper ends by making recommendations on specific investments in ICT infrastructures, climate-sensitive agriculture, and inclusive development to guarantee Pakistan's sustainable food security in the view of changing environmental and demographic conditions.

Keywords: Food Security; Information and Communication Technology; Agri-Food System; Autoregressive Distributed Lag (ARDL); Sustainable Agriculture; Digital Transformation

1. Introduction

Food security has been among the top developmental issues facing Pakistan, a country which is defined by a high population growth rate, climatic instability, inefficiencies in its agricultural sector and its socio-economic imbalances[1]. Despite operating as an agrarian economy where agriculture plays a great role in providing jobs and livelihoods in the rural areas, Pakistan still experiences challenges concerning food availability, food access, food utilization and food stability[2]. Climate change, water shortage, market failure, post-harvest losses and poor institutional coordination are contributing to these issues[3, 4]. As such, the concept of the use of Information and Communication Technology (ICT) in the management of food security has proven to be a transitional approach to improving the productivity of agriculture, market efficiency and policy responsiveness[5, 6]. Food security management is an all-inclusive list of activities, which comprises food production, food storage, and distribution, food pricing, food monitoring, and emergency response[7]. Pakistan has often been relying on incomplete data, tardy reporting, and manual decision-making in the traditional food security systems, which have restricted its responsiveness to shocks like floods, drought, pandemics and international price changes. The lack of real-time data has limited access to the market by the farmers, transparency along the supply

chains, and the effectiveness of the early warning systems. Consequently, the problem of food insecurity remains, especially in rural areas, among the urban poor, and others who are at risk[8].

ICT-food management improves agricultural output by providing farmers with comprehensive information regarding the weather patterns, pest invasion, price of inputs, and the most appropriate farming systems to use[9]. Digital extension platforms and mobile advisory services decrease information asymmetry and enable the small-holder farmers to make well-informed decisions[10]. Moreover, ICT also facilitates precision agriculture by the use of remote sensing and data analytics, which enhances optimal use of resources and controls environmental degradation. Such innovations are especially relevant to Pakistan, where small-scale farmers are the main producers of agricultural products, and they have limited access to knowledge, credit, as well as to the market. In addition to production, ICT is also important in enhancing the food market and distribution[11]. Electronic supply chain management systems, mobile-based price information systems and digital marketplaces would lower the cost of transactions, post-harvest losses, and improve price transparency. ICT also reduces the effects of intermediaries and ensures that income is stabilized by linking the farmer to the buyer[12]. Moreover, online logistics and storage systems have a supportive role in the programs of food distribution by the population, such as strategic grain stocks and local food support programs.

This study offers multiple novel contributions to the food security literature. First, it uniquely integrates information and communication technology (ICT) as a core determinant of national food security in Pakistan, a dimension largely overlooked in prior empirical studies. Second, it expands the analytical scope beyond agricultural production to incorporate environmental, technological, and demographic factors through a multi-dimensional ARDL framework. Third, by utilizing annual time-series data from 2001 to 2023, the study captures the structural impact of digital penetration on food systems over two decades. Fourth, the findings reveal a counter-intuitive positive long-run association between emissions and food security, highlighting complex production–environment trade-offs. Collectively, the study provides original theoretical insights and policy-relevant evidence on how digital transformation can strengthen food system resilience in Pakistan.

2. Literature Review and Theoretical Foundation

The theory of food security is based on the framework of the Food and Agriculture Organization (FAO), which frames the concept of food security on 4 pillars related to each other, which include availability, access, utilization, and stability[13, 14]. This is the framework that offers the reviewing lens to the study of food security as a dependent variable that is dependent on economic, environmental, and institutional factors. With reference to the context of Pakistan, the food security results are not only limited to food production but also to systemic efficiencies, environmental sustainability, and information flows within the agri-food system. The Sustainable Livelihoods Framework is another addition that accompanies the theory of food security, and it stresses how assets, institutions, and vulnerability contexts equally combine to ensure household and national food security[15]. All these theories have an incentive to explain why food security should be considered as a consequence of structural and policy-driven factors and not as a condition on its own.

2.1 Agri-Food System and Food Security

The Systems Theory is the most appropriate answer to explain the relationship between the agri-food system and food security in that food production, processing, distribution, and consumption are a part of a larger system[16, 17]. This school of thought postulates that food availability and stability in the agri-food system can be undermined by any disruption or inefficiency in any aspect of this service. According to the literature on agri-food systems in developing economies, integrated and well-coordinated systems lead to an increment in food security through boosted productivity, eliminated losses after harvest, and efficient conversion of market economies. In Pakistan, poor institutional integration and incomplete supply chains underscore the applicability of Systems Theory as to how systemic changes can be made to the agri-food system to result in more sustainable food security.

2.2 Food Security and Gas Emissions

The Environmental Sustainability Theory and Climate Change Theory are theoretically based when it comes to the association between gas emissions and food security[18, 19]. These hypotheses assume that high levels of greenhouse gases will cause imbalances in the ecological aspect, hence causing climate change, loss of resources, and low capacity to produce agricultural products. The literature highlights that agriculture causes as well as is influenced by gas emissions and hence forms a feedback loop that responds to food security. Climate-related risks like floods and droughts in Pakistan are worsened by increased emissions and endanger food security and food stability. The Environmental sustainability theory thus comes in favour of having gas emission as a key determinant of food security, and therefore, low-emission and climate-resistant agriculture should be adopted[20].

2.3 Drinking Water and Food Security

The Human Needs theory and the Ecological Systems theory are theoretically applicable in the relationship between drinking water and food security[21, 22]. According to the Human Needs Theory, the availability of clean water is described as a universal condition of life as well as health, and this directly affects the use of food and nutritional achievements. The Ecological Systems Theory also describes how agricultural productivity and ecosystem health are influenced by water availability and will result in food security. Water scarcity and contamination affect food production as well as human health in Pakistan, which validates the theoretical perspective of water security being a fundamental pillar of sustainable food security.

2.4 Food Security: Information and Communication Technology

Diffusion of Innovation Theory and Information Asymmetry Theory support the role that information and communication technology (ICT) plays in food security[23, 24]. This is due to the diffusion theory as the new technologies permeate the farmers and institutions, increasing the productivity and performance of agriculture over time. The Information Asymmetry Theory is based on the idea that inefficient decisions and market failures are the result of unequal access to information. ICT helps in minimizing these asymmetries by providing the information on weather, prices, and methods of farming as and when it is needed. ICT-assisted advisory services and online platforms in Pakistan improve the efficiency of decision-making and market access, which improves the availability and accessibility of food. These theories give a formidable conceptual rationale of ICT as the primary force of food security.

2.5 GDP per Capita and Population Growth Control Variables

The Economic Development Theory provides a theoretical basis to the concept of GDP per capita, that is, a higher standard of living is associated with higher income, institutional capacity, and development of infrastructure, which leads to better welfare results, such as food security[25, 26]. An increase in GDP per capita indicates an increase in purchasing power, an increase in the availability of food, and an improvement in public service delivery. The fact that GDP per capita is controllable in empirical food security models means that researchers can then control macroeconomic conditions that could have an impact on access to food independent of sector-specific factors. In the case of Pakistan, the differences in economic capacity can be reflected by changes in the GDP per capita, which can indicate changes in food security.

The Malthusian Theory and Demographic Transition Theory are theoretically used to explain population growth[27]. According to the Malthusian theory, the growth of the population can surpass the increase in food production and result in a lack of resources and food insecurity. The theory of demographic transition offers more of a refined perspective whereby the dynamics of population and technological advancement, as well as economic development, interact. In Pakistan, the large population growth exerts pressure particularly on agricultural resources, water, and food systems, which could counter the technological and institutional developments. This is the reason the consideration of population growth as a control variable is theoretically justifiable to consider the demographic pressures on food security. Conceptual framework is shown in figure 1.

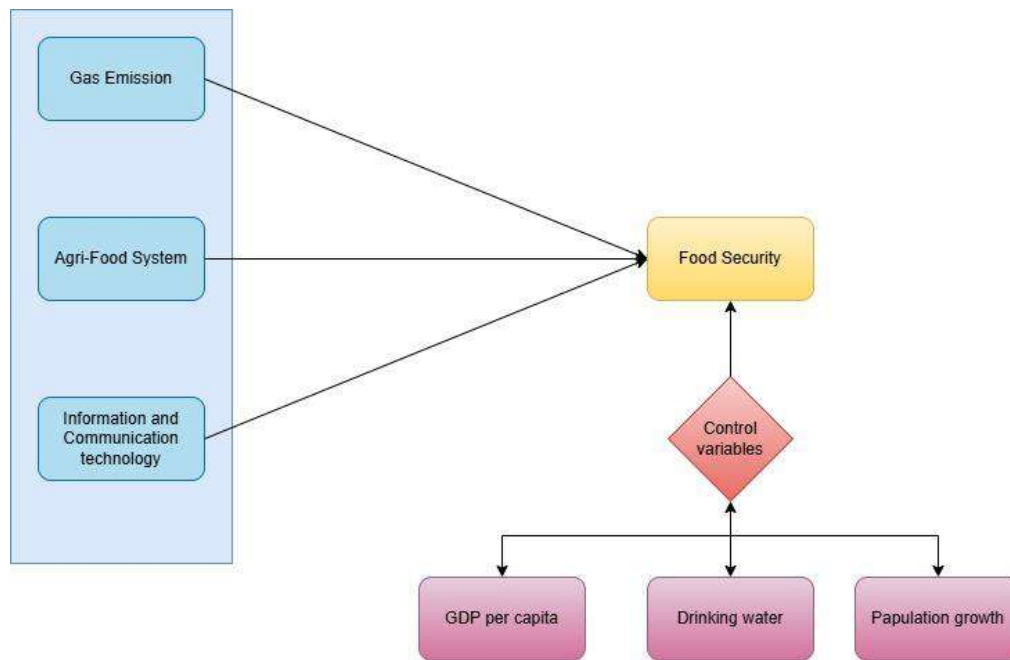


Figure 1: Conceptual Framework

3. Materials and Methodology

This study examines annual data for Pakistan from 2001 to 2023, selected based on the availability of a sufficiently long and consistent time series. Food Security (LFS) is the dependent variable, while gas emission (Lemc), agri-food system (Lafs), and information and communication technology (Lict) serve as the primary independent variables. To provide a more comprehensive evaluation of food security, the analysis also incorporates several control variables, including gdp per capita (Lgdp), drinking water (Ldw), and population growth (Lpg), as presented in Table 1. All variables are sourced from publicly available international databases. Data on GDP, information and communication technology, population growth, and drinking water are obtained from the World Bank's World Development Indicators. Data for food security, agri-food system, and gas emission taken from FAO.

Table 1: List of Variables

Dependent variable	Food security	Food Production	FAO
Independent variable	Agri food system	Estimated value	FAO
	Gas Emission	Emissions (CO2eq) (AR5)	FAO
	Information and communication technology	Individuals using the Internet (% of population)	WDI
Control variables	GDP per capita	Annual Growth	WDI
	Population growth	Annual growth	WDI
	Drinking water	Availability of clean water to drink	WDI

$$FSt = f(emct, afst, ictt) \quad (1)$$

The explanatory variables included in the model are gas emissions (emc_t), agri-food security (afs_t), and information and communication technology (ict_t). Their respective lagged values are denoted as emc_{t-i} , afs_{t-i} , and ict_{t-i} . The endogenous variable is food security (FS_t), with its lagged term represented by FS_{t-i} . Considering the time-lagged effects involved in enhancing the food security, this study employs an autoregressive distributed lag (ARDL) model to examine the impact of gas emissions, agri-food security, and information and communication technology on food security. The ARDL approach is implemented in two stages. In the first stage, the ARDL bounds testing procedure is applied to assess the existence of a long-run causal relationship among the variables. Based on this procedure, the following model is specified:

$$\Delta \ln FSt = \beta_0 + \beta_1 \ln FSt_{-1} + \beta_2 \ln emct_{-1} + \beta_3 \ln afst_{-1} + \beta_4 \ln ictt_{-1} + \varepsilon_t \quad (2)$$

$$\Delta \ln FSt = \beta_0 + \beta_1 \ln FSt_{-1} + \beta_2 \ln emc_{-1} + \beta_3 \ln afst_{-1} + \beta_4 \ln ict_{-1} + \beta_5 \ln gdp + \beta_6 \ln dw + \beta_7 \ln pg + \varepsilon_t \quad (3)$$

In the first step, Δ represented a first-order differential operator, ε_t was white noise, and a, b, c, d were the maximum lag orders determined by AIC or BIC. The presence of a long-term equilibrium relationship among the variables was tested using an F-statistic, with the null hypothesis stating that no such long-term equilibrium existed. Step 2 involved estimating the ARDL model to examine both the long-run and short-run relationships between the variables. The long-term relationship was estimated using the ARDL (p_1, p_2, p_3, p_4) model. Methodology flow chart show in figure 2.

$$\Delta \ln FSt = \beta_0 + \beta_1 \sum_{i=1}^n \Delta LFS_{t-i} + \beta_2 \sum_{i=1}^n \Delta Lemc_{t-i} + \beta_3 \sum_{i=1}^n \Delta Lafs_{t-i} + \beta_4 \sum_{i=1}^n \Delta Lict_{t-i} + \beta_5 \sum_{i=1}^n \Delta Lgdp_{t-i} + \beta_6 \sum_{i=1}^n \Delta Ldw_{t-i} + \beta_7 \sum_{i=1}^n \Delta Lpg_{t-i} + \varepsilon_t \quad (4)$$

while the short-term relationship was captured using an ARDL-based error correction model (ECM), as specified in Equation (4).

$$\Delta \ln FSt = \beta_0 + \beta_1 \sum_{i=1}^n \Delta LFS_{t-i} + \beta_2 \sum_{i=1}^n \Delta Lemc_{t-i} + \beta_3 \sum_{i=1}^n \Delta Lafs_{t-i} + \beta_4 \sum_{i=1}^n \Delta Lict_{t-i} + \beta_5 \sum_{i=1}^n \Delta Lgdp_{t-i} + \beta_6 \sum_{i=1}^n \Delta Ldw_{t-i} + \beta_7 \sum_{i=1}^n \Delta Lpg_{t-i} + \lambda ECM_{t-1} + \varepsilon_t \quad (5)$$

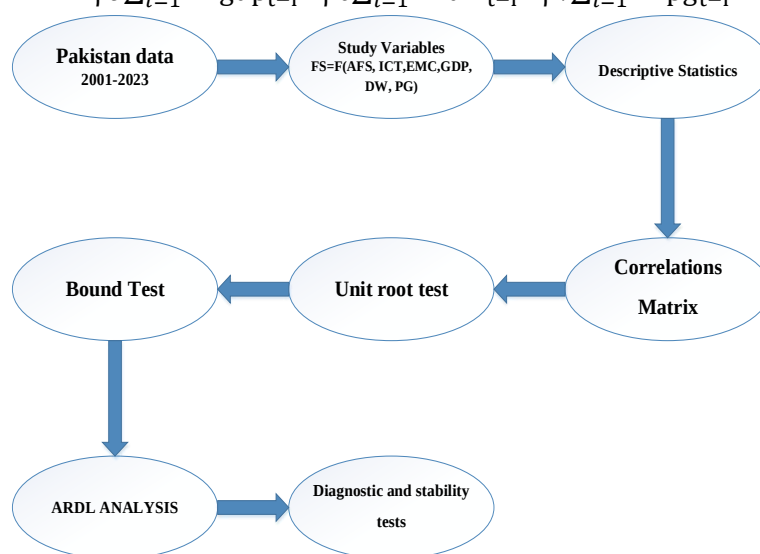


Figure 2: Flow Chart of Methodology

4. Analysis and Results

The empirical analysis will begin with the descriptive statistics shown in table 2, which will provide an overview of the dynamics of the variable over the study period. Food security (LFS) exhibits a high mean and low variance, which means that food security conditions did not fluctuate as much over the period during which this study was conducted. GDP per capita (LGDP), on the other hand, is highly variable, with a temporary change in the increased economic performance. The dispersion among all the variables is the highest among information and communication technology (ICT), which indicates uneven growth and digital infrastructure adoption. The agri-food system, gas emissions (LEMC), drinking water access (LDW), and population growth (LPG) variables show moderate variability, which means that there are no intense structural changes but gradual ones. All in all, the descriptive results show that the dataset is properly organized and can be analyzed using time series.

Table 2: Descriptive Statistics

Variable	Obs	Mean	Std. Dev.	Min	Max
lfs	23	7.583	.084	7.43	7.73
lgdp	23	1.919	2.253	-3.04	5.2
lemc	23	3.403	.067	3.28	3.52
lafs	23	4.395	.052	4.3	4.46
lict	23	11.037	6.817	1.32	27.38
ldw	23	1.603	.06	1.49	1.71
lpg	23	2.038	.479	1.3	2.8

The table 3 correlation matrix determines that there are strong initial relationships between the

variables under study. The relationship between food security and gas emission, agri-food system, information and communication technologies (ICT), and access to drinking water depicts a good and positive correlation, meaning that agricultural infrastructure, technological, and basic utilities improvement accompany a high level of food security. On the other hand, the relationship between population growth and food security is characterized by a negative relationship and is thus in an inverse manner, whereby the growth of population will tend to weaken the food availability and distribution systems. The gross domestic product per capita has poor associations with most variables, indicating that its impact on food security is indirect, as it acts via other structural factors. These correlations provide preliminary information, but they are not causal.

Table 3: Matrix of correlations

Variables	(1)	(2)	(3)	(4)	(5)	(6)
(1) lfs	1.000					
(2) lgdp	-0.044	1.000				
(3) lemc	0.997	-0.056	1.000			
(4) lafs	0.884	-0.091	0.883	1.000		
(5) lict	0.917	-0.097	0.908	0.690	1.000	
(6) ldw	0.640	0.203	0.633	0.662	0.531	1.000
(7) lpg	-0.750	-0.199	-0.749	-0.791	-0.654	-0.612

Before the estimation process, unit-root diagnostics were conducted to determine the stationarity properties of the series under investigation. The diagnostics show that the non-stationary variables are food security, information and communication technology (ICT), gross domestic product per capita, drinking water and population growth all of which satisfies the criterion of non-stationarity when first differenced and thus attain stationarity when first differenced; hence, these can be termed as the integrated of order one (I(1)). On the other hand, agri-food system variable is stationary that is integrated of order zero (I(0)). This heterogeneity of integration warrants the employment of the Autoregressive Search Lag (ARDL) modeling framework that is appropriate whenever there is a need to incorporate variables that are integrated both at I(0), and I(1) as shown in table 4.

Table 4: Unit Root test

Variables	T statistic	p-value	Integration
LFS	-9.060	0.000	I (1)
LICT	-4.325	0.001	I (1)
LAFS	-4.088	0.001	I (0)
LEMC	-9.386	0.000	I (1)
LGDP	-3.190	0.021	I (1)
LDW	-3.756	0.011	I (1)
LPG	-3.560	0.000	I (1)

The ARDL bounds testing (table 5) process supports the presence of a long-run relationship between the variables. The computed F-statistically significantly exceeds the upper bound figures at all traditional levels of significance, thus permitting us to reject the null hypothesis that there is no cointegration. This finding provides solid proof of a long-run equilibrium relationship between food security and the chosen agri-food, environmental, technological, and macroeconomic variables.

Table 5: BOUND TEST

Model	F-stat	Sig. level	I (0)	I (1)	Decision
	106.970	10%	2.12	3.23	Rejected H0
		5%	2.45	3.61	
		2.5%	2.75	3.99	
K	6	1%	3.15	4.43	

There is a long-run estimation that gas emissions have a negative and insignificant impact on food security. The agri-food system has a significant positive impact on food security, and so the development of efficient agricultural structures and food systems is quite important in ensuring sustainable access to food. There is a high positive effect of information and communication

technology, which implies that online connectivity will enhance food security by increasing market presence, flow of information, and agricultural productivity. The same was found with GDP per capita, whose effect is also positive and significant, supporting the fact that economic growth facilitates the attainment of food security through increasing the purchasing power and investment potential. Conversely, the availability of drinking water and population increase can have no statistically significant influence in the long term, which implies that the two factors can contribute to food security indirectly or contextually. The dynamic processes in the short run also indicate a salient adjustment process. The reactions of ICT and GDP per capita to change have a negative, but weakly significant response, implying that in the short term, there are transitional costs or lagged advantages of technological growth and economic alterations. The value of the error-correction term is negative, but very significant, and this confirms that there is a valid process of adjustment in association with the long-run equilibrium. The size of the coefficient implies a quick rate of adjustment, which means that disequilibria are eliminated in a short period of time. All long- and short-term results shown in table 6.

Table 6: ARDL Analysis results

D.lfs	Coefficient	Std. err.	t	P>t	95% conf.	interval]
ADJ						
lfs						
L1.	-1.152	0.066	-17.500	0.000	-1.296	-1.009
LR						
lemc	-0.849	0.082	-10.330	0.099	-0.670	-1.029
lafs	0.228	0.076	3.010	0.011	0.063	0.392
ldw	0.027	0.020	1.360	0.198	-0.016	0.070
lict	0.003	0.001	4.730	0.000	0.002	0.004
lgdp	0.002	0.001	2.860	0.014	0.000	0.003
lpg	0.005	0.005	1.060	0.311	-0.005	0.015
SR						
lict						
D1.	-0.005	0.003	-1.790	0.099	-0.012	0.001
lgdp						
D1.	-0.001	0.001	-1.760	0.103	-0.002	0.000
_cons	4.154	0.370	11.240	0.000	3.349	4.959

The diagnostic and stability tests (table 7) are used, which justifies the strength of the estimated model. The estimated standard errors are credible due to the absence of serial correlation and heteroskedasticity, unlike the Ramsey RESET test, which supports the correct functional form. Normal tests reveal that the residual is normally distributed, and the CUSUM square test shows that the parameter has not changed over the years. All these results confirm the sufficiency of the ARDL specification and the soundness of the estimated relationships. The CUSUM graph shown in figure 3.

Table 7: Diagnostic and stability tests

Model		
Test	Chi2/F-value	Probability
Breusch–Godfrey LM test	0.060	0.8072
Breusch–Pagan/Cook–Weisberg test for heteroskedasticity	0.02	0.8974
Ramsey RESET test	1.12	0.3774
Skewness and kurtosis tests for normality	0.60	0.7402
Shapiro–Wilk W test	-0.819	0.7935
Jarque–Bera normality test	2.54	0.2808
CUSUM Square Test	Stable	

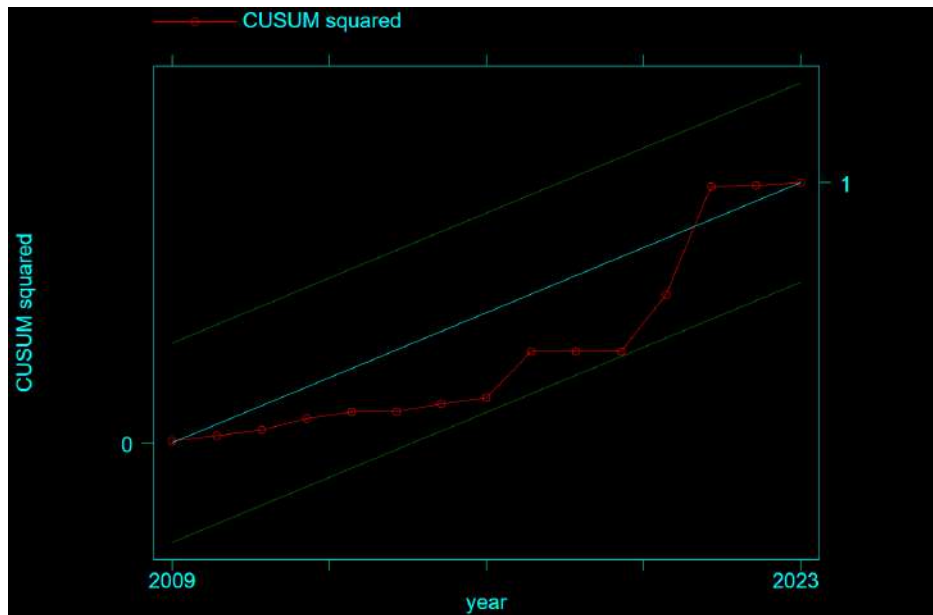


Figure 3: CUSUM Graph of Analysis

5. Discussion

This research has provided clear evidence of what defines food security in Pakistan. These demonstrate that all these factors-structure, technology, and macroeconomic are important. A long-term co-integration test ascertains that food security is not a lone outcome, but it is determined by the interrelation of the agri-food system, the environmental factors, digital infrastructures, and economic performance in the long-run. This is one of the main findings, which justifies applying an ARDL framework and suggests an argumentation concerning the particular long- and short-run processes that the model reveals. Information and Communication Technology (ICT) produce a positive, statistically significant impact on food security in the long run. It is in favour of the Diffusion of Innovation and Information Asymmetry theories. In Pakistan, ICT can enhance access to markets, provide real-time weather and pricing, and enhance agricultural productivity using digital advisory services. A positive impact on the agri-food system is also significant, in which the efficiency of production, processing, and distribution channels has been brought to the fore through the Systems Theory. Gas emissions have a negative long-run coefficient. It could be a sign of the connection between the emissions and increased agricultural and industrial activity already sustaining the consumption of food, yet it brings concerns of environmental sustainability in the long term. Economic Development Theory is also adequately demonstrated by a strong positive impact of the GDP per capita, since economic growth increases the purchasing power and public investment. The long-run model did not show a statistically significant effect of drinking water access and population growth, which can possibly mean that these variables have an indirect or mediating impact.

Short-run analysis displays crucial information and patterns of adjustments. Indicated strong initial adjustment costs or implementation lags are weakly significant negative coefficients of ICT and GDP per capita. The existence of benefits brought about by the technology adoption or economic policy adjustments may not surface quickly, perhaps due to infrastructure constraints, skill differences or the disruption of the transitional markets. Most importantly, the error-correction term is negative and has great significance. This ascertains a stationary, comparatively rapid process that adjusts brief fluctuations of deviations in the long-run equilibrium. Therefore, the food security system is vulnerable to shocks, but internally driven in Pakistan, which gets back to its long-term course as determined by underlying determinants. These conclusions are strong as they are backed by numerous diagnostic tests and stability tests. This model does not indicate any signs of serial correlation or heteroscedasticity, and the Ramsey RESET test makes sure the functional form is correct. The distribution of residuals is

normally distributed, and the CUSUM of squares test confirms there are no changes in the parameters within the study. Combined, both of these diagnostics attest to the received ARDL and to the validity of the relationships inferred between food security and elements that explain it.

6. Conclusion

This study conclusively demonstrates that achieving sustainable food security in Pakistan hinges on the strategic integration of digital technology, systemic agri-food efficiency, and supportive macroeconomic policies. The empirical evidence confirms a robust long-run relationship where Information and Communication Technology (ICT) serve as a transformative force, enhancing market access, information flow, and agricultural productivity, while a resilient agri-food system and rising GDP per capita further solidify the foundation for national food security. These findings validate a forward-looking policy approach that prioritizes ICT infrastructure in rural areas, modernizes supply chains, and fosters inclusive economic growth to build a more resilient food ecosystem. Ultimately, Pakistan's path to food security must balance immediate productivity gains with long-term sustainability. While emissions were negatively linked to food output in this analysis, this signals an urgent need to adopt green agricultural practices and climate-resilient strategies to avoid future trade-offs between food production and environmental health. By embracing technology-driven, system-wide, and ecologically conscious policies, Pakistan can transform its food security challenges into opportunities for sustainable development, ensuring equitable access to food for all its citizens in the decades to come.

References

1. Yaseen, M., et al., *Implementation of Neutrosophic Logic for Food Security and Agricultural Productivity Analysis in South Asian Countries*. Neutrosophic Sets and Systems, 2025. **93**(1): p. 22.
2. Ahmad, M. and U. Farooq, *The state of food security in Pakistan: Future challenges and coping strategies*. The Pakistan Development Review, 2010: p. 903-923.
3. Afzal, M.A., J. Afzal, and Z. Nishtar, *Mega Hydropower Projects and Sustainable Development of Pakistan*. Journal of Engineering, Science and Technological Trends, 2024. **1**(2).
4. Afzal, J. and Z. Nishtar, *A substantial study on history of climate change in south asia for sustainable development*. Journal of History and Social Sciences, 2023. **14**(1): p. 101-112.
5. El Bilali, H. and M.S. Allahyari, *Transition towards sustainability in agriculture and food systems: Role of information and communication technologies*. Information processing in agriculture, 2018. **5**(4): p. 456-464.
6. Nwafor, S., et al., *Role of Information and Communication Technologies towards Sustainability Transitions in Agriculture and Food Systems*. Nigeria Agricultural Journal, 2022. **53**(2): p. 40-45.
7. Bibi, A. and J. Afzal, *Review of Smart Edible Films and Coatings for Perishable Foods and Future of Smart Packaging*. Journal of Engineering, Science and Technological Trends, 2025. **2**(1).
8. Ramsey, R., et al., *Food insecurity among adults residing in disadvantaged urban areas: potential health and dietary consequences*. Public health nutrition, 2012. **15**(2): p. 227-237.
9. Shah, U.S. and A. Dahal, *Biotechnology Innovation and Commercialization*. Biotechnology Innovation and Commercialization, 2011: p. 45.
10. Mbaya, A.K., *The Role of Information and Communication Technology (Ict) in Market Information Access Among Smallholder Potato Farmers in Buuri Sub County, Meru County. A Case Study of Viazisoko Digital Platform*. 2023, University of Nairobi.
11. Van der Vorst, J., A. Beulens, and P. van Beek, *Innovations in logistics and ICT in food supply chain networks*, in *Innovation in agri-food systems*. 2005, Wageningen Academic. p. 245-292.
12. Magesa, M.M., *Linking rural farmers to markets using ICTs*. 2015: CTA.
13. Farsund, A.A., C. Daugbjerg, and O. Langhelle, *Food security and trade: Reconciling discourses in the Food and Agriculture Organization and the World Trade Organization*. Food Security, 2015. **7**(2): p. 383-391.
14. Ecker, O. and C. Breisinger, *The food security system: A new conceptual framework*. 2012.
15. Yaro, J.A., *Theorizing food insecurity: building a livelihood vulnerability framework for researching food insecurity*. Norsk Geografisk Tidsskrift-Norwegian Journal of Geography, 2004. **58**(1): p. 23-37.
16. Zhang, W., et al., *Systems thinking: an approach for understanding 'eco-agri-food systems'*. 2018.
17. Rivera-Ferre, M.G., *Framing of agri-food research affects the analysis of food security: The critical role of the social sciences*. International Journal of sociology of Agriculture and Food, 2012. **19**(2): p. 162-175.



18. Ingram, J., P. Ericksen, and D. Liverman, *Food security and global environmental change*. 2012: Routledge.
19. Ingram, J., *A food systems approach to researching food security and its interactions with global environmental change*. Food security, 2011. **3**(4): p. 417-431.
20. Dragulanescu, P.N., *Some theories of environmental sustainability*. Revista Română de Statistică nr, 2013: p. 15.
21. Yazdanparast, M., et al., *Development of a water security conceptual model by combining human-environmental system (HES) and system dynamic approach*. Water Resources Management, 2023. **37**(4): p. 1695-1709.
22. Jepson, W., et al., *Advancing human capabilities for water security: A relational approach*. Water Security, 2017. **1**: p. 46-52.
23. Jere, N.J. and M.S. Maharaj, *Evaluating the influence of information and communications technology on food security*. South African Journal of Information Management, 2017. **19**(1): p. 1-7.
24. Agunyai, S.C. and V. Ojajorotu, *Data-Driven Innovations and Sustainability of Food Security: Can Asymmetric Information Be Blamed for Food Insecurity in Africa?* Sustainability, 2024. **16**(20): p. 8980.
25. Giovannini, E. and T. Rondinella, *Going beyond GDP: theoretical approaches*, in *Handbook of research on economic and social well-being*. 2018, Edward Elgar Publishing. p. 1-51.
26. Ros, J., *Development theory and the economics of growth*. 2001: University of Michigan Press.
27. Caldwell, J.C., et al., *Demographic transition theory*. 2006: Springer.

Declaration

Conflict of Study: The author declare that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable

Declaration of AI Use: Not Applicable

Author(s) Bio / Authors' Note

Shehar Bano from the School of Geography and Remote Sensing, Hohai University, Nanjing, China. Email: shehar651@gmail.com

Muhammad Adeel Afzal from College of Economics & Management Science, China Three Gorges University, China. Email: adeel@ctgu.edu.cn

Aqsa Nadeem from the Department of Microbiology, University of Karachi, Pakistan. Email: aqsanadeem434@gmail.com

Narmin Nezamdoost-Sani from the Department of Food Science and Technology, Faculty of Agriculture, Urmia University, Urmia, Iran. Email: nezamdoost.narmin@gmail.com





Will International Law Keep Up with the Rise of Hydrogen Energy?

Aftab Haider ¹, Jamil Afzal ¹, Rinel Urazayeva^{1*}

¹School of International Law, Southwest University of Political Science and Law, China

* Corresponding Email: rinelurazaeva@mail.ru

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.10>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Hydrogen energy has emerged as the global power shift towards clean energy sources in the fight against climate change. However, just as technology moves forward at a fast pace, the legal structures that are required to support the growth of hydrogen are not there, which raises many problems. The hydrogen trade is much more complicated and has many restrictions in the international market; developing nations have challenges like restricted access to hydrogen equipment and infrastructure, demonstrating significant shortcomings in international legal frameworks that guarantee fairness. As for emissions from blue hydrogen and safety issues in storage, these issues demonstrate that global liability frameworks have significant vulnerabilities. The lack of a simple and consistent legal basis for hydrogen production and consumption may impede the development of a hydrogen economy. Some of the important issues that this article discusses are whether the existing international laws can accommodate the growth of hydrogen or whether there is a need to create a new framework as a whole. With the hydrogen revolution already underway, it is time for the laws to catch up to enable a fair, inclusive, and sustainable transition.

Keywords: Hydrogen Energy; International Law; Sustainable Energy Transition; Environmental Justice

1. Introduction

The call for a clean energy transition has shifted the focus of the international community on sustainable development to hydrogen energy[1, 2]. With countries seeking ways how to achieve their respective targets set under the Paris Agreement, green hydrogen is seen to revolutionize the process of decarbonizing heavily emitting sectors, cutting down the use of fossil fuels, and promoting a net-zero economy[3, 4]. However, the reality is that behind the idea of hydrogen, several legal, regulatory, and economic issues require a solution[5-7]. Its cleanness and compatibility with renewable power sources make it a basis for future energy planning. Hydrogen has the possibility of enabling sectors such as steel manufacturing, long-distance transportation, and aviation to be green, which are difficult to electrify; however, change to a hydrogen economy requires more than a technological shift[8]. This implies the need for coherent legal regimes at the international level that would support trade in hydrogen and its derivatives, manage environmental challenges, and promote fair distribution of hydrogen technologies. Another critical question arises as to whether modern international laws are well prepared for this change; the answer, however, is no[9, 10]. There is no specific regulation that targets hydrogen, but the current treaties and agreements mainly discuss renewable energy in a general sense[11, 12]. For instance, even as the Paris Agreement offers a global climate blueprint, it does not contain the specifics of how hydrogen energy will be regulated. Trade laws also have issues in governing and addressing the dispute of the intellectual properties of the transportation of hydrogen across borders. If the international community does not respond to this critical issue then the lack of coherent rules may cause trade conflicts, slow down the technological progress, and expand the gap between the developed and the developing nations[13]. Furthermore, the environmental impacts of hydrogen production like emissions from blue hydrogen and risks in hydrogen storage are still not well handled by the international legal frameworks on liability[14]. If there is no coherent strategy for the hydrogen economy, this can only exacerbate global inequality as opposed to mitigating it.



This article critically observes the intersection of hydrogen energy and international law, raising the following main objectives:

- To determine whether current international legal instruments can be used to enhance hydrogen energy or if there is a need for new conventions like the International Hydrogen Protocol.
- To examine the legal issues affecting hydrogen production, trade, and storage, especially in matters of international relations and environmental issues.
- To understand how international organizations and developing countries can contribute to a fair and sustainable hydrogen energy transition.
- To put forward practical suggestions for closing the gap in legislation that may impede the further development of hydrogen energy.

2. Methodology

In this article, the authors have used a multidisciplinary and analytical approach[15] to examine the complicated connection between hydrogen energy and international law. Primary sources include international treaties, legal instruments, and case laws while secondary sources include peer-reviewed articles, reports from International Energy Agency (IEA) and International Renewable Energy Agency (IRENA), and policy briefs. The combination of these different materials reveals the deficiencies of the current legislation and offers practical suggestions on how to overcome them. The study used a comparative analysis as the main approach to data analysis[16, 17]; comparing and contrasting current strategies in hydrogen governance including the EU's Hydrogen Strategy and the issues affecting the developing world. This makes it possible to identify the effect of inequality in the distribution of technology, funding, and legal framework on the advancement of hydrogen energy across the world.

This article raised thought-provoking questions designed to challenge conventional thinking: Is the legal protection of Intellectual Property impeding the formation of partnerships and collaborations for the advancement of green hydrogen technology? Is it possible to uphold trade laws that will also help address hydrogen energy issues and achieve fairness in access for all countries? These questions not only direct the analysis but also help to keep the article practical, addressing real problems and providing practical, comprehensive, and universal solutions. In this methodology, the article aims to appeal to both academics and policymakers through a combination of theoretical analysis and policy-relevant findings that would make a valuable contribution to the existing literature on hydrogen energy and international law.

3. International Legal Gaps in Hydrogen Energy Developments

3.1 International Treaties

The emergence of hydrogen energy as one of the main players in the transition to clean energy has revealed systemic gaps in regulation at the international level[18, 19]. As nations race to embrace hydrogen's potential to decarbonize industries and meet net-zero goals, a critical question arises: How ready are current international treaties such as the Paris Agreement to deal with the complex nature of hydrogen energy? The Paris Agreement signed as a success in climate diplomacy, outlines the global climate goals but lacks clear policy solutions for such emerging sectors as hydrogen energy[20]. Though it focuses on the promotion of renewable energy sources, it lacks any specific information on the methods of producing hydrogen, hydrogen trading, and safety measures[21]. This absence of definition means that hydrogen energy remains in legal limbo, and countries are free to define its function based on their national concerns. For example, is blue hydrogen, which is produced from fossil fuels with the use of carbon capture, a 'clean energy'? Or does it weaken the Paris Agreement's more general aims of emissions reduction? These questions remain unanswered and, therefore, point to a major void in the existing international governance system. Herein, the lack of a single Hydrogen Protocol presents practical issues that might impede the global adoption of hydrogen[22]. Due to the lack of standardized regulations in the production of hydrogen, the methods used differ greatly and thus have a different

potential to harm the environment[23]. For example, while the European Union is promoting green hydrogen under the principle of sustainability, other parts of the world are still using carbon-based processes. This divergence does not only potentially lead to trade conflicts but also impedes the international recognition of hydrogen as a clean energy carrier; also, the legal uncertainty impacts cross-border hydrogen trade. The transportation of hydrogen whether as pipeline hydrogen or liquefied hydrogen needs safety standards which are still different across countries? The lack of international regulation and standards presents practical challenges and makes large-scale hydrogen projects unattractive for the private sector[24].

Further, the ownership of rights over hydrogen technologies is still a problem as the developed countries are controlling the strategic technologies while the developing countries are still struggling to get the technology that they need for the adoption of hydrogen. Is a Hydrogen Protocol the solution? A specific Hydrogen Protocol could be useful as the link between the countries in terms of energy management[25]. Such a protocol would set global benchmarks for hydrogen production, which would exclude unsustainable methods such as grey hydrogen. It might coordinate the safety standards of storage and transportation, which will minimize the probability of incidents and enhance the confidence of trading parties. In addition, it could address equity through a provision that requires technology transfer and financial support to the developing countries to make hydrogen energy an international remedy to climate change[13]. What are the risks of delay? The danger of a lack of determined action on this front is that the world faces a future of a bifurcated hydrogen economy where only a handful of wealthy countries enjoy its benefits, further entrenching global divisions[26]. Worse still, this may create disparate regulations that would cause accidents that are detrimental to the environment and safety hence damaging the reputation of hydrogen as a clean energy source. The message is clear: Hydrogen Energy has the potential to be the future foundation of clean energy, but it needs International Law to deliver on the potential. The world requires more than large climate conventions and treaties; the world needs specific, enforceable, and practical guidelines that fill the existing gaps in hydrogen energy regulation.

3.2 Regulatory Hurdles and Trade Complexities

The transition to a world where hydrogen is the primary energy source is now at a tipping point, but even though it is a technology that holds a great deal of promise for the future, the road forward is not without challenges such as regulatory issues and trade[18, 27]. These challenges not only pose a risk to the timely expansion of hydrogen options but also bring up essential questions about the preparedness of the international legal system for this new age of energy exchange. The question arises: How can hydrogen be traded across borders when the processes of its transport and trade are not yet fully integrated? Perhaps the most obvious one is the lack of clear guidelines for hydrogen transport that could be applied on the international level. Hydrogen being light, flammable, and difficult to transport needs specific logistics for transportation across geographical locations[28]. However, there are also specific requirements for hydrogen transportation at the country level, including pipeline standards and liquefaction procedures. This is because a standardized regulatory platform is yet to be established, which implies that hydrogen cannot go from one country to another as a commodity. For instance, how can a shift to hydrogen be made if there is no consensus on the storage, transportation, or distribution of Hydrogen between the different regions? This absence of standardization results in slower trading, increased expenses, and lost potential for international collaboration, which is critical for hydrogen to live up to its potential in the energy transition process. Also, the essence of the hydrogen trade is even amplified by the fact that it is environment friendly. What measures can be taken to ensure that hydrogen can meet the growing demand while there are variations in the definition of clean hydrogen across nations? For instance, the European Union has taken to supporting green hydrogen produced from renewable energy, while some countries in the Middle East are more inclined towards blue hydrogen which is produced from fossil fuels but with the added process of carbon capture. This lack of

harmonization leads to trade disputes: should nations consider blue hydrogen as a part of their energy portfolio, or should they wait for the more sustainable green hydrogen? While the public and policymakers may have differing opinions on what constitutes clean energy, how can there be a fair and efficient exportation of hydrogen across countries? At the center of these regulatory issues, is a more complicated, even more contentious, question: Should the possession of IPR impede the access of developing countries to advanced green hydrogen technologies? Companies in developed countries primarily control the technology used in green hydrogen production like the electrolyzers from renewable sources[29]. These technologies are frequently patented, which renders them costly and unaffordable for developing nations. Should these innovations be protected under intellectual property laws when they slow down the global use of hydrogen energy for fighting climate change? Can the world continue to support a system where the ability to decide the future of decarbonization of the world rests in the hands of a few large corporations?

For hydrogen to become a potent tool for decarbonizing industries, weaning off fossil energy sources, and electrifying transportation systems, it is important to see how international laws can address these regulatory and trade barriers[6, 13, 30]. How much longer can we wait for solutions to these problems before the chance of a global hydrogen economy is lost? The time is now, and the answers to these questions will determine the future of hydrogen energy. For the global hydrogen market to fully realize its potential there is a need for international laws to adapt to the changing energy markets. The global push for hydrogen energy as a clean fuel of the future raises an uncomfortable question: Is this shift of transfer fair or does it only pose a threat of worsening the inequality in terms of energy between the developed and the developing countries? As the countries of the Global North is actively developing their hydrogen plans, having strong legal support, significant financing, and innovative solutions, the Global South face significant discrepancies. Furthermore, should the countries that export hydrogen produced from blue hydrogen be made responsible for the emissions from the process? This may cause problems, as there are no specific treaties that address hydrogen's risks and, therefore, there are certain areas of uncertainty. Assessment of legal liability for hydrogen-related accidents could disappear into thin air, especially in areas where national laws are either very weak or have little or no enforcement at all.

4. Critical Legal Questions

Does International Law Require a Bespoke Framework for Hydrogen Energy Governance, or Can Existing Mechanisms Suffice?

Hydrogen energy is both a response to the international environmental agenda and a potential source of economic value, but its legal regulation is dispersed[31, 32]. While the Paris Agreement offers guidelines for cutting carbon-emission levels, it does not contain rules on hydrogen production, its export, or potential dangers. This raises an important question: Can current laws, which developed as a random set for various kinds of energy, successfully address the specifics of hydrogen regulation? The answer is that hydrogen is a solution to renewable energy, a dangerous substance, and a commodity at the same time. Current structures like the UNFCCC offer broad direction but lack the details on such issues as how hydrogen will be transported across borders or who is responsible for hydrogen-related leaks or accidents[33]. It is however possible to create a specific framework that would fit the needs of hydrogen and could build a set of safety standards that would be equal for all, and decrease the number of conflicts in the international trade. The formulation of such a framework requires a weighing of global exigency with domestic concerns, a task yet to be solved.

How Can the Principles of State Sovereignty and Common but Differentiated Responsibilities Be Balanced in Hydrogen Regulation?

Hydrogen energy governance highlights a conflict between two foundational principles of international law: the sovereignty of states and the principle of CBDR[34]. While individual nations have a right to control the production of energy within their territory, hydrogen effects are global and require collective

action[35]. How can the national policies be made to conform to the global climate goals without violating state sovereignty? It is only natural for developed nations with enhanced infrastructure and access to funding to spearhead hydrogen technology advances, but this leaves the issue of equity. Should the Global South be subjected to the same levels of regulation and financial responsibility when they are on the receiving end of climate change impacts despite contributing a mere 10% to the emissions? The principle of CBDR does not support this. Hydrogen governance has to be composed of features that are sensitive to these differences, including technology transfer schemes, funding programs, and diverse regulatory requirements. Without such measures, the hydrogen economy could become part of the problem rather than part of the solution to global inequalities[36].

Can Hydrogen Energy Innovation be shielded from Monopolization under Existing IPR Regimes?

Technological advancements in hydrogen energy and more so green hydrogen technology is one of the most crucial forces transforming the global energy system[37]. However, the current IPR system remains a major hindrance to equal access. So, the critical question is: How to avoid the situation when several large corporations or several countries will dominate in hydrogen development, while the rest of the world will remain in the shadows? Modern IPR systems are commonly protectionist, which means that they issue patents that impede the use of essential technologies by the masses. This is especially so for developing countries which may not have the capital to buy or invest in their hydrogen solutions. The question then becomes: Should international law reform IPR protections to give way to global public goods or not? Some of the potential solutions are compulsory licensing, open-source innovations, and international treaties that allow sharing of the technologies without distorting incentives for innovations. This is why it is not only a legal question of how to protect hydrogen energy innovation from monopolization but also a question of morality. A truly sustainable hydrogen economy cannot thrive if access to its benefits remains concentrated in the hands of a privileged few.

5. Hydrogen Policy and Global Energy Transition

5.1 Key Cases

EU Hydrogen Strategies (2020): A Critical Example of Regulatory Innovation and Trade Tensions

The EU's Hydrogen Strategy launched in 2020 targets to generate between five to ten million tons of renewable hydrogen by 2030 and has identified hydrogen as one of the key enablers of the energy transition in Europe[38-40]. This grand strategy aims to dematerialize numerous segments, such as industry and transportation, and curb greenhouse gas emissions. But does this strategy have the effect of sparking trade tensions? EU's high standards and large subsidies for green hydrogen could harm non-EU exporters, especially developing countries, which cannot afford such investments and do not have the necessary technology. This has made issues of fairness in accessing the growing hydrogen market and the likelihood of trade conflicts to be of major concern; also, this strategy raises questions about compliance with the WTO regulations. The EU's focus on local content requirements and subsidies for domestic hydrogen production may be seen as protectionist practices, which may violate WTO policies that promote free and fair trade. These policies may lead to litigation by non-EU countries challenging the EU's hydrogen plans for compliance with global trade laws.

Neubauer et al. v. Germany (2021): Legal Obligations for Transitioning to Clean Energy

In the Neubauer et al. v. Germany case, the Federal Constitutional Court declared the Climate Protection Act ineffective and the state failed to protect the fundamental rights of young individuals in terms of climate protection after the year 2030[41, 42]. The court ordered the government to set more specific and strict milestones for the protection of future generations[43]. This case raises critical questions: Is current legislation sufficient to prompt the transition to clean energy sources? The ruling shows that the judiciary can and will enforce climate action, and weak or no targets are legally impermissible. It also underlines the need for governments to put in place long-term and coherent climate policies that correspond to constitutional duties towards the rights of people.

5.3 Reports by IEA and IRENA on Hydrogen's Global Potential



Both the IEA and IRENA have conducted comprehensive research on the global capabilities of hydrogen and mentioned that hydrogen would be one of the critical components in the future energy mix. The IEA's Global Hydrogen Review highlights significant growth in hydrogen investments, with the number of projects reaching final investment decisions doubling over the past year, primarily driven by China[44, 45]. This trajectory indicates that low-emission hydrogen production could increase fivefold by 2030. However, there are still issues such as low installed capacity and demand risks due to weak demand signals, and financing, regulatory, and operations barriers. The IEA underlines that policymakers should continue demand creation, decrease costs, as well as define even rules to maintain more investments[46].

According to IRENA, global hydrogen production is currently estimated to be at around 75 MtH₂/yr of pure hydrogen and 45 MtH₂/yr as a component of mixed gases, and it contributes to about 3% of the end-use energy[47, 48]. In the longer term, IRENA expects hydrogen and its derivatives to meet 14% of final energy demand in the year 2050, which will require more than a five-fold increase in global hydrogen production from its current level[44].

While both agencies project substantial growth for hydrogen in the global energy mix, several critical questions arise:

1. Investment and Infrastructure Development: As it is evident from the above results and analysis, that the current installed capacity is still low, what measures can be taken to enhance infrastructure development to suit the projected demand?

Analysis: Efficient infrastructure growth demands policy harmonization, supportive policies from the public and private sectors, and sufficient funds. Both government and industry players need to work together to reduce bureaucratic barriers, offer incentives for adoption, and fund advanced technology improvements.

2. Policy and Regulatory Frameworks: What are the possible measures that policymakers can take to adapt to existing uncertainties and promote the scaling up of hydrogen production and use?

Analysis: There is a need to develop and enforce policies that outline acceptable practices in generating, transporting, and consuming hydrogen. This involves targeting the take-off rates for green hydrogen, applying carbon costs to make low-carbon hydrogen cost-competitive, and establishing safety frameworks to make hydrogen more acceptable to the public.

6. Recommendations Regarding Gaps in Hydrogen Energy Governance

Establishing a Unified Hydrogen Protocol

Hydrogen production and international trade are not currently governed by any set of standardized global regulations. Is the future of hydrogen best served by a patchwork of disjointed national policies or does it require a coherent global system? An International Hydrogen Protocol should be established and anchored under the umbrella of the United Nations. This protocol has to align the definitions of 'clean hydrogen,' which must be consistent across green, blue, and other hydrogen classifications. It should also establish global safety and transportation guidelines to facilitate the efficient export and import of hydrogen and minimize risks. Further, it has to ensure that the protocol encourages sharing technologies and funding mechanisms to help developed and developing countries. If such a strategy does not exist, then the use of hydrogen as an energy source can become scattered and uncoordinated on a global level.

Tackling the IP Barrier

Current frameworks of intellectual property rights provide significant protection to green hydrogen innovation, which is not easily accessible to the countries in the development phase. Is the world ready to leave the fate of the hydrogen transition in the hands of intellectual property monopolies? International law should also provide provisions for compulsory licensing and public-private partnerships to make green hydrogen technologies affordable to developing nations. Similarly, models such as open source for non-critical innovations should be promoted to enhance collaboration. Thus,

the breakdown of these barriers will make hydrogen development more equitable and inclusive across the globe which will be beneficial for the advancement of technology and sustainability.

Improving the International Liability Regime

Accidents involving hydrogen are potentially dangerous to the environment and human beings. Is current regulation sufficient to address these issues? National and international laws, for example, a new Liability Convention for Hydrogen Energy, should outline the responsibilities of parties in case of cross-border hydrogen energy-related accidents and liabilities. Moreover, they should set rules for the safety audit as well as insurance for hydrogen storage and transportation schemes. Thus, the environmental and financial costs associated with liability risks can deter hydrogen's potential as a clean energy source.

Prioritizing Equitable Access for Developing Nations

The industrialized countries, through entities such as the Green Climate Fund, have to provide long-term financing for investments and human resource development in the Global South. They should also adopt variable regulatory measures that are in proportion to economic and technological development. The latter directly contributes to the achievement of the goal to make hydrogen energy available for all countries and bring the hydrogen revolution to everyone.

Accelerating Technological Development

In its current state, hydrogen is expensive and difficult to scale up as a usable energy source. What inventions are needed to overcome these barriers? The governmental and private sectors need to focus on the development of efficient and low-cost electrolyzers and renewable energy sources, good storage, and transportation methods like ammonia-based carriers and hydrogen pipelines. Through speeding up technological development and decreasing the costs of hydrogen energy, the world can move from the stage of exploring a new type of energy to a stage of having a new main type of energy.

7. Conclusion

Hydrogen energy can be viewed as a symbol of the technological advancement and energy revolution that is yet to come, but it also raises questions of the legal nature and equitable transition path. This article has analyzed the legal, economic, and environmental aspects of hydrogen energy governance and brought out the issues of fragmented regulation and trade, calling for international cooperation. Challenges to the hydrogen economy's development include emissions of blue hydrogen and safety issues related to storage, raising questions about liability regimes and international environmental law. The establishment of a Hydrogen Protocol, including changes to Intellectual Property Rights or IPRs, and proper funding frameworks is critical to making hydrogen energy safe, secure, and available in every country. The potential of hydrogen energy to become a global force for climate justice and economic inclusion can only be achieved through international collaboration. It is impossible to wait any longer – this is the time of hydrogen energy and the laws that will govern it.

References

1. Capurso, T., et al., *Perspective of the role of hydrogen in the 21st century energy transition*. Energy Conversion and Management, 2022. **251**: p. 114898.
2. Kovač, A., M. Paranos, and D. Marciuš, *Hydrogen in energy transition: A review*. International Journal of Hydrogen Energy, 2021. **46**(16): p. 10016-10035.
3. Sadik-Zada, E.R., *Political economy of green hydrogen rollout: A global perspective*. Sustainability, 2021. **13**(23): p. 13464.
4. Wappler, M., et al., *Building the green hydrogen market—Current state and outlook on green hydrogen demand and electrolyzer manufacturing*. International Journal of Hydrogen Energy, 2022. **47**(79): p. 33551-33570.
5. Ball, M. and M. Weeda, *The hydrogen economy—vision or reality?* International Journal of Hydrogen Energy, 2015. **40**(25): p. 7903-7919.
6. Bade, S.O., et al., *Economic, social, and regulatory challenges of green hydrogen production and utilization in the US: A review*. International Journal of Hydrogen Energy, 2024. **49**: p. 314-335.
7. Ahmad, I., J. Afzal, and S. Ahmad, *Legal Framework of Green Hydrogen Production and Hydrogen Economy for Sustainable Development*.



8. Boretta, A. and B.G. Pollet, *Hydrogen economy: Paving the path to a sustainable, low-carbon future*. 2024, Elsevier. p. 307-319.
9. Ballo, A., et al., *Law and policy review on green hydrogen potential in ECOWAS countries*. *Energies*, 2022. **15**(7): p. 2304.
10. Ahmad, I., Afzal, J., & Ahmad, S., *Regulatory Analysis of Energy Law and Hydrogen Economy*, in *Legal Framework of Green Hydrogen Production and Hydrogen Economy for Sustainable Development*. 2025. p. 89-111.
11. Dolci, F., et al., *Incentives and legal barriers for power-to-hydrogen pathways: An international snapshot*. *International Journal of Hydrogen Energy*, 2019. **44**(23): p. 11394-11401.
12. Ahmad, I., Afzal, J., & Ahmad, S., *International Conventions and Regional Treaties Shaping the Hydrogen Economy*, in *Legal Framework of Green Hydrogen Production and Hydrogen Economy for Sustainable Development*. 2025. p. 128-154.
13. Bade, S.O. and O.S. Tomomewo, *A review of governance strategies, policy measures, and regulatory framework for hydrogen energy in the United States*. *International Journal of Hydrogen Energy*, 2024. **78**: p. 1363-1381.
14. Andreasson, L.M. and M. Roggenkamp, *Deliverable 2.2, 2.3-Regulatory Framework: Legal Challenges and Incentives for Developing Hydrogen Offshore*. 2020.
15. Bridson, J.H., et al., *Leaching and extraction of additives from plastic pollution to inform environmental risk: a multidisciplinary review of analytical approaches*. *Journal of Hazardous Materials*, 2021. **414**: p. 125571.
16. Legrand, P., *Comparative legal studies and commitment to theory*. 1995, JSTOR.
17. De Cruz, P., *Comparative law in a changing world*. 2024: Taylor & Francis.
18. Hassan, Q., et al., *Hydrogen role in energy transition: A comparative review*. *Process Safety and Environmental Protection*, 2024.
19. Cheekatamarla, P., *Hydrogen and the Global Energy Transition—Path to Sustainability and Adoption across All Economic Sectors*. *Energies*, 2024. **17**(4): p. 807.
20. Hosseini, S.E., *Hydrogen Diplomacy*. 2024: Future Publishing LLC.
21. Kuramochi, T., et al., *Supporting the Paris Agreement through international cooperation: potential contributions, institutional robustness, and progress of Glasgow climate initiatives*. *npj Climate Action*, 2024. **3**(1): p. 31.
22. Islam, A., et al., *Accelerating the green hydrogen revolution: A comprehensive analysis of technological advancements and policy interventions*. *International Journal of Hydrogen Energy*, 2024. **67**: p. 458-486.
23. Hassan, Q., et al., *Hydrogen as an energy carrier: properties, storage methods, challenges, and future implications*. *Environment Systems and Decisions*, 2024. **44**(2): p. 327-350.
24. White, L.V., D. Gourlay, and E. Aisbett, *Potential market failures inhibiting the development of a green hydrogen export industry*, in *Towards Hydrogen Infrastructure*. 2024, Elsevier. p. 39-58.
25. Hassan, Q., et al., *Green hydrogen: A pathway to a sustainable energy future*. *International Journal of Hydrogen Energy*, 2024. **50**: p. 310-333.
26. Ahmad, I., Afzal, J., & Ahmad, S., *Legal Framework for Hydrogen Economy and Future Directions of Global Green Hydrogen Economy*, in *Legal Framework of Green Hydrogen Production and Hydrogen Economy for Sustainable Development*. 2025. p. 155-185.
27. Blay-Roger, R., et al., *Natural hydrogen in the energy transition: Fundamentals, promise, and enigmas*. *Renewable and Sustainable Energy Reviews*, 2024. **189**: p. 113888.
28. Patel, S.K.S., et al., *Recent developments in hydrogen production, storage, and transportation: Challenges, opportunities, and perspectives*. *Fire*, 2024. **7**(7): p. 233.
29. Nnabuike, S.G., et al., *Integration of renewable energy sources in tandem with electrolysis: A technology review for green hydrogen production*. *International Journal of Hydrogen Energy*, 2024.
30. Ashari, P.A. and K. Blind, *The effects of hydrogen research and innovation on international hydrogen trade*. *Energy Policy*, 2024. **186**: p. 113974.
31. Fleming, R., *The Cambridge Handbook of Hydrogen and the Law*. 2024: Cambridge University Press.
32. Flath, L., J. Kemmerzell, and M. Knodt, *Hydrogen governance in Germany: a challenge for federal coordination*. *Regional & Federal Studies*, 2024. **34**(5): p. 757-779.
33. Rigas, F., *Hydrogen Safety: Production, Transport, Storage, Use, and the Environment*. 2024: CRC Press.
34. Olawuyi, D.S., et al., *Net Zero and Natural Resources Law: Sovereignty, Security, and Solidarity in the Clean Energy Transition*. 2024: Oxford University Press.
35. Pereira, E.G., T.L. Muinzer, and P.R. Baker, *Energy Law and the Sustainable Development Goals: Host Government Instruments for Sustainability in Oil and Gas Operations*. 2024: Taylor & Francis.
36. Rifkin, J., *The hydrogen economy*. 2003: Penguin.

37. Winter, C.-J., *Hydrogen energy—Abundant, efficient, clean: A debate over the energy-system-of-change*. International journal of hydrogen energy, 2009. **34**(14): p. S1-S52.
38. Genovese, M., et al., *Power-to-hydrogen and hydrogen-to-X energy systems for the industry of the future in Europe*. International Journal of Hydrogen Energy, 2023. **48**(44): p. 16545-16568.
39. Undertaking, H.J., *Hydrogen roadmap Europe: a sustainable pathway for the European energy transition*. 2019.
40. Lagioia, G., M.P. Spinelli, and V. Amicarelli, *Blue and green hydrogen energy to meet European Union decarbonisation objectives. An overview of perspectives and the current state of affairs*. International Journal of Hydrogen Energy, 2023. **48**(4): p. 1304-1322.
41. Gentile, C., *Climate Change and the Extraterritorial Reach of the State Duty to Protect*, in *Yearbook of Sustainable Smart Mining and Energy 2022: Technical, Economic and Legal Framework*. 2023, Springer. p. 125-142.
42. Ahmad, I., Afzal, J., & Ahmad, S, *Critical Analysis of Hydrogen Energy Development: Germany's Approach to Balancing Economic Rights and Environmental Sustainability*, in *Legal Framework of Green Hydrogen Production and Hydrogen Economy for Sustainable Development*. 2025. p. 112-127.
43. Kotzé, L.J., Neubauer et al. versus Germany: Planetary Climate Litigation for the Anthropocene? German Law Journal, 2021. **22**(8): p. 1423-1444.
44. Marzouk, O.A., *Expectations for the role of hydrogen and its derivatives in different sectors through analysis of the four energy scenarios: IEA-STEPS, IEA-NZE, IRENA-PES, and IRENA-1.5 C*. Energies, 2024. **17**(3): p. 646.
45. Ségur-Eltz, P., *Strategic geoeconomics of hydrogen: shaping Europe's future energy market*. 2024, Technische Universität Wien.
46. Avila, N., et al., *The energy challenge in sub-Saharan Africa: A guide for advocates and policy makers*. Generating Energy for Sustainable and Equitable Development, Part, 2017. **1**: p. 1-79.
47. Khaleel, M., et al., *Towards hydrogen sector investments for achieving sustainable electricity generation*. Journal of Solar Energy and Sustainable Development, 2024. **13**(1): p. 71-96.
48. Monforti Ferrario, A., et al., *Role of Hydrogen in Low-Carbon Energy Future*. Technologies for Integrated Energy Systems and Networks, 2022: p. 71-104.

Declaration

Conflict of Study: The author declare that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable

Declaration of AI Use: Not Applicable





AI-Generated Content and Violation of Human Rights: United Nations Initiatives and International Community Response

Jalil Ahmad ^{1*}

¹Human Rights Institute, Southwest University of Political Science & Law, China

* Corresponding Email: jalilkhan4400@gmail.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.11>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

While technologies offer significant social and economic benefits, they have also new forms of harm, including non-consensual deepfakes, synthetic child sexual abuse material, and large-scale disinformation. These practices pose direct threats to internationally protected human rights, particularly the rights to privacy, dignity, equality, freedom of expression, and participation in public life. The article demonstrates that current international and domestic responses struggle to address challenges related to attribution of responsibility, enforcement, and victim protection in cases involving synthetic media. It concludes that a more targeted, human-rights-based approach to AI-generated content is required, one that moves beyond general ethical principles and provides clear legal guidance, shared responsibility among key actors, and meaningful remedies for affected individuals. This article argues that although the United Nations has increasingly acknowledged the human rights risks associated with artificial intelligence, its existing governance frameworks remain largely abstract and insufficiently tailored to the specific harms caused by AI-generated content. The absence of precise legal standards and enforceable obligations has contributed to fragmented national responses, inconsistent platform accountability, and limited access to effective remedies for victims. Using a doctrinal and policy-analysis approach, the study examines relevant UN initiatives alongside comparative regulatory practices in the United States, European Union, United Kingdom, China, Russia, and Pakistan.

Keywords: AI-Generated Content; Violation of Human Rights; International Community; Human Rights

1. Introduction

AI systems that generate text, images, audio, and video have moved rapidly from experimental tools to influential actors within global information ecosystems. Generative AI now affects how people communicate, form opinions, engage in political processes, and construct social reality[1]. Alongside legitimate uses in creativity, education, and innovation, these technologies have made it significantly easier to fabricate realistic but false content, impersonate individuals, and scale abuse at unprecedented speed[2]. Practices such as non-consensual sexual deepfakes, synthetic child sexual abuse material, and automated disinformation campaigns have transformed the nature of digital harm[3]. These practices directly interfere with internationally protected rights, including privacy, dignity, equality, freedom of expression, and participation in public affairs[4]. Unlike earlier forms of online manipulation, AI-generated content often lacks clear human authorship, complicating traditional legal concepts of intent, responsibility, and liability. At the international level, the United Nations and its agencies have increasingly addressed the human rights implications of artificial intelligence through resolutions, thematic reports, and ethical guidelines[5][6]. Instruments developed by the Office of the High Commissioner for Human Rights and UNESCO reflect a growing consensus that AI systems must operate in ways that respect human dignity and fundamental freedoms[7]. However, these initiatives tend to treat AI as a broad category, offering high-level principles while giving limited attention to the specific and recurring harms produced by generative content.

This article argues that this gap has concrete consequences. The absence of clear, enforceable guidance on AI-generated content at the UN level has contributed to fragmented national responses, uneven



platform practices, weak accountability, and limited access to remedies for victims. By treating AI-generated content as a distinct human rights challenge rather than a secondary issue within general AI governance, this study aims to clarify the nature of the harm, assess the adequacy of existing international frameworks, and identify more effective regulatory approaches grounded in human rights law.

2. AI-Generated Content as a Source of Human Rights Violations

AI-generated content constitutes a direct and practical source of human rights harm rather than a speculative future risk[8]. Generative tools enable the rapid and inexpensive production of highly realistic images, videos, and audio, often without the knowledge or consent of the individuals depicted[9]. This fundamentally alters how violations occur: harm can be inflicted remotely, anonymously, and at scale, with limited traceability and accountability[10]. One of the most severe forms of harm arises in the context of sexual and gender-based abuse. Non-consensual intimate deepfakes disproportionately target women and girls, reinforcing existing patterns of gender inequality. Faces sourced from social media or public records are digitally inserted into explicit material or used to generate entirely fabricated sexual images[11]. Although the content is synthetic, victims experience real consequences, including reputational damage, loss of employment, psychological distress, and social exclusion. These practices violate the rights to privacy and dignity and undermine the principle of non-discrimination under international human rights law[12]. Children face particularly acute risks. Generative AI is increasingly used to produce artificial child sexual abuse material by manipulating real images or generating child-like representations. While such material may not involve direct physical contact with a child, it normalizes sexual exploitation, creates demand for abuse-related content, and may retraumatize identifiable victims whose likenesses are used[13]. These practices undermine children's rights to protection from sexual exploitation and challenge legal frameworks that were designed around the identification of direct perpetrators and victims.

AI-generated content also affects freedom of expression and participation in public life. Deepfake videos and fabricated audio recordings are used to intimidate journalists, discredit political opponents, and target minorities[14]. Rather than facilitating open debate, these practices create hostile environments that silence individuals through fear and harassment. The resulting chilling effect is particularly pronounced for women journalists, human rights defenders, and activists, many of whom withdraw from public discourse to protect their safety[15]. Beyond individual harms, widespread synthetic media erodes the social conditions necessary for the enjoyment of human rights. When realistic images and audio can no longer be trusted, genuine documentation of abuse or wrongdoing may be dismissed as fake, while false content circulates as truth. This collapse of shared factual reference points weakens accountability mechanisms and undermines the right to information. Human rights protection depends not only on formal legal rules but also on public trust in evidence and institutions; AI-generated content increasingly disrupts both. A central concern across these harms is the lack of effective remedies. Victims often face uncertainty about who bears responsibility: the individual user, the platform, or the AI developer. Many legal systems have not yet adapted to address this diffusion of responsibility, leaving victims with slow takedown processes, limited access to compensation, and weak institutional support. This gap between harm and remedy exposes structural weaknesses in existing human rights protection frameworks when confronted with generative technologies[16].

3. Methodology

This study adopts a qualitative doctrinal and policy-analysis approach to examine how AI-generated content gives rise to human rights violations and how these risks are addressed within United Nations frameworks and selected national legal systems. Given that the central issues concern legal responsibility, regulatory design, and access to remedies, doctrinal analysis provides an appropriate method for evaluating the adequacy of existing norms. Primary sources include international human

rights treaties, resolutions and reports of the UN General Assembly and Human Rights Council, thematic reports of UN Special Rapporteurs, and policy instruments issued by bodies such as the Office of the High Commissioner for Human Rights and UNESCO. To assess how international guidance is translated into practice, the study examines legislation and official policy documents from the United States, European Union, United Kingdom, China, Russia, and Pakistan. Secondary sources consist of peer-reviewed academic literature and reports by civil society organizations documenting harms linked to AI-generated content, including non-consensual deepfakes, child sexual abuse material, and coordinated disinformation campaigns. The analysis proceeds in three stages: mapping forms of AI-generated content against affected rights; evaluating how UN instruments conceptualize these harms and allocate responsibility; and comparing national responses to identify areas of convergence, divergence, and regulatory gaps. The study does not include empirical interviews or technical testing. Its contribution lies in clarifying normative and institutional shortcomings and identifying where more precise human-rights-based responses to AI-generated content are required.

4. United Nations Initiatives on AI and Human Rights: Progress and Limitations

In recent years, the United Nations has increasingly recognized the human rights risks associated with artificial intelligence. Various UN bodies, including the Office of the High Commissioner for Human Rights (OHCHR), UNESCO, and the Human Rights Council, have produced reports, resolutions, and policy instruments aimed at promoting a human-rights-based approach to AI governance. These initiatives represent an important step in acknowledging that AI systems can interfere with fundamental rights and must therefore be subject to international human rights standards. The OHCHR has repeatedly warned that AI technologies may undermine rights such as privacy, equality, freedom of expression, and non-discrimination if deployed without adequate safeguards. Similarly, UNESCO's Recommendation on the Ethics of Artificial Intelligence emphasises principles such as human dignity, transparency, accountability, and fairness. These documents reflect a growing consensus that AI governance should not be driven solely by innovation and efficiency but must also prioritize the protection of human rights. However, despite this normative progress, UN initiatives remain largely high-level and abstract when addressing AI-generated content. Most instruments discuss AI risks in general terms and do not sufficiently distinguish between different forms of AI use. As a result, specific and recurring harms caused by generative technologies—such as non-consensual deepfakes, synthetic child sexual abuse material, and AI-driven disinformation—receive limited direct attention. This lack of specificity makes it difficult for states and platforms to translate international guidance into concrete legal obligations.

A key limitation of UN frameworks lies in their reliance on non-binding, ethics-based language. While ethical principles are valuable, they do not create enforceable duties or clear accountability mechanisms. Victims of AI-generated harm are rarely mentioned as rights-holders entitled to effective remedies. UN instruments provide little guidance on who should bear responsibility when harm results from the interaction of users, platforms, and AI developers, leaving significant gaps in protection and enforcement. Moreover, UN initiatives offer limited direction on access to justice and remedies. Issues such as rapid takedown of harmful synthetic content, compensation for victims, and cross-border enforcement are largely absent from existing guidance. This omission is particularly problematic given the transnational nature of AI-generated content and the speed at which harm can spread. Without clearer standards on remedies and due diligence obligations, victims are often left dependent on platform discretion rather than enforceable legal rights.

5. Community Norms and AI-Generated Content

Community norms play a central role in shaping how rights are respected or violated in everyday life. They define informal expectations about consent, privacy, truth, and acceptable behavior, both online and offline. AI-generated content places significant strain on these norms by enabling practices that were previously difficult, costly, or socially discouraged[17]. When realistic synthetic images, videos,

and audio can be produced and shared with minimal effort, behaviors that would once have been seen as clearly abusive or deceptive risk becoming normalized, even in the absence of explicit legal approval. One of the most visible shifts concerns norms around consent and personal dignity. In many societies, there is a widely shared understanding that using another person's image for sexual, humiliating, or deceptive purposes without permission is unacceptable. AI-generated content disrupts this understanding by introducing the claim that harm is reduced when the material is "not real." This framing weakens the social meaning of consent and allows perpetrators to distance themselves from responsibility. As synthetic intimate images and deepfake memes circulate more widely, victims are often expected to tolerate or ignore the abuse, while objections are dismissed as overreactions (Flynn et al., 2025). Over time, this erodes respect for bodily autonomy and personal dignity, particularly for women and girls.

AI-generated content also challenges norms related to truth and trust. Visual and audio media have traditionally carried strong evidentiary weight in public discourse. The spread of convincing synthetic media undermines this assumption, making it harder for communities to agree on what is real. False content can be shared as authentic, while genuine documentation of abuse or wrongdoing can be rejected as fabricated [19][20]. This dynamic weakens the social foundations of accountability and public debate, creating an environment in which deception becomes easier and denial more plausible. The resulting uncertainty does not affect all actors equally; those with power and resources are better able to contest evidence, while marginalized individuals face higher barriers to being believed. Norms governing public participation and speech are also affected. AI-generated harassment, impersonation, and coordinated disinformation campaigns are increasingly used to intimidate journalists, activists, and political opponents. When such practices become common, they reshape expectations about who can safely speak in public and at what cost. Many individuals, particularly women, minorities, and human rights defenders, respond by withdrawing from online spaces or limiting their participation to avoid further harm [21][22]. This informal exclusion does not rely on formal censorship, yet it has a comparable effect on freedom of expression and democratic engagement.

Children and young people are especially vulnerable to these normative shifts. For many, digital platforms are primary spaces for social interaction, learning, and identity formation. Regular exposure to AI-generated sexualized imagery, humiliation, or dehumanizing content can alter perceptions of consent, privacy, and respect. When synthetic manipulation of images is treated as entertainment or humor, young users may internalize the idea that other people's bodies and identities are freely available for modification and circulation. These early normative lessons can have lasting consequences for how rights and boundaries are understood later in life [23]. Online platforms and digital communities play a decisive role in reinforcing or resisting these changes. Platform rules and moderation practices signal what kinds of behavior are tolerated. Where AI-generated abuse remains visible, spreads rapidly, or is inconsistently moderated, users receive an implicit message that such conduct falls within acceptable limits. Conversely, clear labelling of synthetic content, rapid removal of non-consensual material, and visible support for victims can help sustain norms that prioritize dignity and consent [24]. At present, platform responses remain uneven, particularly across languages and regions, contributing to fragmented normative environments. Cultural and social context further shapes how AI-generated content affects community norms. In societies where honor, reputation, and family standing are deeply embedded social values, a single synthetic image can cause severe social consequences, including exclusion or violence against the victim. In other contexts, stronger emphasis on expressive freedom may lead to the initial dismissal of synthetic abuse as harmless or humorous [25]. These differences highlight that AI-generated content does not operate in a social vacuum; it interacts with existing inequalities and power relations, often amplifying them.

6. Key Challenges for AI-Generated Content Regulations

Regulating AI-generated content presents a set of challenges that differ in both scale and nature from earlier forms of digital governance. Existing legal frameworks were largely designed for human-created content, identifiable authorship, and slower modes of dissemination. Generative AI disrupts these assumptions by enabling rapid, large-scale production of realistic content with limited traceability[26]. As a result, even where laws addressing online harm exist, they often struggle to capture the specific risks posed by synthetic media. A first challenge concerns legal definition. Many jurisdictions lack clear and consistent definitions of AI-generated content, deepfakes, or synthetic media. Some legal approaches focus narrowly on impersonation of real individuals, while others rely on broader concepts such as “false” or “manipulated” information. This lack of precision creates uncertainty for courts, regulators, and platforms. Narrow definitions leave harmful practices unregulated, while overly broad rules risk restricting legitimate expression, including satire, artistic work, and political criticism[27]. The absence of clear legal categories also complicates international cooperation, as states often regulate similar harms under incompatible terms.

A second challenge lies in responsibility and attribution. Harmful AI-generated content typically involves multiple actors, including users who generate the content, platforms that host and amplify it, and developers that design and release generative models. Existing liability frameworks rarely clarify how responsibility should be distributed among these actors(Ganai & Naikoo, 2025). Victims therefore face uncertainty about whom to hold accountable and which legal pathways are available. This diffusion of responsibility weakens the right to an effective remedy and allows harmful practices to persist without meaningful consequences. Detection and enforcement present a third major challenge. As generative models become more advanced, distinguishing synthetic content from authentic material becomes increasingly difficult. Technical detection tools exist, but they are unevenly available, often controlled by private companies, and subject to continuous technological competition. Many regulators, courts, and law-enforcement agencies lack the technical expertise or resources required to assess synthetic media reliably[29]. This gap between legal standards and enforcement capacity means that regulatory obligations frequently remain ineffective in practice.

The cross-border nature of digital platforms further complicates regulation. AI-generated content can be created in one jurisdiction, hosted in another, and accessed globally within seconds. National laws on privacy, free expression, and platform liability vary widely, allowing harmful content to circulate through jurisdictions with weaker regulatory oversight[30]. Existing international cooperation mechanisms are slow and poorly adapted to the speed at which synthetic content spreads, leaving victims without timely protection and limiting the reach of domestic enforcement actions. Another significant challenge involves balancing the protection of human rights. Measures aimed at restricting harmful AI-generated content must protect individuals from abuse, exploitation, and disinformation without becoming tools for censorship or political control. In some contexts, broadly framed rules on “fake news” or “misuse of technology” have been used to silence journalists, critics, and human rights defenders[31]. This risk is particularly acute where judicial independence is weak or regulatory powers are concentrated in executive bodies. Effective regulation therefore requires safeguards that prevent abuse while addressing genuine harm. Regulatory dependence on private platforms and technology companies also poses structural concerns. In practice, platforms often act as primary decision-makers regarding content removal, labelling, and visibility. Their policies and enforcement practices are shaped by commercial priorities and vary across regions and languages. Communities in the Global South frequently receive less effective moderation and slower responses, reinforcing existing inequalities in protection. This form of private governance raises questions about transparency, accountability, and democratic oversight in the protection of human rights.

7. Notable Practices from the International Community

Different countries are trying to deal with AI-generated content in very different ways. None of them has a perfect model, but each offers useful ideas for how to protect people’s rights while still allowing

innovation. This section highlights some of the more promising approaches from the USA, EU, UK, China, Russia and Pakistan, especially where they focus on consent, transparency, platform duties and victim protection.

7.1 United States

In the United States, regulation of AI-generated content is mostly built from the bottom up. Many rules come from individual states rather than a single national law. Several states now have specific deepfake laws, for example banning deceptive deepfakes in election campaigns close to voting day, or treating non-consensual sexual deepfakes as a form of image-based sexual abuse[32]. These laws are narrow but practical: they focus on clear harms (election manipulation, sexual exploitation) and give prosecutors concrete tools. A major federal step is the *take it down act 2025*. This law requires online platforms to remove non-consensual intimate “visual deceptions” – including AI-generated deepfake nudes – within a short time after a victim reports them[33]. It creates a standard process: victims can send a notice, platforms must act quickly, and failure to remove content can trigger legal consequences. While it does not solve all problems, it is a strong example of a victim-centered removal regime for AI-generated sexual abuse. The US debate also shows another “best practice”: thinking beyond punishment. Some federal proposals, such as the *deep fakes accountability act*, would require clear labels or watermarks on AI-generated audio, video and images, so that viewers know when content is synthetic. Although these proposals are not yet fully in force, they reflect an important idea: prevention and transparency (for example, labelling and detection tools) should go together with criminal and civil liability[34].

7.2 European Union

The European Union has taken one of the most systematic approaches. The *EU AI Act* (Regulation 2024/1689) is a broad, risk-based law that covers many uses of AI, not just deepfakes. For AI systems that generate or manipulate images, audio or video, the Act creates transparency duties: when content is AI-generated or heavily altered, users should be told clearly, unless this is already obvious[35]. This is meant to protect fundamental rights such as privacy, dignity and freedom of information. The AI Act works together with the *Digital Services Act (DSA)*, which sets strict obligations for very large online platforms. Platforms must assess and reduce “systemic risks”, including disinformation, gender-based violence and election manipulation linked to deepfakes, and they must be more transparent about their content moderation decisions and algorithms[36]. This combination, duties on AI providers plus duties on platforms, is a key feature of the EU model. The EU is also updating its *criminal and victim-protection laws*. A new directive on violence against women and domestic violence recognizes non-consensual intimate images, including those generated with AI, as a serious form of abuse that requires protection and remedies. Reforms to child sexual abuse law also aim to cover AI-generated material involving minors[37]. Taken together, the EU offers a strong example of how to integrate AI-generated content into a wider human-rights and platform-governance framework.

7.3 United Kingdom

The United Kingdom focuses heavily on online safety and image-based abuse. The *Online Safety Act 2023* creates a duty of care for platforms to tackle illegal and harmful content and makes the sharing and threatening to share intimate images, including deepfakes, a criminal offence. Regulators can demand risk assessments, transparency and better reporting tools, especially where children are involved[38]. Building on this, the government has announced new offences that will specifically criminalize the creation of sexually explicit deepfakes, not only their sharing. This is an important shift: it recognizes that harm begins at the point of fabrication, especially when victims are blackmailed or humiliated even before the content goes viral. Enforcement is handled by Ofcom, which has already started to use its powers, for example by fining pornography websites that fail to put strong age-verification and other safety checks in place under the new law[39]. While the Online Safety Act is

controversial and raises free-speech questions, it offers a concrete model of how to combine criminal offences, platform duties and an independent regulator with real sanctions.

7.4 China

China was among the first states to adopt detailed rules directly aimed at synthetic media. The *Administrative Provisions on Deep Synthesis Internet Information Services* require providers of “deep synthesis” tools (including deepfakes) to ensure that AI-generated content is clearly labelled, often through visible marks or watermarks, and not used to create fake news or other illegal information[40]. Providers must also obtain consent before using a person’s biometric data (e.g. face or voice) in deep synthesis services. In 2023, China also introduced the *Interim Measures for the Management of Generative AI Services*, which cover public-facing generative AI models. These measures require service providers to monitor content, respond quickly to illegal use, protect users’ personal information and add marks to AI-generated images and videos in line with the deep synthesis rules. The rules sit on top of broader laws on cyber security, data security and personal information[41]. As a result, China’s framework illustrates a strong “provider-responsibility” model: AI and deepfake service providers are treated as content producers, with duties to label, filter and correct harmful content. From a human-rights perspective, this shows how far proactive obligations can go, but it also raises serious concerns about over-broad content control and the chilling of legitimate expression.

7.5 Russia

Russia does not yet have a single deepfake law, but it has started to regulate AI-generated content through its existing information-control framework[42]. In 2022, *Federal Law No. 32-FZ* changed the Criminal Code to punish the spread of “false information” about the armed forces, which includes manipulated videos and deepfakes used for disinformation about military operations[43]. This links deepfake regulation very closely to national security and information warfare. Public debate in Russia has moved towards more specific rules. Opinion polls and legal discussions show broad support among lawyers and citizens for the idea that deepfakes should be regulated at the legislative level, and lawmakers are considering rules that would require labelling AI-generated content and clarifying liability. The main “best practice” element here is the early recognition that deepfakes are not only a private or civil issue but also a serious challenge for information integrity and public order. At the same time, there is a real risk that such laws can be used to target political speech rather than to protect victims of harassment or sexual abuse.

7.6 Pakistan

Pakistan’s main tool for dealing with online harms is the *Prevention of Electronic Crimes Act (PECA) 2016* updated by later rules and amendments[44]. PECA was written before the deepfake era, but some of its provisions can be used against AI-generated abuse[45]. Section 21 criminalizes image-based abuse, including capturing, editing, sharing or threatening to share sexually explicit images or videos, and digital rights groups now interpret this to cover deepfake sexual content as well[46]. Section 37 gives the Pakistan Telecommunication Authority (PTA) power to remove or block unlawful online content, and has been used to block pornography and other harmful material[47]. In 2025, new amendments introduced Section 26-A, which criminalizes the intentional dissemination of false and fake information online. This can be applied to certain deepfake disinformation campaigns, especially when they target public figures or state institutions[48]. The Federal Investigation Agency’s Cyber Crime Wing investigates cases under PECA and has already registered FIRs against people who allegedly uploaded deepfake “immoral” videos of political leaders. Pakistan also shows how legal measures can be supported by civil society and international partners. Reports by UNFPA and local NGOs document technology-facilitated gender-based violence and deepfake abuse, and call for better victim support, digital evidence handling and specialized training for police and courts. These efforts, together with awareness campaigns about Section 21 PECA, are slowly building a practical response to AI-generated abuse even before a dedicated deepfake law exists[49]. At the same time, scholars and

rights groups' note that PECA's broad language is sometimes used to restrict journalism and free expression, and that the law still does not clearly mention synthetic media or AI-generated content. The lesson from Pakistan is that existing cybercrime and image-based abuse laws can be used as a starting point, but clearer and more balanced rules are needed to deal with AI-generated content in a way that protects both victims and fundamental freedoms.

8. Conclusion

This study shows that AI-generated content is not just a “tech problem” or a “social media issue.” It has become a direct pathway to human rights harm. When synthetic images, videos, and audio are used for non-consensual pornographic deepfakes, child sexual abuse material, targeted harassment, hate campaigns, and political manipulation, the damage is real: people lose dignity, privacy, safety, and equal access to public life. A second key finding is that AI-generated content also weakens community norms that normally protect society. Consent starts to look optional, truth becomes unclear, and online cruelty is treated like entertainment. This creates a dangerous cycle: once harmful synthetic content becomes common, victims are blamed or ignored, and abusers feel encouraged. Over time, the result is a colder and less trustworthy information environment where women, children, minorities, journalists, and human rights defenders carry the heaviest burden. Regulation must be guided by human rights principles, especially dignity, privacy, equality, and child protection, rather than leaving decisions mainly to private companies or treating the issue as a side topic of “general AI governance”.

References

- [1] J. Afzal, “Development of Legal Framework of Digital Laws,” in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, Singapore: Springer Nature Singapore, 2024, pp. 139–154. doi: 10.1007/978-981-97-7106-6_7.
- [2] A. O. Mohamed, “The Effect of Simulating Virtual Scenes using Artificial Intelligence Techniques in Producing Various Media Materials,” *J. Ecohumanism*, vol. 3, no. 8, Nov. 2024, doi: 10.62754/joe.v3i8.4771.
- [3] J. Afzal, “Best Practice of Digital Laws and Digital Justice,” in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*, J. Afzal, Ed., Singapore: Springer Nature Singapore, 2024, pp. 95–120. doi: 10.1007/978-981-97-7106-6_5.
- [4] J. Afzal, *Contemporary Theory of Digitalization (CToD)*. 2026. doi: 10.2139/ssrn.6018858.
- [5] J. Afzal, *Implementation of digital law as a legal tool in the current digital Era*. Springer, 2024.
- [6] J. Afzal, *Exploring the New Horizons of International Law Concerning Globalization of Economy*. Springer Nature.
- [7] F. R. Moreno, “Generative AI and deepfakes: a human rights approach to tackling harmful content,” *Int. Rev. Law Comput. Technol.*, Sept. 2024, Accessed: Jan. 20, 2026. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/13600869.2024.2324540>
- [8] K. de Vries, “Let the Robot Speak! AI-Generated Speech and Freedom of Expression,” in *YSEC Yearbook of Socio-Economic Constitutions 2021: Triangulating Freedom of Speech*, S. Hindelang and A. Moberg, Eds., Cham: Springer International Publishing, 2022, pp. 93–115. doi: 10.1007/16495_2021_38.
- [9] D. V. Voinea, “AI AND COPYRIGHT - WHO OWNS AI GENERATED CONTENT?,” July 2023, doi: 10.5281/ZENODO.15252004.
- [10] Y. Wang, “Synthetic Realities in the Digital Age: Navigating the Opportunities and Challenges of AI-Generated Content,” Aug. 18, 2023. doi: 10.36227/techrxiv.23968311.v1.
- [11] S. Firmino Pinto, “AI Friend? Risks, Implications, and Recommendations on Generative AI for Children,” 2024.
- [12] S. Ali *et al.*, “Children as creators, thinkers and citizens in an AI-driven future,” *Comput. Educ. Artif. Intell.*, vol. 2, p. 100040, Jan. 2021, doi: 10.1016/j.caeai.2021.100040.
- [13] Z. Li, W. Zhang, H. Zhang, R. Gao, and X. Fang, “Global Digital Compact: A Mechanism for the Governance of Online Discriminatory and Misleading Content Generation,” *Int. J. Human–Computer Interact.*, Jan. 2025, Accessed: Jan. 21, 2026. [Online]. Available: <https://www.tandfonline.com/doi/abs/10.1080/10447318.2024.2314350>
- [14] J. Ahmad and A. Haider, “Firewall Technology Testing in Pakistan: The Fine Line Between National Security and Freedom of Expression,” *J. Eng. Sci. Technol. Trends*, vol. 2, no. 1, 2025, Accessed: Jan. 21, 2026. [Online]. Available: <https://journals.scopua.com/index.php/JESTT/article/view/11>
- [15] K. Goth, “AI-Generated Content and the Pollution of the Information Sphere: A Freedom of Expression Analysis under Article 10 ECHR,” Master Thesis, 2025. Accessed: Jan. 21, 2026. [Online]. Available: <https://studenttheses.uu.nl/handle/20.500.12932/49552>



- [16] N. Ahmad, A. W. Ali, and M. H. B. Yussof, "The Challenges of Human Rights in The Era of Artificial Intelligence," *UUM J. Leg. Stud. UUMJLS*, vol. 16, no. 1, pp. 150–169, Jan. 2025.
- [17] R. Q. Idrees, S. Kiyani, and A. Shahid*, "The Role of International Law in Protecting Human Rights Globally," *Law Res. J.*, vol. 3, no. 2, pp. 71–85, May 2025.
- [18] A. Flynn, A. Powell, A. Eaton, and A. J. Scott, "Sexualized Deepfake Abuse: Perpetrator and Victim Perspectives on the Motivations and Forms of Non-Consensually Created and Shared Sexualized Deepfake Imagery".
- [19] T. Yu, Y. Tian, Y. Chen, Y. Huang, Y. Pan, and W. Jang, "How Do Ethical Factors Affect User Trust and Adoption Intentions of AI-Generated Content Tools? Evidence from a Risk-Trust Perspective," *Systems*, vol. 13, no. 6, June 2025, doi: 10.3390/systems13060461.
- [20] J. Afzal, C. Yongmei, A. Fatima, and A. Noor, "Review of various Aspects of Digital Violence," *J. Eng. Sci. Technol. Trends*, vol. 1, no. 2, 2024.
- [21] S. Nasiri and A. Hashemzadeh, "The Evolution of Disinformation from Fake News Propaganda to AI-driven Narratives as Deepfake," *J. Cyberspace Stud.*, vol. 9, no. 1, Jan. 2025, doi: 10.22059/jcss.2025.387249.1119.
- [22] J. Afzal, *Exploring the New Horizons of International Law Concerning Globalization of Economy*. Springer Nature.
- [23] A. Machado, A. Pesqueira, J. Rodrigues dos Santos, A. Sacavem, M. Sousa, and F. Teixeira, "ESG and Digital Transformation in Organizations," 2025, pp. 1–32. doi: 10.1007/978-3-031-86079-9_1.
- [24] C. Easttom, "Malicious Use of Artificial Intelligence," in *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2025, pp. 00499–00507. doi: 10.1109/CCWC62904.2025.10903787.
- [25] M. Krkić, "Cultural perspectives on AI usage and regulation in deepfake creation: how culture shapes AI practices," *Int. Commun. Chin. Cult.*, vol. 12, no. 2, pp. 225–237, June 2025, doi: 10.1007/s40636-025-00330-5.
- [26] H. Qudah, "Tracing the development of environmental, social and governance (ESG) performs: a systematic review and bibliometric analysis," *Future Bus. J.*, vol. 12, Jan. 2026, doi: 10.1186/s43093-025-00705-5.
- [27] K. Ding, "A Tiered Framework for Copyright Ownership in AI-Generated Content," *INNO-PRESS J. Emerg. Appl. AI*, vol. 1, no. 9, Dec. 2025, doi: 10.65563/jeaai.v1i9.52.
- [28] P. A. Ganai and I. A. Naikoo, "The Ethical Paradox of AI-Generated Texts: Investigating the Moral Responsibility in Generative Models".
- [29] G. Pandey, A. Murugan, and V. Pugazhenth, "Generative AI: Transforming the Landscape of Creativity and Automation," *Int. J. Comput. Appl.*, Jan. 2025, doi: 10.5120/ijca2025924392.
- [30] A. Gaidartzi and I. Stamatoudi, "Authorship and Ownership Issues Raised by AI-Generated Works: A Comparative Analysis," *Laws*, vol. 14, no. 4, Aug. 2025, doi: 10.3390/laws14040057.
- [31] M. Anderljung, J. Hazell, and M. von Knebel, "Protecting society from AI misuse: when are restrictions on capabilities warranted?," *AI Soc.*, vol. 40, no. 5, pp. 3841–3857, June 2025, doi: 10.1007/s00146-024-02130-8.
- [32] A. D. Andriani, "The Future of Digital Content: AI-Generated Texts, Images, Videos, and Real-Time Production," in *Impacts of AI-Generated Content on Brand Reputation*, IGI Global Scientific Publishing, 2025, pp. 143–170. doi: 10.4018/979-8-3373-4327-3.ch006.
- [33] T. [R-T. Sen. Cruz, "All Info - S.146 - 119th Congress (2025-2026): TAKE IT DOWN Act." Accessed: Jan. 21, 2026. [Online]. Available: <https://www.congress.gov/bill/119th-congress/senate-bill/146/all-info>
- [34] V. Ugwuoke and M. R. Sanfilippo, "The Current Landscape of Deepfake Legislation in the United States: Analysis of State-Level Responses," *J. Inf. Policy*, June 2025, doi: 10.5325/jinfopoli.15.2025.0004.
- [35] D. Hartmann, J. R. L. de Pereira, C. Streibörger, and B. Berendt, "Addressing the regulatory gap: moving towards an EU AI audit ecosystem beyond the AI Act by including civil society," *AI Ethics*, vol. 5, no. 4, pp. 3617–3638, Aug. 2025, doi: 10.1007/s43681-024-00595-3.
- [36] L. Nannini, E. Bonel, D. Bassi, and M. J. Maggini, "Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act," *AI Ethics*, vol. 5, no. 2, pp. 1241–1269, Apr. 2025, doi: 10.1007/s43681-024-00467-w.
- [37] M. Palade-Ropotan, "MEANS OF PROTECTING VICTIMS OF CRIME AT EUROPEAN LEVEL," *Int. J. Leg. Soc. Order*, vol. 5, no. 1, pp. 1–15, 2025.
- [38] P. Coe, "Tackling online false information in the United Kingdom: The Online Safety Act 2023 and its disconnection from free speech law and theory*," *J. Media Law*, vol. 15, no. 2, pp. 213–242, July 2023, doi: 10.1080/17577632.2024.2316360.
- [39] S. Law, "Effective enforcement of the Online Safety Act and Digital Services Act: unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation," *J. Media Law*, vol. 16, no. 2, pp. 263–300, July 2024, doi: 10.1080/17577632.2025.2459441.

- [40] M. Sheehan, "China's AI Regulations and How They Get Made," *Ho Ri Zo NS*, 2023.
- [41] S. Migliorini, "China's Interim Measures on generative AI: Origin, content and significance," *Comput. Law Secur. Rev.*, vol. 53, p. 105985, July 2024, doi: 10.1016/j.clsr.2024.105985.
- [42] E. Trikoz, E. Gulyaeva, and K. Belyaev, "Russian experience of using digital technologies and legal risks of AI," *E3S Web Conf.*, vol. 224, p. 03005, 2020, doi: 10.1051/e3sconf/202022403005.
- [43] D. Moskwa, "Russia's battle for remembrance. Memory laws in Vladimir Putin's Russia exemplified by the Russo-Ukrainian war," *Rocz. Inst. Eur. Środ.-Wschod.*, vol. 22, no. 1, pp. 105–121, Nov. 2024, doi: 10.36874/RIESW.2024.1.6.
- [44] C. Yongmei and J. Afzal, "Impact of enactment of 'the prevention of electronic crimes act, 2016' as legal support in Pakistan," *Acad. Educ. Soc. Sci. Rev.*, vol. 3, no. 2, pp. 203–212, 2023.
- [45] I. U. Haq and S. M. Zarkoon, "Cyber Stalking: A Critical Analysis of Prevention of Electronic Crimes Act-2016 and Its Effectiveness in Combating Cyber Crimes, A Perspective from Pakistan," *Pak. Multidiscip. J. Arts Sci.*, pp. 43–62, 2023, doi: 10.5281/zenodo.10450177.
- [46] S. Naseer and C. Ashraf, "Gender-Based Violence in Pakistan's Digital Spaces," *Fem. Leg. Stud.*, vol. 30, no. 1, pp. 29–50, Apr. 2022, doi: 10.1007/s10691-021-09473-3.
- [47] S. Khan, P. M. Tehrani, and M. Iftikhar, "Impact of PECA-2016 Provisions on Freedom of Speech: A Case of Pakistan," *J. Manag. Info*, vol. 6, no. 2, pp. 7–11, 2019, doi: 10.31580/jmi.v6i2.566.
- [48] M. A. Abbas and M. R. A. Tullah, "Criminalizing Disinformation in Pakistan: A Constitutional Analysis of Section 26-A of PECA and Freedom of Expression," *Pak. J. LAW Anal. WISDOM*, vol. 4, no. 12, pp. 67–77, Dec. 2025.
- [49] T. Nazakat and F. E. Malik, "Empowering Justice through AI: Addressing Technology-Facilitated Gender-Based Violence with Advanced Solutions," *J. Law Soc. Stud.*, vol. 7, no. 1, pp. 26–42, Mar. 2025, doi: 10.52279/jlss.07.01.2642.

Declaration

Conflict of Study: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.



Women Journalists in Pakistan under Digital Siege: A Human Rights Law Analysis of Platform-Enabled Harassment

Anza Fatima ^{1*}

¹School of Human Rights, Southwest University of Political Science and Law, China

* Corresponding Email: anzeafzal4@gmail.com

Published Online: 24 January 2026 by JCPP

DOI: <https://doi.org/10.64060/ICPP.06>

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy) and powered by International Conference Proceedings Publication (ICPP). Publisher stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Digital harassment of women journalists in Pakistan is not a marginal online problem but a pervasive violation of fundamental human rights that reshapes who can speak, what can be said, and at what cost. This paper situates such harassment within Pakistan's volatile media environment, characterized by censorship, political pressure, and entrenched misogyny, where the rapid uptake of digital platforms has expanded women's visibility while simultaneously deepening their exposure to gendered abuse. It argues with reference to international human rights instruments, including the ICCPR, CEDAW, ICESCR, and their interpretive General Comments and Recommendations, that technology-facilitated attacks on women journalists directly threaten rights to freedom of expression, privacy, and dignity, equality and non-discrimination, freedom from violence, and the right to work in conditions of safety. The analysis traces how specific forms of online violence, such as doxxing, deepfakes, and other sexualized imagery, rape and death threats, and coordinated disinformation or trolling campaigns, produce tangible chilling effects on speech and participation, restricting the professional horizons and everyday security of women journalists. It then turns to Pakistan's domestic legal and policy framework, examining constitutional protections, Articles 14, 19, and 25, the Prevention of Electronic Crimes Act 2016, and the Journalists Protection Act 2021 to show how formal guarantees are undercut by weak implementation, patriarchal institutional cultures, and limited access to effective remedies. In parallel, the paper interrogates the role of global technology companies whose inadequate local language moderation, opaque engagement-driven algorithms, and minimal safety infrastructure in Pakistan create enduring accountability gaps. Building on the UN Guiding Principles on Business and Human Rights, the paper clarifies the complementary responsibilities of the state to protect and of corporate actors to respect and support human rights in digital spaces. On this basis, it advances a set of forward-looking proposals rooted in feminist and human rights-based approaches to digital governance, gender sensitive reform of cybercrime and media law, stronger institutional accountability and independent oversight platform commitments to algorithmic transparency and robust local language moderation, and structured collaboration between state agencies, media organizations, and civil society. Conceptually, the paper frames online attacks on women journalists as a form of structural gender injustice that polices women's presence in the public sphere and erodes the conditions for pluralistic democratic debate. It concludes that building safe, egalitarian, and enabling digital spaces for women journalists in Pakistan is not only a matter of occupational safety but a prerequisite for meaningful press freedom and substantive gender equality.

Keywords: Women Journalists; Human Rights; Platform-Enabled Harassment; Digital Siege

1. Introduction

The digital age has transformed journalism worldwide, offering unprecedented opportunities for connectivity, visibility, and the democratization of voices[1]. Yet, for many women journalists, particularly in Pakistan, this visibility has become a double-edged sword[2]. As digital platforms expand the reach of journalistic work, they also expose women in media to intensified forms of gender-based violence online. The targeting of women journalists is not incidental; it is deeply tied to the intersection of gender, visibility, and political vulnerability. In Pakistan's often volatile media landscape, women journalists occupy a complex position: they are visible symbols of professional



independence in a male-dominated field yet simultaneously subjected to patriarchal scrutiny amplified by digital technologies[3]. Their visibility makes them easily identifiable and accessible online, blurring the line between professional criticism and gendered abuse. Women reporters covering politics, human rights, or military affairs often face especially severe attacks, as their work challenges both power structures and societal gender norms[4]. The backlash is thus not merely personal but structural it seeks to silence women's voices, reassert patriarchal hierarchies, and deter other women from public participation. Unlike many of their male peers, women journalists often navigate online spaces saturated with sexualized threats, character assassination, and explicit intimidation. Troll networks weaponize gender to question women's credibility and morality, employing tactics that exploit cultural stigmas linked to femininity and honor[5]. The result is a form of digital violence that reinforces offline marginalization and renders the journalistic sphere less accessible to women. In this sense, visibility for women journalists, once seen as a marker of professional success now functions paradoxically as a site of vulnerability.

Social media and online platforms have redefined journalism's operational and ethical boundaries[6]. For Pakistani journalists, digital technologies enable real-time reporting, public engagement, and transnational solidarity. Yet they also create what can be described as "harassment ecosystems," where offenders exploit algorithmic amplification, anonymity, and weak moderation to perpetuate gendered abuse. Platforms such as X (formerly Twitter), Facebook, and YouTube become spaces where orchestrated attacks spread rapidly, magnified by coordinated networks and political actors seeking to delegitimize critical reporting. The lack of robust content regulation and accountability mechanisms compounds the problem[7]. Women journalists frequently report that abusive content remains online despite complaints, forcing them to self-censor or withdraw from digital spaces entirely[8]. In a landscape where online identity is integral to professional credibility, this retreat translates into material losses, diminished visibility, fewer opportunities, and exclusion from the public conversation. Digital violence thus transcends individual suffering; it reshapes who gets to participate in knowledge production and public discourse[9].

Analyzing these environments through a socio-legal lens reveals how harassment, when left unaddressed, normalizes gendered subjugation in digital spaces[10]. The online sphere becomes a continuation of patriarchal power, merely translated into algorithmic form. This raises urgent questions about the adequacy of domestic and international legal frameworks in protecting women journalists as both workers and rights-holders in the digital era. Understanding online violence against women journalists requires more than a policy or security response; it demands a rights-based approach grounded in international human rights law. Freedom of expression, equality before the law, and the right to security are all directly implicated. Instruments such as the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) obligate states to ensure both freedom of expression and protection from gender-based violence, including online forms[11-13]. The UN Human Rights Council and UNESCO have repeatedly emphasized that digital violence against women journalists constitutes a breach of multiple rights simultaneously: it restricts freedom of the press, violates dignity, and suppresses gender equality[14].

In Pakistan, however, the implementation gap between international commitments and domestic practice remains significant. While the country's Prevention of Electronic Crimes Act (PECA) 2016 nominally addresses online harassment, enforcement is inconsistent, often weaponized against dissenters, and lacks a gender-sensitive framework[15]. The absence of effective mechanisms to investigate digital abuse against women journalists reflects a broader institutional neglect of both women's rights and freedom of expression[16]. So, Pakistani women journalists operate within a legal paradox: theoretically protected by both domestic and international law yet practically exposed to systematic violations[17].

By bridging human rights law and digital gender-based violence, this research contributes to an emerging field that connects media freedom, technology regulation, and feminist jurisprudence. It exposes how digital spaces in Pakistan operate as contested arenas of rights realization and denial, where women journalists embody the broader struggle for equality, safety, and voice. Through a critical reading of both legal doctrine and digital realities, the study illuminates how addressing online violence is not only essential for women's empowerment but also fundamental to preserving press freedom and democratic participation in the digital age. This study seeks to address three key questions:

- How does platform-enabled harassment affect women journalists in Pakistan?
- Which human rights are violated in such digital violence?
- How do Pakistan's legal frameworks align or fail to align with international human rights standards?

2. Women Journalists in Pakistan

Women journalists in Pakistan occupy a contradictory space in the national media landscape, visible as symbols of modernity and democratic progress, yet deeply vulnerable to misogyny, harassment, and structural exclusion[18]. Their participation has expanded over the past two decades, driven by private news channels, digital platforms, and the rise of social media as a journalistic frontier. But visibility has come at a cost: with greater public engagement comes heightened exposure to political attacks, online hate, and gendered violence. Their experiences reveal how entrenched patriarchy intersects with media precarity and shrinking press freedom, creating a landscape that is both promising and perilous. Pakistan's media operates under chronic threat[19]. The country consistently ranks among the most dangerous places for journalists, where physical attacks, intimidation, and abductions remain common. Political pressures come from multiple fronts: state agencies, political parties, religious groups, and even corporate lobbies that use coercion or censorship to silence dissent. Although constitutional protections exist for freedom of expression, informal restrictions are enforced through red lines on reporting sensitive topics like the military, religion, or separatist movements.

In recent years, increasing digital surveillance and draconian cybercrime laws have further constrained independent journalism. The Prevention of Electronic Crimes Act (PECA) has been used to target critical voices on social media[20]. Women journalists who use these platforms for commentary or accountability reporting face not only state scrutiny but also organized harassment campaigns designed to silence or discredit them. The risks faced by women journalists are not simply additive to those of their male colleagues; they are qualitatively different. Attacks against women often draw from deep reservoirs of misogyny and social conservatism. Female reporters and anchors are routinely subjected to moral policing, accused of violating "cultural values," or demeaned through sexualized insults. Their credibility is attacked not through professional criticism but through character assassination: suggestions that they have "improper" relationships with sources or that their professional success stems from personal compromise.

Such gendered targeting serves a dual purpose: to punish women for entering a public sphere historically dominated by men, and to deter others from following. The harassment is not only verbal but can include doxing, threats of sexual violence, and the circulation of doctored images intended to shame or intimidate. Unlike men, women journalists must constantly negotiate between personal safety, family honor, and professional duty, a balancing act that exhausts emotional and creative energy. While digital media has opened new avenues for journalistic expression, it has also magnified danger[21]. Online platforms sustain a 24/7 news cycle and demand constant visibility what some scholars call "always-on labor". For Pakistani women journalists, this perpetual exposure translates into permanent vulnerability. Every tweet, article, or video becomes a potential flashpoint for abuse.

3. Platform-Enabled Harassment



Digital platforms have transformed journalism, giving women reporters unprecedented visibility and access to audiences[22]. Yet, these same technological infrastructures have enabled new, insidious forms of harassment that threaten not only the safety of women journalists but also press freedom itself. Online abuse is not an isolated or trivial phenomenon; it reflects and reinforces systemic gender inequalities. This section explores how digital platforms facilitate harassment, the architecture that sustains it, and why it must be understood as a gendered human rights concern rather than “mere online abuse.” Digital harassment encompasses a spectrum of threats that range from invasive privacy violations to coordinated disinformation campaigns. While men in media also face trolling, women journalists are subjected to distinct, gendered forms of harm that exploit social stigma, sexuality, and cultural norms.

3.1 Doxxing and stalking

One of the most common and dangerous tactics is doxing, the deliberate exposure of a journalist’s personal information, such as home addresses, phone numbers, or family details, on public forums. Once exposed, women become vulnerable to stalking, blackmail, and even physical attacks[23]. In deeply patriarchal contexts, doxing carries an additional layer of menace[24]: it transforms the digital sphere into a conduit for real-world control, where threats to “come to your house” are not dismissed as online theatrics but as plausible dangers. Many women journalists develop defensive online habits, locking their profiles, using pseudonyms, or deleting their digital footprints to conceal their identities[25]. But such self-protection often limits their professional visibility and mobility, constraining what they can safely report or publish.

3.2 Deepfakes and sexualized imagery

The rise of artificial intelligence has introduced another dimension of abuse through the fabrication of deepfake pornography, realistic yet manipulated videos and images that place a journalist’s face or body onto sexual content. For women, this represents not only a professional weaponization of technology but also a form of psychological violation[26]. Deepfakes rely on the cultural logic of shame and honor: they intend to destroy credibility, instill fear, and silence women by making them appear complicit in their degradation. Even when proven false, these images circulate widely, leaving lasting reputational scars.

3.3 Threats of rape, death, and violence

Direct threats of sexual violence and murder remain routine for women journalists who express critical or oppositional viewpoints[27]. These threats often spike after political commentary or investigative reporting that challenges powerful actors. The goal is intimidation through fear, asserting that a woman’s voice carries a physical cost. Many of these messages combine misogyny with nationalism or religious invective, accusing women of being immoral, Westernized, or agents of foreign powers. Unlike spontaneous trolling, such patterns often suggest organized coercion meant to silence dissenting narratives.

3.4 Coordinated political propaganda

Coordinated abuse frequently originates from political communication networks that weaponize social media for partisan advantage. Women journalists who question state institutions or party leaderships may face blitzes of synthetic outrage: hundreds or thousands of identical posts labeling them “traitors” or “foreign-funded”. These brigades use hashtag campaigns to manipulate algorithmic trends, ensuring that the journalist’s name becomes synonymous with controversy or scandal. The architecture of digital virality turns targeted harassment into entertainment, with each retweet or comment fueling visibility for the abuse[28].

3.5 Character assassination and disinformation

Digital assaults also exploit misinformation ecosystems. Fabricated screenshots, altered quotes, or misrepresented videos are circulated to portray journalists as biased, unprofessional, or morally corrupt. Female reporters are particularly susceptible to rumormongering about their integrity or loyalty[29].

Such tactics erode professional credibility and undermine public trust not only in individuals but in independent journalism. Once misinformation embeds itself in social networks, correction rarely achieves equal reach, a phenomenon scholars call the “liar’s dividend”.

4. International Legal Framework Analysis

Digital harassment of women journalists is not an isolated manifestation of online misconduct; it constitutes a systemic violation of internationally recognized human rights. When women reporters are subjected to digital violence through doxxing, deepfakes, coordinated threats, or reputational assaults the impact extends beyond individual harm[30]. It undermines freedom of expression, erodes privacy and dignity, reinforces gender inequality, perpetuates violence, and compromises the ability of women to exercise their economic and social rights on equal terms[31]. International human rights law, interpreted through treaties such as the International Covenant on Civil and Political Rights (ICCPR), the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), and the International Covenant on Economic, Social and Cultural Rights (ICESCR), provides a coherent framework for analyzing these violations. The UN Human Rights Committee, the CEDAW Committee, and other mechanisms have repeatedly affirmed that states bear positive obligations to prevent, investigate, and remedy gender-based violence—including in digital environments. This section examines these obligations thematically across five key rights domains. At the core of journalism lies the right to freedom of opinion and expression, enshrined in Article 19 of the ICCPR. This right protects not only the ability to express ideas but also the freedom to seek, receive, and impart information. When women journalists are harassed, silenced, or forced offline, this right is directly curtailed. The UN Human Rights Committee’s General Comment No. 34 (2011) provides authoritative guidance on Article 19’s scope. It explicitly states that freedom of expression is indispensable both for individual dignity and societal progress, and that any restrictions must pass strict tests of legality, necessity, and proportionality. Importantly, the Committee underscores that states must create a “safe and enabling environment” for journalists to perform their work, free from threats and harassment. Applying this interpretation, digital attacks that inhibit women journalists’ participation constitute *de facto* violations of Article 19. Even when the state is not the direct perpetrator, failure to prevent or respond to online violence represents a breach of the state’s positive obligation to safeguard expressive freedoms. In Pakistan and other contexts, the proliferation of online gender-based attacks without effective accountability mechanisms negates women’s equal access to the freedoms Article 19 guarantees.

4.1 Right to Privacy and Dignity

Digital harassment frequently involves the invasion of privacy and the degradation of personal dignity. Article 17 of the ICCPR protects individuals from arbitrary or unlawful interference with privacy, family, or reputation. These protections extend fully into digital spaces. Doxxing exposure of home addresses, contact details, or private photographs directly contravenes Article 17’s safeguards. It constitutes an arbitrary interference with privacy because it lacks lawful justification and serves no legitimate public interest. The Human Rights Committee has interpreted Article 17 broadly to include both state and private intrusions where the state fails to provide sufficient legal or practical protection. Cases of women journalists whose personal data appear online accompanied by threats exemplify the composite nature of such violations: they fuse privacy invasion with gender-based intimidation. The mental distress and fear that follow are inseparable from the structural dimension of the harm. While the ICCPR emphasizes privacy, the CEDAW framework highlights dignity as a central concept. Article 5(a) of CEDAW requires states to modify social and cultural patterns that perpetuate stereotypes of gender inferiority. When digital harassment takes the form of sexualized images, degrading memes, or deepfakes, it violates this dignity norm by portraying women as objects of humiliation rather than subjects of rights. The CEDAW Committee’s General Recommendation No. 35 (2017) explicitly extends its protection to online spaces, clarifying that gender-based violence includes “acts that result in or are likely to result in physical, sexual, or psychological harm or suffering to women, whether

occurring in the public or private sphere.” Deepfakes, doxxing, and reputational attacks meet this description.

4.2 Right to Equality and Non-Discrimination

Human rights law is grounded in the principle of equality before the law and protection from discrimination, codified in Articles 2 and 3 of the ICCPR and elaborated in CEDAW Articles 1–2[32, 33]. The targeting of women journalists reveals discriminatory treatment both in frequency and in character: they experience harassment that is inherently gendered, drawing upon sexuality, family roles, and physical appearance in ways male colleagues rarely confront. Data from global organizations such as UNESCO, the International Federation of Journalists (IFJ), and Reporters Without Borders consistently show that women journalists are overwhelmingly more likely to face sexualized online abuse. This constitutes a pattern of discriminatory impact. Such inequality of treatment fulfills CEDAW’s broad definition of discrimination as “any distinction, exclusion or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women of human rights and fundamental freedoms.” Consequently, persistent inaction toward online gendered abuse equates to state complicity in discrimination. States cannot claim neutrality in digital governance while ignoring its gendered consequences.

4.3 Economic and Social Rights

Beyond civil and political rights, online harassment inflicts profound consequences on women’s economic and social rights[34, 35]. The ICESCR guarantees in Article 6 the right of everyone “to gain their living by work which they freely choose or accept” and obligates states to ensure safe and healthy working conditions. Persistent online abuse limits women journalists’ employment prospects. Some employers, seeking to avoid controversy, may sideline or terminate journalists targeted by harassment campaigns. Others decline to hire outspoken women altogether, considering them liabilities. This is a direct infringement on the right to work and on the principle of equal opportunity under Article 7 of the ICESCR. Moreover, self-imposed retreat from digital engagement, often necessary for safety, restricts professional visibility and income. Freelance journalists, in particular, rely on online platforms for networking, sourcing, and publication; their economic viability depends on maintaining an accessible digital persona. When harassment drives them away from these venues, it jeopardizes their right to livelihood.

4.4 Right to work in safe conditions

Article 7(b) of the ICESCR explicitly provides for safe and healthy working conditions. The notion of workplace safety must evolve to include digital workplace environments, spaces where modern journalism is conducted. For women whose reporting relies on digital communication, harassment transforms the online workspace into one of hostility and danger. States and employers share concurrent obligations here. Media organizations must implement workplace policies addressing online harassment as an occupational risk, offering counseling, legal assistance, and digital security support. States, for their part, should require such standards under labor law and provide accessible remedies when violated. The Committee on Economic, Social and Cultural Rights (CESCR) has long held that the right to work entails both opportunity and conditions that respect human dignity[36]. When online violence forces women from their profession or subjects them to constant psychological strain, it compromises this dignity-oriented standard and violates the covenant’s spirit.

5. Pakistan’s Domestic Legal and Policy Framework

5.1 The Constitution of Pakistan

The Constitution forms the normative core of Pakistan’s human rights architecture[37]. Three provisions Articles 14, 19, and 25 establish the principles of dignity, freedom of expression, and equality that collectively underpin protection from digital harassment.

Article 14(1) declares that “the dignity of man and, subject to law, the privacy of home, shall be inviolable.” Although phrased in gender neutral terms, this article grounds constitutional recognition of

dignity as a fundamental right, extending to protection from degradation, public humiliation, and psychological harm. Harassment through doxxing, deepfakes, or sexualized online defamation directly undermines this dignity. Judicial interpretations such as in *Benazir Bhutto v. Federation of Pakistan* (1988) have linked dignity to the right of every individual to live without fear or humiliation. Thus, when women journalists are targeted online with content that shames or sexualizes them, the state's failure to protect constitutes a constitutional lapse.

The privacy dimension of Article 14 has grown increasingly relevant in the digital age. Unauthorized publication of a journalist's personal data or photos amounts to a constitutional interference. Yet, privacy jurisprudence in Pakistan remains nascent, with courts rarely extending this protection to online contexts, and an interpretive gap that leaves many victims without recourse.

Article 19 guarantees the right to freedom of speech and the press, albeit subject to "reasonable restrictions." For journalists, this article is the constitutional foundation of their professional activity. Digital harassment, however, produces the same chilling effect as legal censorship; it coerces silence through fear. The constitutional right to expression, therefore, imposes not only a negative duty on the state to refrain from censorship but a positive obligation to ensure that all persons, including women, can exercise this right safely.

In practice, however, state authorities have often invoked Article 19's restrictions to suppress dissent rather than to protect victims. Women journalists critical of government policies have been accused of "anti-state" activity or subjected to online vilification from official or party-affiliated accounts. The contradiction between formal guarantees and their selective application reveals the fragility of constitutional protections in politically charged digital environments.

Article 25(2) affirms that "there shall be no discrimination based on sex," forming the bedrock of constitutional equality. The state also holds an affirmative obligation under Article 25(3) to make "special provision for the protection of women." These clauses create a compelling legal basis for addressing gender based online abuse. Yet courts and enforcement agencies have been reluctant to treat digital harassment as discrimination, viewing it instead as a technical offense rather than part of gender inequality. Bridging this conceptual gap is essential to realizing constitutional equality in the digital sphere.

5.2 The Prevention of Electronic Crimes Act (PECA)

Enacted to regulate cybercrime, PECA 2016 stands as Pakistan's primary legislative instrument addressing digital offenses. It criminalizes behaviors such as unauthorized access to data, cyberstalking, transmission of offensive content, and the non-consensual use of personal information or images. In principle, these provisions could protect women journalists from precisely the abuses they face.

5.3 The Journalists' Protection Act 2021

The Protection of Journalists and Media Professionals Act 2021 marked a milestone by explicitly acknowledging journalists' safety as a state responsibility[38]. It obliges the government to prevent violence, intimidation, or arbitrary arrest of journalists and to provide assistance where violations occur.

5.4 Institutional Weaknesses

The gap between legislation and implementation lies largely in institutional design. The FIA's Cybercrime Wing functions as the principal enforcement body under PECA, but its capacity to respond effectively to gender-based harassment remains limited.

6. Reforms

6.1 Legal reforms

Amending the Prevention of Electronic Crimes Act (PECA) through a gender lens is a central step. Current provisions address cyberstalking, unauthorized access, and online harassment, but they do not clearly capture the gendered and coordinated nature of attacks against women journalists, including deepfakes, political dogpiling, and networked disinformation. Explicit recognition of technology-facilitated gender-based violence covering threats of sexual violence, non-consensual image use, and

targeted campaigns would help investigators and courts treat these cases as serious rights violations rather than minor “online issues”. Institutional accountability mechanisms also need strengthening. Cybercrime units and the Federal Investigation Agency should be subject to clear performance benchmarks on response times, victim support standards, and case outcomes in complaints involving women journalists. Regular public reporting disaggregated by gender and type of offense would create pressure for improvement and allow civil society to monitor whether laws are functioning as intended. Independent oversight bodies, such as an ombudsperson or a multi-stakeholder digital safety commission, could review complaint handling, recommend disciplinary action where officials fail victims, and advise on necessary procedural reforms.

6.2 Platform responsibility reforms

Given the central role of social media and digital platforms, reforms must also focus on corporate practices[39]. Algorithmic transparency is essential: platforms should be required to conduct and publish human-rights impact assessments that examine how their recommendation and ranking systems affect women journalists, particularly in contexts where political trolling is common. Such assessments can reveal whether outrage-driven ranking is systematically amplifying misogynistic abuse and suggest changes to reduce the visibility of coordinated harassment without suppressing legitimate criticism. Improved local-language moderation is equally critical. Platforms need substantial investment in Urdu and regional-language content review, including partnerships with local experts who understand slang, dog whistles, and political context. This should be matched with clear, accessible safety tools tailored to journalists: prioritized reporting channels for accounts at risk, options to limit replies or mentions during pile-ons, easy evidence-preservation tools, and rapid review of threats that include sexual or physical violence. These features already exist in limited forms in some jurisdictions, but they are often unavailable, invisible, or under-resourced in Pakistan.

7. Discussion

A human-rights-based approach requires that state and industry policies be anchored in principles of equality, participation, accountability, and transparency. National guidelines could clarify the duties of ministries, regulators, law enforcement agencies, and media organizations in preventing and responding to online violence against women journalists. Such guidelines might cover minimum standards for complaint handling, data protection, cooperation with platforms, and the integration of digital safety into journalist protection schemes. Gender-responsive digital safety training should become a core component of professional development in both state and media institutions. For law enforcement and the judiciary, training would focus on understanding technology-facilitated gender-based violence, avoiding victim-blaming, and using digital evidence effectively. For media houses, it should address newsroom protocols for supporting targeted staff, risk assessment for online work, and responsible use of staff social media guidelines that do not penalize women for being visible. Collaboration between NGOs, media organizations, and state agencies can help design curricula that reflect lived experiences and international best practices while remaining locally grounded. Multi-stakeholder coordination is vital. NGOs bring survivor-centered perspectives and monitoring expertise, media houses understand professional pressures and newsroom culture, and state agencies hold regulatory and enforcement powers. Structured forums, such as national task forces or permanent working groups, can enable these actors to share data, evaluate policy impacts, and refine interventions over time.

Feminist frameworks emphasize that digital harassment of women journalists is not a personal failing to be managed through resilience or better “online hygiene,” but a systemic gender injustice rooted in power inequalities. Moving from individualized coping to structural protection means shifting the focus from advising women to stay silent, hide, or toughen up, toward transforming the conditions that make harassment effective: platform design, impunity, patriarchal norms, and precarious employment structures. Recognizing online harassment as a systemic problem reframes it as an issue of collective responsibility. This perspective supports demands for binding obligations on platforms, proactive state

regulation consistent with international human rights law, and institutional reforms within media organizations to share the burden of risk rather than offloading it onto individual women. It also validates the emotional and professional harm experienced by survivors, positioning psychological safety and dignity as non-negotiable components of journalistic freedom. Embedding feminist approaches into digital safety policy encourages intersectional analysis, considering how gender interacts with class, ethnicity, language, and political identity to shape risk. For women journalists in Pakistan, this means acknowledging that those from marginalized communities or covering sensitive beats may face heightened danger and therefore require tailored protections. Ultimately, pathways forward must aim not merely to help women endure hostile digital environments, but to transform those environments so that visibility no longer comes at the cost of safety and equality.

8. Conclusion

Digital harassment of women journalists in Pakistan emerges from the intersection of shrinking press freedom, patriarchal norms, and insecure digital architectures, and it systematically undermines their rights to expression, equality, safety, and work. The preceding analysis has shown how online abuse, ranging from doxxing and deepfakes to coordinated trolling and threats of sexual violence, operates as a tool of gendered control rather than random incivility. It exploits existing social stigmas, reinforces harmful stereotypes, and drives women out of digital and professional spaces that are essential to democratic life. Understanding this phenomenon through a human rights lens makes clear that digital harassment is a serious rights violation, not a peripheral “online issue.” It impairs women journalists’ freedom of expression, invades their privacy and dignity, entrenches discrimination, and contributes to a broader continuum of gender-based violence. International frameworks, particularly the ICCPR, CEDAW, and ICESCR, as interpreted through General Recommendations 33 and 35, confirm that states have positive duties to prevent technology-facilitated violence, address structural inequalities, and ensure access to justice. When women self-censor, leave journalism, or withdraw from online spaces due to fear and exhaustion, the harm is both individual and collective: public debate is narrowed, accountability weakens, and society loses vital perspectives. The urgency of reform lies in the scale and normalization of these harms. Domestic laws such as the Prevention of Electronic Crimes Act and journalists’ protection measures remain under-implemented, prone to political misuse, and largely insensitive to gendered dynamics.

References

1. Pandey, S., *Media in the Digital Age: Trends, Tools, and Cultural Impact*. 2025: Academic Guru Publishing House.
2. Adnan, M., *A double-edged sword? The role of mobile media in press freedom in Pakistan*. Mobile Media & Communication, 2025: p. 20501579251343754.
3. Afzal, J., et al., *Review of various Aspects of Digital Violence*. Journal of Engineering, Science and Technological Trends, 2024. **1**(2).
4. Konow-Lund, M. and M. Høiby, *Female investigative journalists: overcoming threats, intimidation, and violence with gendered strategies*. Journalism Practice, 2023. **17**(8): p. 1591-1606.
5. Snyder, C.K., *Navigating online misogyny: strategies, methods, and debates in digital feminism*. Feminist Studies, 2022. **48**(3): p. 776-789.
6. Afzal, J., *Implementation of digital law as a legal tool in the current digital Era*. 2024: Springer.
7. Afzal, J., *Legal challenges regarding digital operations*, in *Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 23-45.
8. Posetti, J., et al., *Online violence against women journalists*. Book Online Violence against Women Journalists’, edn., UNESCO, 2020.
9. Afzal, J., *Comparative Review on Acceptance of Digital Evidence within the Legal Frameworks of Pakistan and China*. International Journal of Law and Legal Advancement, 2025. **1**(1).
10. Sharma, S. and T. Alam, *MAPPING DIFFERENCES IN SEVERITY OF CYBER HARASSMENT: A SOCIO-LEGAL STUDY OF GENDERED EXPERIENCES IN INDIA*. Cyber Threat: Navigating Legal Challenges in the Digital Age Volume 2, 2025: p. 19.

11. Alfredsson, G. and A. Eide, *The Universal Declaration of Human Rights: a common standard of achievement*. 2023: Martinus Nijhoff Publishers.
12. Joseph, S., *International covenant on civil and political rights (ICCPR)*. 2022, Edward Elgar Publishing.
13. Orta, L.C.G., *The Convention on the Elimination of all forms of Discrimination Against Women (CEDAW): from its radical preamble to its contemporary intersectional approach*. *Women's History Review*, 2025. **34**(1): p. 79-92.
14. Lu, A., J. Posetti, and N. Shabbir, *Legal and normative frameworks for combatting online violence against women journalists*. 2022.
15. Yongmei, C. and J. Afzal, *Impact of enactment of 'the prevention of electronic crimes act, 2016' as legal support in Pakistan*. *Academy of Education and Social Sciences Review*, 2023. **3**(2): p. 203-212.
16. Posetti, J., et al., *The chilling: Global trends in online violence against women journalists*. New York: United Nations International Children's Emergency Fund (UNICEF), 2021.
17. Jamil, S., *Suffering in silence: The resilience of Pakistan's female journalists to combat sexual harassment, threats and discrimination*. *Journalism Practice*, 2020. **14**(2): p. 150-170.
18. Baloch, H.u.R., et al., *Pakistani women journalists: Occupational hazards in their intersectionalities of gender, culture and profession*. *Journalism Practice*, 2025. **19**(9): p. 1986-2002.
19. Malik, Z.U.A., et al., *Globalization and threat to the security of Pakistan*. *Linguistica Antverpienisa*, 2021. **3**(3): p. 4918-4946.
20. Haider, W., A. Ali, and M. Zubair, *Prevention of Electronic Crime Act, 2016: An Analysis of the Act's Effectiveness in Controlling Misuse of Social Media in Pakistan*. *Journal of Educational Research and Social Sciences Review (JERSSR)*, 2023. **3**(2): p. 48-54.
21. Afzal, J., *Development of Legal Framework of Digital Laws, in Implementation of Digital Law as a Legal Tool in the Current Digital Era*. 2024, Springer. p. 139-154.
22. Gupta, S.S., *DIGITAL REVOLUTION: JOURNALISM IN THE INTERNET AGE*. *HISTORY OF JOURNALISM*: p. 65.
23. Sobieraj, S., *Credible threat: Attacks against women online and the future of democracy*. 2020: Oxford University Press.
24. Anderson, B., *Doxxing to destroy: The convergence of transphobic hate speech and non-consensual disclosure on X*. *Crime, Media, Culture*, 2025: p. 17416590251345736.
25. Posetti, J., *The new frontline: Women journalists at the intersection of converging digital age threats*, in *Insights on Peace and Conflict Reporting*. 2021, Routledge. p. 121-138.
26. Harris, B.A., *Technology and violence against women*, in *The Emerald handbook of feminism, criminology and social change*. 2020, Emerald Publishing Limited. p. 317-336.
27. Baker, A. and U.M. Rodrigues, *Reporting on sexual violence in the# MeToo era*. 2022: Taylor & Francis.
28. Duncombe, C., *Social media and the visibility of horrific violence*. *International Affairs*, 2020. **96**(3): p. 609-629.
29. Yadav, M. and P. Dutta, *Navigating Online Hostility: Gendered Trolling of Indian Women Journalists, Legal Interventions, and the Role of Media Literacy*. 2025.
30. Fatima, A., et al., *Reproducing Rights: How New Technologies Challenge the Legal Foundations of Genetic Relatedness and Human Dignity*.
31. Amjad, B., et al., *Towards Automation and Digital Justice: A Review of Digital Twin Technology for Automation in Justice System*. *Journal of Asian Development Studies*, 2025. **14**(3): p. 49-62.
32. Fatima, A., A. Haider, and A. Batool, *The Human Rights Implications of Scientific Progress: A Case Study on Gene Editing and Disability Rights*. *Journal of Engineering, Science and Technological Trends*, 2025. **2**(1).
33. Chakraborty, S., *Human Rights Approaches to Gender-Based Poverty: Evaluating the Role of CEDAW and ICESCR in Promoting Equality*. 2025.
34. Jain, M., *FUTURE DIRECTIONS IN WOMEN'S HUMAN RIGHTS ADVOCACY: TOWARDS NEW PATH*. *A HANDBOOK OF WOMEN'S HUMAN RIGHTS*: p. 90.
35. Afzal, J., *International Law and Emerging Economic Issues*, in *Exploring the New Horizons of International Law Concerning Globalization of Economy*. 2026, Springer. p. 79-95.
36. Gomes, V.B., *The right to work and rights at work*, in *Research handbook on economic, social and cultural rights as human rights*. 2020, Edward Elgar Publishing. p. 227-249.
37. Sajid, Z. and M.A. Asim, *Evaluating the Fundamentals of Human Rights in South Asia: A Comparative Analysis with a Focus on Pakistan*. *Insights of Pakistan, Iran and the Caucasus Studies*, 2024. **3**(3): p. 1-11.
38. Salman, H.M., *Historical Evolution of Media Laws in Pakistan*. Available at SSRN 4746518, 2023.
39. Rochefort, A., *Regulating social media platforms: A comparative policy analysis*. *Communication Law and Policy*, 2020. **25**(2): p. 225-260.

Declaration

Conflict of Study: The author declare that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.



Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of AI Use: The author declares that the AI tool "ChatGPT" was used to assist with drafting in the preparation of this manuscript. All content was critically reviewed, verified, and edited by the author, who take full responsibility for the accuracy and integrity of the work.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable