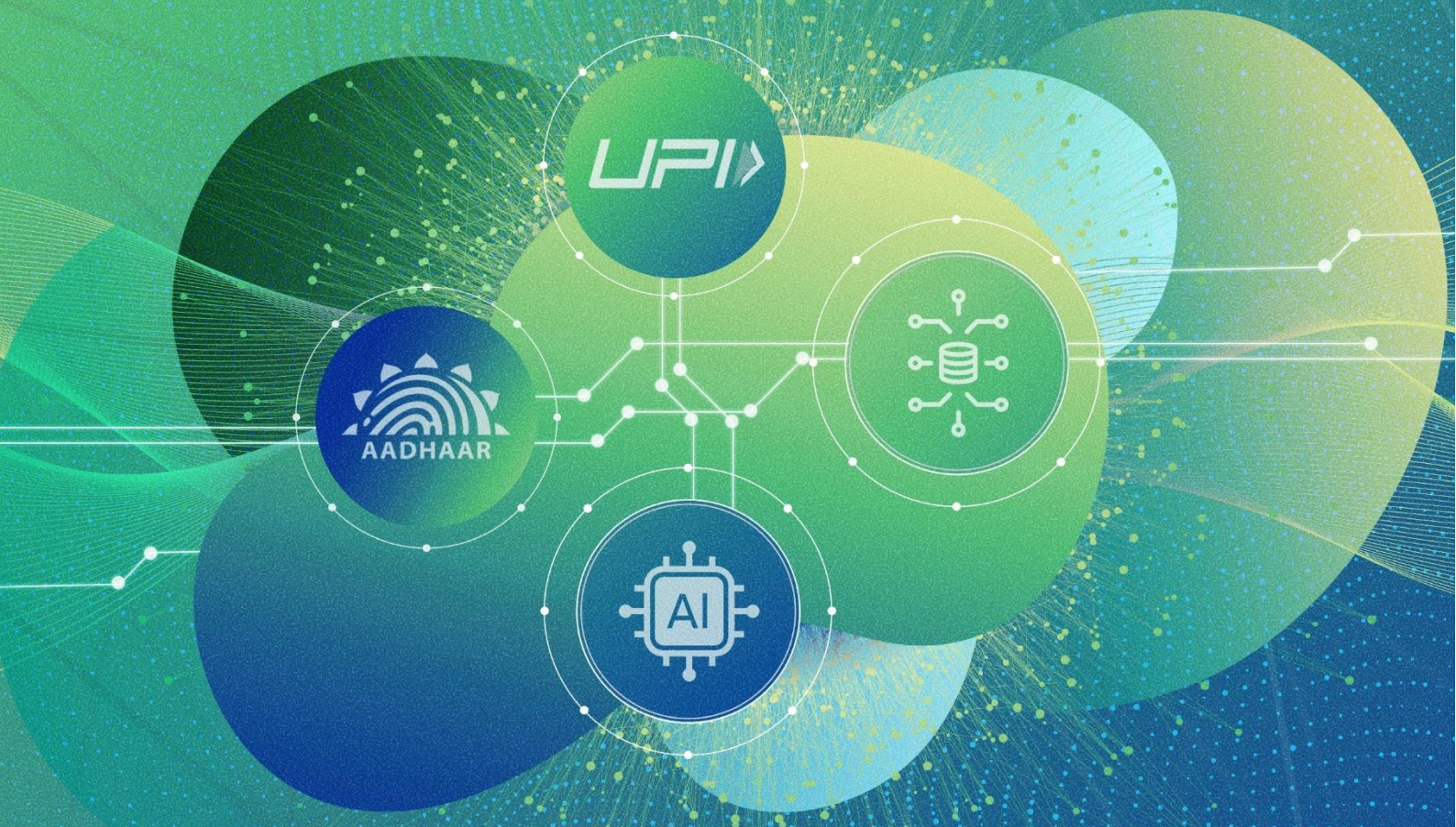
The Dialogue®
INFORM ENGAGE IDEATE

RESEARCH REPORT

RESPONSIBLE HARNESSING OF AI INNOVATION ACROSS DIGITAL PUBLIC INFRASTRUCTURES



SEPTEMBER
2025

RESEARCH REPORT

RESPONSIBLE HARNESSING OF AI INNOVATION ACROSS DIGITAL PUBLIC INFRASTRUCTURES

Authors:

The Dialogue in association with **Rama Vedashree**

Meemansa Agarwal,
Kamesh Shekar

Copyeditor: Akriti Jayant

Thematic Designer : Shivam Kulshrestha

(C) 2025 The Dialogue®. All rights reserved.

The Dialogue® is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue® has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information
www.thedialogue.co

Suggested Citation
Vedashree, R., Agarwal, M. & Shekar, K. (2025, September). Research Report - Responsible Harnessing of AI Innovation Across Digital Public Infrastructures. The Dialogue®

Catalogue No
TD/ET/RP/0925/09

Publication Date
September 30, 2025

Disclaimer
The facts and information in this report may be reproduced only after giving due attribution to the authors and The Dialogue®.

Rama Vedashree
Former CEO, Data Security Council of India (DSCI)

Kazim Rizvi
Founding Director, The Dialogue

Foreword

India's journey in reimagining governance through technology has been nothing short of transformative. By building world-class Digital Public Infrastructures (DPIs) such as Aadhaar, UPI, Digilocker, and Account Aggregators, India has demonstrated how Digital Public Goods (DPGs) can create scalable, interoperable, and cost-efficient systems that advance financial inclusion and enable delivery of services to citizens at the last mile. This model of innovation has not only reshaped service delivery domestically but has also positioned India as a global leader in digital governance.

Today, we stand at the cusp of a new frontier. With the launch of the IndiaAI Mission, India is preparing to embed Artificial Intelligence (AI) into its governance and innovation ecosystems. The integration of AI and DPI holds immense promise AI can enhance the efficiency, reach, and adaptability of DPI, addressing long-standing gaps in accessibility, responsiveness, and trust.

This paper explores how AI can be strategically integrated into the various layers of DPI to unlock new possibilities while ensuring safety, fairness, transparency, and accountability. It highlights real-world use cases, identifies areas for future innovation, and underscores the importance of a governance framework that ensures AI integration is responsible, equitable, and trustworthy. Building on nine globally inspired principles for trustworthy AI outlined in our earlier work, the paper offers practical insights on operationalising values such as non-discrimination, safety, and reliability within the DPI ecosystem.

As India prepares to host the AI Impact Summit in 2026, it is imperative that we showcase not only our technological achievements but also our commitment to deploying AI responsibly within DPIs. Just as India demonstrated leadership through its success with DPIs and its stewardship of the G20 and GPAI Presidency in 2023, the next chapter calls upon us to lead in the responsible integration of AI, an integration that is both transformative and anchored in trust.
This paper is a step in that direction, providing a forward-looking perspective on how AI and DPI, when brought together, can shape a more inclusive, intelligent, and resilient digital future for India and the world.

Aadhaar is the very foundation of India's Digital Public Infrastructure and has enabled countless innovations that place citizens at the centre of governance and service delivery. At UIDAI, our constant endeavour has been to strengthen Aadhaar's role as a people-first platform, continuously upgrading technology, safeguarding trust, and improving ease of living for every resident. The integration of Artificial Intelligence marks the next chapter in this journey. From enhancing security and reducing fraud to enabling seamless, citizen-centric services, AI has the potential to significantly expand Aadhaar's impact. This report comes at a timely moment, delving deeply into the transformative use cases of AI in Aadhaar. I believe it will serve as a guide for innovators and ecosystem partners to build upon, so that together we can shape the next generation of inclusive and trustworthy digital public services for India.

Bhuvnesh Kumar
Chief Executive Officer,
Unique Identification
Authority of India (UIDAI)

India is uniquely positioned to unlock transformative use cases of its Digital Public Infrastructure by harnessing the innovation power of AI. The challenge for us is how can we infuse our DPI's with AI and create population scale impact. As we chart out the future roadmap for our DPIs, I see immense potential to overlay Artificial Intelligence and scale up the way both Government and Industry services citizens. Indian Languages and Voice can play a pivotal role in bringing DPIs and AI Innovation to scale. India's UPI and Fintech success story has demonstrated the power of DPIs and AI. This success needs to be replicated across all DPIs and domains like healthcare and Citizen Services

Nandan Nilekani
Co-founder and Chairman, Infosys;
Founding Chairman, UIDAI

While DPI and AI are orthogonal in design, their convergence unlocks extraordinary non-linear value. For DPI to truly deliver impact at the population scale and reach the last mile, it must overcome barriers of language and information asymmetry, challenges for which AI is uniquely suited. By building this bridge, AI can supercharge the DPI ecosystem, ensuring it is inclusive, scalable, and impactful. That is why I believe this study is both timely and relevant, as it takes stock of how AI is getting integrated into DPIs, and how AI can further amplify the potential of DPI.

Dr. Pramod Varma
Former Chief Architect, India Stack

Acknowledgement

The authors would like to thank the following experts for their expert comments, inputs and/or peer review of the paper. All errors and omissions that remain are those of the authors.

1. **Dr. Pramod Varma**, Co-Chair, Centre for Digital Public Infrastructure; CTO, EkStep Foundation; Chief Architect, Aadhaar & India Stack; Founding Architect, Beckn Protocol.
2. **Alpan Raval**, Chief Scientist, AI/ML, Wadhwani AI
3. **Tanveer Hasan**, Executive Director, Centre for Internet & Society
4. **Mitesh Bidawatka**, Group Head Data & AI, Jio Financial Services
5. **Amol Pai**, Chief Technology Office, Jio Finance Limited
6. **Sundaraparipurnan Narayanan**, Researcher & Consultant – Tech Ethics, AI Tech Ethics
7. **Lakshay Narang**, Senior Research Associate, Artha Global
8. **Kazim Rizvi**, Founding Director, The Dialogue
9. **Ranjeet Rane**, Partner and Fintech & Sustainable Finance Lead, The Dialogue
10. **Sachin Dhawan**, Deputy Director, The Dialogue
11. **Anuradha Bhattacharya**, Senior Research Associate, The Dialogue

Table of Contents

Executive Summary

Our report examines the evolving role of Artificial Intelligence (AI) in India's Digital Public Infrastructures (DPIs), with a focus on Aadhaar, UPI, and the Account Aggregator (AA) framework. DPIs have already transformed digital service delivery by enabling accessibility, scalability, and efficiency at population scale. An assessment of the existing DPI landscape shows that AI is already being applied in diverse domains such as fraud detection, workflow automation, conversational interfaces, and data analytics, demonstrating promising results in enhancing efficiency, security, and citizen engagement. However, our findings indicate that significant gaps remain in personalisation, real-time decision-making, operational efficiency, and governance. For instance, multilingual and context-aware interfaces for under-served populations are limited, data standardisation and analytics capabilities are fragmented, and emerging security applications such as deepfake detection, AI-powered biometrics, and federated learning are yet to be fully systematised. Similarly, opportunities for advanced AA use cases, including alternate-data credit scoring, automated KYC, NLP-based standardisation, and real-time consent management, remain underexplored.

Based on these findings, our report suggests a set of actionable interventions and emerging use cases that draw on successful applications both within India and across other sectors and jurisdictions. These include AI-driven conversational payments, grievance resolution chatbots, routing optimisation, predictive fraud detection, and context-sensitive citizen engagement platforms. We also identify opportunities for novel interventions such as deepfake detection, multilingual chatbots, federated learning for fraud prevention, AI-powered voice biometrics, and expanded AA applications to unlock consented data utility. We have divided these AI use cases into five buckets: **(E) Experience Enhancement**, which improves user-facing processes and ensures smoother, more accessible interactions; **(K) Knowledge Access**, which enhances information retrieval and understanding; **(P) Process Productivity**, which automates or streamlines workflows and reduces manual tasks; **(S) Security/Fraud**, which detects and prevents malicious activities while strengthening authentication; and **(D) Decision Making**, which leverages analytics, underwriting, and other AI-driven outcomes. Taken together, these solutions can enhance citizen experiences, improve operational efficiency, strengthen security, and enable data-driven decision-making across the DPI ecosystem.

The report further highlights the need for a robust governance framework that aligns AI integration with transparency, fairness, privacy, and accountability principles while clearly defining stakeholder roles and responsibilities. We emphasise that public-private collaboration is critical to drive innovation, secure financial and strategic support, and ensure that AI adoption in DPIs remains aligned with national objectives. By addressing these gaps and exploring the proposed use cases, AI can significantly augment the value of DPIs, enabling services that are technologically advanced, deeply user-centric, and capable of meeting the diverse needs of India's population.We invite all stakeholders to engage with us as we embark on this essential exploration.

1. Introduction

DPIs have revolutionised the accessibility, efficiency, and scalability of digital services, reshaping both financial and civic ecosystems. Built as interconnected layers, these infrastructures create foundational digital frameworks that enable seamless interoperability across public and private services. In doing so, they foster innovation and allow state and private sector stakeholders to deliver more citizen-centric solutions.

At the heart of this ecosystem lies Aadhaar, India's foundational digital identity layer, which enables trusted authentication and underpins services across sectors. Building on this identity infrastructure, financial tools like the UPI and AA framework have created new ways for people to pay, share data, and access financial services. Together, these DPIs have driven efficiency, expanded financial inclusion, boosted innovation and attracted international attention.

With this strong foundation in place, the next frontier is integrating AI into DPIs. AI can enhance functionality, improve service delivery, and scale these systems to meet the demands of a rapidly growing population, an approach strongly supported by the Indian government.[1] In its recent report, the Reserve Bank of India's FREE-AI Committee[2] (Framework for Responsible and Ethical Enablement of Artificial Intelligence) recommended the purposeful integration of AI with DPI. Such integration would create a next-generation layer—**Digital Public Intelligence (DPI 2.0)**—as an open, innovation-driven, and trust-anchored ecosystem where financial services remain tailored, inclusive, secure, and impactful. This framework would also empower regulated entities (REs), FinTechs, and innovators to design solutions accessible even to individuals without technical expertise or fluency in the language of digital services.

Accordingly, the Committee called for an enabling framework to integrate AI with DPI, accelerating the delivery of inclusive and affordable financial services at scale. This vision also aligns with India's global leadership: during its G20 Presidency,[3] India actively promoted AI-driven DPI solutions as enablers of inclusive digital growth. The approach received formal recognition in the G20 communiqué, which acknowledged AI-enhanced DPIs as critical drivers of sustainable economic development, improved public welfare, and broader access to digital services.

AI integration into the DPI ecosystem can broadly take two forms: (a) embedding AI into existing DPI systems to enhance performance and expand their functional capacities; or (b) utilising DPI frameworks to facilitate the responsible development and deployment of AI solutions across various layers of the DPI stack. This paper confines its scope to the former, examining how AI is, or could be, integrated into the different layers of DPI to improve service delivery.

For this purpose, the paper focuses on Aadhaar, UPI, and the AA framework. These DPIs have matured considerably, achieved widespread adoption, and developed strong

[1] Abhishek Singh, "AI has potential to make India's DPI significantly more efficient", IndiaAI (2023) https://indiaai.gov.in/article/ai-has-potential-to-make-india-s-dpi-significantly-more-efficient-abhishek-singh
[2] FREE-AI Committee Report - Framework for Responsible and Ethical Enablement of Artificial Intelligence, 13 Aug, 2025. https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=1306#CH43
[3] Prime Minister's Office, "Declaration on Digital Public Infrastructure, AI and Data for Governance - Joint Communiqué by the G20 Troika (India, Brazil and South Africa)," Press Information Bureau, November 20, 2024 https://pib.gov.in/PressReleasePage.aspx?PRID=2074832

interconnections, making them ideal examples for assessing AI integration across India's broader DPI ecosystem.

Through real-world use cases, this paper highlights the practical impact of embedding AI into DPIs and identifies future opportunities for deeper integration. Finally, this paper also outlines a governance framework to ensure that AI deployment within DPIs remains responsible, transparent, and trustworthy.

2. Methodology

The paper adopted a two-pronged methodological approach:

- **Primary Research and Engagement:** (a) The team conducted focused group discussions and one-on-one interviews with representatives from financial services, specially fintech organisations, along with civil society actors, lawyers, and other stakeholders These conversations provided insights on the future of DPI-AI integration, helped surface bottlenecks, and informed the development of guiding principles and a governance framework. (b) We also carried out case study analysis by inviting use cases from ecosystem players (*FinTechs, SaaS providers, RegTech firms etc.*) that demonstrate AI integration within DPI at the application level.

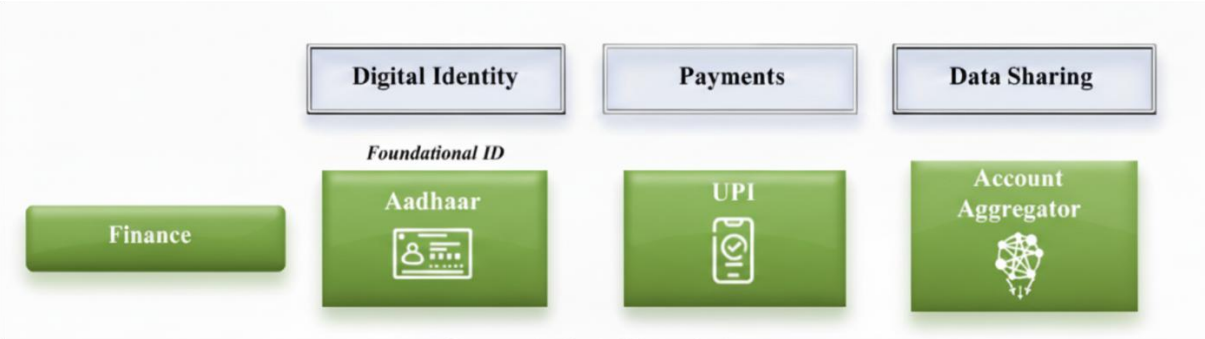
- **Secondary research:** We undertook a meta-analytic literature review of existing DPI scholarship to identify gaps and areas where AI could be integrated. By critically examining and evaluating this body of knowledge, we identified fundamental guiding principles, assessed prevailing challenges within the DPI ecosystem, and explored how AI could address them.

3. An Overview of DPI in India

India has built a range of DPIs, particularly within the financial ecosystem, structured to complement one another across different layers. These include Aadhaar (identity layer), UPI (payments layer), and the AA (data-sharing layer), each designed to advance the overarching goal of enabling seamless interoperability and innovation across the ecosystem.

These DPIs operate in a coordinated fashion. For instance, Aadhaar (identity layer) provides a foundational digital identity, which UPI leverages to facilitate real-time authenticated transactions. Similarly, the AA framework is built on both the identity and payment layers to enable secure transfer and sharing of financial data between regulated entities, allowing individuals access to a suite of financial services, including credit, insurance, etc. This interconnected DPI architecture ensures that each component reinforces the others, creating a robust and innovation-friendly financial ecosystem. Based on their functions, DPIs can be classified in broader categories, as illustrated below.

Figure 1: Digital Public Infrastructure in India



(Source: Author's illustration)

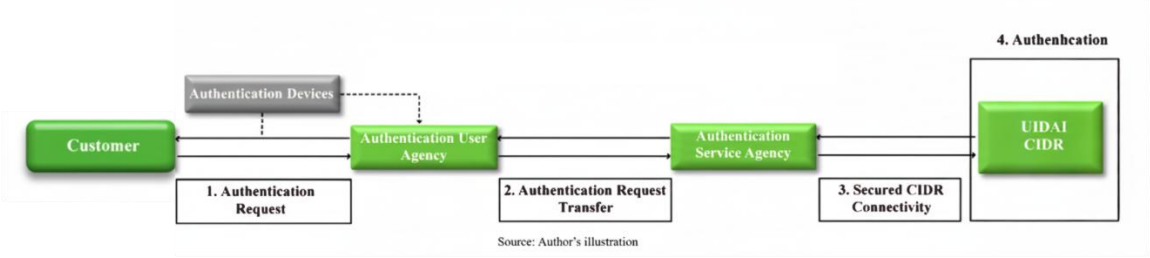
3.1. Digital Identification (Aadhaar)

From a design perspective, digital identification has been described as "*the reimagination of the citizen-state relationship that is centered on a technology platform.*"[4] Digital IDs serve a dual purpose: they enhance convenience for individuals while reducing administrative costs and improving efficiency in public service delivery for the government. The digital identification system seeks to redefine multiple aspects of the citizen-state relationship, particularly in terms of: (a) how the government creates a social contract[5] with citizens by providing proof of identity through verification; (b) how databases created through these digital identities are used to target welfare and social protection measures; and (c) how digital IDs are used for authenticating and delivering welfare to the targeted population.

[4] Jean Dreze, Dissent on Aadhaar
[5] Markus Loewe, Tina Zintl, Annabelle Houdret, The social contract as a tool of analysis: Introduction to the special issue on "Framing the evolution of new social contracts in Middle Eastern and North African countries", World Development, Volume 145, 2021, 104982, ISSN 0305-750X, https://doi.org/10.1016/j.worlddev.2020.104982

Digital identification systems provide individuals with proof of legal identity, facilitating seamless transactions and services through identity verification and authentication processes. Traditionally, such systems verify basic personal attributes, such as name, date of birth, and mobile number, forming the backbone for routine Know Your Customer (KYC) processes. In India, the credibility and legitimacy of digital identification took a transformative leap with the pioneering launch of Aadhaar, a distinctive, verified, and duplication-free form of digital identity.[6] Managed centrally by the Unique Identification Authority of India (UIDAI), Aadhaar incorporates biometric verification methods, including fingerprint and iris scanning, thereby enhancing the reliability of authentications. Studies highlight that UIDAI aimed to create a platform to initially collect residents' identity details and subsequently provide identity authentication services for use by the government and commercial service providers.[7] This has firmly established Aadhaar as a trusted foundation within India's broader digital governance infrastructure. The following figure illustrates the Aadhaar authentication process involving various players.

Figure 2: Aadhaar Authentication Proces



(Source: Author's illustration[8])

The Aadhaar ecosystem comprises multiple stakeholders, each playing a vital role in ensuring secure and efficient identity verification. The UIDAI manages Aadhaar and provides authentication and verification services through two key components: the Enrolment & Update Ecosystem, where Registrars and Enrolment Agencies collect biometric and demographic data, and the Authentication Ecosystem, where UIDAI designates Authentication Service Agencies (ASAs) and Authentication User Agencies (AUAs) across government and private sectors to facilitate authentication.

Box 1: Use-cases of Aadhaar Authentication

The National Payments Corporation of India (NPCI) has integrated Aadhaar with financial transactions, enabling secure digital payments through initiatives such as the Aadhaar-Enabled Payment System (AEPS) for rural banking, BHIM Aadhaar Pay for merchant transactions, the Aadhaar Payment Bridge (APB) for Direct Benefit Transfers (DBT), and e-RUPI for targeted, cashless welfare distribution.

The government is the largest adopter of Aadhaar, using it to enhance governance, transparency, and fraud prevention. It supports DBT, social security programs such as EPFO, NPS, and Ayushman

[6] Umar Bashir Mir, Arpan K. Kar, Yogesh K. Dwivedi, M.P. Gupta, R.S. Sharma, *Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India*, Government Information Quarterly, Volume 37, Issue 2, 2020, 101442, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2019.101442
[7] Srijoni Sen, *A Decade of Aadhaar: Lessons in Implementing a Foundational ID System*, ORF (2019) https://www.orfonline.org/public/uploads/posts/pdf/20230916141151.pdf
[8] Author's illustration

Bharat, and taxation compliance through Aadhaar-PAN linking. Additionally, Aadhaar eKYC streamlines SIM card registration and telecom verification, while state governments leverage it for public service delivery.

The private sector has also widely adopted Aadhaar authentication across e-commerce, travel, hospitality, healthcare, credit rating, and education, ensuring seamless identity verification and an efficient service delivery.

This research paper focuses on the Aadhaar Authentication System, which verifies an Aadhaar number along with demographic or biometric data against records in the Central Identities Data Repository (CIDR). The CIDR then responds with a "yes" or "no" based on the accuracy of the submitted information. The UIDAI maintains the CIDR and oversees the authentication framework, while Authentication User Agencies (AUAs) request authentication services and Authentication Service Agencies (ASAs) act as intermediaries, securely transmitting authentication requests. In the authentication process, an individual provides their Aadhaar number and relevant data to an AUA, which forwards the request through an ASA to the CIDR. The CIDR verifies the information and returns a response confirming or rejecting the authentication request. This system is critical for ensuring secure and efficient identity verification, supporting a broad range of public and private services.

3.2. Payments (UPI)

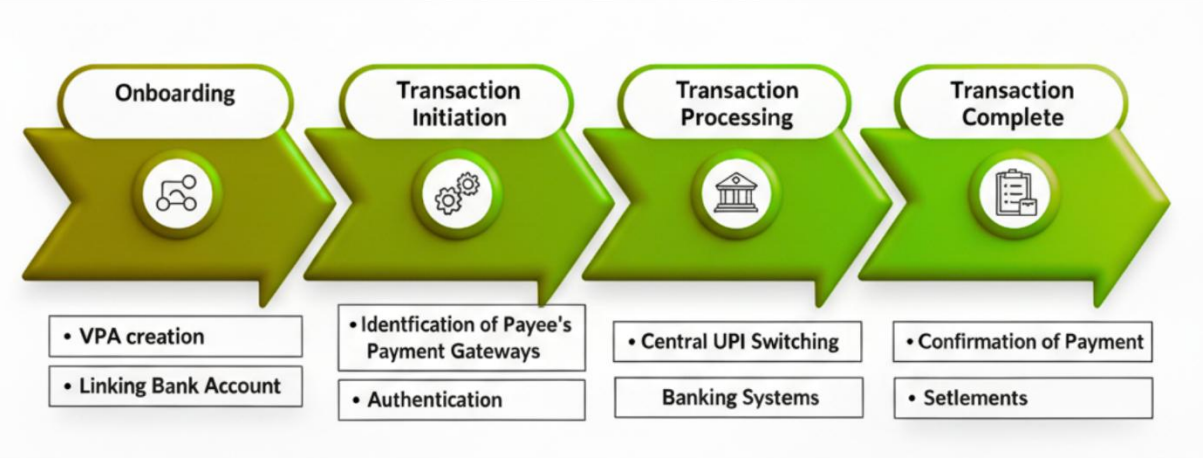
United Payment Interface (UPI), launched in 2016, has become a torchbearer of India's financial revolution, fundamentally reshaping the digital payments landscape and has achieved remarkable milestones[9]. Introduced by the National Payments Corporation of India (NPCI), UPI aims to create a fast and convenient payment system. It enables users to make instant, and real-time payments via smartphones, advancing the country towards a cashless economy. Its interoperability allows different banks to send and receive funds seamlessly.

Interoperability plays a critical role in the digital ecosystem, ensuring that data can be easily accessed, shared, and utilised to its fullest potential. The Indian government has been at the forefront of driving interoperability at the domestic level, with notable examples such as the UPI system. UPI supports both horizontal and vertical interoperability.[10] Horizontally, it allows different platforms and systems to be interoperable, enabling users across various platforms and apps to transact seamlessly. Vertically, it enables interoperability between payment apps and platforms and complementary products and services, facilitating convenient, one-stop payment solutions. This approach has revolutionised digital payments in India, with businesses and vendors adopting a wide range of digital payment methods through payment service providers. This interoperability process involves multiple components and different players at each level, as illustrated below in Figure 3.

[9] Chirag Chopra, Piyush Gupta, India's digital leap: the Unified Payment Interface's unprecedented impact on the financial landscape,World Economic Forum (2023) https://www.weforum.org/stories/2023/06/india-unified-payment-interface-impact/

[10] Hitesh Vyas, *UPI QR Code-Central Bank Digital Currency interoperability: How does it work and how do customers, benefit?, Indian Express (2023)* https://indianexpress.com/article/explained/explained-economics/upi-qr-code-cdbc-banks-explained-e-rupee-8925038/

Figure 3: UPI Components & Ecosystem

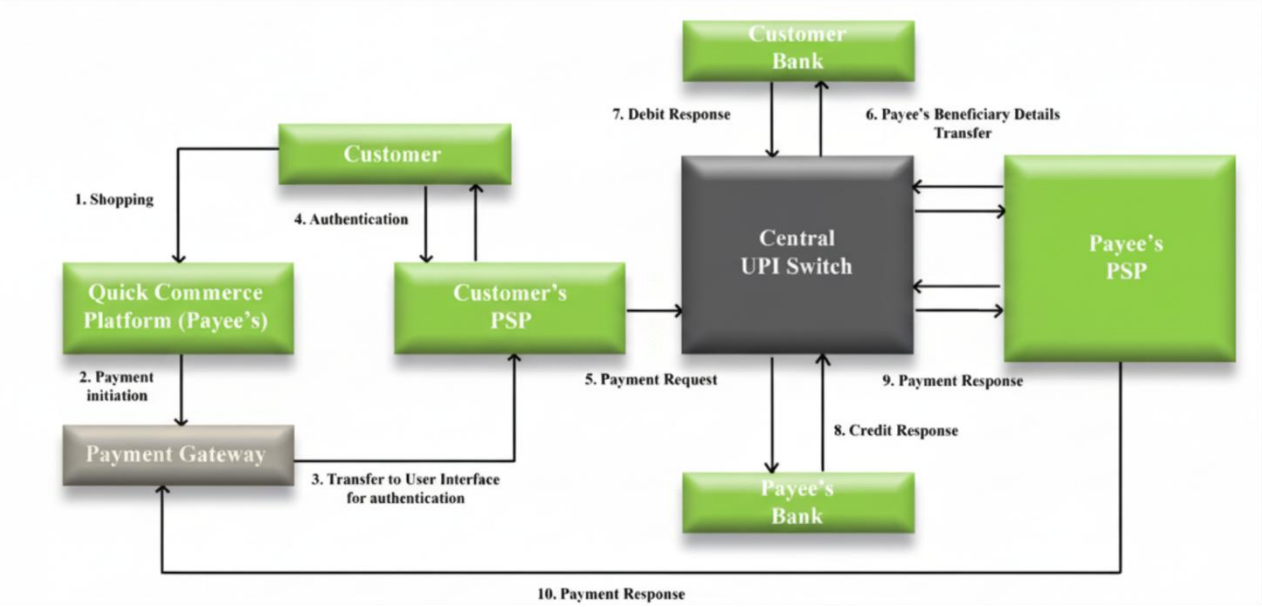


(Source: Author's illustration)

- **Onboarding Process:** To use UPI, individuals need to create a Virtual Payment Address (VPA)[11], which serves as a unique identification address. Third-party payment service providers create the user interface and link the VPA to the individual's bank account, often using SMS services.

- **Transaction Initiation & Processing:** Individual can initiate a UPI transaction multiple ways, such as by searching for the payee's VPA, scanning the QR code, or using a payment gateway. After selecting the recipients of the payment, the individual authenticates the transaction using a password to initiate processing of such transactions. Figure 4 illustrates a typical UPI transaction scenario.

Figure 4: UPI Transaction Scenario



(Source: Author's illustration)

- **Transaction Complete:** Once the transaction is processed, the customer receives a notification on the status of the payment. While the transaction reflects immediately on the user's interface, UPI typically takes a few hours to settle funds between banks, marking the transaction as fully complete.

3.3. Data Sharing (Account Aggregator)

In 2016, the Reserve Bank of India (RBI) introduced master directions for the constitution of an account aggregator ("AA") ecosystem in India, a new category of Non-Banking Financial Companies (NBFCs) mandated to operate as consent managers for citizens.[12] This framework was conceptualised by the

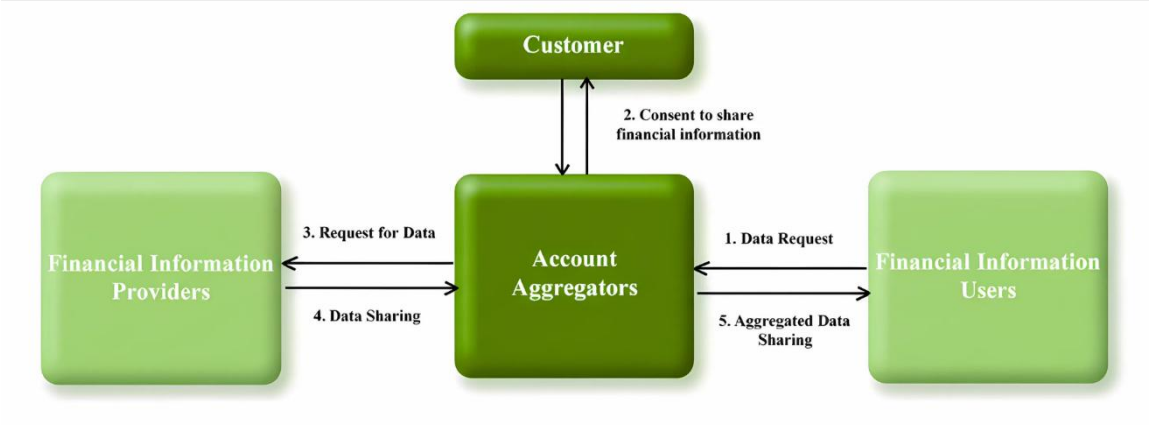
[11]RazorPay, What is UPI? Unified Payments Interface Features and How UPI Works
https://razorpay.com/blog/what-is-upi-and-how-it-works/
[12] Reserve Bank of India - Master Directions.
https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598
Since 2016, the mandate has been amended frequently, the latest amendment being 6th Septmeber, 2024.

Financial Stability and Development Council (FSDC) during its 2014 - 2015 meetings[13] and later implemented by the RBI in the form of the aforementioned master directions. It enables the collection and provision of information on customers' financial assets in a consolidated, organised, and retrievable manner, strictly based on the customer's consent.

This novel classification not only facilitates diverse advancements in financial technology in India but also rests on the principles of financial inclusion and the establishment of an interoperable financial data management system. This framework is designed to provide a wide range of financial services at reduced costs to consumers, encompassing material expenses as well as resource, time, and effort investments in financial management. Furthermore, it holds the potential to significantly enhance not only financial management but also social services, including pensions, insurance, and securities.[14]

The AA framework involves three key stakeholders: (i) Financial Information Users (FIUs), (ii) AAs, and (iii) Financial Information Providers (FIPs).[15] FIPs include banking companies, non-banking financial companies (NBFCs), insurance providers, taxation platforms, etc., that transact with customers and maintain their financial data. FIUs are defined as regulated entities by any financial sector regulator, including lenders, insurers, wealth managers, etc. FIPs and FIUs are not mutually exclusive categories; a FIP entity can also be an FIU. AAs, as a creation, are meant to be the bridge between FIPs and FIUs, enabling customers to 'manage' their financial data and access a host of services. All AAs are licensed by the RBI. Figure 5 illustrates how AAs operate as consent managers.

Figure 5: Account Aggregator Framework



(Source: Author's illustration)

[13] Department of Economic Affairs, Ministry of Finance. Retrieved September 10, 2024, from https://dea.gov.in/fsdc.
[14] Expected Evolution of Account Aggregator Ecosystem 2023-2027 - Sahamati. (2022, November 25). Sahamati. https://sahamati.org.in/expected-evolution-of-account-aggregator-ecosystem-2023-2027/ [hereinafter "White Paper 2023-2027, Sahamati"].
[15] According to Sahamati, Technology Service Providers (TSPs), while a part of the ecosystem, fall outside of the regulatory ambit; they provide multiple technical services to the key stakeholders, including (i) the development of AA protocols and flows per ReBIT norms, (b) designing front end journeys for FIUs, (c) providing data analytics solutions to process the raw data received from FIPs through AAs, and (d) offering certification and audit services. DigiSahamati. Retrieved September 10, 2024, from https://sahamati.org.in/tsp/.

4. Diagnostics of the Financial DPI Ecosystem

Having explored the structure, design, and operational mechanisms of India's key financial DPIs, Aadhaar, UPI, and the Account Aggregator, in Chapter 3, we now turn our attention from understanding how these systems function to evaluating how they perform in practice. Chapter 4 undertakes a diagnostic assessment of the Financial DPI ecosystem, examining not only their achievements but also the subtle challenges and gaps that arise during implementation. By identifying these areas, we lay the groundwork for later chapters, where we explore how artificial intelligence can be strategically leveraged to address these gaps, enhance system efficiency, and expand the reach and impact of India's financial DPIs.

4.1. Aadhaar

Designed to provide every resident with a reliable, digitally verifiable identity, Aadhaar has grown into the world's most extensive digital identity program. It enables seamless authentication and facilitates the delivery of services, benefits, and subsidies. Today, with over 138 crore Aadhaar numbers issued,[16] the system has strengthened trust in government processes and streamlined access to essential services.

Its integration with social welfare programs has significantly improved efficiency and accountability.[17] By simplifying identity verification, Aadhaar has strengthened India's digital infrastructure, which continues to serve as a cornerstone of inclusive governance. While Aadhaar has enhanced public service delivery by improving efficiency and accessibility, opportunities remain to further optimise its effectiveness.

Table 1: Opportunities for Strengthening Stakeholder Roles and Workflows in Aadhaar Authentication

Workflow (Refer to figure 2)	**Stakeholders (Refer to figure 2)**	**Mapping Venues for Enhancement**
Authentication Request	Authentication User Agencies (AUA) Common Service Centres (CSC) Customer Service Point (CSP)/Banking kiosk	**Biometric Quality:** Authentication can sometimes be affected by variations in biometric quality. Natural factors such as fingerprint wear, ageing, and medical conditions affecting skin texture can impact the accuracy of biometric

[16] MeiTY, *"Government of India taking measures to enhance the reach of Indian Digital Public Infrastructure"* (26th July 2024) https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2037598
[17] MeiTY, *"Aadhaar: A Unique Identity For The People"* (24th October 2024) https://pib.gov.in/PressReleasePage.aspx?PRID=2067940

		recognition systems. Alternative verification options may not always be readily available[18]. **Fraud:** The authentication process faces the risk of fraud due to (a) identity spoofing and document forgery,[19] and (b) the involvement of multiple players at Customer Service Points.[20] **Data Concerns:** Data protection concerns arise in two ways: (a) There is limited information on how AUA maintains data collected as part of the authentication requests, and (b) involvement of private players at CSCs or CSPs might complicate data management process[21] **Grievance Redressal:** Beneficiary document-related concerns may adversely affect authentication. A system that communicates appropriate resolution pathways to individuals to correct their documents is currently lacking.[22] **Human Errors:** Authentication processes can be affected if Aadhaar information is not fully or accurately seeded into the relevant databases.[23] A key reason for these delays is a shortage of human resources, resulting in backlogs due to delayed manual data entry processes and human errors in feeding data.
Secured CIDR Connectivity	Authentication Service Agency (ASA)	**Latency Delay:** Authentication delays could happen due to potential latency delays in authentication request processing, particularly during the peak processing hours, due to the system's technical limitations. This could also

[18] Indian Express Article on *"Aadhaar biometrics not reliable in India's climate: What Moody's has said"* (26th September 2023) https://indianexpress.com/article/explained/explained-economics/aadhaar-biometrics-reliable-moodys-climate-8955019/

[19] Economic and Political Weekly's Paper on *"Aadhaar Failures: A Tragedy of Errors"* (5th April 2019) https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare

[20] Dvara Research's Article on "*Agent Fraud in Welfare Transfers: A Case Study in Exclusion:* (September 1, 2020) https://dvararesearch.com/agent-fraud-in-welfare-transfers-a-case-study-in-exclusion/

[21] INC42 Article on *"CAG Flags Concerns On Aadhaar Data Collection And Management; UIDAI's Next Step Awaited"* (14th April 2022) https://inc42.com/buzz/cag-flags-concerns-on-aadhaar-data-collection-and-management-uidais-next-step-awaited/ ; https://dvararesearch.com/agent-fraud-in-welfare-transfers-a-case-study-in-exclusion/

[22] Dvara Research's Article on *"Aadhaar Related Delay in Obtaining Ration Card: A Case Study in Exclusion"* (19 March, 2021) https://dvararesearch.com/aadhaar-related-delay-in-obtaining-ration-card-a-case-study-in-exclusion/;

[23] Vrinda Bhandari & Renuka Sane, *A critique of Aadhaar Framework,* National Law School of India Review, (2019) https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1257&context=nlsir

		occur due to network congestion and limited pipeline capacity.[24]
Authentication	UIDAI	**Database Error:** Authentication can also be affected due to errors in beneficiary records, biometric mismatches, and other database-related inconsistencies.[25] These issues may arise due to clerical errors during data entry, as mentioned earlier, or during the validation process, where the authentication request is cross-referenced with existing database entries. In many cases, mismatches occur because of minor discrepancies in names, addresses, or biometric data, which prevent successful verification. A key underlying factor is the sheer volume of data being processed. **Fraud detection:** The system, which extensively supports welfare schemes and financial services, is increasingly vulnerable to malicious activities. It is therefore essential to deploy technologies that detect suspicious patterns, such as repeated failed attempts, or unusual geographic access, by analysing existing data.

4.2. UPI

UPI has democratised financial access, making person-to-person (P2P) and person-to-merchant (P2M) transactions easier, safer, and more efficient.[26] Despite its widespread adoption, UPI faces certain structural and operational challenges that could affect its long-term sustainability and efficiency.

[24] The Hindu article on "*Delay in authentication of Aadhaar with SATS deprives 26 lakh students of various government programmes in Karnataka"*(8 February, 2025) https://www.thehindu.com/news/national/karnataka/delay-in-authentication-of-aadhaar-with-sats-deprives-26-lakh-students-of-various-government-programmes-in-karnataka/article69146438.ece

[25] Dvara Research's Article on *"Exclusion from PM Kisan due to delay in correction of beneficiary records in PFMS"* (20 August, 2020) https://dvararesearch.com/exclusion-from-pm-kisan-due-to-delay-in-correction-of-beneficiary-records-in-pfms/

[26] Ministry of Finance "*UPI: Revolutionizing Digital Payments in India"* (1st December 2024) https://pib.gov.in/PressReleasePage.aspx?PRID=2079544

Table 2: Opportunities for Strengthening Stakeholder Roles and Workflows in UPI

Workflow (Refer to figure 3)	**Stakeholders (Refer to figure 3)**	**Mapping Venues for Enhancement**
Onboarding	Third-party payment service providers Banks	**Mobile Number Issues:** The most common reason for Virtual Payment Address (VPA) registration failures is that the mobile number provided is not linked to the bank account intended to be used. Since VPA relies primarily on mobile-based authentication (where an SMS from the registered mobile number verifies account credentials), any mismatch between the mobile number and the bank's records would lead to unsuccessful verification. **Connectivity issues:** Connectivity problems can occur in two ways. (a) A lack of stable internet connectivity may disrupt the verification process, and (b) A lack of telecom reception could disrupt the verification process due to the unsuccessful delivery of verification SMS. **Technical Issues:**. Although UPI has demonstrated remarkable resilience and scalability in handling billions of transactions, technical issues can arise, specially during the VPA registration process. These may result from temporary network congestion, maintenance windows, or localised bank server bottlenecks. While rare, such instances can affect the smooth registration of new VPAs.
Transaction Initiation	Payment Gateways Third-party payment service providers	**Fraud:** The payment initiation stage is a critical point where fraud risks arise, especially in the form of unauthorised transactions. PSPs rely primarily on the user's credentials (e.g., password or PIN) as proof of consent, which makes it challenging for them to independently verify the user's genuine intention beyond the possession of these credentials
Transaction Processing	Third-party payment service providers Banks	**Processing Delay/Failure:** Technical issues may cause processing delays or failures, particularly during peak processing hours. System's technical limitations, and network

	Central UPI Switch (NPCI)	congestion may also contribute to these delays.[27] **Uneven Interoperability:** Despite UPI's success in enabling interoperability, the system faces concerns about uneven interoperability with other payment infrastructures. Different payment systems use distinct APIs, protocols, data management approaches, and security standards, which can cause transaction failures, prolonged transaction times, and security concerns, specially for international transactions[28]. **Multi-Account Transaction:** UPI allows users to link and manage multiple bank accounts within a single PSP application. However, frequently switching accounts for transactions can cause glitches, leading to transaction failures due to application-level errors or synchronisation delays. **Fraud detection:** UPI supports low- and high-value transactions, making it a critical component of digital payments. However, as its adoption grows, so does its exposure to malicious activities and security threats. Deploying advanced technologies capable of analysing transaction data for suspicious patterns, such as repeated failed attempts, access from atypical geographic locations, and other anomalies, is crucial to mitigate these risks.
Transaction Completion	Third-party payment service providers Banks Central UPI Switch (NPCI)	**Grievance Redressal:** The UPI system features a three-tier grievance redressal mechanism involving third-party payment service providers, banks, NPCI, and the Banking Ombudsman. However, enhancing this mechanism to ensure timely and efficient resolution of issues remains essential.

4.3. Account Aggregator Framework (AA)

Designed to serve India's vast and complex financial landscape, the AA system aims to enhance consumer access to financial products by providing a secure, consent-driven mechanism for data exchange. While adoption rates (approximately 112 million

[27] ORF's article on *"UPI at Scale: Outages and the Push for Resilient Systems"* (21 June 2025) https://www.orfonline.org/expert-speak/upi-at-scale-outages-and-the-push-for-resilient-systems
[28] Rungcharoenkitkul, P., 2024. Generative AI in central banking. *BIS Papers*, p. 1–21

users) indicate growing trust in the AA ecosystem, certain gaps and challenges persist, limiting the framework from reaching its full potential.

Table 3: Opportunities to Strengthen Stakeholder Roles and Workflows in the AA Framework

Workflow (Refer to figure 5)	**Stakeholders (Refer to figure 5)**	**Mapping Venues for Enhancement**
Data Request	Financial Information Providers (FIUs) AA	**Real-Time Anomaly Detection:** Monitoring and flagging suspicious API calls can be cumbersome.[29] The AA framework involves multiple players, including various types of financial service providers, each following different logging standards. Consequently, monitoring, logging, correlating, and analysing API traffic across players becomes cumbersome. Additionally, because API requests occur in real time, there is little room for delayed batch analysis.
Consent to share financial information	AA Customers	**Trust Concerns:** Although the AA framework is designed as a credential-free, consent-based system, many consumers lack understanding, making it difficult to distinguish from credential-based systems. For instance, individuals may mistakenly believe that AAs or FIUs can access their credentials, leading to erosion of trust.[30] **Visibility Concerns:** Once data is shared, individuals worry about exposure to leaks, hacks, or unauthorised use. While AAs provide information on who accessed users' data, what was shared, and for how long, users still experience opacity in the process. **Fraud detection:** Effectively mitigating risks requires deploying advanced technologies capable of analysing request data for patterns indicative of suspicious behaviour.

[29] Green, J.R. and Craven, A.E., 2017. Account aggregation tools: History and use for the future. *Academy of Business Research Journal,* p. 77
[30] Green, J.R. and Craven, A.E., 2017. Account aggregation tools: History and use for the future. *Academy of Business Research Journal,* p. 77

Aggregated Data Sharing	AA Financial Information Users	**Information Gap:** FIUs often face gaps in accessing comprehensive financial information, relying on multiple sources or APIs outside the AA system. This limits their ability to obtain a complete view of an individual's financial profile, potentially delaying transactions.[31] Despite over 80 FIPs theoretically participating, many remain inactive in practice, either failing to respond to data requests from AAs or providing only partial information.[32]

[31]Livemint article on *"A fintech startup's challenges with India's vaunted account aggregator framework",* (20 Nov, 2024)
https://www.livemint.com/money/account-aggregator-fintech-startup-fold-money-bank-savings-fixed-deposit-credit-loans-mutual-funds-rbi-11732084804979.html
[32] *FIP-AA Mapping | FIP - Account Aggregator mapping - Sahamati*. (August 13, 2024). Sahamati. https://sahamati.org.in/fip-aa-mapping/.

5. Existing AI Use Cases Within Financial DPIs

Building on the diagnostic assessment of the Financial DPI ecosystem in the previous chapter, which highlighted the subtle gaps in implementation, this chapter now examines how these gaps are already being addressed and where artificial intelligence has begun to make an impact. We explore areas within financial DPIs where AI has been effectively deployed, as well as potential domains where it could further enhance functionality, efficiency, and the overall user experience.

For the purposes of this paper, AI applications are classified into five core functional areas, each defined by their principal benefits and impact, as outlined in Table 4. Each AI-driven use case (or potential application) is mapped to one or more categories to demonstrate its primary functions and advantages.

Moreover, this mapping exercise draws on the workflow architecture of financial DPIs introduced in Chapter 4. By aligning AI innovations with the operational flows and component layers of these systems, this chapter identifies where AI can have the greatest impact, directly building on the enhancement opportunities outlined earlier.

This chapter presents a non-exhaustive overview of AI integration within the financial DPI ecosystem. While many other AI-driven innovations are likely emerging across different components, the examples highlighted here come from primary and secondary research conducted during this study. The aim is to illustrate the range and diversity of current AI applications that enhance functionality, security, and user experience across financial DPIs, while recognising that the landscape continues to evolve rapidly.

Table 4: AI Functional Areas and Use Cases

Use-case	Relevance
(**E**) Experience Enhancement	Improves user-facing processes and creates smoother, more accessible interactions
(**K**) Knowledge Access	Expands how users retrieve and understand information.
(**P**) Process Productivity	Automates and streamlines workflows, reducing manual tasks
(**S**) Security/Fraud	Detects and prevents malicious activity while strengthening authentication
(**D**) Decision Making	Applies analytics, underwriting, or other AI-driven outcomes to guide actions

5.1 Existing AI Integrations

This section examines the current landscape of AI integration within the architecture of financial DPIs. It systematically identifies concrete use cases across multiple layers and component levels, ranging from foundational infrastructure to application interfaces. By mapping these use cases to specific

architectural components, the section illustrates how AI-driven innovations enhance operational efficiency, security, user experience, and service delivery.

5.1.1. AI Integration in Aadhaar

AI is being integrated into multiple components of the Aadhaar ecosystem to enhance accuracy, efficiency, and responsiveness across the workflow. It strengthens identity verification, improves service delivery, and supports grievance redressal.

For instance, advanced machine learning technologies improve identity matching and reduce false positives. On the fraud detection front, AI systems identify suspicious patterns in documents, bolstering security and trust. Moreover, AI also optimises processing times by accelerating documentation, updates, and grievance resolution. In addition, chatbots and virtual assistants provide real-time responses to user queries, guide individuals through complaint registration, and share status updates. Table 5 outlines some key use cases within the Aadhaar workflow and maps them to the functional areas defined in Table 4.

Table 5: Existing Use Cases of AI Integration within the Aadhaar Ecosystem

Workflow	Stakeholders	Existing Use Cases	AI Functional Areas
Authentication Request	AUA	**Aadhaar Masking:** Solutions like AutomationEdge[33] help enterprises mask Aadhaar details in compliance with RBI mandates.[34] These providers leverage AI-driven intelligent document processing tools, such as Optical Character Recognition (OCR) and Natural Language Processing (NLP), to automate Aadhaar masking. They can be configured to conceal sensitive information, including names, dates of birth, Aadhaar numbers, and QR codes. AI-powered Aadhaar masking solutions streamline KYC workflows in the Banking, Financial Services, and Insurance (BFSI) sector by removing manual tasks, accelerating processing, and ensuring regulatory compliance. They also enhance operational efficiency and safeguard data security.	(P S)

[33] AutomationEdge, *AADHAAR card masking made easy with intelligent document processing.* (31st August 2021) https://automationedge.com/blogs/aadhaar-card-masking-made-easy-with-intelligent-document-processing/
[34] Cashefree Payments Blog on "*Why is Aadhaar Masking mandatory for businesses?"* (June 10, 2024) https://www.cashfree.com/blog/why-is-aadhaar-masking-mandatory-for-businesses/

	UIDAI	**Fraud Alert:** UIDAI, in collaboration with Sarvam AI, is developing AI solutions to detect unusual patterns in authentication requests and alerting users to potential security threats.[35]	(E S)
Authentication	UIDAI	**Facial Authentication System:** The Unique Identification Authority of India (UIDAI) has deployed facial authentication technology as an alternative authentication method.[36] This scalable, non-invasive biometric solution complements traditional fingerprint- and iris-based systems while enhancing security and user convenience. Powered by AI-driven algorithms, the system analyses and matches facial features in real time, adding an extra layer of protection to the authentication process. UIDAI also launched the Aadhaar FaceRD app, which allows citizens to link their facial biometrics to their Aadhaar number for remote authentication. This feature reduces reliance on fingerprint or iris scans, particularly when biometric quality is poor.	(**E** **S**)
		Record–Finger Image Record (FMR-FIR): UIDAI developed an AI/ML-based Finger Minutiae[37] Record–Finger Image Record (FMR-FIR) system to counter spoofed or cloned fingerprints. The system enhances security with liveness detection, which distinguishes genuine fingerprints from fake ones, and applies two-factor authentication by combining minutiae and image analysis for robust verification.	(**P** **S**)
		Aadhaar Data Vault (ADV): UIDAI has mandated the centralised storage of Aadhaar numbers in an encrypted repository called the Aadhaar Data Vault . The ADV enhances the security of Aadhaar numbers and related data while ensuring compliance with data protection standards. Beyond secure storage, it uses AI	(**P** **S**)

[35]Legality Simplified blog on "*AI to enhance user experience of Aadhaar services"* (March 19, 2025) ttps://www.legalitysimplified.com/ai-to-enhance-user-experience-of-aadhaar-services/

[36] Airtel Payments Bank. (n.d.). *AEPS for face authentication: What does this mean?.* https://bankingpoint.airtel.in/airtel-payments-bank/banking-point-in-new-delhi/banking-point-in-phase-4/airtel-payments-bank-banking-point-in-phase-4-new-delhi--f1edad6b-34b4-42f0-8572-2f12d1035ecb/articles/aeps-for-face-authentication-what-does-this-mean--43dca092-8863-44fe-a1c3-1a97fa5f2163

[37] Stanly, M, UIDAI is using AI to confront payment fraud. INDIAai. (August 2024) https://indiaai.gov.in/article/uidai-is-using-ai-to-confront-payment-fraud

		algorithms to improve data quality and integrity. These AI models detect and remove duplicate records within the Aadhaar ecosystem, enabling more accurate identity resolution and reducing redundancy. [38]	
		Aadhaar Mitra: Aadhaar Mitra[39] is UIDAI's chatbot designed to address queries and concerns related to Aadhaar. Users can type their questions directly into the chatbot and receive instant responses. Currently, the Aadhaar Chatbot is available in Hindi and English.	(**E** **K**)
		Voice-based Aadhaar Services: UIDAI has partnered with Sarvam AI to enable voice-driven Aadhaar service interactions. Users can check enrollment status, request updates, or receive real-time instructions through simple voice commands, making services more accessible for individuals less comfortable with text-based applications.[40]	(**E** **K**)

5.1.2. AI Integration in UPI

Like the Aadhaar ecosystem, the UPI ecosystem integrates AI technologies to enhance security, efficiency, and user experience. A key application lies in fraud detection and risk management, where ML models analyse transaction patterns and flag anomalies in real time. At the user level, AI supports better financial management by helping individuals track and understand their spending habits. In addition, NLP further expands accessibility by enabling conversational interfaces and chatbots within UPI applications. Users can interact with payment systems through voice or text in multiple languages, making the platform more inclusive.

Table 6 highlights key use cases of AI integration across the UPI workflow and maps them to AI functional areas discussed in Table 4.

[38] IBM on *"Building Aadhaar Data Vault Solution on IBM LinuxONE"* https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/sandeep-batta/2024/05/09/aadhaar-data-vault-on-linuxone

[39] The Times of India on "Explained: What is Aadhaar Mitra and how to use it" https://timesofindia.indiatimes.com/gadgets-news/explained-what-is-aadhaar-mitra-and-how-to-use-it/articleshow/108178637.cms

[40] Tice article on "*Worried About Aadhaar Fraud? UIDAI's New AI Tech Might Be the Solution*", https://www.tice.news/know-this/uidai-partners-with-sarvam-ai-to-improve-aadhaar-services-using-ai-8868005

Table 6: Existing Use Cases of AI Integration within the UPI Ecosystem

Workflow	Stakeholders	Existing Use Cases	AI Functional Areas
Transaction Initiation	NPCI	**Hello UPI:** AI-powered chatbots and virtual assistants drive multilingual voice-based UPI payments. With RBI's support, NPCI launched *Conversational Payments on UPI* to expand convenience and financial inclusion. Unlike traditional text-based navigation, Hello! UPI[41] enables users to make payments via voice commands in regional languages that are accessible on smartphones, feature phones, and even IoT devices. This innovation simplifies digital transactions and improves accessibility for senior citizens, digitally inexperienced users, and the visually impaired.	(E K P)
Transaction Processing	Banks Third-party payment service providers	**AI Behaviour Analytics (Fraud Detection):** Various banks have deployed AI-based behaviour analytics to study user interaction patterns and combat fraud. For instance, HDFC Bank reported a 22% drop in UPI-related fraud after applying AI-driven behavioral analytics to transaction activity.[42] Similarly, banks and third-party payment providers use Convolutional Neural Networks (CNNs) to analyse spending behaviour and spot anomalies. The process involves compiling labeled transaction data, preprocessing it, extracting key features such as transaction amounts and user behaviour, and training CNN models to distinguish genuine transactions from fraudulent ones. Real-time evaluation automatically flags or blocks suspicious activity and alerts banks without manual	(P S)

[41]Hello UPI! https://www.npci.org.in/what-we-do/hello-upi/product-overview
[42] Revolutionizing Digital Payments: The Impact of AI-Driven UPI Integration in 2024 https://www.linkedin.com/pulse/revolutionizing-digital-payments-impact-ai-driven-upi-vinit-choudhary-gurtc

		intervention. Platforms like Razorpay[43] and PhonePe already leverage AI/ML-based systems to monitor transactions, detect irregularities, and strengthen security, thereby activating timely fraud prevention. NPCI is spearheading these efforts by deploying AI/ML-driven analytical models to proactively detect fraudulent activity. Its systems assign dynamic risk scores to accounts, drawing on transaction histories and money flow patterns. For instance, accounts attempting multiple suspicious transfers are flagged in real time, with NPCI either alerting banks or, in certain cases, directly declining the transactions. This federated model, where NPCI shares its AI-generated scores with banks, who in turn add their own customer insights, creates a multi-layered safeguard. By combining demographic profiling from banks with transaction and device intelligence from NPCI, the approach enhances accuracy, minimizes false positives, and strengthens the overall fraud-prevention architecture of India's digital payments ecosystem.[44] Research shows that advanced ML algorithms, including Random Forest, XGBoost, and LSTM networks, achieve 98.6% precision in UPI fraud detection, outperforming traditional rule-based systems by 44%.[45]	
		AI Behaviour Analytics (Transaction Failure Control): Banks also use AI analytics to reduce transaction failures. Razorpay's routing engine processes millions of merchant transactions and achieves nearly 10% higher success rates	(P E)

[43]Razorpay's article on "*Fraud Detection in Financial Transactions: Types & How To Detect It*" https://razorpay.com/learn/fraud-detection-in-financial-transactions/

[44] Medianama article on "*NPCI Pilots AI Models to Curb UPI Fraud After Rs 1,087 Crore in Losses*" https://www.medianama.com/2025/04/223-npci-ai-upi-fraud-detection/

[45]UNIFIED PAYMENT INTERFACE FRAUD DETECTION USING MACHINE LEARNING, International Research Journal of Modernization in Engineering Technology and Science https://www.irjmets.com/uploadedfiles/paper/issue_2_february_2025/68059/final/fin_irjmets1740397305.pdf

		than conventional routing. This approach leverages real time adaptability rather than static rules.[46] Paytm's AI Router is an intelligent aggregator that optimises payment routing by linking multiple payment gateways through a single integration. Unlike traditional PA setups, which often face higher failure rates and operational complexity, the AI Router dynamically selects the best-performing gateway in real-time. Solutions like Paytm's AI Router further streamline UPI transactions by bypassing intermediaries. Using customisable routing logic and strong analytics, AI-driven payment routing boosts efficiency, minimises disruptions, and gives merchant greater control over their transactions.[47]	

5.1.3. AI Integration in the Account Aggregator (AA) Ecosystem

AI is playing an increasingly vital role in the AA ecosystem, enhancing secure, user-consented data sharing to support financial inclusion and innovation. Various stakeholders drive AI innovation at multiple levels. Financial institutions and fintechs leverage AI to create alternative credit scoring models, using insights from user-consented financial data, including cash flows, transaction patterns, and behavioural indicators, to assess creditworthiness more accurately, particularly for underbanked users. In parallel, AA entities also deploy AI to tackle the challenge of integrating fragmented data, ensuring consistency in data formats. Furthermore, as in the UPI and Aadhaar ecosystems, AI is widely used for fraud detection within the AA framework.

Table 7 highlights key use cases of AI integration across the AA workflow and maps them to the AI functional areas discussed in Table 4.

[46] Razorpay's blog on Enhancing Payment Efficiency with AI-Powered Dynamic Routing
Enhancing Payment Efficiency with AI-Powered Dynamic Routing - Razorpay Blog
[47] Introducing Paytm AI Router https://business.paytm.com/airouter

Table 7: Existing Use Cases of AI Integration within the AA Ecosystem

Workflow	Stakeholders	Existing Use Cases	AI Functional Areas
Data Request	Financial Information Providers (FIPs)	**AI for Underwriting and Transactions:** Financial service providers use AI to overcome underwriting delays and data fragmentation. For instance, CRIF Connect leverages its *NEOS* AI/ML engine on AA data for instant transaction categorisation and credit scoring, improving risk assessment efficiency.[48] Similarly, lending-focused FIUs (e.g., small NBFCs) use cloud-based AI to process consolidated AA data, reducing manual loan approvals from days to minutes[49]. Technology service providers are also building infrastructure to help FIUs harness AI within the AA ecosystem. For instance, Setu, in collaboration with Sarvam AI, introduced a domain-specific LLM *Sesame* to process AA-fetched data for credit underwriting, enabling advanced detection of patterns in borrower cash flows.[50]	(D P)
	Account Aggregators (AAs)	**AI for Verification:** AI powers a seamless verification process, reducing manual intervention when processing or syncing large datasets. For example, Protean SurakshAA introduced an AI-powered CKYC solution to automate compliance checks and streamline customer record verification.[51]	(P E)
Aggregated Data Sharing	Account Aggregators (AAs)	**AI for Standardisation:** While AA aggregate data, they face fragmentation due to varied formatting patterns. To address this AA players use AI for data standardisation. For instance, Cygnet AA employs AI-driven modules (e.g., OCR and	(P S)

[48] CRIF (2024) *Embracing the future: CRIF's approach to AI and innovation*. Available at: https://www.crif.com/knowledge-events/news-events/embracing-the-future-crif-s-approach-to-ai-and-innovation/.
[49] Vaidya, A., Digital Lending in India. *INDIA BANKING AND FINANCE REPORT 2024,* p. 167
[50] Economic Times (2024) *Pine Labs-owned Setu teams up with Sarvam AI to build LLM for financial services*. Available at: https://economictimes.indiatimes.com/tech/startups/pine-labs-owned-setu-teams-up-with-sarvam-ai-to-build-llm-for-financial-services/articleshow/109926155.cms?from=mdr.
[51] Protean (2024) *Protean CKYC Solution*. Available at: https://www.proteantech.in/articles/Protean-CKYC-Solution/.

		NLP) to automate mortgage paperwork and maintain consistent data formats for partner lenders[52]. Similarly, various OCR/NLP modules process bank statements from multiple FIPs, bridging gaps where APIs are not fully standardised.	
		AI for Personal Finance: AAs also offer AI-based personal finance management solutions to FIUs through their APIs. For instance, Finvu provides AI-driven personal finance dashboards that allow FIUs to deliver real-time spending insights to their customers using aggregated account data.[53]	(E K)

5.2 Potential Avenues for AI Integrations

Building on the previous section's review of current AI innovations across the financial DPI ecosystem, this section highlights potential areas for future AI integration. It identifies opportunities where AI can enhance functionality, scalability, and inclusivity within financial DPIs. The objective is to provide a forward-looking perspective on strategically embedding AI to address existing limitations, anticipate emerging needs, and support the development of a more intelligent and adaptive financial infrastructure.

5.2.1. Potential Avenues for AI Integration within the Aadhaar Ecosystem

Although the Aadhaar ecosystem has already adopted multiple forms of AI integration, this section explores how different stakeholders can further leverage AI to enhance security, user experience, inclusivity, etc.

Table 8 outlines key potential use cases of AI integration across the Aadhaar workflow and maps them to the AI functional areas discussed in Table 4.

[52] Cygnet (2024) *Cyg AI Solutions*. Available at: https://www.cygnet.one/solutions/cyg-ai.
[53] Finvu (2024) *Solutions - Building Use Cases*. Available at: https://finvu.in/solutions#:~:text=Building Use Cases ,analysis%2C forecasting and budget information.

Table 8: Potential Use Cases of AI Integration within the Aadhaar Ecosystem

Workflow	Stakeholders	Potential Use Cases	AI Functional Areas
Authentication	UIDAI	**AI for Fraud Detection:** Machine learning-based anomaly detection can significantly enhance Aadhaar authentication security. For example, Singapore already uses AI to analyse large volumes of login and transaction data to detect unusual patterns in Singpass.[54] In contrast, Aadhaar currently relies on basic fraud detection mechanisms such as flagging terminals with high authentication failure rates or blacklisting suspicious devices, which are still largely rule-based rather than adaptive. UIDAI could strengthen its approach by developing an AI-driven fraud analytics platform to analyse authentication logs and detect misuse patterns, such as repeated fingerprint images across multiple Aadhaar IDs, which may indicate synthetic identity fraud. With over a billion Aadhaar holders, UIDAI has a dataset large enough to train machine learning models that can proactively identify and prevent scams.	(S)
		Deepfake Detection: As UIDAI expands facial authentication technology as an alternative method, it should invest in or collaborate on AI models that can detect deepfakes.	(S)
		Multilingual Chatbot: The Aadhaar Mitra chatbot can use NLP to support users with queries in diverse languages.	(E K)
		Voice Biometrics: While UIDAI has introduced facial authentication, a voice-based system could serve individuals without internet access or those using feature phones. AI can help UIDAI develop technology to recognise unique voice characteristics such as pitch, accent, tone,	(E P)

[54] Singpass https://www.smartnation.gov.sg/initiatives/singpass/

		etc., for verification. For instance, Citibank and Standard Chartered Bank already use[55] voice prints to authenticate customers over the phone.[56]	

5.2.2. Potential Avenues for AI Integration within the UPI Ecosystem

Similar to the previous section, this section outlines how different stakeholders within the UPI ecosystem can leverage AI to strengthen security, improve user experience, and promote greater inclusivity, etc. Table 9 highlights potential use cases of AI integration across the UPI workflow. It also maps these use cases to the areas of AI introduced in Table 4.

Table 9: Potential Use Cases of AI Integration within the UPI Ecosystem

Workflow	Stakeholders	Potential Use Cases	AI Functional Areas
Onboarding	Banks NPCI	**Telephonic Authentication:** NPCI, in collaboration with banks, could explore a telephonic authentication system as an alternative to SMS-based methods. Such a system could use AI-powered voice-response technologies to enable secure and seamless authentication through automated calls. By integrating speech recognition and NLP, users could be authenticated via voice prompts or simple spoken inputs. This approach would improve accessibility, specially for individuals with limited literacy or in areas with weak mobile network connectivity.	(E P S)
Transaction Processing	Central UPI Switch (NPCI)	**AI for Standardisation:** AI technologies could enhance UPI interoperability with other payment systems, ensuring consistency in protocols, data management, and security standards. This interoperability could reduce transaction failures, shorten processing times, and strengthen security, particularly for international transactions.	(E P)

[55] Standard Chartered https://www.sc.com/en/press-release/weve-kicked-off-a-major-roll-out-of-biometric-technology-across-asia-africa-and-the-middle-east/; https://www.bbc.com/storyworks/banking-on-innovation/biometrics

[56] Forbes article on *"Citi Uses Voice Prints To Authenticate Customers Quickly And Effortlessly"* https://www.forbes.com/sites/tomgroenfeldt/2016/06/27/citi-uses-voice-prints-to-authenticate-customers-quickly-and-effortlessly/?sh=2da86b6e109c

	Third-party payment service providers	**AI for Error Management:** Third-party payment providers could apply AI to address synchronisation delays in multi-account transactions. Machine learning models trained on historical transaction patterns and network latency could optimise transaction batching and sequencing, reducing the apparent delays for end users and improving overall financial coordination.	(E P)
	Banks NPCI	**Federated Learning for Collaborative Security:** Similar to initiatives by Google Cloud and Swift[57], UPI could implement federated learning, where banks train fraud detection models locally and share only insights without exposing sensitive transaction data. Google Cloud and Swift are pioneering advanced AI and federated learning technologies to help combat fraud. This approach creates a form of 'Decentralised Threat Intelligence', enabling AI models to identify emerging fraud patterns across multiple banks while maintaining privacy and regulatory compliance.	(S)
Transaction Complete	Banks NPCI Third-party payment service providers	**AI-based Grievance Redressal:** The UPI system currently follows a three-tier grievance redressal process involving third-party payment providers, banks, NPCI, and the Banking Ombudsman. AI could be integrated to streamline this mechanism, enabling faster issue resolution, automated routing of complaints, and improved tracking across all tiers.	(E P)

5.2.3. Potential Avenues for AI Integration within the AA Ecosystem

The AA ecosystem holds significant potential for AI integration. As the ecosystem evolves and scales, this section explores opportunities to embed AI to enhance its capabilities. Table 10 highlights key potential use cases of AI integration across the AA workflow and maps them to the AI functional areas discussed in Table 4.

[57] SWIFT on Google Cloud
https://cloud.google.com/security/swift

Table 10: Potential Use Cases of AI Integration within the AA Ecosystem

Workflow	Stakeholders	Potential Use Cases	AI Functional Areas
Data Request	Financial Information Providers (FIPs)	**Federated Learning for Fraud Models:** FIPs could implement federated learning systems for fraud management. FIPs can collaborate by sharing only algorithmic parameters (not raw data), to collectively improve fraud detection.[58] This approach allows them to train fraud detection models together while maintaining data privacy and regulatory compliance. By pooling insights in this privacy-preserving way, participants can detect emerging fraud patterns more effectively and strengthen the robustness of their systems without compromising user confidentiality.	(P S)
	AAs	**Conversational AA:** Similar to Hello UPI!, AAs could develop a conversational consent management system using AI technologies. By NLP, speech recognition, and contextual understanding, this system could enable users to grant, review, modify, or revoke consent through voice or text-based interactions in their preferred language.	(E K)
Consent to share financial information	AAs	**Multilingual Chatbot:** AAs could implement chatbots in vernacular languages to reduce consent fatigue and confusion, particularly in rural areas. These chatbots would guide users through the consent process in a conversational, easy-to-understand manner, clarifying data-sharing scopes, durations, and purposes. They could also explain the difference between credential- and consent-based systems.	(E K)
Aggregated Data Sharing	FIUs	**NPA Monitoring:** FIUs could automate "recurring data fetch" from AAs to track post-loan disbursal usage, helping reduce NPAs by identifying early signs of borrower	(P D)

[58] OpenFHE (2024) *AAAI 2024 Lab Materials*. Available at: https://openfheorg.github.io/aaai-2024-lab-materials/,p. 31.

		stress.[59] This would allow FIUs to proactively identify early signs of financial distress and take timely corrective measures.	
	AAs	**Post-Quantum Cryptography:** AAs could deploy lattice-based encryption alongside AI-driven migration strategies to safeguard data flows against future quantum threats.[60] This combined approach would ensure that AA infrastructure remains secure, adaptive, and compliant with evolving cybersecurity standards, even in a post-quantum era.	(S)

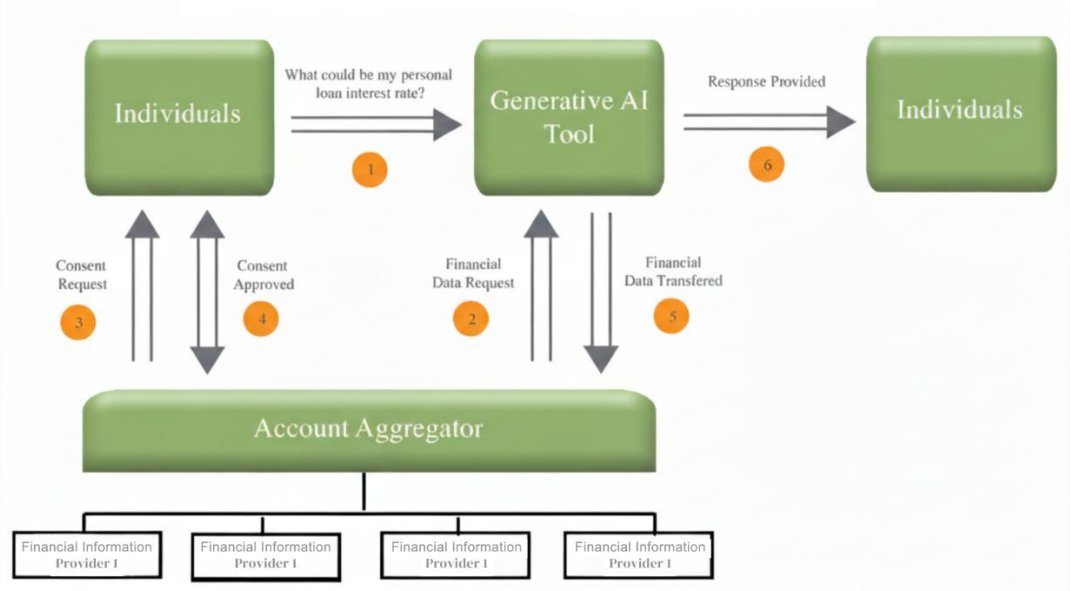
Box 2: Enhancing Business Viability of the Account Aggregator Framework Using AI

In recent years, NBFCs and banks have adopted the AA ecosystem to expand digital lending services. Looking ahead,, lending will remain a critical use case, given the centrality of bank account statements in credit assessments.[61] However, from a business perspective, expanding the use cases and paving the way for innovations such that AA find value propositions and competitive advantages in running the business is essential. Expanding the use cases beyond the credit-lending ecosystem would be one way forward. Keeping up with the recent innovation curve, this section discusses how the AA framework could be integrated with AI.

There could be AI integration in two forms: (a) integrating AI into existing DPIs to solve some of the existing issues and enhance the solution's capabilities, And (b) DPI could aid in the responsible development and deployment of AI solutions by providing infrastructure across the layers of the AI stack. The illustration below showcases one form of AAs integration within AI applications, highlighting the latter form of integration.

[59] Sahamati. (2024). *Data Capital: Unlocking Formal Finance for a Billion Indians*. https://sahamati.org.in/wp-content/uploads/2024/12/Sahamati-Annual-Report-2024.pdf, p. 21.
[60] Z1 Labs (2024) *Cypher: Unlocking confidential computing for AI with the first fully homomorphic encryption (FHE) and EVM integration*. https://z1labs.ai/blog/cypher-unlocking-confidential-computing-for-ai-with-the-first-fully-homomorphic-encryption-fhe-and-evm-integration/.
[61] White Paper 2023-2027, Sahamati.

Figure 6: Use Case of AI and Account Aggregator Integration



(Source: Author's illustration)

Explanation: (1) Individuals enquire with a generative AI tool about the interest rate for their personal loan, (2) To provide precise information and a tailored response, the generative AI tool requires the individual's financial information. With AA integration, the tool reaches out to the AA for this data, (3) The AA seeks the consent of the individual on the generative AI platform itself, (4) The individual provides consent, (5) The financial information is shared with the generative AI tool, (6) The tool responds to the individual with precise answers.

This use case serves a dual purpose. *Firstly*, consent is the bedrock on which not only the EU-GDPR but also India's Digital Personal Data Protection Act, 2023 rests, as both mandate that personal data may be processed only after obtaining consent from data principals at the commencement of processing.[62] Through this integration, we could reimagine how individuals' agency over financial and personal data used to train algorithms across the data lifecycle is protected and ensured. *Secondly*, this integration could help AAs expand their Financial Information User base beyond banks and NBFCs to include AI platforms. Therefore, while this integration represents a step in the right direction to enhance and unlock the framework's full potential, the financial information handled by the AA ecosystem must expand beyond bank account statements.

[62] DPDP Act, 2023, section 6.

6. Snapshot: DigiLocker and AI Integration

While we have tried to cover Aadhaar, UPI, and Account Aggregator in detail, we understand and acknowledge that the financial DPI space is much larger and has expanded to include other offerings such as DigiLocker as well. This chapter provides a brief snapshot of similar developments in this space.

6.1. Introduction

DigiLocker, with **53.92 crore registered users,**[63] has emerged as a cornerstone of India's DPI. It provides citizens with secure, paperless access to official documents anytime and anywhere, reducing administrative overheads for both government and private entities while ensuring authenticity and legal validity under the IT Act, 2000.

The value proposition of DigiLocker rests on several interlinked advantages. First, it delivers convenience and accessibility by serving as a single, centralised repository for crucial records. Second, it fosters a paperless ecosystem, cutting costs related to printing, storage, and verification, while supporting India's broader sustainability goals. Third, the platform enhances authenticity and validation by offering tamper-proof, verifiable documents that significantly reduce fraud and forgery risks.[64]

6.2. AI-Enabled Use Cases in DigiLocker

AI Capability	Application in DigiLocker & Benefit	Current Use-Cases
Auto-Classification	AI can intelligently classify and label uploaded documents (e.g., IDs, certificates, policies, tax records). This reduces manual sorting, ensures consistency, and enables faster retrieval during verification or service delivery.	**HyperVerge**[65] integrates DigiLocker APIs with AI to automatically categorise documents while extracting key attributes like expiry dates, registration details, and policy numbers, enhancing both accuracy and retrieval speed.

[63] PIB press note on *"Ten Years of Digital Progress Building an Inclusive and Future-Ready India"* (30 June 2025) https://www.pib.gov.in/PressNoteDetails.aspx?id=154788&NoteId=154788&ModuleId=3
[64] Angel One's article on "*What Is Digilocker and How To Use It?"* https://www.angelone.in/knowledge-center/personal-finance/what-is-digilocker
[65] Drapcode https://drapcode.com/integration/hyperverge/digilocker-api.

NLP-Based Search	NLP allows users to search their digital vault using conversational queries (e.g., *"Show my latest health insurance policy"*). It makes the platform more user-friendly, particularly for first-time users.	While not yet widely deployed, **HyperVerge's[66] intelligent search prototypes** demonstrates this potential. AI-driven NLP search can make DigiLocker more engaging and accessible, reducing friction in navigation and use.
OCR/Data Extraction	Optical Character Recognition (OCR) extracts critical fields from both digital and scanned documents (e.g., tax IDs, insurance policy numbers). This transforms static files into actionable data, reducing manual tagging and audit delays.	**HyperVerge[67]** enables OCR-powered digitisation, making documents searchable. **Olyv + Decentro[68]** use OCR in combination with AI to streamline customer onboarding, ensuring faster KYC and accurate, automated verification processes.
Fraud Detection	Machine learning models can identify manipulated documents or unusual user behavior (e.g., multiple log-ins from different locations). This adds a dynamic, real-time layer of security, complementing encryption and authentication.	**AadhaarKYC.io[69]** integrates AI, biometrics, and computer vision with DigiLocker APIs for real-time fraud detection. It ensures only authentic users are onboarded, with video KYC processes that are both precise and regulatory compliant.
Workflow Automation	AI can route compliance workflows, approve/reject documents, and auto-complete verification steps. This reduces human bottlenecks, lowers turnaround times, and ensures regulatory adherence with minimal manual oversight.	**Olyv, in partnership with Decentro,[70]** implemented AI-assisted DigiLocker APIs to automate KYC and onboarding funnels for lending and digital banking. Their solution improved efficiency and increased DigiLocker adoption by 200%.

[66] Drapcode https://drapcode.com/integration/hyperverge/digilocker-api.
[67] Drapcode https://drapcode.com/integration/hyperverge/digilocker-api.

[68] Decentro https://decentro.tech/blog/olyv-case-study/
[69] AadharKYC.io https://aadhaarkyc.io/products/digilocker-apis-and-sdk/
[70] Decentro https://decentro.tech/blog/olyv-case-study/

Predictive Reminders	AI can scan stored documents and proactively issue alerts for key deadlines (e.g., license renewals, insurance premiums, tax filings). It also improves preparedness in emergencies by securing family access to vital records.	**Smarana**[71] provides AI-powered reminders for renewals, payments, and expirations. It also enables families to set emergency protocols for accessing critical records, while offering personalised insights such as education or financial planning.

[71] Smarna article on "*Digilocker in the AI Era: A Deep Dive into its Pros, Cons, and the Future of Digital Document Management*" https://www.mysmarana.com/2025/07/28/digilocker-vs-smarana-ai-document-storage-2025/

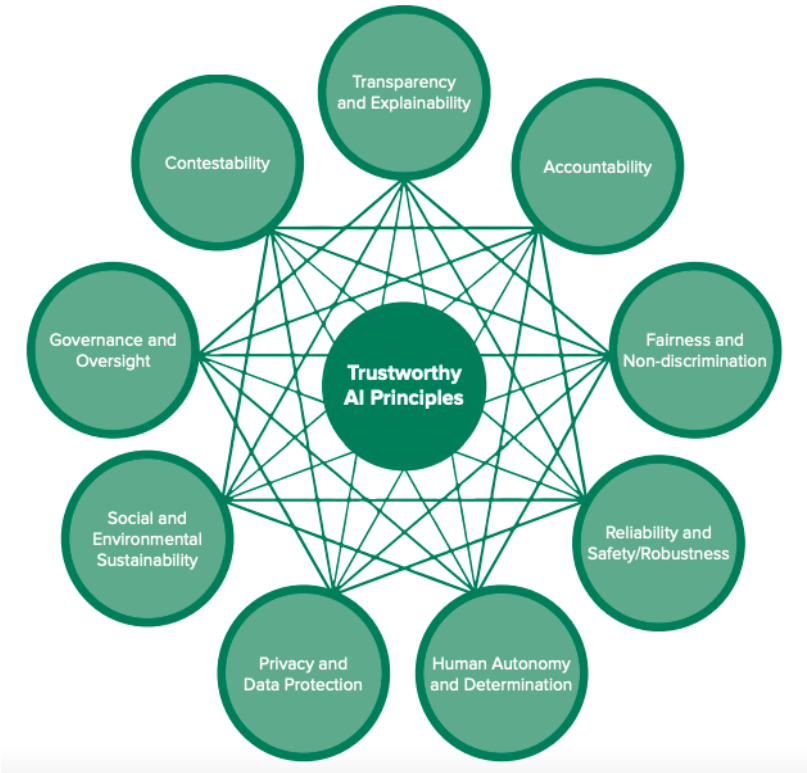
7. Guiding Principles and Governance Framework for AI and DPI Integration

AI integration within the financial DPI ecosystem is essential, as discussed in previous chapters. However there is a pressing need for a governance framework to oversee this integration and to address concerns around responsibility and accountability. Similar to the Data Empowerment and Protection Architecture (DEPA) framework, which defines governance structures and guiding principles for critical DPIs such as Account Aggregators, a dedicated governance framework is required to manage AI integration within financial DPIs.

This chapter outlines guiding principles for AI integration with financial DPIs, structured according to different layers and mapped to the stakeholders operating within them. Alongside these guiding principles, this presents a governance framework that details the roles, responsibilities, and accountability mechanisms of different actors. Some of the key principles relevant across financial DPIs are illustrated below.

It must be noted that the following chapter does not claim to provide an exhaustive set of AI principles or a comprehensive operational framework. Rather, it adopts an illustrative approach to explore how trustworthy AI principles may be embedded in the integration of AI within financial DPIs.

Figure 7: Key AI Governance Principles



(Source: Author's illustration; Advised by The Dialogue research on Trustworthy AI principles[72])

[72] The Dialogue's report on "*Towards Trustworthy AI: Sectoral Guidelines for Responsible AI Adoption*", Feb 8, 2024. https://thedialogue.co/wp-content/uploads/2024/02/Research-Paper-Towards-Trustworthy-AI-1.pdf

7.1. Responsible Integration of AI within the Aadhaar Ecosystem

Embedding a responsibility framework into AI integration within the Aadhaar ecosystem is essential. While AI integration amplifies the system's potential, it also heightens the associated risks. This is particularly critical because the Aadhaar ecosystem deals with highly sensitive personal information and underpins the delivery of essential services, including social security abenefits, access to financial services, etc.

Therefore, any AI deployment within Aadhaar must be guided by clear principles of accountability, transparency, fairness, and privacy. Table 11 outlines how different stakeholders can embed responsibility considerations when integrating AI within Aadhaar architecture.

Table 11: Principled AI Deployment in the Aadhaar Ecosystem

Workflow	Stakeholders	Existing Use Cases	Operationalising Trustworthy AI Principles
Authentication Request	UIDAI	Fraud Alert	**Contestability:** Implement mechanisms for users to challenge wrongful denials or authentication failures. UIDAI must provide accessible channels for inquiries, appeals, or reviews of AI-driven decisions that directly affect users. This empowers individuals to contest decisions where they have concerns or disagreements.
Authentication	UIDAI	Facial Authentication System	**Transparency & Explainability**: Clearly document and communicate how facial authentication works so users understand why their authentication may succeed or fail. Integrate model explainability tools such as LIME (Local Interpretable Model-Agnostic Explanations) or SHAP (SHapley Additive exPlanations) to provide insights into how specific predictions were made. **Reliability & Safety**: AI-driven facial authentication should be robust against variations in lighting, angles, or facial expressions to ensure consistent performance. Rigorous validation protocols must be implemented to continuously assess model performance. Models should be regularly updated models to adapt to changing data patterns and external factors,

			reducing the risk of unintended consequences. This practice is essential for the timely identification of anomalies and biases, and unintended consequences, thereby enabling prompt corrective actions. An alert system can notify stakeholders of upcoming periodic validations, ensuring uniform and timely assessments. Additionally, ad-hoc alerts triggered by anomalies can be incorporated to enable swift corrective measures and maintain the model's reliability and ethical standards. **Privacy & Data Protection:** Facial data should be securely stored and used solely for authentication, with strong safeguards against misuse. Various privacy-enhancing technologies can be employed. For instance, encryption at rest secures data stored on devices and servers by converting it into ciphertext that only authorised personnel with the encryption key can decode.[73] **Fairness & Non-discrimination**: AI models must be trained on diverse datasets to prevent biases that could disproportionately affect certain demographics. Special care should be taken to ensure that no specific groups are unfairly flagged for fraud. UIDAI should collaborate with end users to establish fairness standards for Facial Authentication Systems, conducting research to capture their views on fairness and non-discrimination and incorporating this feedback into the evaluation process. Ethicists, legal experts, sociologists, and others can contribute expertise to define fairness standards that align with societal values and norms.[74] This interdisciplinary approach ensures that AI systems are designed and deployed in a way that meaningfully incorporates ethical and societal considerations.[75]

[73] The Dialogue's report on "*Privacy Technologies in India, Strategies to enhance the ecosystem"* (July 20, 2023) https://thedialogue.co/wp-content/uploads/2023/07/FinalPrivacy-Technologies-in-India-Strategies-to-Enhance-the-Ecosystem-print_Kamesh-1.pdf

[74] Mantelero, A. (2022). The social and ethical component in AI systems design and management. In Information technology & law series (pp. 93–137). https://doi.org/10.1007/978-94-6265-531-7_3

[75] Open Loop Program on "*Responsible AI Principles through Stakeholder Engagement"* https://openloop.org/programs/open-loop-india-program/

		FMR-FIR	**Privacy & Data Protection:** Protecting stored fingerprint data from unauthorised access is essential. Also, ensuring compliance with data security regulations. UIDAI can explore identity management technologies such as access management solutions, which control access to necessary information, and pseudonym management solutions, which generate proxies.[76] **Security & Robustness:** It is essential to enhance security protocols using different techniques. For instance, liveness detection and two-factor authentication can strengthen security by preventing spoofing attempts. **Accountability**: Conduct regular audits and impact assessments to ensure AI models do not falsely reject legitimate users. Audit mechanisms for the model and algorithms that check results against baseline datasets help prevent unfair treatment or discrimination. One way to achieve this is by deploying a "first-order temporal logic" tool.[77]

7.2. Responsible Integration of AI within the UPI Ecosystem

Given the central role of the UPI ecosystem in India's DPI, integrating AI must be approached in a safe, fair, and secure manner. AI systems should remain transparent, auditable, and free from discriminatory biases to maintain trust and stability in one of the world's most widely used real-time payment systems.

Table 12 illustrates how different stakeholders can incorporate principles of responsibility when integrating AI into the UPI architecture.

[76] Hansen, M., Berlich, P., Camenisch, J., & Clauß, S. (n.d.). Privacy-Enhancing Identity Management. 2004: Information Security Technical Report. Retrieved from Information Security Technical Report.
[77] GeeksforGeeks. (2023, February 22). Artificial Intelligence Temporal logic. https://www.geeksforgeeks.org/aritificial-intelligence-temporal-logic/

Table 12: Principled AI Deployment in the UPI Ecosystem

Workflow	Stakeholders	Existing Use Cases	Operationalising Trustworthy AI Principles
Transaction Processing	Banks Third-party PSPs	AI Behaviour Analytics (Fraud Detection)	**Transparency & Explainability:** UPI's federated learning models should include transparent documentation on how fraud patterns are detected, what data is used, and how local insights contribute to the global model. Model decisions should be interpretable to both financial institutions and regulators. **Accountability:** Participating banks and the central coordinating authority (e.g., NPCI) should clearly define roles and responsibilities. Logs, audit trails, and periodic reviews must be instituted to ensure ethical development and deployment of AI models. Banks/Financial service providers should establish comprehensive governance frameworks with unambiguous lines of accountability across the AI lifecycle, from design to deployment. This may require enhancements to existing operational protocols. Internal model governance frameworks should also be refined to more effectively address risks arising from AI utilisation. **Fairness & Non-discrimination:** Fraud detection models must be regularly tested for bias, ensuring they do not unfairly flag users based on geography, demography, or socio-economic status. Using diverse data inputs from multiple banks helps build equitable systems. **Reliability & Robustness:** Federated models should maintain accuracy across varied datasets and remain resilient against adversarial attempts such as data poisoning or model inversion attacks. Continuous testing and retraining are necessary to sustain performance over time. **Human Autonomy and Determination:** Banks should retain final decision-making

			authority even when AI detects fraud patterns. Customers flagged by AI systems must have access to human-led redressal mechanisms to contest or explain anomalies. A structured framework for human intervention ensures that significant financial decisions are not made by AI alone, reducing the risk of errors and losses. **Contestability:** Users must be able to challenge false positives in fraud detection via transparent mechanisms. Banks should maintain clear channels for dispute resolution and ensure that AI decisions can be explained and reviewed. Financial institutions should create well-defined protocols for addressing customer challenges and communicating them prominently to ensure awareness. In cases of discrepancies, deployers must have mechanisms in place to investigate, mediate, and resolve disputes effectively.

7.3. Responsible Integration of AI within AA Ecosystem

As the scope of AI integration within the AA ecosystem expands, it is essential to ensure that such integration is undertaken in a responsible and trustworthy manner. Given the sensitive nature of financial data and the critical role the AA framework plays in enabling consent-based data sharing, AI systems must be designed with strong safeguards to ensure privacy, fairness, transparency, and accountability.

Table 13 illustrates how each stakeholder can incorporate a responsibility framework when integrating AI within the AA ecosystem.

Table 13: Principled AI Deployment in the AA Ecosystem

Workflow	**Stakeholders**	**Existing Use Cases**	**Operationalising Trustworthy AI Principles**
Data Request	Financial Information Providers (FIUs)	AI for Underwriting and Transaction	**Transparency & Explainability:** Embrace regular audits to ensure transparency and explainability in AI models, wherever possible. For instance, in the context of a bank's AI-driven credit scoring model, regular audits scrutinize the model's behavior over time. Auditors assess whether the model provides clear explanations for its

			credit decisions and whether these align with established principles of transparency and accountability. **Accountability:** Internal risk management teams should take accountability for deploying AI-based financial products and services. They must fully understand the models they oversee and be able to explain their functioning to senior management and/or designated committees. **Fairness & Non-discrimination:** FIUs should ensure ethical collection of financial data through AA, making it representative and preventing bias or discrimination against any customer groups based on religion, caste, gender, low purchasing power, etc. **Reliability & Safety:** FIUs should create blind test datasets specific to financial applications. These datasets should remain separate from the model selection and validation process to provide an accurate estimate of the model's generalisation performance in real-world scenarios. **Human Autonomy:** While AI models may handle credit underwriting, there should be a structured framework for human intervention when necessary.

8. Conclusion

AI integration into India's DPI is a vast and evolving subject, far larger than this paper can cover in full. Questions of talent, cost, evaluation, and governance are layered and complex, ranging from GPU and data requirements to the institutional readiness of actors like NPCI or UIDAI. These challenges demand continuous assessment across multiple dimensions, accuracy, robustness, fairness, explainability while recognising that adoption is not an overnight transformation but a sustained effort in design, implementation, and trust-building.

This paper merely initiates a broader conversation. Many facets, including skilling, institutional capacity, public-private partnerships, sandboxing timelines, capital requirements, deserve dedicated exploration. Starting this dialogue is critical. If India can thoughtfully align AI with its DPI, it will not only enhance DPI better, it will supercharge it, enabling transformative impact at population scale. Let this serve not as the conclusion of the debate, but as the beginning of a sustained national journey.

Authors

RAMA VEDASHREE

Former CEO, Data Security Council of India (DSCI)

Rama Vedashree, former CEO of the Data Security Council of India (DSCI) with over 35 years in the tech industry including NIIT Technologies, Microsoft, and NASSCOM, is also the editor of "Digital++, Reimagining Security & Privacy." She collaborated with The Dialogue on "Towards Trustworthy AI: Sectoral Guidelines for Responsible Adoption," a research report exploring AI's transformative potential across finance, healthcare, and education, while addressing challenges like bias, data privacy, and workforce impact. It outlines principle-based, sector-specific guidelines emphasizing fairness, transparency, accountability, and security, promoting responsible AI adoption through collaboration, regulation, and ethical governance.

MEEMANSA AGARWAL

Programme Manager - Artificial Intelligence, The Dialogue

Meemansa Agarwal is a Programme Manager at The Dialogue, specialising in artificial intelligence. With a law degree from Symbiosis Law School, Pune, and prior experience as a Tech Policy and Legal Affairs Associate at the office of Dr. Amar Patnaik, former Member of Parliament (Rajya Sabha), she brings a unique blend of legal expertise and policy acumen to her role. Passionate about the intersection of law and technology, Meemansa focuses on emerging areas like online gaming, artificial intelligence, and the metaverse. She is committed to advocating for balanced regulations that foster responsible technological innovation while safeguarding user interests.

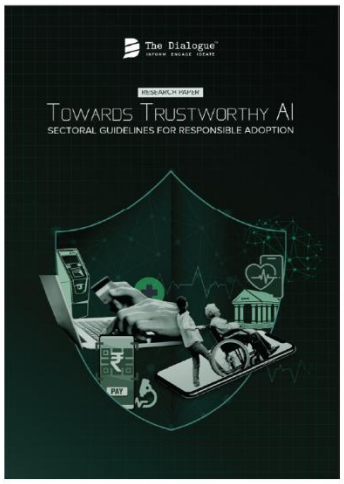
KAMESH SHEKAR

Associate Director, Research and Strategy, The Dialogue

Kamesh Shekar is Associate Director (Research and Strategy) at The Dialogue, where he leads research initiatives and strategic planning across the organization. He continues to spearhead the Privacy and Data Governance vertical and co-leads the Artificial Intelligence vertical. Kamesh also serves as a Youth Ambassador for The Internet Society.

He holds a PGP in Public Policy from the Takshashila Institution, an MA in Media and Cultural Studies, and a BA in Social Sciences from the Tata Institute of Social Sciences. At The Dialogue, Kamesh is deeply involved in analyzing emerging policy challenges shaped by evolving, data-driven digital technologies. His work focuses on the impact of policies and regulations on India's technology ecosystem, including the forthcoming Data Protection Regime, and on advancing research in tech policy and data governance.

More from our Research



RESEARCH PAPER

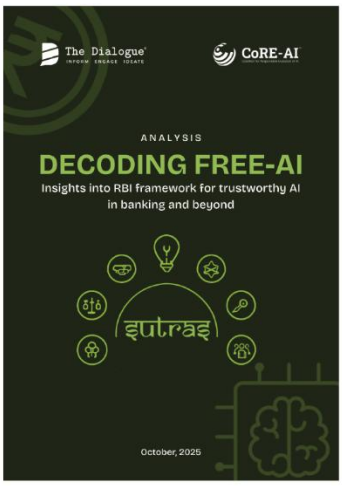
Towards Trustworthy AI: Sectoral Guidelines for Responsible Adoption

RESEARCH REPORT

Stakeholder Engagement for Responsible AI

PRIMER

Driving Cloud Adoption – Transforming Banking and Finance Sector



ANALYSIS

Decoding FREE-AI Insights into RBI framework for trustworthy AI in banking and beyond

thedialogue.co

@_DialogueIndia

@TheDialogue_Official

@The-Dialogue-India

@TheDialogue