



Role of Digital Public Infrastructure (DPI) in Strengthening AML/KYC for Developing Economies

Muhammad Nawaz Shahid ^{1,2*}

¹Public Prosecution Department, Government of Punjab, Pakistan

²Human Rights Institute, Southwest University of Political Science & Law, China

* Corresponding Email: muhmmadnawazshahid719@gmail.com

Received: 21 December 2025 / Revised: 05 March 2026 / Accepted: 09 March 2026 / Published online: 11 March 2026

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/>). International Journal of Law and Legal Advancement (IJLLA) ISSN(e) 3105-0034 published by Scientific Collaborative Online Publishing Universal Academy (SCOPUA). SCOPUA stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

ABSTRACT

Digital Public Infrastructure (DPI) has emerged as a transformative framework for enhancing financial governance and strengthening regulatory compliance in developing economies. This paper examines the role of DPI in reinforcing Anti-Money Laundering (AML) and Know Your Customer (KYC) mechanisms, with particular focus on Pakistan. This study analyzes how Pakistan's evolving digital ecosystem, particularly the national digital identity system managed by the National Database and Registration Authority (NADRA) and digital payment initiatives led by the State Bank of Pakistan, contributes to strengthening AML/KYC compliance. The research employs a qualitative case study approach, reviewing policy documents, regulatory frameworks, and existing literature to evaluate the effectiveness of DPI-based systems in improving compliance mechanisms. The findings suggest that DPI significantly improves the efficiency, accuracy, and scalability of AML/KYC processes. However, challenges remain, including data privacy concerns, regulatory capacity gaps, and the need for stronger institutional coordination. The paper concludes that strategic investment in DPI, accompanied by robust legal safeguards and international cooperation, can substantially strengthen financial integrity frameworks in developing economies.

Keywords: Digital Public Infrastructure; AML/KYC; Developing Economies; Pakistan

1. Introduction

The integrity of the global financial system is continuously challenged by the unlawful flows of money generated from criminal activities, corruption, and the financing of terrorism (Gaviyau and Sibindi 2023). To combat this, countries worldwide have adopted strict regulatory frameworks centered on Anti-Money Laundering (AML) and Know Your Customer (KYC) protocols (Rusman and Budianto 2025, Afzal 2026). These measures require financial institutions to verify the identities of their clients, understand the nature of their transactions, and report any suspicious activity to the authorities (Sterling 2015). However, for developing economies, implementing these standards is particularly hard. These nations often struggle with deeply rooted informal economies, a lack of reliable identification documentation among large segments of the population and limited technological resources within their regulatory bodies (Centeno and Portes 2006, Meagher 2013). This creates a significant compliance gap, where the rigorous standards set by international bodies like the Financial Action Task Force (FATF) clash with the practical realities on the ground.

Scholars and policy analysts have widely documented the challenges developing countries face in meeting international AML/KYC standards (Thommandru and Chakka 2023, Gaisina and Finger 2025). A significant body of literature highlights the "de-risking" phenomenon, where global banks sever ties with local financial institutions in high-risk jurisdictions, further isolating them from the global financial system (També Bearpark and Demetis 2022, Pilkington 2024). Other studies have focused on the limitations of traditional, paper-based KYC methods, which are not only costly but also highly prone to forgery and human error in contexts where documentary infrastructure is weak (Malhotra, Saini et al. 2022, Mansoor, Antora et al. 2023). More recently discussion has shifted toward the potential of technology, with research exploring the role of biometrics, blockchain, and digital identity in creating stronger and more inclusive AML frameworks. The concept of Digital Public Infrastructure (DPI), comprising national digital ID, real-time payment systems, and data exchange platforms, has been identified by institutions (Mazzucato, Eaves et al. 2024, Dhiman and Madan 2025). The World Bank and the Bank for International Settlements serve as a foundational layer that can address these long-standing challenges by enabling remote, secure, and instant identity verification (Paleti 2025).

Despite this growing global interest in DPI as a tool for financial governance, there remains a noticeable gap in the literature. Especially when it comes to in-depth, empirical case studies from developing nations that are in the phase of building and implementing such infrastructure. Much of the existing research remains theoretical or focuses on the technological aspects in isolation, without examining the complex balance between DPI, regulatory enforcement, and real-world financial crime outcomes. This paper seeks to fill that gap by focusing on Pakistan, a country that offers a unique and timely laboratory for investigation. Pakistan has developed world-class DPI assets, most notably its national identity system managed by NADRA. Its simultaneous struggle to exit the FATF grey list and expand financial inclusion presents a critical paradox worth exploring. This research is therefore essential for providing evidence-based insights that can guide policymakers in Pakistan and other emerging economies seeking to join digital transformation for a more secure and equitable financial future.

2. Conceptual Framework: DPI and AML/KYC

2.1 Digital Public Infrastructure

Digital Public Infrastructure (DPI) refers to a set of shared digital systems that are secure, interoperable, and designed to enable the delivery of public and private services at a population scale (Clark, Marin et al. 2025, Sakyi-Nyarko, Ahmad et al. 2026). Unlike siloed digital tools or platforms developed by individual private sector entities, DPI is typically built and governed as a public good, allowing both government agencies and private enterprises to build innovative services upon it. Drawing on frameworks developed by institutions such as the World Bank and the Bank for International Settlements, DPI can be understood as resting on three foundational pillars. The first is a “digital identity system”, which provides a unique, verifiable, and often biometrically secured identity to every resident or citizen (Akhison 2025). The second is a “real-time payment system”, which enables instant, low-cost digital transactions between individuals, businesses, and government entities (Oleti 2025). The third is a “consent-based data exchange layer”, which allows individuals to securely share their personal data across different service providers with their explicit permission. Together, these three layers create a digital fabric upon which an inclusive and transparent financial ecosystem can be built. India's "India Stack" is perhaps the most cited example of such infrastructure, but other nations, including Pakistan with its NADRA-led digital identity system, are actively developing similar architectures tailored to their national contexts.

2.2 How DPI Enhances AML/KYC

The integration of DPI into a country's financial regulatory framework fundamentally transforms how AML/KYC compliance is conducted, shifting it from a manual, document-heavy, and often irregular process to one that is digital, continuous, and verifiable in real-time (Akbar, Hussain et al. 2025, Islam 2025). This enhancement operates through several distinct mechanisms. First, DPI enables “biometric and cryptographic identity verification”. When a national digital ID is linked to biometric data such as fingerprints or iris scans, financial institutions can verify a customer's identity with near-absolute certainty. This eliminates the risk of identity fraud associated with forged paper documents and ensures that each individual is who they claim to be. In Pakistan, for example, banks can verify a customer's identity against NADRA's database in seconds, a process that previously required physical document inspection and manual verification (Abro, Maitlo et al. 2025). Second, DPI facilitates “interoperability and data sharing”. With a secure data exchange layer, financial institutions can access verified customer data from government sources such as tax records or utility bill histories with the customer's consent. This not only streamlines the onboarding process but also enables more sophisticated risk profiling. A customer's transaction patterns can be cross-referenced with other official data to identify irregularities that may indicate money laundering or other illicit activities.

Third, DPI supports “continuous monitoring and auditability”. Traditional KYC is often a point-in-time exercise conducted when an account is opened, after which customer information may become outdated. DPI-enabled systems allow for ongoing verification, where any changes in a customer's status, such as a change of address or legal name, can be automatically updated across all linked financial accounts. Furthermore, every verification and transaction leave a digital trail that can be audited by regulators, creating a transparent and tamper-evident record of compliance. Fourth, DPI promotes “financial inclusion”, which indirectly strengthens AML/KYC regimes. When individuals are brought into the formal financial system through accessible digital wallets and mobile banking platforms, their transactions become visible to regulators and subject to monitoring. This reduces the size of the informal economy, where cash-based transactions often serve as a veil for illicit financial flows. By lowering the cost of compliance and customer onboarding, DPI makes it economically viable for financial institutions to serve low-income and rural populations who were previously excluded (Gandhi and Kak 2025, Harish, Sharma et al. 2025). Likewise, DPI enables “regulatory innovation” through tools like “supervisory technology” or SupTech. Regulators can leverage the data generated by DPI systems to conduct real-time monitoring of the financial sector, identify emerging risks, and target their enforcement efforts more effectively. The State Bank of Pakistan, for instance, may implement data analytics tools to better understand money laundering risks across the banking system.

3. Methodology

This study employs a qualitative case study research design to examine the role of Digital Public Infrastructure (DPI) in strengthening AML/KYC frameworks in developing economies, with a specific focus on Pakistan. A case study

approach is appropriate as it allows for an in-depth, contextually grounded exploration of a contemporary phenomenon within its real-world setting.

3.1 Data Collection Sources

Data was gathered from diverse secondary sources to ensure comprehensiveness and triangulation. Academic literature was sourced from Google Scholar, JSTOR, and Scopus using keywords such as "Digital Public Infrastructure," "AML/KYC," "digital identity," and "Pakistan". This provided the conceptual foundation for the study. Government and regulatory publications were collected from the official websites of the National Database and Registration Authority (NADRA), the State Bank of Pakistan (SBP), and the Financial Monitoring Unit (FMU). These included annual reports, AML/KYC regulations, and branchless banking guidelines. International organization reports from the Financial Action Task Force (FATF), Asia/Pacific Group on Money Laundering (APG), World Bank, and IMF were reviewed to understand Pakistan's compliance status and international benchmarks. News media and investigative journalism from Pakistani publications such as Dawn, The News International, and The Express Tribune were consulted to identify notable money laundering cases and their implications. Industry and think tank reports on digital finance and financial crime in Pakistan supplemented the analysis with practitioner perspectives.

3.2 Time Frame and Selection Criteria

The study primarily focuses on materials published between January 2020 and December 2025. This five-year window captures the most recent developments in Pakistan's digital transformation and FATF-related compliance efforts. Foundational documents published before 2020 were included where necessary for context. Selection was guided by principles of authority, relevance, and credibility, prioritizing peer-reviewed articles, official documents, and reports from recognized organizations.

3.3 Limitations

This study has certain limitations due to time and constraints. Reliance on publicly available secondary data means internal perspectives of regulators and financial institutions may not be fully captured. The rapid evolution of both DPI and financial crime means some findings may become outdated. The single-country focus, while allowing depth, limits generalizability to other contexts. Nevertheless, the rich detail of the Pakistani experience offers valuable insights for comparative research and policy learning in other developing economies.

4. Case Study of Pakistan

Pakistan offers a compelling rationale for selection as a case study due to its unique convergence of demographic scale, digital momentum, and regulatory pressure. As the world's fifth most populous country, including a young and increasingly technologically proficient population, Pakistan presents both significant challenges and opportunities for implementing AML/KYC frameworks (Arif, Gul et al. 2022, Liaquat 2025). Critically, Pakistan possesses one of the developing world's most sophisticated national digital identity systems, operated by NADRA, which has issued over millions of biometrically secured Computerized National Identity Cards (CNICs) that enable real-time identity verification for financial services (Malik 2022, Mohsin 2025). Furthermore, Pakistan's recent experience on the FATF Grey List (2018-2022) created intense regulatory pressure to strengthen its AML/CFT regime, accelerating the integration of digital infrastructure into compliance processes. The combination of a large unbanked population, world-class digital identity assets, and recent FATF-driven reforms makes Pakistan an ideal case study for examining how DPI can simultaneously enhance financial integrity and expand financial inclusion.

4.1 Role of NADRA in Pakistan

The National Database and Registration Authority (NADRA) serves as the cornerstone of Pakistan's Digital Public Infrastructure and plays a pivotal role in enabling robust KYC compliance across the financial sector (Rehman 2026). NADRA is particularly valuable for AML/KYC purposes because of its integration of biometric data, including fingerprints and photographs, into each identity record, creating a verifiable and tamper-resistant link between an individual and their legal identity. It provides a centralized verification platform, accessible to banks, microfinance institutions, and digital wallet providers through secure Application Programming Interfaces (APIs). This allows financial institutions to verify a customer's identity against the government's official database in real-time, eliminating the need for manual document inspection and reducing the risk of identity fraud. The Biometric Verification System (BVS), launched in collaboration with the State Bank of Pakistan, enables banks to authenticate customers through fingerprint scans at the point of account opening, ensuring that the person presenting themselves is the legitimate cardholder. NADRA facilitates enhanced due diligence for higher-risk customers. When a financial institution identifies a customer or transaction that requires additional scrutiny, NADRA's database can be queried for supplementary information, such as family lineage, address history, or death records, helping to build a more comprehensive risk profile. This capability proved particularly valuable during Pakistan's FATF-mandated reforms, where authorities needed to demonstrate that beneficial ownership information and customer identities could be reliably verified. NADRA supports ongoing monitoring and updating of customer information (Baloch 2025). Through its automated systems, NADRA can notify financial institutions when a customer's CNIC expires, is renewed, or is cancelled due to death or a change in legal status. This enables banks to keep their customer records current, a key requirement of international KYC standards.

4.2 Digital Wallets in Pakistan



Digital wallets have emerged as a transformative force in Pakistan's financial landscape, particularly in advancing both financial inclusion and KYC compliance(Iqbal and Noman 2025, Malik, Khan et al. 2025). Operated under the State Bank of Pakistan's Branchless Banking Regulations, digital wallets such as JazzCash, Easypaisa, Keenu, and SadaPay allow users to perform financial transactions through their mobile phones without requiring a traditional bank account. As of 2024, these platforms collectively serve over 50 million active users, many of whom were previously unbanked and outside the formal financial system(Butt 2025, Shoaib, Shoaib et al. 2025). The KYC process for digital wallets operates on a tiered model, balancing accessibility with regulatory compliance. At the lowest tier, users can open a wallet with basic, simplified due diligence, allowing small-value transactions to promote financial inclusion. For higher transaction limits, wallets require biometric verification through NADRA's database, ensuring the customer's identity is authenticated against the national registry. This integration enables digital wallet providers to onboard customers remotely while maintaining compliance with AML regulations.

Digital wallets contribute to AML/KYC objectives in several ways(Hasan, Talukder et al. 2024, Oludoyi 2025). First, they create a digital transaction trail for millions of individuals who previously operated entirely in cash, bringing previously invisible economic activity under regulatory oversight. Second, the biometric verification requirement at account opening prevents the creation of fake or anonymous accounts. Third, these platforms employ transaction monitoring systems to detect suspicious patterns, such as unusually large cash-ins or rapid movement of funds, which are reported to the Financial Monitoring Unit. However, challenges persist; the tiered KYC model, while inclusive, creates potential loopholes where multiple low-limit wallets could theoretically be used to circumvent transaction limits. Additionally, agent networks responsible for onboarding customers in rural areas have occasionally been implicated in fraudulent verifications.

4.3 Mobile Banking in Pakistan

Mobile banking represents the more sophisticated tier of Pakistan's digital financial ecosystem, offering full-fledged banking services through smartphone applications(Bouza, Hlayhel et al. 2024, Harichandana 2025). Unlike digital wallets, which are often linked to branchless banking accounts, mobile banking is provided by traditional commercial banks such as HBL, National Bank, UBL, and Meezan Bank, allowing existing account holders to conduct transactions, manage accounts, and access financial services remotely. From an AML/KYC perspective, mobile banking applications serve as a critical compliance touchpoint. When customers are onboarded through mobile apps, banks are required to perform the same level of due diligence as they would for in-person account opening. This is achieved through integration with NADRA's verification systems, where customers submit photographs of their CNICs and perform liveness checks or video calls to confirm their identity. Some banks have begun experimenting with e-KYC (electronic KYC) solutions, allowing fully paperless account opening subject to biometric verification. Mobile banking strengthens AML compliance through several features. Transaction monitoring algorithms analyze customer behavior in real-time, flagging unusual patterns such as high-value transactions inconsistent with a customer's profile, rapid movement of funds across multiple accounts, or transactions with high-risk jurisdictions. Many mobile apps now incorporate geo-location tracking and device fingerprinting to detect anomalies, such as a transaction attempted from a location inconsistent with the customer's registered address. Additionally, mobile banking platforms generate auditable digital records of all customer interactions, providing regulators with transparent evidence of compliance. The COVID-19 pandemic significantly accelerated mobile banking adoption in Pakistan(Ahmed, Naz et al. 2022). The State Bank of Pakistan actively encouraged digital onboarding during lockdowns, issuing temporary relaxations while maintaining KYC rigor through biometric verification. This period demonstrated that mobile banking could serve as both a tool for financial inclusion and a robust platform for regulatory compliance.

5. Implementation of AML/KYC

5.1 Current Status of Implementation

AML/KYC implementation in Pakistan operates through a multi-layered regulatory architecture. The primary regulators include the State Bank of Pakistan (SBP), which oversees banks, microfinance institutions, and digital financial services; the Securities and Exchange Commission of Pakistan (SECP), responsible for non-banking financial institutions, insurance companies, and capital markets; and the Financial Monitoring Unit (FMU), which serves as the country's financial intelligence unit, receiving, analyzing, and disseminating Suspicious Transaction Reports (STRs) to law enforcement agencies. Financial institutions in Pakistan are required to conduct Customer Due Diligence (CDD) at multiple levels: at the time of account opening, during occasional transactions above prescribed thresholds, and on an ongoing basis for existing customers. The integration of NADRA's biometric verification system has made identity authentication more reliable, with over 60 million biometric verifications conducted by financial institutions annually(Malik 2022, Dommari and Mishra 2024). Suspicious transaction reporting has also increased substantially, with the FMU receiving thousands of STRs and currency transaction reports (CTRs) each year, enabling more effective analysis and dissemination to investigative agencies.

5.2 Alignment with International Standards

Pakistan's AML/KYC framework is designed to align with the FATF's 40 recommendations, which constitute the international standard for combating money laundering and terrorist financing. The country's progress in this regard has been evaluated through mutual evaluation reports conducted by the Asia/Pacific Group on Money Laundering (APG),



a FATF-style regional body. Regulators have adopted a risk-based approach to AML/KYC, requiring financial institutions to assess the money laundering and terrorist financing risks associated with different customer categories, products, and delivery channels. Higher-risk customers, such as Politically Exposed Persons (PEPs) or those from high-risk jurisdictions, are subject to Enhanced Due Diligence (EDD). Mechanisms for implementing United Nations Security Council sanctions related to terrorism and proliferation financing have been enhanced. Pakistan has established procedures for freezing assets of designated individuals and entities without delay, in compliance with FATF requirements. Pakistan has improved its mechanisms for international cooperation, including mutual legal assistance and extradition, enabling more effective cross-border collaboration in money laundering investigations.

5.3 Notable Legislation in Pakistan

The Anti-Money Laundering Act, 2010 (as amended), is the primary legislation governing AML/CFT in Pakistan (Usman Kemal 2014). It criminalizes money laundering, establishes the legal framework for confiscation of proceeds of crime, and provides the legal basis for the FMU's operations. The Act has been amended multiple times, most significantly in 2015 and 2020, to incorporate international standards and address FATF-identified deficiencies. Key amendments expanded the definition of money laundering, strengthened provisions for provisional attachment of property, and enhanced the powers of investigating agencies.

The Anti-Terrorism Act, 1997, legislation addresses terrorist financing offenses and provides the legal framework for implementing UN Security Council sanctions related to terrorism (Parvez and Rani 2015). It criminalizes the collection and provision of funds for terrorist purposes and establishes procedures for the seizure and forfeiture of assets linked to terrorism.

The State Bank of Pakistan has issued comprehensive AML/CFT regulations for banks, microfinance banks, and development finance institutions (Hassan, Hussain et al. 2022). These regulations, updated periodically, detail the specific requirements for customer due diligence, record-keeping, suspicious transaction reporting, and internal controls. They mandate the use of biometric verification for account opening and require institutions to implement transaction monitoring systems.

The Securities and Exchange Commission of Pakistan has issued similar regulations for non-banking financial institutions, including modarabas, leasing companies, insurance companies, and capital market intermediaries (Cheema, Shah et al. 2006). These regulations require these entities to establish AML/CFT compliance programs and report suspicious transactions to the FMU.

The Companies Act, 2017, includes provisions requiring companies to maintain records of their beneficial owners and to provide this information to regulators upon request. It supports the implementation of transparency requirements for legal persons (Gul and Khan 2023, Khan and Akhtar 2024).

NADRA Ordinance, 2000, is concerned with identity management. This ordinance provides the legal basis for NADRA's collection and maintenance of biometric data and its use for verification purposes by third parties, including financial institutions (Hashmi 2021, Hasan and Junejo 2022).

Pakistan Telecommunication (Re-organization) Act, 1996, is legislation, along with regulations issued by the Pakistan Telecommunication Authority, that governs the digital infrastructure that supports mobile banking and digital wallets, including data protection and cybersecurity requirements (Shahid, Shou-lian et al. 2007, Authority 2018).

6. Reported Notable Cases

6.1 The Axact Fake Degrees and Money Laundering Scandal

One of the most high-profile cases illustrating the intersection of financial crime, digital operations, and AML/KYC challenges in Pakistan is the Axact scandal (Hashmi 2022, Hashmi 2023). It unfolded prominently between 2015 and 2018. Axact, a Pakistani software company based in Karachi, operated a sophisticated global network selling fake academic degrees online through hundreds of fictitious universities (Ezell 2023). The case is particularly relevant to this study because it involved digital platforms, cross-border financial flows, and exposed significant gaps in Pakistan's AML framework at the time.

Axact, led by its CEO Shoaib Sheikh, ran a global fraudulent scheme that generated hundreds of millions of dollars by selling fake diplomas, degrees, and accreditations to customers worldwide through elaborately designed websites posing as legitimate educational institutions. The company employed thousands of people in Pakistan who posed as admission officers and academic counselors, targeting primarily customers in the Middle East, Europe, and the United States. Proceeds from this illegal activity were routed through complex financial channels, including shell companies, offshore accounts, and digital payment platforms, making them difficult to trace. The scandal broke in May 2015 when the Federal Investigation Agency (FIA), acting on a tip-off and media investigations by outlets such as The New York Times, raided Axact's headquarters in Karachi. Authorities seized documents, computers, and records revealing the scale of the operation. Subsequent investigations uncovered that those millions of dollars had been funneled through informal money transfer networks known as hundi/hawala, as well as through legitimate banking channels using falsified documentation. What transformed this from a simple fraud case into a significant money laundering prosecution was the method by which Axact disguised and integrated its illicit proceeds.

Following the raid, the FIA registered multiple First Information Reports (FIRs) against Shoaib Sheikh and other key executives under provisions of the Pakistan Penal Code, the Cyber Crime Law, and the Anti-Money Laundering Act,

2010. The case was investigated jointly by the FIA and the Financial Monitoring Unit, which analyzed transaction data obtained from banks and digital payment processors. In 2018, a special court in Islamabad convicted Shoaib Sheikh and 22 other accused persons, sentencing them to prison terms and imposing heavy fines. The court also ordered the confiscation of assets acquired through the proceeds of crime, including properties and bank accounts. However, in 2019, the Islamabad High Court suspended the sentences and ordered a retrial, citing procedural irregularities. As of 2025, the case continues to wind through Pakistan's legal system, with some convictions upheld and others under appeal.

6.2 The Sindh Bank and Omni Group Scandal

One of Pakistan's most significant money laundering cases involved the Omni Group, a business conglomerate owned by the family of former President Asif Ali Zardari, and its alleged use of Sindh Bank to facilitate illicit financial flows (Jafri 2017, Gul and Khan 2023). The case emerged from investigations by the National Accountability Bureau (NAB) and the Federal Investigation Agency (FIA) following the 2018 general elections, which brought a new government committed to anti-corruption enforcement. Allegations centered on the use of fake bank accounts to launder billions of rupees through suspicious transactions. Investigators claimed that Sindh Bank was used to facilitate transactions for the Omni Group without proper due diligence. The scheme allegedly involved routing funds through a network of front companies and benami (proxy) accounts, with the proceeds used for political purposes and personal enrichment.

The case prompted a wide-ranging investigation by NAB and the FIA, resulting in the arrest of several key suspects, including Omni Group executives and bank officials. In 2021, an accountability court convicted Abdul Ghani Majeed, a key Omni Group executive, and others, ordering confiscation of assets and imposing prison sentences. However, higher courts later suspended some convictions, and the case remains entangled in legal appeals. The State Bank of Pakistan also took regulatory action, imposing fines on Sindh Bank for AML compliance failures and ordering remedial measures. The scandal exposed weaknesses in the banking sector's oversight of politically exposed persons (PEPs) and the need for enhanced due diligence.

6.3 The Securities and Exchange Commission of Pakistan (SECP) Beneficial Ownership Enforcement

While not a traditional criminal prosecution, a notable enforcement action by the Securities and Exchange Commission of Pakistan (SECP) in 2023 demonstrates the application of AML/KYC principles in the corporate sector. SECP, acting on intelligence from the Financial Monitoring Unit, investigated multiple shell companies suspected of being used for money laundering through real estate purchases (Haidar, Saeed et al. 2025, RAZA and Siddiqui 2025). The investigation revealed that several companies registered with SECP had submitted false information about their shareholders and directors, concealing the identities of the true beneficial owners. These companies had been used to purchase high-value properties in Islamabad and Lahore, with funds traced to sources outside Pakistan. The transactions were structured to avoid triggering reporting thresholds, a technique known as smurfing or structuring.

6.4 Hawala/Hundi Network Dismantlement in Peshawar

In 2022, the Federal Investigation Agency (FIA), in coordination with the State Bank of Pakistan, dismantled a major hawala/hundi network operating in Peshawar, near the Afghanistan border (Ali, Malik et al. 2025). The network had been facilitating the transfer of billions of rupees to and from Afghanistan, Iran, and Gulf countries, bypassing formal banking channels entirely. The investigation began when the Financial Monitoring Unit detected anomalies in the transaction patterns of several small businesses in Peshawar's currency market. Using data analytics and human intelligence, investigators identified a network of hawala dealers operating through seemingly legitimate businesses such as general stores, travel agencies, and exchange companies. The network processed an estimated 50 billion rupees annually, with funds originating from both legal trade and illicit activities, including drug trafficking and smuggling. The FIA raid resulted in the arrest of 15 key operatives and the seizure of records, cash, and assets worth millions of rupees. Cases were registered under the Anti-Money Laundering Act and the Foreign Exchange Regulation Act. Convictions were obtained against several operatives, though some remain at large across the border. The State Bank of Pakistan used the case to issue new guidelines for exchange companies and money changers, requiring enhanced due diligence and real-time reporting of large transactions. The case also informed Pakistan's strategy for formalizing cross-border trade with Afghanistan, including pilot projects for digital settlement systems.

7. Challenges Faced by Pakistan

7.1 Data Privacy and Security Concerns

The centralization of biometric and personal data within NADRA's database, while enabling robust identity verification, also creates significant privacy and security vulnerabilities. Several high-profile data breaches have raised public concern, including incidents where personal data of Pakistani citizens was reportedly found for sale on dark web forums. Furthermore, the absence of a comprehensive data protection law in Pakistan exacerbates these risks. While a Personal Data Protection Bill has been under consideration for several years, it has yet to be enacted, leaving citizens without clear legal recourse in cases of data misuse. Financial institutions that access NADRA's database for KYC purposes also store customer data on their own systems, creating additional points of vulnerability. The tension between accessibility for legitimate compliance purposes and protection against unauthorized access remains unresolved.

7.2 Regulatory Capacity and Enforcement Gaps



While Pakistan's legal and regulatory framework for AML/KYC has improved substantially, the capacity of regulatory agencies to enforce these rules consistently and effectively remains constrained. The State Bank of Pakistan, despite its technical expertise, faces challenges in supervising a rapidly expanding digital financial sector. The proliferation of digital wallets, mobile banking apps, and agent networks has outpaced the regulator's ability to conduct on-site inspections and monitor compliance in real-time. Similarly, the Financial Monitoring Unit, while strengthened during Pakistan's FATF engagement, operates with limited human and technological resources relative to the volume of suspicious transaction reports it receives. Analysis and dissemination of intelligence to law enforcement agencies often face delays, reducing the effectiveness of AML efforts. Prosecution rates for money laundering offenses, while improving, remain low compared to the volume of reported suspicious transactions, reflecting weaknesses in the criminal justice system's handling of complex financial crimes.

7.3 Informal Economy and Hawala/Hundi Networks

The most formidable challenge to Pakistan's AML/KYC regime is the sheer scale of its informal economy. Estimates suggest that a significant portion of Pakistan's economic activity occurs outside the formal financial system, with cash transactions dominating in rural areas, wholesale markets, and many service sectors. This informal economy provides fertile ground for money laundering, as illicit funds can be commingled with legitimate cash-based businesses and moved through informal value transfer systems such as hawala/hundi. These informal networks operate on trust and relationships, leaving no paper trail or digital record for regulators to monitor. They are particularly prevalent in cross-border trade with Afghanistan and Iran, where formal banking channels are limited or subject to sanctions. Even as DPI brings more Pakistanis into the formal financial system, the parallel informal economy continues to offer an alternative channel for those seeking to avoid scrutiny. Addressing this challenge requires not only technological solutions but also broader economic reforms to incentivize formalization and deter informal transactions.

7.4 Financial Inclusion Versus Regulatory Rigor

Pakistan faces an inherent tension between the goals of financial inclusion and regulatory rigor. The tiered KYC approach adopted for digital wallets allows millions of previously unbanked individuals to access basic financial services with simplified due diligence. While this promotes inclusion, it also creates potential loopholes. Multiple low-limit wallets could theoretically be used to circumvent transaction monitoring, and the agents responsible for onboarding customers in remote areas have occasionally been implicated in fraudulent verifications. Striking the right balance remains challenging. If KYC requirements are too stringent, they exclude the very populations that digital financial services aim to serve. If they are too permissive, they create vulnerabilities that can be exploited for money laundering. Pakistan's regulators must continuously calibrate this balance, drawing on data and risk assessments to adjust requirements as the financial landscape evolves.

7.5 Technological Infrastructure Gaps

While Pakistan's DPI has advanced significantly, gaps in technological infrastructure persist, particularly in rural and remote areas. Internet connectivity remains unreliable in many regions, with frequent disruptions and slow speeds hampering real-time verification and digital transactions. Electricity shortages further compound these challenges, as both bank branches and agents may be unable to process transactions during power outages. Digital literacy is another significant barrier. A substantial portion of Pakistan's population, particularly among older adults, women, and rural communities, lacks the skills and confidence to use digital financial services effectively. This not only limits the reach of DPI-enabled AML/KYC but also creates opportunities for fraudsters who exploit users' unfamiliarity with technology. Addressing these gaps requires sustained investment in infrastructure and education, alongside the development of user interfaces that are accessible to populations with limited literacy.

7.6 Political Interference and Institutional Independence

High-profile money laundering cases involving politically exposed persons have repeatedly raised concerns about political interference in investigations and prosecutions. This undermines public confidence in the AML regime and allows politically connected individuals to evade accountability. Ensuring the independence of institutions such as NAB, FIA, and the FMU from political influence remains an ongoing challenge. While legal protections exist, their effectiveness depends on the broader political environment and the commitment of successive governments to uphold the rule of law. International pressure, including FATF monitoring, has helped insulate these institutions to some extent, but domestic political dynamics continue to pose risks.

7.7 Evolving Nature of Financial Crime

The increasing sophistication of cybercrime, including phishing attacks, ransomware, and business email compromise, creates new channels for acquiring and laundering illicit funds.

8. Conclusion

This study examines the role of Digital Public Infrastructure in strengthening Anti-Money Laundering and Know Your Customer frameworks within developing economies, using Pakistan as a detailed case study. The findings reveal a nuanced picture. DPI has unquestionably strengthened Pakistan's AML/KYC capabilities in significant ways. The cases examined in this study demonstrate that while financial criminals continue to find ways to evade detection, they now face considerably higher hurdles than in the past. The research also makes clear that DPI is not a panacea. The challenges documented in this paper and the constantly evolving nature of financial crime all serve as reminders that technology

alone cannot solve deeply embedded structural problems. When accompanied by robust legal safeguards, adequate regulatory capacity, effective inter-agency coordination, and sustained political commitment, DPI can dramatically enhance the efficiency, accuracy, and reach of financial integrity mechanisms. When these supporting elements are weak, however, even the most sophisticated digital infrastructure will fall short of its potential.

9. Recommendations

Based on the findings of this study and the challenges identified in Pakistan's DPI-enabled AML/KYC framework, the following recommendations are offered for policymakers, regulators, financial institutions, and international partners.

Enact Comprehensive Data Protection Legislation: The absence of a dedicated data protection law creates significant privacy and security vulnerabilities. Pakistan should urgently enact the Personal Data Protection Bill with strong enforcement mechanisms, clear consent requirements, and meaningful remedies for citizens whose data is misused. This will build public trust in digital financial services and align Pakistan with international best practices.

Strengthen Regulatory Capacity and Resources: The State Bank of Pakistan, Securities and Exchange Commission of Pakistan, and Financial Monitoring Unit require enhanced human and technological resources to supervise a rapidly expanding digital financial sector. This includes increasing staffing for on-site inspections, investing in advanced transaction monitoring systems, and providing specialized training for financial crime analysis.

Develop a Unified Inter-Agency Data Sharing Platform: The persistence of data silos among regulatory and law enforcement agencies hampers the effective investigation of complex financial crimes. Pakistan should develop a secure, interoperable digital platform enabling real-time information sharing between SBP, SECP, FMU, FIA, NADRA, and the Federal Board of Revenue, with appropriate privacy safeguards.

Invest in Digital Infrastructure and Literacy: Gaps in internet connectivity, electricity reliability, and digital literacy, particularly in rural areas, limit the reach of DPI-enabled AML/KYC. Sustained public and private investment in telecommunications infrastructure, coupled with nationwide digital literacy programs targeting women, older adults, and rural populations, is needed to ensure inclusive access.

Enhance Cross-Border Cooperation and Border Management: Pakistan's porous borders and informal cross-border trade create significant money laundering vulnerabilities. Strengthened cooperation with neighboring countries, particularly Afghanistan and Iran, on information sharing and joint investigations is essential. Investment in digital customs systems and coordination between customs authorities and financial regulators can help detect trade-based money laundering.

Insulate Financial Crime Investigations from Political Interference: The perception of selective justice in politically connected cases undermines public confidence and the effectiveness of the AML regime. Legal and institutional safeguards should be strengthened to protect investigative and prosecutorial independence, ensuring that all cases are pursued consistently regardless of the individuals involved.

References

- Abro, A., Maitlo, A., & Mahar, M. H. (2025). IDENTITY THEFT RISK ASSESSMENT TOOLS IN THE BANKING SECTOR OF PAKISTAN. *Journal of Emerging Technology and Digital Transformation*, 4(2), 137-150.
- Afzal, J. (2026). *Exploring the New Horizons of International Law Concerning Globalization of Economy*. Springer Nature.
- Ahmed, S., Naz, F., & Aslam, S. (2022). COVID-19 Emergency and Changes in the Usage Intention of Mobile Banking Services in Pakistani Peri-Urban Areas. *Business & Economic Review*, 14(1), 47-72.
- Akbar, F., Hussain, J., Usman, M. B., & Afzal, J. (2025). The Impact of Financial Scams on Consumer Trust in the Banking Sector: A Qualitative Analysis. *International Journal of Discovery in Social Sciences*, 1(1).
- Akhison, G. (2025). Towards a Universal Digital Identity: a blockchain-based framework for borderless verification. *Frontiers in Blockchain*, 8, 1688287.
- Ali, L., Malik, G., & Daudani, T. A. (2025). Strategic Interventions to Combat Terrorism Financing in Pakistan: Challenges and Pathways. *Annals of Human and Social Sciences*, 6(3), 86-97.
- Arif, G., Gul, X., Ashfaq, S., Fatima, M., & Qureshi, T. (2022). Population Challenges in a Changing World: An Overview of the 22nd Annual Research Conference of the Population Association of Pakistan. *NUST Journal of Social Sciences and Humanities*, 8(3), 1-15.
- Authority, P. T. (2018). Pakistan telecommunication authority. *2018 Annual Report*.
- Baloch, M. U. F. (2025). Importance Of Big Data: Pakistan's Struggle With Big Data Governance. *Policy Vanguard*, 1(1), 1-10.
- Bouza, S., Hlayhel, B., Kroen, T., Miccoli, M. M., Mircheva, B., Polo, G., Sakha, S., & Yang, Y. (2024). *Central bank digital currencies in the middle east and central asia*. International Monetary Fund.
- Butt, A. S. (2025). Government Policies and Digital Transformation During COVID-19 in Pakistan: an Analysis of Digital and Financial Inclusion. *Digital Society*, 4(3), 81.
- Centeno, M. A., & Portes, A. (2006). The informal economy in the shadow of the state. *Out of the shadows: Political action and the informal economy in Latin America, 2006*, 23-48.
- Cheema, M., Shah, S. A., & Burki, A. A. (2006). *The Role of Mutual Funds and Non-Banking Financial Companies in Corporate Governance in Pakistan*. Lahore University of Management Sciences, Centre for Management and Economic
- Clark, J., Marin, G., Ardic Alper, O., & Galicia Rabadan, G. (2025). Digital Public Infrastructure and Development.
- Dhiman, T., & Madan, P. (2025). From Vision to Reality: How Digital Public Infrastructure is Shaping Service Delivery. *Journal of Marketing & Social Research*, 2, 368-381.



- Dommari, S., & Mishra, R. K. (2024). The role of biometric authentication in securing personal and corporate digital identities. Available at SSRN 5259335.
- Ezell, A. (2023). Yesterday, today, and tomorrow: A tour of Axact, the “world’s largest diploma mill”. In *Fake degrees and fraudulent credentials in higher education* (pp. 49-94). Springer.
- Gaisina, A., & Finger, M. (2025). Central Bank Digital Currencies (CBDCs): a countermeasure to Anti-Money Laundering (AML) challenges posed by cryptocurrencies? *Digital finance*, 7(2), 201-254.
- Gandhi, V., & Kak, R. (2025). India’s DPI Experiment and Digital Finance Revolution. In *Sustainable Digital Finance* (pp. 419-443). Springer.
- Gaviyau, W., & Sibindi, A. B. (2023). Global anti-money laundering and combating terrorism financing regulatory framework: A critique. *Journal of Risk and Financial Management*, 16(7), 313.
- Gul, K., & Khan, M. Z. (2023). Analyzing anti money laundering laws in Pakistan and comparison of the AML laws of Pakistan with FATF standards. *Pakistan Research Journal of Social Sciences*, 2(4).
- Haidar, A., Saeed, T., Jamal, T., & Khan, A. (2025). Impact of Blockchain Adoption on Financial Auditing and Regulatory Compliance in Pakistan’s Banking Sector. *The Critical Review of Social Sciences Studies*, 3(3), 732-749.
- Harichandana, A. (2025). Digital Payment Adoption in Emerging Markets. *IJSAT-International Journal on Science and Technology*, 16(3).
- Harish, V., Sharma, R., Karthik, A., Rana, G., Balaji, R., & Kumar, R. (2025). Financial Inclusion Through Fintech: Bridging the Gap. In *Sustainable Finance: Strategies and Tools to Manage Climate Risk* (pp. 87-109). Springer.
- Hasan, M., & Junejo, W. (2022). An Analysis of the Obstacles Faced by Women and Other Gender Minorities While Obtaining National Identification Cards and Their Consequences. *RSIL L. Rev.*, 57.
- Hasan, M., Talukder, O., Saju, R. K., & Lysuzzaman, M. (2024). KYC-Driven Cryptocurrency Wallet: A Solution To Regulatory Compliance. 2024 27th International Conference on Computer and Information Technology (ICIT),
- Hashmi, S. (2022). Analysis of the News Coverage on Axact Software Company and BOL TV Channel in the News International-Karachi From May 2015 to May 2017. *Media and Communication Review*, 2(2), 79-94.
- Hashmi, S. R. A. (2023). An Analysis of the News International Karachi’s Portrayal of AXACT Scam and Its TV Channel Bol. *SBBU Journal of Social Sciences*, 1(2), 116-126.
- Hashmi, Z. (2021). Making reliable persons: managing descent and genealogical computation in Pakistan. *Comparative Studies in Society and History*, 63(4), 948-978.
- Hassan, S. S. U., Hussain, M. A., & Sajid, S. (2022). The effectiveness of anti-money laundering legislation in Islamic banking of Pakistan: experts’ opinion. *Journal of Money Laundering Control*, 25(1), 135-149.
- Iqbal, J., & Noman, M. (2025). Digital Financial Technologies as Drivers of Inclusive Growth: A Strategic Review of Pakistan’s Fintech Landscape. *Journal of Business and Economic Options*, 8(4), 12-22.
- Islam, S. (2025). Machine Learning–Based AML/KYC Transaction Monitoring for Suspicious Activity Detection and Compliance Risk Reduction in Digital Banking. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 1740-1775.
- Jafri, A. R. (2017). Public service ethics in Pakistan. In *Public administration in South Asia* (pp. 429-438). Routledge.
- Khan, A., & Akhtar, N. (2024). An analytical study of compliance of banking institutions of Pakistan with anti-money laundering regulations: legal challenges and a way forward. *Islamabad Law Review*, 8(1), 74-105.
- Liaquat, H. M. S. (2025). Regulatory Challenges and Opportunities for Cryptocurrency in Pakistan’s Financial Markets.
- Malhotra, D., Saini, P., & Singh, A. K. (2022). How blockchain can automate KYC: Systematic review. *Wireless Personal Communications*, 122(2), 1987-2021.
- Malik, M., Khan, L., Maqbool, H. N., & Anwar, M. (2025). Mobile Wallets and Digital Payments: Assessing the Impact on Financial Inclusion and Consumer Trust in Pakistan. *Review of Applied Management and Social Sciences*, 8(3), 1349-1362.
- Malik, T. (2022). Digital transformation through the prism of digital identity. *Journal of Public Policy Practitioners*, 1(2), 33-48.
- Mansoor, N., Antora, K. F., Deb, P., Arman, T. A., Manaf, A. A., & Zareei, M. (2023). A review of blockchain approaches for KYC. *IEEE Access*, 11, 121013-121042.
- Mazzucato, M., Eaves, D., & Vasconcellos, B. (2024). Digital public infrastructure and public value: What is ‘public’ about DPI?
- Meagher, K. (2013). Unlocking the informal economy: A literature review on linkages between formal and informal economies in developing countries. *Work. ePap*, 27, 1755-1315.
- Mohsin, A. (2025). Infrastructures of excess: Politics of biometric and data-based citizenship in Pakistan’s cash transfers program. *Flux*, 139140(1-2), 83-96.
- Oleti, C. S. (2025). Real-time payment systems: transforming global economic infrastructure through digital financial innovation. *World Journal of Advanced Research and Reviews*, 25, 2464-2477.
- Oludoyi, I. O. (2025). Effect of KYC and AML Regulations on Cryptocurrency Exchange Preference Among Nigerian Users. *Journal of Economics, Business, and Commerce*, 2(2), 1-9.
- Paleti, S. (2025). *Smart finance: Artificial intelligence, regulatory compliance, and data engineering in the transformation of global banking*. Deep Science Publishing.
- Parvez, T., & Rani, M. (2015). *An appraisal of Pakistan’s anti-terrorism act*. JSTOR.
- Pilkington, P. (2024). The Risk of Decoupling and De-risking. HIIA. [https://hiia.hu/en/decoupling-and-de-risking/\(open in a new window\)](https://hiia.hu/en/decoupling-and-de-risking/(open%20in%20a%20new%20window)).
- RAZA, H. R., & Siddiqui, D. A. (2025). CBDC vs Cryptocurrency in Pakistan: A Comparative Review. *International Journal of Social Science & Entrepreneurship*, 5(3), 87-109.
- Rehman, A. U. (2026). From Fragmentation To Integration: The Economic Case For Uniform Citizen Data Systems, Legal Framework And Hazards In Pakistan. *Pakistan Journal of Social Science Review*, 5(1), 657-676.
- Rusman, R., & Budianto, A. (2025). Strengthening Know Your Customer (KYC) and Anti-Money Laundering (AML) Policies in the Fintech Industry to Prevent Money Laundering Crimes. *Journal of World Science*, 4(7), 871-881.

- Sakyi-Nyarko, C., Ahmad, A. H., Murinde, V., & Arun, T. (2026). Digital Public Infrastructure: Foundations and Futures. In *The Routledge Handbook of Infrastructure Finance* (pp. 604-622). Routledge.
- Shahid, M. K., Shou-lian, T., & Liu, C. (2007). Competition and liberalization policies and regulations for telecommunications industries in China and Pakistan: a comparative analysis. *International Journal of Management Science and Engineering Management*, 2(4), 268-277.
- Shoaib, A., Shoaib, M., & Nabi, W. G. (2025). Fin-Tech-Enabled Remittances and Economic Stability: UBL.
- Sterling, S. (2015). Identifying money laundering: Analyzing suspect financial conduct against the speed, cost, and security of legitimate transactions. *Journal of Money Laundering Control*, 18(3), 266-292.
- També Bearpark, N., & Demetis, D. (2022). Re-thinking de-risking: a systems theoretical approach. *Journal of Money Laundering Control*, 25(1), 27-49.
- Thommandru, A., & Chakka, B. (2023). Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks. *Sustainable Futures*, 5, 100107.
- Usman Kemal, M. (2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control*, 17(4), 416-427.

Declaration

Conflict of Study: The author declares that he 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: There are no ethical issues. All data in this paper is publicly available.

Declaration of AI Use: Not Applicable.

Consent to Publish: Not Applicable.

Ethical Approval: Not Applicable

Consent to Participate: Not Applicable

Acknowledgment: Not Applicable