

WHITEPAPER ON

FinTech

Enabled by Nextgen Networks and
Other Emerging Technologies



Financial
Ecosystem



India's Digital &
Inclusion Ecosystem

Important Notice

Individual copies of the present document can be downloaded from www.tdsi.in Users of the present document should be aware that the document may be subject to revision or change of status.

Copyright Notification

No part may be reproduced except as authorized by written permission from TSDSI. The copyright and the foregoing restriction extend to reproduction/copying in all media. All copyright notices are to be expressly displayed/affixed wherever they appear in the document.

© TSDSI 2026.

All rights reserved.

**Telecommunications Standards Development Society, India
(TSDSI)**

Registered Office Address

C-DOT Campus, Mandi Road, Mehrauli,

New Delhi, India – 110030

www.tdsi.in

Foreword

As a part of its ongoing focus on vertical sectors, Telecom Standards Development Society, India (TSDSI) has undertaken studies on FinTech, Agri Tech, Health and other vertical sector/ domains to assess readiness of existing Digital Infrastructure and enhancements required to support use cases with advanced LTE, 5G and beyond, as well as other enabling technologies.

This whitepaper deals with FinTech technologies enabled by the next generation networks and evolving AI techniques to address the solutions to the challenges posed by emerging requirements and cohesive FinTech ecosystem in the country to help all the players of the FinTech ecosystem to provide seamless services both for citizens and the businesses with ease of operations as well as for the satisfaction of the user.

While, the current FinTech systems have significantly improved accessibility and transaction efficiency, they continue to face challenges related to interoperability, security, scalability, latency and cost optimization. The study therefore examines possible role of NGN, AI and other enabling technologies in addressing these challenges, while also considering emerging requirements related to real-time processing, seamless cross-platform integration, dynamic resource management, and enhanced trust and compliance mechanisms.

The whitepaper examines the key gaps and challenges across the ecosystem, including interoperability, security and privacy, scalability, latency, legacy infrastructure, digital and financial inclusion, distributed operations, resilience and cost efficiency.

The whitepaper highlights the potential of AI and Next Generation Networks (NGN), edge and cloud computing, IoT, network slicing, service-based architectures and secure APIs, to progressively address these challenges. Their convergence can enable more intelligent, secure, scalable and efficient financial services while supporting real-time decision-making, automation, personalization, fraud management and improved service delivery.

TSDSI acknowledges all the experts and external stakeholders from the industry supported by members of the roadmap committee facilitated by TSDSI Secretariat who worked in collaboration to bring out comprehensively the status, challenges and solutions for the FinTech ecosystem.

A.K Mittal

Director General, TSDSI

Table of Contents

Foreword	3
Table of Contents	4
List of Figures	6
List of Tables	6
List of Abbreviations	7
Executive Summary	11
1. Background and Context.....	12
2. Scope and Objectives	13
2.1. Scope.....	13
2.2. Objectives	13
3. FinTech Ecosystem: Key Stakeholders, Evolution, Technologies and Emerging Opportunities....	15
3.1. Stakeholders and their roles in the Fintech Ecosystem.....	15
3.1.1. End Users expectations	15
3.1.2. Innovators	16
3.1.3. Incumbent Players.....	16
3.1.4. Regulators and Government	16
3.2. Key Business Domains and Technology Enablers in FinTech.....	17
3.2.1. Key Business Domains in FinTech.....	17
3.2.2. Key Technology Enablers.....	17
3.3. Current FinTech Platforms and Digital Financial Services	18
3.4. Emerging FinTech Use Cases.....	19
3.5. Evolution and Emerging Features of the FinTech Ecosystem.....	20
3.6. Digital Public Infrastructure and the Evolution of Modern FinTech Ecosystem	21
3.7. Telecom as a Foundational Layer for FinTech.....	22
3.8. Emerging FinTech Innovations and Market Developments	22
4. Challenges in the FinTech Industry	24
4.1. Overall Challenges.....	24
4.2. Challenges from Indian Context	24
4.3. User and Digital Inclusion Challenges	25
4.4. Legacy and Technology Infrastructure Challenges	25
4.5. Data Privacy, Distributed Operations and Sustainability Challenges.....	25
4.6. Financial Stability and Market Structure Challenges	25
4.7. Key Gaps Identified in Existing and Evolving FinTech Ecosystem.....	26
5. Addressing the identified Gaps with Enabling Technologies.....	28
5.1. Phased Approach to address Gaps	28

5.2. AI and Network Technology Solutions for the Classical FinTech Scenario	29
5.3. AI–NGN Convergence and Advanced FinTech Capabilities	29
5.4. AI enabled FinTech Evolution.....	30
5.5. Next-Generation Technology Enablers and Solutions for the Evolving FinTech Ecosystem.....	31
5.6. FinTech Requirements and AI–NGN Technology Mapping.....	32
5.7. AI & NGN Enable Future FinTech Ecosystem Architecture	34
6. Recommendations to Support Evolution of FinTech Ecosystem	35
7. Conclusion	38
8. References.....	39
9. List of Contributors.....	40
Annexures	41
Annexure 1 - Detailed Mapping of AI–NGN Technology for FinTech	41
Annexure 2 - Identities for Privacy Preserving, Inclusive Trust	44
Annexure 3 - Excerpt from RBI Report on QR Codes	47
Annexure 4 – UPI-Enabled ATM Services: Conceptual Framework and System Architecture	48
Annexure 5 - Details of Fintech Use Cases	49
Annexure 6 – Technology support for existing and Emerging FinTech Use Cases.....	53

List of Figures

Figure 1: Illustrative FinTech Technology and Service Landscape	18
Figure 2: AI and NGN Enabled Future FinTech Ecosystem Architecture	34
Figure 3: High-Level Architecture of UPI-Enabled ATM Services	48
Figure 4: Pilot Structure for including the Bank Branch	51

List of Tables

Table 1: Key Gaps Identified in the Existing and Evolving FinTech Ecosystem	26
Table 2: FinTech Requirements and AI-NGN Technology Mapping.....	33
Table 3: Detailed AI-NGN Technology Mapping for FinTech	41
Table 4: FinTech Use Case Realization and Technology Mapping	52

List of Abbreviations

Abbreviation	Full Form
AAA	Authentication, Authorization and Accounting
AEPS	Aadhaar Enabled Payment System
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
AR	Augmented Reality
ATM	Automated Teller Machine
BC	Business Correspondent
BCP	Business Continuity Planning
BFS	Banking and Financial Services
BFSI	Banking, Financial Services and Insurance
CBDC	Central Bank Digital Currency
CBS	Core Banking Solution
CDD	Customer Due Diligence
CERSAI	Central Registry of Securitisation Asset Reconstruction and Security Interest of India
CIF	Customer Information File
CPE	Customer Premises Equipment
CSP	Cloud Service Provider
CUG	Closed User Group
CSS	Chirp Spread Spectrum
DASH7	DASH7 Alliance Protocol
DLT	Distributed Ledger Technology
DND	Do Not Disturb
DoS	Denial of Service
DoT	Department of Telecommunications
DPI	Digital Public Infrastructure
DR	Disaster Recovery
DRM	Digital Rights Management
e-KYC	Electronic Know Your Customer
EMI	Equated Monthly Instalment

EMV	Europay, Mastercard and Visa
eSIM	Embedded Subscriber Identity Module
FASTag	Electronic Toll Collection System using RFID
FATF	Financial Action Task Force
FinTech	Financial Technology
GenAI	Generative Artificial Intelligence
GEO	Geosynchronous Earth Orbit
GRC	Governance, Risk and Compliance
GST	Goods and Services Tax
ICT	Information and Communication Technologies
ID	Identification
IDRBT	Institute for Development and Research in Banking Technology
IMPS	Immediate Payment Service
INFINET	Indian Financial Network
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
KYC	Know Your Customer
LEO	Low Earth Orbit
LLM	Large Language Model
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWAN	Low-Power Wide-Area Network
LTE	Long-Term Evolution
LTE-M	LTE for Machines
MAC	Media Access Control
M2M	Machine-to-Machine
MEC	Multi-access Edge Computing
MIS	Management Information System
MMID	Mobile Money Identifier
mMTC	Massive Machine-Type Communications
MOCN	Multi-Operator Core Network

MORAN	Multi-Operator Radio Access Network
MPIN	Mobile Personal Identification Number
N3IWF	Non-3GPP Interworking Function
NB-IoT	Narrowband Internet of Things
NFC	Near Field Communication
NGN	Next Generation Network
NLP	Natural Language Processing
NPN	Non-Public Network
NPCI	National Payments Corporation of India
NSDL	National Securities Depository Limited
OCR	Optical Character Recognition
OCEN	Open Credit Enablement Network
ONDC	Open Network for Digital Commerce
OTP	One-Time Password
PA	Payment App
PAN	Permanent Account Number
P2M	Person-to-Merchant
P2P	Peer-to-Peer
PDC	Primary Data Centre
PHY	Physical Layer
PII	Personally Identifiable Information
PLMN	Public Land Mobile Network
PoS	Point of Sale
QR	Quick Response
RAN	Radio Access Network
RB	Radio Bearer
RFID	Radio Frequency Identification
RBI	Reserve Bank of India
REST	Representational State Transfer
RTGS	Real-Time Gross Settlement
RU	Rogue User
SDN	Software-Defined Networking

SI	System Integrator
SIM	Subscriber Identity Module
SME	Small and Medium Enterprise
SMS	Short Message Service
STK	SIM Application Toolkit
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TSP	Telecom Service Provider
TPAP	Third Party Application Provider
TRIP	TSDSI Roadmap Item Proposal
TREDS	Trade Receivables Electronic Discounting System
UID	Unique Identification
ULIP	Unit Linked Insurance Plan
UPI	Unified Payments Interface
UPS	Uninterruptible Power Supply
URLLC	Ultra-Reliable and Low-Latency Communications
USSD	Unstructured Supplementary Service Data
VPA	Virtual Payment Address
VPN	Virtual Private Network
VR	Virtual Reality
Wi-Fi	Wireless Fidelity
Wi-SUN	Wireless Smart Utility Network
WLAO	White Label ATM Operator
XAI	Explainable Artificial Intelligence
XR	Extended Reality

Executive Summary

This whitepaper examines the evolving FinTech ecosystem in India, covering its key business domains, existing digital platforms, emerging use cases, Digital Public Infrastructure (DPI), connectivity requirements and technology developments. It identifies the growing requirements for financial services that are scalable, interoperable, secure, inclusive, affordable and capable of supporting diverse users and business scenarios.

The whitepaper examines the key gaps and challenges across the ecosystem, including interoperability, security and privacy, scalability, latency, legacy infrastructure, digital and financial inclusion, distributed operations, resilience and cost efficiency.

It further examines the potential role of emerging advances in AI, connectivity enabled by 4G/5G and future 6G networks, edge and cloud computing. The use of IoT, LPWAN, private networks, service-based architectures and secure APIs in addressing these requirements are also studied as enabling features of evolving FINTECH.

Based on these challenges, the whitepaper presents a phased technology approach, mapping key FinTech requirements with relevant AI and network capabilities. It also presents a high-level AI-NGN-enabled FinTech architecture and identifies potential use cases, technology enablers and areas for further development. Detailed technology mapping and use-case realization both in plain text and interlinked tabulated manner are provided in the annexures at the end of the paper.

The whitepaper further provides recommendations for financial institutions, FinTech providers, telecom operators, device and platform providers, cloud and system-integration stakeholders. These recommendations focus on secure modernization, interoperability, privacy-preserving data sharing, digital inclusion, AI-enabled automation, advanced connectivity, edge computing and resilient infrastructure, while enabling existing systems to progressively evolve towards next-generation capabilities.

1. Background and Context

The Department of Telecommunication (DoT) had encouraged the Telecom Standards Development Society, India (TSDSI) to undertake studies on FinTech, AgriTech and other vertical sectors to assess readiness of existing Digital Infrastructure and enhancements required to support use cases with advanced LTE, 5G and beyond, as well as other enabling technologies.

In this context, TSDSI constituted an IoT/M2M TRIP Forum to engage relevant stakeholders and undertake studies across priority vertical domains. Following studies of various sectors, the forum identified four priority domains, namely Agriculture, Smart Cities, Healthcare and FinTech. The respective activities were undertaken by expert groups with support from relevant stakeholders. The present whitepaper focuses on the FinTech domain and examines its evolving technology, architecture, connectivity and interoperability requirements.

Telecom networks have supported banking and FinTech services by providing connectivity for their datacentres, branches and their field offices. Telecom networks have also enabled internet and mobile banking feasible. It has also enabled the platforms like UPI, Point-of-Sale (PoS) / Business Correspondent (BC) channels. It also plays a key role in identity and authentication workflows.

The whitepaper investigates the aspects like convergence of AI and NGN technologies, edge computing, cloud-native architectures, network slicing, IoT connectivity and advanced AI technologies such as machine learning, federated learning, predictive analytics, and intelligent automation, when tightly integrated with advanced network capabilities like ultra-low latency, high reliability, and distributed edge intelligence, enable real-time financial services, dynamic risk management, and personalized user experiences can be effectively leveraged to bridge existing gaps in a step-by-step manner.

It demonstrates how advanced network capabilities and AI as enablers can offer seamless, interoperable, secure, and cost-efficient financial services by supporting real-time decision-making, intelligent automation, and optimized network performance. The study also identifies high-level use cases, enabling technologies, and additional gaps in current platforms, and proposes potential requirements and solutions for next-generation FinTech systems.

2. Scope and Objectives

2.1. Scope

The scope of this study is to explore in-depth the challenges and opportunities for FinTech in India by first examining existing financial technologies, services, platforms, and present-day use cases that have enabled digital financial services at scale.

While these current FinTech systems have significantly improved accessibility and transaction efficiency, they continue to face challenges related to interoperability, security, scalability, latency and cost optimization. The study therefore examines possible role of NGN (), AI and other enabling technologies in addressing these challenges, while also considering emerging requirements related to real-time processing, seamless cross-platform integration, dynamic resource management, and enhanced trust and compliance mechanisms.

The paper focuses on FinTech sector for all citizens and businesses and use of technologies rather than suggesting regulatory changes, while also addressing the high-level expectations from the same for ease of business, governance, and expectations of users about ease, seamless delivery, security, privacy and trust etc.

2.2. Objectives

The objectives of this whitepaper are to examine the evolving Fintech ecosystems from the perspective of technology, architectures, connectivity, provisions, business and citizen services, features, solutions and ongoing innovations.

The study aims to identify opportunities to enhance the ecosystem to support the growing range of financial while ensuring seamless, secure, and user-friendly access for the beneficiaries, service providers, and other stakeholders involved in monitoring and supporting these services. It further focuses on promoting inclusivity, ubiquity, affordability, trust, and cross-platform integration, thereby creating a sustainable and win-win situation for all the stakeholders.

An additional objective of the study is to identify challenges in the existing FinTech systems as also those that may arise as the ecosystem evolves. It further examines possible measures to address the challenges using the possible role of Next Generation Networks (NGN), AI and other enabling technologies, including possible architectures of connectivity and service provisioning and delivery, normative standards/ specifications and interconnecting APIs to meet all the possible requirements, features and other aspects related to FinTech deployments, evolving new features for further comprehensive use cases, applications and services provided in the FinTech sector.

The study also considers and explains the concepts about the possible development of a FinTech-specific roadmap and strategic directions, including potential pilots and testbeds, to validate proposed solutions and standards. These activities intended to support the evolution of current and future financial ecosystems towards greater resilience, scalability, and alignment with emerging technological developments.

In support of these objectives, the system needs to become more automated as desired in the new sets of requirements and use cases. Further there would be an attempt to include possible architecture and its parameters with necessary changes in some of the critical processes and workflows.

The whitepaper further aims to seek and define a unified technological framework that ensures seamless integration across heterogeneous platforms, enhances interoperability through standardized

interfaces, and reduces operational costs via intelligent resource optimization. It also aims to support future-ready FinTech innovations by providing insights into scalable architectures, AI-driven network intelligence, API-driven frameworks and the role of emerging technologies in enabling inclusive and autonomous financial services.

Towards these objectives, by leveraging AI capabilities such as predictive analytics, intelligent automation, and real-time decision-making, in conjunction with advanced network features like ultra-low latency, edge computing, network slicing, and high reliability, the whitepaper outlines how these gaps can be progressively addressed to enable a more efficient and resilient financial ecosystem.

3. FinTech Ecosystem: Key Stakeholders, Evolution, Technologies and Emerging Opportunities

The ecosystem comprises a diverse set of stakeholders, including end users, financial institutions, technology providers, innovators, regulators, government agencies, digital platforms, and infrastructure operators. Each stakeholder plays a distinct role in enabling secure, interoperable, and inclusive financial services. End users increasingly expect financial services to be accessible anytime and anywhere through intuitive, multilingual, and frictionless digital experiences. At the same time, financial institutions continue to provide trusted banking services, risk management, regulatory compliance, and operational resilience, while technology providers and innovators contribute advanced capabilities such as Artificial Intelligence (AI), Machine Learning (ML), Cloud Computing, analytics, digital identity, and secure digital platforms that accelerate service innovation.

The FinTech ecosystem is heavily exploiting the India Stack utilizing presence less Aadhaar, cashless UPI, paperless DigiLocker and consent-based data sharing Account Aggregator. India Stack is inspired by the concept of open-source software and interoperability. India stack has a set of open APIs that can explore the financial and social inclusions.

The ecosystem must also adapt to evolving customer behaviour and expectations. Different generations and demographic groups approach financial services with varying levels of trust, digital familiarity, and service preferences. Modern users increasingly expect financial services to be available through digital-first channels, social media platforms, conversational interfaces, and emerging virtual environments. Consequently, FinTech providers must continuously innovate to meet changing user expectations while maintaining security, trust, and simplicity.

Consequently, the end users participate in the FinTech ecosystem through a variety of roles and personas, including citizens, merchants, entrepreneurs, enterprises, government agencies, regulators, independent auditors, Micro enterprise/ small merchants, SMB, Large enterprise, etc, for varied use cases.

Each stakeholder category has distinct financial needs, risk profiles, compliance obligations, and service expectations. Therefore, future FinTech ecosystems must be designed to support role-based services, personalized experiences, and inclusive access while ensuring seamless interoperability, security, privacy, and trust across all stakeholder groups.

FinTech provides essential service as public social good. In addition, it also provides avenues for FinTech solution providers to offer new products and services and make money in the process. Worldwide governments and regulators have shown varied degrees of both the controls and the flexibility on encouraging innovation for FinTech sector.

Many efforts in India were made around managed services for ATM and subsequently usage of business correspondents or Mitra to reach out to unbanked people in remote areas.

3.1. Stakeholders and their roles in the Fintech Ecosystem

3.1.1. End Users expectations

- i). **Ease of access, usage and affordability:** UPI Payments is a good example. While it simplified payments using QR code, newer innovations are attempting to use voice enabled UPI payments for scenarios where data network may be lacking or smart devices may not be available.

- ii). **Products and services offered in their context** may include customized service, offered using terminology they understand or workflows that they are used to, multiple innovations are happening in this space.
- iii). **Education and awareness:** In context of diverse country like India, this is a big gap on three fronts namely general literacy, digital literacy and financial literacy. FinTech can especially create solutions for financial literacy and explore extending them towards niche products like investment advisory etc.
- iv). **Changing customer behaviour and needs:** Various demography of people are approaching financial products with different mind-set. Further, the customers are expecting access / presence in metaverse and social media platforms.
- v). **Diversity:** Besides the demographic diversity in the user group – there is a big diversity in the type of transactions. At one end of spectrum, we have micro-transactions and machine triggered workflows while at the other end we have merchants and traders looking at loans for goods and services that they have delivered.

3.1.2. Innovators

- i). **Tech stack / expertise:** the start-ups and innovation teams bring in technical expertise in specific technology horizontal. E.g. AI/ML, cloud technologies, user experience and NLP etc.
- ii). **Platform players and service providers:** Multiple platforms like Amazon, Ola/Uber, Zepto, Facebook, X (formerly twitter), etc. have significant customer and enterprise engagement through their platforms. They can leverage the same to enable new FinTech use cases. Frequently they may have to partner with banks or other regulated entities to offer innovative solutions.
- iii). **Lateral entrants:** Few platform players may create financial services arm to ensure that they comply with rules and regulations for the services that they offer. E.g. vehicle manufactures may start lending business primarily for their vehicles while also for other industries, or a telecom operator may acquire payments bank license etc.
- iv). **SI / start-ups / open source / community based:** many of the innovation may come because of innovation by system integrators.

3.1.3. Incumbent Players

Financial services are built on elements of trust. This is especially relevant in countries like India where there is significant population that may be financially and digitally illiterate, and citizen level policing and legal processes are still scaling to serve the masses. Hence, incumbent players like banks are heavily regulated and monitored for both fiscal and technology risks. Further, few of the large entities including big banks and financial network operators like NPCI are classified as too big to fail and actively monitored from Cyber-Security readiness as well.

Such organizations have to ensure that they have strong change controls procedures as well as resilient and scalable IT architectures to handle the heavy load on the platforms.

3.1.4. Regulators and Government

FinTech provides essential service as public social good (with numerous schemes targeting people at bulk of the pyramid). In addition, it also provides avenues for FinTech solution providers to offer new products and services and make money in the process. Worldwide governments and regulators have shown varied degree of flexibility on encouraging innovation from FinTech.

Initial efforts in India have been around managed services for ATM and subsequently usage of business correspondents or bank-mitra* to reach out to unbanked people in remote areas.

Typically, the governments and regulators stay neutral on technology platforms while ensuring that the appropriate controls are in place to minimize the risks for workflows enabled on FinTech platforms. Increasingly APIs enabling automation through supervisory technology and regulatory technologies are being deployed to expedite the process, to reduce the costs and to minimize the errors associated with human based reporting.

3.2. Key Business Domains and Technology Enablers in FinTech

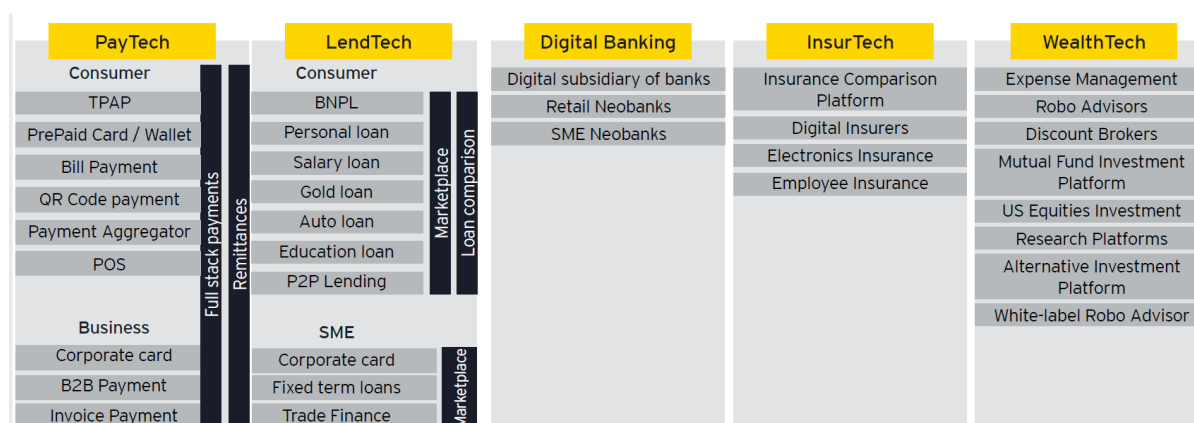
3.2.1. Key Business Domains in FinTech

Following are the key business domains in FinTech vertical. (To reexamine the need of the subtitle). Bullets to be changed into roman numbers. Or bracketed alphabets.

- i). Transaction delivery: Free apps / super apps: commission / cross sell
- ii). Lending: Peer-to-peer, small ticket loans, alternative credit scoring, opportunistic lending, trade receivables discounting etc.
- iii). Payments: gateways, digital wallets, digital currency and cross-border payments
- iv). Wealth Tech: Asset management, personal finance management, pension etc.
- v). Digital Banking: No frills, Digital Banking Units, Business Correspondents etc.
- vi). Insurance technologies: Digital Insurance / alternative insurance underwriting / embedding in workflows etc.
- vii). On boarding: loan lead/origin capture, new customer acquisition etc.
- viii). Relationship management: CRM, rewards management, minimize loan defaults, up-sell / cross-sell etc.
- ix). Reg-Tech: governance, risk, and compliance: automated audit, self-reporting to regulator, fraud risk monitoring etc.
- x). Retail-tech: many of the physical and digital retail and service platforms have fin-tech enablers like buy-now-pay-later, automated EMI offerings etc.

3.2.2. Key Technology Enablers

The following are key technology and service enablers supporting the FinTech ecosystem. The landscape includes major FinTech domains such as PayTech, LendTech, Digital Banking, InsurTech, WealthTech, Finance FinTech and RegTech, together with supporting platforms and services.



TechFin	Payment Gateway	Collections Management	Conversational Platforms	Claims Management	White-label Robo Advisor
	Card networks	Credit Bureau	Account Aggregators	Sales Platform	Portfolio Mgmt Suite
	API/ White-label solutions	Alternate Credit Scoring	API Providers and Aggregators	Underwriting Risk Management	CapTable Management
	Payment Security	Lending-as-a-Service	Banks with Open APIs	Insurance Infra API	
		LMS and LOS	Banking as a Service	Insurance Product Configurator	
			Core Banking	Policy Admin System	
Finance FinTech					
Accounting Enterprise SMB Micro		Procure to Pay	Quote to Cash	Taxation	Reconciliation
RegTech					
KYC / Digital Onboarding		Fraud Detection	AML	Banking Compliance and Risk Management solutions	

Source: EY Analysis

Figure 1: Illustrative FinTech Technology and Service Landscape

Ref. EY (Winds of change. 2021)

The FinTech ecosystem is heavily exploiting the India Stack (iSpirit foundation) utilizing Aadhaar (presenceless), UPI (cashless), DigiLocker (paperless) and Account Aggregator (consent-based data sharing). India Stack is inspired by the concept of open-source software and interoperability. India stack has a set of open APIs that can explore the financial and social inclusions.

3.3. Current FinTech Platforms and Digital Financial Services

There are many current initiatives as a part of the digital payment methods and cashless India. These initiatives are empowering the financial and economic growth of the countries in many ways. The various initiatives are listed below.

i). Aadhaar Enabled Payment System (AEPS):

AEPS allows online interoperable financial transactions using Aadhar authentication at PoS (Point of Sale / Micro ATM) with a bank model. For implementing this the individual should remember his/her Aadhaar, present physically near a biometric registration machine for fingerprint scan or IRIS scan, give details of the bank and use PoS/MicroATM providing AEPS services.

ii). Unstructured Supplementary Service Data (USSD):

The Unstructured Supplementary Service Data (USSD) channel is used for this innovative payment service *99#. This mobile banking service can be availed using basic feature mobile phones that even does not have mobile internet data facility. This facility is to promote more online financial and banking transactions of underbanked society. The *99# service brings together diverse ecosystem partners such as Banks & TSPs (Telecom Service Providers) and provide unique interoperable direct to consumer service. To use the service, the individual must register for the USSD service and get the MMID (Mobile Money Identifier) and MPIN (Mobile PIN).

iii). Unified Payments Interface (UPI):

It is a real-time payment system developed by National Payments Corporation of India (NPCI) and is regulated by the Reserve Bank of India (RBI). This system separately links with the various bank accounts appropriately with highly secure features into mobile application and use banking features for seamless fund routing & merchant payments into simple interface. The interface is

called UPI ID which is used to transfer money. The application runs as a sort of open-source application programming interface (API) over the Immediate Payment Service (IMPS). The services can also be configured to collect bills or payments on schedule and can be paid as per requirement and convenience. UPI Apps are developed for Android, Windows and iOS mobile platforms depending on the choice of the Banks and users.

Additional considerations related to QR-based payment security are provided in Annexure 3.

iv). Open Network for Digital Commerce (ONDC)

It is an open network expected to bring collaborative services offered by small merchants joining hands with big firms to render distribution services to exchange goods. This initiative is based on the Unified Payments Interface (UPI) project, which can give equitable possibilities to all marketplace participants. This is an open-sourced methodology built with open specifications and network protocols. ONDC currently has proven scope to digitise the whole value chain, standardize processes with enhanced operational features such as: more inclusion of suppliers, improvements in logistic efficiency, and increase customer value.

v). Open Credit Enablement Network (OCEN)

It is an initiative towards providing a transparent business model for small businesses involving lenders and borrowers. The OCEN is an API framework that allows lenders and borrowers to easily interact on a common platform. The scoring system used in the OCEN helps in assessing the credibility and categorizing the borrowers. The shared credit data among the lenders is used for analyses and lending decisions.

An illustrative UPI-enabled ATM architecture and related implementation considerations are provided in Annexure 4.

3.4. Emerging FinTech Use Cases

i). Machine based transaction and workflows

Many of the transactions are auto initiated based on standing instructions from the end customer. Further FastTag based transactions are also automatically made by scanning the ID from pre-authorized terminals like toll plazas and parking lots. In future more and more of these transactions would be auto triggered (e.g. wallet connected to refrigerator, equipment rental with pay-per-use model etc). Some of them may use lightly regulated platforms like closed wallets, while others may utilize more open platforms like card networks / UPI etc.

Phygital ecosystems like Amazon Go or similar corner stores would also blur some of the aspects of human vs. machine-based transactions to ease of use for urban scenarios.

ii). Micro-Transactions

The next generation transaction platforms will have to be efficient and affordable to handle low-value transactions in a secure and auditable manner. While platforms like digital wallets and UPI (especially UPI Lite) have made transactions for small denominations (below Rs. 50) easy, they still have technical costs that are presently borne by the banks and app providers. Digital electric meters with wallets allow usage control with granularity of 15 minutes to an hour, by backing it with a wallet of relatively high balance to reduce recharge transactions frequency. In future we may have examples of pay per-use scenarios where insurance may be collected per kilometre of driving

for rented bikes. For optimal flexibility to the end user (rider of rented bike) these may need transactions to be executed for amounts below a rupee every few minutes.

iii). Voice Based Transactions

For people in the global south, the level of engagement with digital technology is not easy. Further, many of them may not be literate. Local language support and voice-based workflows become significant for these demographics. Standalone applications have started providing audio assisted workflows. Standardization may further accelerate such scenarios. It will also help reduce the adaptation needed across numerous languages used in countries like India.

iv). Payment soundbox

Payment soundbox provide audible notification on received payments. From merchant's perspective lack of standardization and interoperability implies that they have to pay for multiple sound boxes to accept payments from multiple wallet / payment app providers.

v). Audio QR

Audio QR is already used by few FinTech Applications. Study of best practices around it would further accelerate this technology.

vi). Other partner innovations

Voice based payments, UPI with credit card/overdraft etc. are evolving innovations from ecosystem.

Detailed FinTech use cases and illustrative implementation flows are provided in Annexure 5.

3.5. Evolution and Emerging Features of the FinTech Ecosystem

The whitepaper describes the vision and goals for a new modernised FinTech and its features and requirements system progressively for both short and long terms.

The future FinTech ecosystem is envisioned as a comprehensive, intelligent, and inclusive digital framework capable of accommodating emerging services and evolving requirements while ensuring a balanced and mutually beneficial environment for all stakeholders, including end users, regulatory agencies, governments, financial service providers, and associated institutions. This vision emphasizes the creation of a win-win ecosystem, where technological advancements are aligned with user expectations, regulatory compliance, and operational efficiency.

At its core, the future ecosystem aims to deliver ease of use and seamless service experience. Financial services should be accessible with minimal complexity, enabling users to perform transactions, access credit, manage assets, and interact with financial systems in a frictionless manner. This requires intuitive interfaces, simplified workflows, and intelligent automation powered by Artificial Intelligence (AI), which can reduce user effort through features such as conversational interfaces, automated decision-making, and context-aware financial assistance.

A key objective is to expand the scope and diversity of financial services and use cases. The future ecosystem will support a wide range of applications, including embedded finance, micro-transactions, IoT-enabled financial services, digital lending, insurance, and wealth management. This expansion will enable new business models and innovative services, catering to the evolving needs of individuals, enterprises, and industries.

The future FinTech ecosystem is expected to evolve into a seamless, interoperable, secure, inclusive, and cost-efficient digital environment, driven by the convergence of AI and advanced network technologies. By aligning technological innovation with stakeholder needs and regulatory frameworks, this ecosystem will enable sustainable growth, foster innovation, and create a robust foundation for next-generation financial services.

Financial inclusion remains a key objective of the evolving ecosystem. Although initiatives such as Jan Dhan Yojana, Aadhaar, and mobile-based financial services have significantly expanded access to formal banking, challenges related to affordability, connectivity, digital literacy, and accessibility continue to exist. Addressing these challenges requires localized services, voice-enabled interfaces, low-bandwidth applications, and innovative service delivery models capable of serving rural communities, underserved populations, micro-enterprises, and the informal economy.

The rapid digitization of businesses is creating demand for integrated financial services that extend beyond traditional banking. Small and medium enterprises (SMEs), merchants, start-ups, and large enterprises increasingly require real-time payments, digital invoicing, merchant financing, supply-chain finance, working capital management, and cross-border transaction capabilities. Simultaneously, embedded finance is enabling financial services to be seamlessly integrated into e-commerce platforms, mobility services, healthcare, education, and other digital ecosystems, creating new business models and improving customer experiences.

Customer expectations are also shifting toward intelligent, personalized, and context-aware financial services. Advances in AI and data analytics are enabling adaptive financial products, automated credit assessment, personalized investment recommendations, smart insurance, fraud detection, and AI-assisted financial advisory services. The growing adoption of connected devices, IoT ecosystems, and smart infrastructure is further expanding the ecosystem through machine-to-machine payments, autonomous commerce, and intelligent financial workflows.

3.6. Digital Public Infrastructure and the Evolution of Modern FinTech Ecosystem

The evolution of modern FinTech ecosystems is driven by the transition from traditional, institution-centric financial services toward agile, digital, customer-centric models. Emerging FinTech solutions increasingly focus on faster service delivery, simplified onboarding and transactions, automated decision-making, personalized financial products, and improved access to credit for underserved users. Digital platforms have enabled new approaches to payments, lending, consumer finance, investment, insurance, and other financial services by combining digital interfaces, data-driven decision-making, alternative data sources, and automated workflows. These developments have reduced transaction costs and processing time while enabling financial services to reach users who may have limited access to conventional financial infrastructure.

A key development in this transformation is the emergence of Digital Public Infrastructure (DPI) as a shared foundation for digital financial services. DPI generally consists of interoperable digital systems such as digital identity, digital payments, and secure data-sharing mechanisms that can be used by multiple public and private service providers. Such infrastructure allows FinTech applications to build innovative services without independently developing every underlying capability, thereby reducing integration costs, improving interoperability, and accelerating the deployment of new financial products.

The combination of digital identity, real-time payment infrastructure, consent-based data sharing, and open interfaces can support a broad range of FinTech applications, including digital onboarding, electronic KYC, payments, lending, credit assessment, insurance, investment services, and embedded

finance. Standardized and interoperable interfaces allow different financial institutions, FinTech providers, technology platforms, and public-service systems to communicate and exchange information more efficiently. This infrastructure-based approach can therefore improve scalability, reduce duplication, support financial inclusion, and enable innovation by allowing multiple service providers to operate over common digital foundations.

The development of such ecosystems also changes the role of FinTech providers. Instead of operating as isolated financial applications, FinTech solutions can increasingly function as components within a wider interoperable ecosystem. Platform-based models can combine financial services with non-financial digital services, while data-driven technologies can improve credit assessment, personalization, fraud detection, risk management, and customer engagement. Research from the BIS indicates that digital platforms and FinTech can reduce costs and improve financial inclusion, although issues relating to competition, consumer protection, data governance, and financial stability also need to be addressed.

The evolution of DPI therefore represents a shift from individual digital financial applications toward a shared, interoperable and scalable digital financial ecosystem. Digital identity, payment systems, data-sharing frameworks, open APIs, and common standards provide the foundational layer, while FinTech applications and services operate above this layer to address specific user and business requirements. This model can support both public-interest objectives such as financial inclusion and private-sector innovation such as personalized lending, embedded finance, automated financial services, and new digital business models.

3.7. Telecom as a Foundational Layer for FinTech

Broadly, the term “financial technology” can apply to any innovation in how people transact business, from the invention of digital money to double-entry bookkeeping. Since the internet revolution, financial technology has grown explosively.

3.8. Emerging FinTech Innovations and Market Developments

Popular and well-funded fintech startups aim to disrupt traditional financial providers by being more agile, serving underserved populations, or offering faster and better services.

For example, financial company Affirm seeks to cut credit card companies out of the online shopping process by offering a way for consumers to secure immediate, short-term loans for purchases. While rates can be high, Affirm claims to offer a way for consumers with poor or no credit a way to secure credit and build their credit history.

Similarly, Better Mortgage seeks to streamline the home mortgage process with a digital-only offering that can reward users with a verified pre-approval letter within 24 hours of applying. GreenSky seeks to link home improvement borrowers with banks by helping consumers avoid lenders and save on interest by offering zero-interest promotional periods.

For consumers with poor or no credit, Tala (Tala is AI-native credit infrastructure for the global majority) offers consumers in the developing world microloans by doing a deep data dig on their smartphones for their transaction history and seemingly unrelated things, such as what mobile games they play. Tala seeks to give such consumers better options than local banks, unregulated lenders, and other microfinance institutions.

Some FinTech technologies, processes and might affect financial stability by changing the market structure in financial services. As used in this report, market structure refers to the interrelation of

companies in a market that impacts their behaviour and their ability to make profits. Market structure is characterised by such factors as the number and size of market participants, barriers to entry and exit, and accessibility of information and technologies to all participants. In certain speculative scenarios, these in turn may have an impact on the stability of the financial system.

The evolution of the FinTech ecosystem, including current digital financial platforms, emerging use cases, Digital Public Infrastructure and advanced connectivity requirements, introduces new challenges related to interoperability, security, scalability, latency, cost optimization, inclusion, privacy and resilience.

These challenges and the associated gaps in existing and evolving FinTech systems are discussed in section 4.

4. Challenges in the FinTech Industry

4.1. Overall Challenges

Building on the evolution of the FinTech ecosystem discussed in the previous section, the current FinTech ecosystem faces several limitations, including latency due to cloud dependency, reactive security mechanisms, fragmented service architectures, and high operational costs. Over the next 5 – 10 years, FinTech is expected to transition toward fully intelligent, real-time, and autonomous systems. Future financial ecosystems will feature AI-driven decision-making, embedded and invisible finance integrated into everyday applications, blockchain-based financial infrastructures, and hyper-personalized services. The gap between current and future systems lies in the lack of real-time intelligence, limited automation, and insufficient integration across platforms and technologies.

While India has achieved remarkable success in domestic digital payments, certain advanced FinTech capabilities are more mature in other countries. Globally, there is significant progress in cross-border real-time payment systems, embedded finance integrated into digital platforms, open banking frameworks, and tokenized financial assets. In contrast, India is still evolving in areas such as seamless global payment interoperability, advanced open banking ecosystems, and large-scale deployment of AI-native financial systems. This creates a gap where India leads in scale and accessibility while requiring further advancement in global integration, platform-level innovation, and intelligent automation.

As the FinTech ecosystem expands, security, privacy, trust, interoperability, and regulatory compliance become increasingly critical. Future platforms must provide secure digital identity management, robust authentication mechanisms, privacy-preserving data sharing, cybersecurity protection, fraud prevention, and standardized interfaces that enable seamless interaction among financial institutions, technology providers, government platforms, and digital service ecosystems. Common APIs, interoperable data exchange frameworks, and harmonized digital identity mechanisms will play a central role in ensuring secure and efficient service delivery.

Scalability and real-time responsiveness are equally important as digital transaction volumes continue to increase. Future financial infrastructures must reliably process billions of transactions while supporting real-time payments, lending decisions, fraud detection, compliance verification, customer engagement, and emerging digital commerce applications. Cloud-native architectures, distributed computing, and Next Generation Networks will be essential for meeting these performance and reliability requirements.

4.2. Challenges from Indian Context

India with its unique demography and innovations like UPI, Aadhaar have some very disruptive solutions that are already utilizing connectivity provided by telecom systems. There are still challenges related to some of the following

- i). Balanced information sharing/flow, coupled with privacy safeguards, including scenarios of benefit transfers from government.
- ii). Many citizens lack digital enablement (both digital literacy and access to network/device)
- iii). Regulator maturity given the rapid innovations and emerging threats.
- iv). regulators and government.

4.3. User and Digital Inclusion Challenges

- i). **Varied digital and financial literacy for end users:** Diversity in literacy level, digital inclusion, languages etc. makes it extremely challenging to offer products and solutions. Further lack of awareness increases risk for naïve users. While many of them hesitate and resist move to digital platform out of fear, few of them take too much risk out of greed without understanding the consequences.

4.4. Legacy and Technology Infrastructure Challenges

- i). **Legacy core (non- Service Based Architectures):** many of the elements of financial technology stack are based on “Legacy Core” which has embedded into workflows making it difficult to get away from. E.g. for banks with millions of customers, their transactions are stored in “Core Banking Solution”
- ii). **Lack of skilled resources:** many of the incumbents BFS entities struggle to upskill and retain staff for latest technology stack. Collaboration with FinTech and System Integrators is crucial to fill the gap. Further the existing resources (both in-house and vendors) should be continued.

4.5. Data Privacy, Distributed Operations and Sustainability Challenges

- i). **Data privacy, localization and related concerns:** Data protection and privacy requirements are becoming increasingly important for FinTech ecosystems. The General Data Protection Regulation (GDPR) in Europe provides an important reference for data protection, while in India, the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Digital Personal Data Protection Rules, 2025 establish the evolving framework for protection and processing of digital personal data. FinTech platforms and supporting network infrastructure will need to incorporate appropriate privacy, consent, security, accountability and data-governance mechanisms as the regulatory framework comes into effect.
- ii). **Multi-site service orchestration and visibility:** For business continuity most of the BFS entities and FinTech run their solutions from more than one site. Few leverage public cloud providers for the same. Advent of edge technologies (5G and beyond) will further distribute the execution platforms. Orchestration of applications and services becomes challenging in such environments. Further industry best practices and regulatory concerns mandates that the platforms are cyber-safe and auditable for financial / regulatory compliance. The distributed operations are challenging to manage.
- iii). **Cost of hardware refresh/green computing:** By leveraging cloud, FinTech have partially reduced the need for refreshing their hardware. All the same, endpoint devices (for example ATMs, PoS, Tablets/ Smartphones) still need to be upgraded in cyclical basis. Besides increasing the cost for the enterprise, it also negatively impacts the environment. There is need to create solutions that last longer and leave minimal carbon footprint.

4.6. Financial Stability and Market Structure Challenges

Some FinTech technologies, processes and might affect financial stability by changing the market structure in financial services. As used in this report, market structure refers to the interrelation of companies in a market that impacts their behaviour and their ability to make profits. Market structure is characterised by such factors as the number and size of market participants, barriers to entry and exit, and accessibility of information and technologies to all participants. In certain speculative scenarios, these in turn may have an impact on the stability of the financial system.

4.7 Challenges in Using 5G and AI as Enabling Technologies

- i). **Security Risks:** The increased number of connected devices (IoT) expands the attack surface, making it easier for hackers to exploit potential vulnerabilities.
- ii). **Infrastructure Costs:** The high capital investment needed to upgrade legacy infrastructure to 5G is a significant barrier.
- iii). **Data Management & Privacy:** Strict regulations, such as data protection laws (e.g., GDPR), require robust data handling frameworks.
- iv). **Infrastructure Costs:** Upgrading to 5G infrastructure requires significant investment, which may create a "digital divide" between urban and rural areas.
- v). **Security Risks:** The increased connectivity expands the attack surface, necessitating robust, AI-powered security measures.
- vi). **Future Trends:** As 5G adoption increases, AI-native services including agentic AI, are expected to increasingly support complex financial workflows. Their deployment will also require appropriate governance, risk management, transparency, human oversight and accountability mechanisms.

4.7. Key Gaps Identified in Existing and Evolving FinTech Ecosystem

Based on the challenges discussed above, the key gaps in the existing and evolving FinTech ecosystem as given in the table below:

Table 1: Key Gaps Identified in the Existing and Evolving FinTech Ecosystem

Area	Key Gap
Interoperability	Fragmented platforms and limited standardized interfaces
Performance	Latency and limited real-time processing capabilities
Scalability	Increasing transaction volumes and distributed workloads
Security	Reactive security mechanisms and increasing attack surface
Privacy	Data sharing, localization and privacy concerns
Digital Inclusion	Digital literacy, financial literacy, language, device and connectivity gaps
Legacy Infrastructure	Dependence on legacy core systems and difficulty in modernization
Distributed Operations	Complexity of managing multi-site, cloud and edge environments
Skills and Resources	Lack of skilled resources for adoption and management of emerging technologies
Cost and Sustainability	Infrastructure investment, hardware refresh requirements and environmental impact
AI/5G Adoption	Infrastructure costs, security, privacy and adoption challenges
Resilience and Trust	Need for secure, reliable, auditable and trusted financial service delivery

These gaps highlight the need for a phased and technology-enabled approach to modernize existing FinTech platforms while supporting emerging use cases and future requirements. The possible role of AI, Next Generation Networks, edge computing, cloud-native architectures, open APIs, privacy-preserving technologies and other enabling technologies in addressing these gaps is discussed in the following section.

5. Addressing the identified Gaps with Enabling Technologies

To address the gap between the current limitations and future requirements of the FinTech ecosystem, a comprehensive technological transformation is necessary. This transformation involves the integration of multiple advanced technologies to create a unified, intelligent, and scalable financial ecosystem. Artificial Intelligence (AI) will play a central role in this transformation by enabling predictive analytics, real-time fraud detection, personalized financial services, and autonomous decision-making. AI-driven systems will shift the paradigm from reactive to proactive operations, significantly enhancing efficiency and security.

The deployment of 5G and future 6G networks will serve as the backbone for next-generation FinTech systems, providing ultra-low latency, high bandwidth, and massive device connectivity. These capabilities will be further enhanced by edge computing, which brings computation closer to the user, reducing latency and enabling real-time processing. Together, these technologies will support time-critical applications and improve user experience.

Cloud-native architectures, based on microservices and containerization, will enable scalability, flexibility, and cost optimization. These architectures will allow financial institutions to rapidly deploy and scale services while maintaining resilience. Open APIs and open banking frameworks will facilitate interoperability and ecosystem integration, enabling seamless data exchange and collaboration among various stakeholders.

Blockchain and Distributed Ledger Technologies (DLT) will address trust and transparency issues by enabling secure, tamper-proof transactions and smart contracts. These technologies will be particularly useful for cross-border payments and decentralized financial services. Additionally, the integration of IoT and embedded finance will expand the reach of financial services by embedding them into everyday devices and applications.

Advanced networking technologies such as Software-Defined Networking (SDN) and network slicing will ensure reliable and high-performance communication by providing dedicated network resources for financial services. Privacy-preserving technologies, including federated learning and secure multi-party computation, will enable data-driven innovation while protecting user privacy. Furthermore, regulatory technologies will automate compliance processes and enable real-time monitoring, reducing regulatory burdens and improving governance.

5.1. Phased Approach to address Gaps

Bridging the identified gaps requires a structured and phased approach. Initially, existing systems can be enhanced by integrating AI for fraud detection, automation, and performance optimization. The next step involves enabling real-time capabilities through the deployment of 5G-enabled edge computing, allowing faster data processing and decision-making. Subsequently, interoperability can be achieved through standardized APIs and open frameworks, enabling seamless integration across platforms. As systems mature, autonomous financial operations driven by AI agents can be introduced, followed by global integration through cross-border payment systems and tokenized financial infrastructures. This step-by-step approach ensures a smooth transition from current systems to future-ready FinTech ecosystems.

The phased approach workflow is given below:

Current FinTech systems → AI-enabled enhancement → NGN and edge-enabled real-time services → API-based interoperability → intelligent and autonomous financial services → globally connected and future-ready FinTech ecosystem

5.2. AI and Network Technology Solutions for the Classical FinTech Scenario

The FinTech ecosystem can leverage Artificial Intelligence (AI) and Next Generation Networks to improve financial inclusion, operational efficiency, compliance, and trust.

- i). **AI Technologies:** Machine Learning (ML), Natural Language Processing (NLP), Conversational AI, Generative AI, Predictive Analytics, and Intelligent Automation can support multilingual voice banking, financial literacy, fraud detection, risk assessment, automated compliance, and supervisory monitoring.
- ii). **Network Technologies:** NGN, Edge Computing, Cloud-Native Infrastructure, Network Slicing, Secure APIs, and Satellite Connectivity can provide reliable connectivity for rural and remote areas, enable real-time financial transactions, improve service availability, and support secure data exchange between financial institutions and regulators.
- iii). **Combined Benefits:** AI and advanced networks together can enable seamless digital banking, intelligent customer support, automated regulatory reporting, secure financial transactions, reduced operational costs, enhanced cybersecurity, and wider financial inclusion, particularly for underserved populations and remote regions.

AI provides the intelligence and automation, while NGN technologies provide the connectivity, scalability, reliability, and low-latency infrastructure required for next-generation FinTech services.

5.3. AI-NGN Convergence and Advanced FinTech Capabilities

The convergence of Artificial Intelligence (AI) with Next Generation Networks is transforming the FinTech ecosystem from conventional digital services to intelligent, real-time, and highly automated financial platforms. High-speed connectivity, ultra-low latency, edge computing, and cloud-native architectures enable AI-driven applications to process and analyse large volumes of financial data with minimal delay, improving operational efficiency, customer experience, and service delivery.

This convergence enables several advanced FinTech capabilities, including:

- i). **Real-Time Fraud Detection and Risk Management:** AI models can continuously analyse transaction patterns and user behaviour to detect anomalies, identify fraudulent activities, and support proactive risk management. The high bandwidth and low latency of NGN enable near real-time analysis and response, helping financial institutions prevent fraud before transactions are completed.
- ii). **Personalized Customer Experience:** AI-powered virtual assistants, conversational banking, and recommendation systems can deliver personalized financial advice, product recommendations, and multilingual customer support. Advanced network capabilities further enable seamless video banking, remote advisory services, and interactive digital customer engagement.
- iii). **Autonomous Financial Services:** AI-driven applications such as robo-advisors, automated portfolio management, algorithmic trading, and intelligent financial decision support can

operate more efficiently through high-speed, low-latency network infrastructure that enables rapid processing of market data.

- iv). **IoT-Enabled Financial Services:** The ability of NGN networks to support massive IoT deployments allows financial services to be integrated into connected devices such as wearables, smart vehicles, and home automation systems, enabling secure, contactless, and always-available payment services.
- v). **Enhanced Financial Inclusion:** Reliable broadband connectivity, satellite communication, and AI-enabled digital services can extend banking, lending, insurance, and financial literacy initiatives to rural, remote, and underserved communities where conventional banking infrastructure is limited.
- vi). **Intelligent Digital Branches:** AI combined with NGN technologies enable smart banking branches featuring automated customer assistance, facial recognition, voice-enabled kiosks, virtual consultations, and immersive digital experiences using Augmented Reality (AR) and Virtual Reality (VR), improving operational efficiency while enhancing customer engagement.
- vii). **Intelligent Lending and Credit Assessment:** AI can analyse both traditional and alternative data sources including transaction history, digital behaviour, and other consent-based information to improve credit assessment, accelerate loan approvals, and expand access to financial services for individuals and small businesses with limited credit histories.
- viii). **Secure Edge Computing and Digital Identity:** Processing sensitive financial data closer to end users through edge computing reduces latency, enhances privacy, and supports secure digital onboarding, remote identity verification, and authentication services, strengthening trust across digital financial ecosystems.

Further details on telecom identities, privacy-preserving mechanisms and trust considerations are provided in Annexure 2.

5.4. AI enabled FinTech Evolution

In the present state of the industry, and the related financial services AI has already shown potential to drive advancements in efficiency, personalization, and security. As AI technologies evolve, more-sophisticated AI models will likely be able to provide even deeper insights and more-accurate predictions. LLMs and GenAI-driven personal assistants will potentially be able to engage customers with greater empathy and the ability to understand customer intentions, leading to greater personalization. AI's role in risk management and fraud detection will become more robust, keeping pace with digital threats and acting on real-time data to secure transactions and protect assets.

Looking forward, the integration of DPI with Artificial Intelligence, cloud computing, edge computing, IoT, and Next Generation Networks can further transform the FinTech ecosystem. AI can support intelligent decision-making, fraud and risk detection, personalization, automated customer assistance, and regulatory compliance, while advanced networks can provide connectivity, low latency, reliability, scalability, and distributed computing capabilities required by increasingly real-time financial applications.

The resulting ecosystem can progressively move toward more seamless, intelligent, secure, interoperable, and inclusive financial services, while maintaining appropriate safeguards for privacy, security, consumer protection, and responsible use of data and AI. This direction is consistent with emerging thinking around interconnected digital financial ecosystems and future-ready financial infrastructure.

AI Governance and Management as AI-native and agentic systems become increasingly integrated into FinTech workflows, appropriate governance, risk management, transparency and accountability mechanisms will become important. ISO/IEC 42001:2023, which specifies requirements for establishing, implementing, maintaining and continually improving an Artificial Intelligence Management System (AIMS), provides a structured management-system approach for the responsible governance of AI.

In parallel, regulatory frameworks such as the EU AI Act provide risk-based legal requirements for AI systems, including requirements relating to risk management, data quality, traceability, documentation, human oversight, robustness and cybersecurity for applicable high-risk systems.

These approaches can be considered complementary, management-system standards such as ISO/IEC 42001 can support organizational AI governance and continuous improvement, while regulatory frameworks establish applicable legal obligations and safeguards. For FinTech applications involving AI-native and agentic systems, alignment with such governance and risk-management principles can support responsible deployment, auditability, transparency and trust.

Deploying AI in financial services not only has the potential to drive operational efficiency while also creates more opportunities to better understand and interact with customers.

Overall, these innovations help empower FSI businesses to be more competitive and adaptive while helping them meet strict regulatory and compliance requirements.

5.5. Next-Generation Technology Enablers and Solutions for the Evolving FinTech Ecosystem

India has emerged as one of the world's leading digital financial ecosystems through transformative initiatives such as Digital Public Infrastructure (DPI), India Stack, Aadhaar, Unified Payments Interface (UPI), the Account Aggregator framework, and widespread mobile connectivity. These initiatives have significantly enhanced financial inclusion, digital payments, and access to formal financial services, enabling citizens, businesses, and government agencies to participate more effectively in the digital economy. As digital adoption accelerates, the FinTech ecosystem is evolving beyond payment processing into a comprehensive digital environment that supports financial services, commerce, governance, and emerging digital business models.

While telecom networks are heavily leveraged in people centric application, next generation FinTech innovations may be machine driven and rely on low-power wide area coverage provided by them. Wi-Fi with its affordable connectivity would also play a role for the same. The section below captures salient features for connectivity and management aspects for these technologies.

Its analysis the evolving FinTech ecosystem by examining existing architectures and identifying key technological and operational gaps that hinder the realization of seamless, interoperable, secure, and cost-efficient financial services. It highlights critical challenges related to latency, scalability, interoperability, security, and financial inclusion, which limit the effectiveness of current systems. Based on this analysis, the whitepaper proposes a unified AI-enabled network architecture that leverages advanced technologies to enable frictionless transactions, enhance financial inclusion, and ensure resilient and scalable service delivery. It also outlines how such an integrated approach can support future-ready innovations, including autonomous finance, embedded financial services, and AI-driven regulatory compliance.

The FinTech ecosystem must further accommodate a high degree of transactional and operational diversity. Financial activities range from low-value microtransactions and machine-to-machine

payments in IoT-enabled environments to high-value commercial transactions, trade finance, merchant payments, and enterprise lending. Supporting this broad spectrum of use cases requires scalable, interoperable, and intelligent financial platforms capable of serving diverse operational requirements.

Another fundamental goal is achieving true interoperability across platforms and systems. As the FinTech landscape comprises diverse entities such as banks, payment service providers, telecom operators, and third-party application developers, it is essential to ensure that these systems can communicate and operate cohesively. This can be realized through standardized interfaces, open APIs, and common data exchange frameworks, enabling seamless integration and interoperability not only within national ecosystems while also across international boundaries.

Ensuring trusted, secure, and high-quality services is a critical pillar of the future vision. Financial systems must guarantee data integrity, privacy, and protection against evolving cyber threats. The integration of AI with advanced network capabilities enables proactive and predictive security mechanisms, real-time fraud detection, and continuous monitoring of transactions and network behaviour. Additionally, the adoption of robust authentication frameworks and compliance with regulatory requirements will further enhance trust among users and stakeholders.

The vision also prioritizes enhanced financial inclusivity, aiming to extend the reach of financial services to underserved and unbanked populations. By leveraging emerging technologies such as AI, Next Generation Networks (NGN), and mobile connectivity, financial services can be made accessible in remote and rural regions. AI-driven personalization, multilingual interfaces, and alternative credit assessment models can empower individuals who are traditionally excluded from formal financial systems, thereby promoting inclusive economic growth.

In parallel, there is a strong emphasis on achieving low-cost and efficient operations. The adoption of AI-driven automation, cloud-native architectures, and intelligent network management can significantly reduce operational and infrastructure costs for financial institutions. Technologies such as network slicing, edge computing, and software-defined networking enable optimized resource utilization, ensuring that high-quality services are delivered efficiently and sustainably.

The realization of this vision is heavily dependent on the effective use of enabling technologies and standardized systems. AI acts as the intelligence layer, enabling real-time analytics, automation, and decision-making, while NGN technologies provide the underlying connectivity with ultra-low latency, high reliability, and scalability. Furthermore, the development and adoption of standardized frameworks, protocols, and APIs are essential to ensure interoperability, consistency, and compliance across the ecosystem.

Artificial Intelligence and Next Generation Networks together form the foundation for addressing existing FinTech challenges and enabling future capabilities. AI acts as the intelligence layer, providing predictive analytics, automated decision-making, and personalized services. Meanwhile, advanced network technologies offer ultra-low latency, high reliability, and support for edge computing, which are essential for real-time financial operations. The convergence of AI and networks enables faster processing, improved security, and seamless service delivery, thereby transforming the FinTech ecosystem into a more efficient and intelligent environment.

Additional technology examples currently in use are provided in Annexure 6.

5.6. FinTech Requirements and AI-NGN Technology Mapping

The following mapping identifies how key FinTech requirements can be supported through AI technologies and network technologies.

Table 2: FinTech Requirements and AI-NGN Technology Mapping

Requirement / FinTech Area	AI Technologies	How AI Helps	Network Technologies	How Networks Help
Financial Inclusion	NLP, Conversational AI, Multilingual LLMs, AI Assistants	Enables voice banking, local language interaction, financial literacy support, and AI-assisted onboarding.	5G, 6G, Satellite Networks, Edge Computing	Extends financial services to rural and remote areas through reliable and low-cost connectivity.
Personalized Financial Services	Machine Learning, Predictive Analytics, Recommendation Engines	Provides customized lending, investment, insurance, and financial advisory services.	Edge Computing, Cloud-Native Networks	Supports real-time processing and delivery of personalized financial products.
Real-Time Payments & Transactions	AI Transaction Optimization, Fraud Analytics	Optimizes transaction routing, reduces failures, and detects anomalies instantly.	5G URLLC, Edge Computing, Network Slicing	Enables low-latency, highly reliable, and real-time payment processing.
Security, Privacy & Trust	Fraud Detection AI, Behavioural Analytics, Explainable AI (XAI)	Detects fraud, identity theft, suspicious activities, and improves transparency.	Zero Trust Networks, Secure Network Slicing, AI-Native Security	Provides secure communication channels and cyber-resilient infrastructure.
Interoperability	AI-driven API Management, Intelligent Orchestration	Automates integration, workflow coordination, and intelligent service discovery.	Open APIs, Service-Based Architecture, Cloud-Native Networks	Enables seamless communication among banks, FinTech, regulators, and merchants.
Scalability & High Transaction Volumes	AI Resource Optimization, Predictive Capacity Planning	Dynamically allocates resources and predicts traffic demand.	NGN, SDN, NFV, Distributed Cloud	Supports massive transaction volumes while maintaining performance and availability.
SME & Enterprise Services	AI Credit Scoring, Risk Analytics, Intelligent Automation	Improves lending decisions, credit evaluation, and supply-chain finance.	Edge Computing, Private 5G Networks	Enables secure and responsive enterprise financial services.
Embedded Finance	Context-Aware AI, Recommendation Systems	Delivers financial services within non-financial applications	API Ecosystems, 5G Connectivity	Supports seamless integration across platforms
IoT & M2M Payments	AI Decision Engines, Autonomous Agents	Enables autonomous transaction decisions by devices.	Massive IoT (mMTC), 5G, 6G	Provides connectivity for billions of devices and machine-triggered payments.
Regulatory Compliance	Generative AI, NLP, Intelligent Automation	Automates compliance monitoring, reporting, and document analysis	Cloud-Native Networks, Secure APIs	Enables secure real-time reporting to regulators
Cross-Border Payments	AI Risk Analytics, Currency Forecasting	Optimizes exchange rates and fraud monitoring	Global NGNConnectivity, API Frameworks	Accelerates international transaction processing
Future Autonomous Finance	Agentic AI, Generative AI, Federated Learning	Creates autonomous financial agents capable of acting on behalf of users	6G, Distributed Edge Intelligence, AI-Native Networks	Provides real-time, secure, and intelligent infrastructure for autonomous

			financial ecosystems
--	--	--	----------------------

The integration of 5G and AI is paving the way for "invisible banking," where financial services are integrated into daily life seamlessly.

A detailed mapping covering additional FinTech requirements, AI capabilities, network technologies and their potential contributions is provided in Annexure 1.

5.7. AI & NGN Enable Future FinTech Ecosystem Architecture

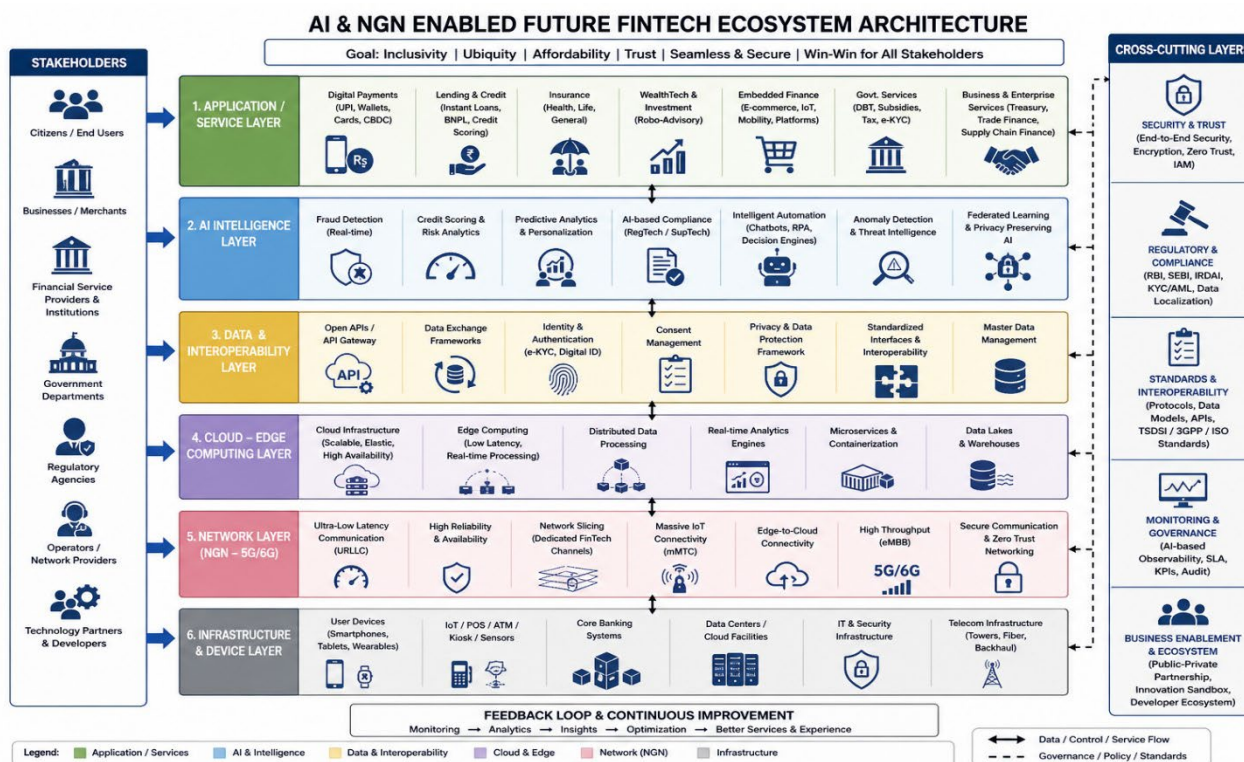


Figure 2: AI and NGN Enabled Future FinTech Ecosystem Architecture

The proposed AI and NGN enabled FinTech ecosystem architecture provides a high-level framework for integrating financial services, AI capabilities, advanced networks, cloud and edge computing, and interoperable digital platforms. It supports secure, scalable, low-latency and intelligent delivery of emerging FinTech services.

The architecture enables AI-driven decision-making and automation, while NGN, edge computing and cloud infrastructure provide connectivity, scalability and reliability. Standardized APIs and interoperability mechanisms enable seamless integration across banks, FinTech, telecom operators, regulators and other ecosystem stakeholders, with security, privacy, identity and trust mechanisms applied as cross-cutting requirements.

The architecture is intended to support the progressive evolution of existing FinTech systems towards more intelligent, inclusive, interoperable, secure and resilient financial services.

6. Recommendations to Support Evolution of FinTech Ecosystem

The recommendations outlined below are intended to support a phased evolution of the FinTech ecosystem, rather than requiring immediate replacement of existing infrastructure. Stakeholders should focus on interoperability, secure modernization, digital inclusion, privacy-preserving data sharing, AI-enabled automation, advanced connectivity, edge computing, and resilient infrastructure while maintaining compatibility with existing financial systems and services. This approach can enable the progressive transition towards a more secure, inclusive, interoperable, intelligent, resilient, and cost-efficient FinTech ecosystem.

The following recommendations are intended to support the evolution of the FinTech ecosystem towards more inclusive, secure, interoperable, efficient, and technology-enabled financial services. The recommendations cover ecosystem-level requirements as well as specific considerations for device, telecom, Cloud Service Provider (CSP), platform, and system-integrator stakeholders.

1. **Further enhancements in Efficiency of delivery channels (self-service, assisted, managed services):** Payment's products/apps and mobile/online banking and investments channels, are enabling users to self-service for majority of their financial needs. However, it is important that constant monitoring is done to prevent frauds and allay the fears of users especially the senior citizens and others needing assistance.
2. **Metaverse enabled platforms:** Future technologies (e.g. digital twins etc.) will enable richer experience for users besides workflow, capacity and desired quality of service to be provided. These also have potential for technology assisted workflows. It is desirable that the experts and specialists guide/train generic resources and help improve productivity for the BFS enterprises
3. **Inclusion:** There is tremendous focus on financial inclusion in India and FinTech adoption has accelerated over the last decade. There is still a very strong need to continue improving digital and financial literacy, particularly for sections of society that are not digitally and financially savvy. Awareness programmes and communication initiatives should be adapted through media channels such as WhatsApp and other social media in various languages. FinTech stakeholders have an important role in addressing the challenges by developing educational tools, financial awareness platforms, and AI-driven advisory services that empower users to make informed financial decisions and responsibly utilize digital financial products.
4. **Shared devices:** Business Correspondents carry shared devices with them to remote areas and illiterate masses in India for providing basic banking services for people in the community. Fintech need to create solutions keeping these nuances in mind. Privacy aspects need strong consideration.
5. **Improved workflow audit / visibility to minimize frauds:** If the fraud originates/terminates in another state/country, it creates significant challenges for law enforcement. Next generation innovations should improve audit/visibility for reducing such risks.
6. **Regulatory Technology / Compliance / Due Diligence etc.:** Increasingly the financial ecosystem has to bear the high cost associated with customer-due-diligence, anti-money-laundering etc. Innovations in Regulatory Technology stacks will improve automation for the same.

These implementations would need to ensure that they comply with data privacy laws, reduce burden for customers while achieving the regulatory objectives. Increasing use of trusted AI/ML would make these processes more efficient.

7. **Next gen APIs / capabilities of networks for improved data-sharing and security controls:** Various industry verticals need to create data exposure APIs for usage in FinTech. For example, access to education/land records for loans, health/vehicle records for insurance, utility bills.
8. **Customer Preference, Identity and protection Repository:** While few repositories and data exchange mechanism exists today, they need to be standardized for improving their effectiveness. For example, many social media platforms, government mandated platforms (DND registry) and vertical industries have access to this data in semi-structured manner.
9. **Security / risk** -Repositories may be needed for privacy preserving change in such records to offer protection for the customer. For example, SIM / device / ownership change should be informed for additional inference if OTP is sent to the device. Similarly, repositories for newly opened accounts / dormant accounts can be used to reduce risks for payment/loan transactions.
10. **Preference** – End users’ preference for language, mode/channel of communication, time of communication, products/services (black-list / white-list), and social media handles/emergency contacts etc. This can create one or more persona/digital twin for the user, with appropriate controls on data sharing etc.
11. **Delegation / assistance** – For people with special needs or under emergency scenarios, the repository platform should allow an authorized person to manage the entries in the repository with appropriate checks and balances. For example, identified relative may monitor and control these details for elderly person or an advocate / financial advisor may audit and suggest best practices.
12. **SIM-based Mobile Money services:** Communication service providers are actively engaging with BFSI industry and regulatory to provide SIM based mobile money services. This can particularly benefit rural areas with limited smart phone and internet penetration. However, for wider adoption, digital literacy through telecom service providers will be required.
13. **SIM tool kit (STK applications):** Telecom operators could offer STK applications that provide access to financial services. STK applications can operate without internet connectivity.
14. **SIM card as secure element:** The SIM card can be used as a secure element to store sensitive information, like cryptographic keys and digital certificates.
15. **End to end encryption for communication between the SIM card and the financial service provider:** Multiple methods are available for SIM card-based encryption. Suggest baseline/best practice should be analysed and adopted.
16. **Edge Computing for Resource-Intensive FinTech and Enterprise Applications:** Many of the resource intensive applications may be accelerated by edge. Language translation, video conferencing, distributed ledgers, caching of static content are some of the examples. As Metaverse usage increases, it will be heavily reliant on edge. Future enterprise IT architecture may also leverage edge to reduce the costs and complexity related to physical infrastructure in their field offices.

17. **End-User Devices as Edge Resources and Private Network Integration:** Many of the upcoming end user devices may be powerful with high-speed connectivity to offer their resources to be used as edge devices. Few of them may also support inherent mobility. PoS devices in bullet trains and entertainment systems in buses and airplanes may offer such services. The next generation enterprises will gradually move to standalone or integrated private networks with policies and controls using the core-network.
18. **PLMN-Supported Private Networks and Multi-Vendor Interoperability for Banks and FinTech:** Most of the banks and FinTech have a very distributed customer / field office presence. They may find it challenging to set up and operate a completely standalone private network. When deploying PLMN support private enterprise networks, they need to avoid single vendor lock-in.
19. **Distributed Ledgers, Smart Contracts, and Service-Based Architecture for Next-Generation Financial Workflows:** Current platforms provide secure and seamless financial workflows in a limited manner. Distributed ledgers, smart contracts and service-based architecture of beyond 5G can enable next generation innovations.
20. **Transitioning / hybrid deployments** Existing bank infrastructure, particularly on-premises infrastructure continues to have significant residual value. Existing applications may also require several years to transition towards service-based architectures through initiatives such as hollow-the-core approaches. Managing heterogeneous environments requires careful consideration from security, interoperability, operational-efficiency, and lifecycle-management perspectives.

7. Conclusion

The FinTech ecosystem is undergoing significant transformation driven by digitalization, advanced connectivity, interoperable platforms, AI and Digital Public Infrastructure. India has established a strong foundation for delivering digital financial services at scale through initiatives such as Aadhaar-enabled services, UPI, DigiLocker, Account Aggregator and other elements of DPI. At the same time, the evolving ecosystem presents challenges related to interoperability, security, privacy, scalability, resilience, legacy infrastructure, digital inclusion and reliable connectivity.

The whitepaper highlights the potential of AI and Next Generation Networks (NGN), edge and cloud computing, IoT, network slicing, service-based architectures and secure APIs, to progressively address these challenges. Their convergence can enable more intelligent, secure, scalable and efficient financial services while supporting real-time decision-making, automation, personalization, fraud management and improved service delivery.

The future FinTech ecosystem will increasingly depend on interoperable platforms, open and standardized interfaces, secure data sharing and collaboration among financial institutions, FinTech providers, telecom operators, technology providers and other stakeholders. At the same time, inclusion, affordability, digital and financial literacy, privacy, trust and responsible AI need to remain integral to the evolution of these services.

The transition should be phased and interoperable, enabling existing and legacy systems to progressively integrate with next-generation capabilities rather than requiring immediate replacement. Pilots, testbeds and industry collaboration can further validate emerging architectures, use cases and technology requirements. This provides a pathway towards a secure, inclusive, interoperable, intelligent, resilient and cost-efficient FinTech ecosystem, capable of supporting current requirements while enabling future innovation.

8. References

1. [Neal Ford, Comparing Service-Based Architectures.](#)
2. [EY, Regulatory Technology \(RegTech\): The New Frontier in Regulatory Compliance.](#)
3. [EY India, The Winds of Change: Trends Shaping India's FinTech Sector, 2021.](#)
4. [Reserve Bank of India \(RBI\), Payments Vision 2025, Department of Payment and Settlement Systems, June 2022.](#)
5. [Mobile World Live / Telit, Why Payment Providers Must Embrace "Connectivity by Design".](#)
6. [D. D'Silva, Z. Filková, F. Packer and S. Tiwari, The Design of Digital Financial Infrastructure: Lessons from India, BIS Papers No. 106, Bank for International Settlements, December 2019.](#)
7. [OECD, Digital Public Infrastructure for Digital Governments, OECD, 2024.](#)
8. [Committee on Payments and Market Infrastructures \(CPMI\) and World Bank Group, Payment Aspects of Financial Inclusion in the Fintech Era, CPMI Papers No. 191, April 2020.](#)
9. [E. Feyen, J. Frost, L. Gambacorta, H. Natarajan and M. Saal, Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy, BIS Papers No. 117, Bank for International Settlements, July 2021.](#)
10. [Bank for International Settlements \(BIS\), Finternet: The Financial System for the Future, BIS Working Papers No. 1178, 2024.](#)
11. [World Bank Group, Global Digital Public Infrastructure Program: From Foundations to Scale, 2026.](#)
12. [OECD, Digital Government Outlook 2026: Strengthening Digital Public Infrastructure and Data Governance, OECD, 2026.](#)
13. [Reserve Bank of India \(RBI\), Report of the Committee on the Analysis of QR \(Quick Response\) Code, July 2020.](#)
14. [National Payments Corporation of India \(NPCI\), Unified Payments Interface \(UPI\): Product Overview and Features.](#)
15. [National Payments Corporation of India \(NPCI\), UPI Product Statistics.](#)
16. [India Stack, India Stack: Open APIs and Digital Public Infrastructure.](#)
17. [EY India, Seven Key Trends Shaping the Future of FinTech Industry, 2022.](#)
18. [Reserve Bank of India \(RBI\), Concept Note on Central Bank Digital Currency, FinTech Department, October 2022.](#)
19. [Reserve Bank of India \(RBI\), Account Aggregator Framework / Financial Awareness Material on Account Aggregator.](#)
20. [Basel Committee on Banking Supervision, Sound Practices: Implications of FinTech Developments for Banks and Bank Supervisors, Bank for International Settlements, 2018.](#)
21. [J. Ehrentraud, D. Garcia Ocampo, L. Garzoni and M. Piccolo, Policy Responses to FinTech: A Cross-Country Overview, FSI Insights No. 23, Bank for International Settlements, 2020.](#)
22. [K. Croxson, J. Frost, L. Gambacorta and T. Valletti, Platform-Based Business Models and Financial Inclusion, BIS Working Papers No. 986, 2022.](#)
23. [Open Network for Digital Commerce \(ONDC\), Open Network for Digital Commerce – Overview and Network Resources, Government of India initiative.](#)
24. [Digital Personal Data Protection Act, 2023, Government of India, Ministry of Electronics and Information Technology.](#)
25. [Digital Personal Data Protection Rules, 2025, Government of India, Ministry of Electronics and Information Technology.](#)
26. [Government notifies DPDP Rules to empower citizens and protect privacy.](#)
27. [Digital Personal Data Protection Rules, 2025](#)
28. [ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system, International Organization for Standardization.](#)
29. [European Union, Regulation \(EU\) 2024/1689 – Artificial Intelligence Act.](#)

9. List of Contributors

TSDSI acknowledges and sincerely appreciates the valuable contributions of all contributors, supporters, financial-sector experts, government representatives, and members of the IoT/M2M TRIP Forum, whose efforts have been instrumental in the success of this initiative.

The work was chaired by **Suresh V (C-DAC)** and **Abhishek Thakur (IDRBT)**, with the whitepaper championed by **Abhishek Thakur (IDRBT)**, and supported by several dedicated individuals and the TSDSI Secretariat. Their combined expertise and collaboration have significantly enriched the process, and we are grateful for their valuable contributions.

S No	Name	Affiliation
1	Abhishek Thakur	Institute for Development and Research in Banking Technology (IDRBT)
2	Arzad Alam Kherani	IIT Bhilai
3	Alok Mittal	STMicroelectronics
4	Anuradha Vettam	IIIT Hyderabad
5	Dharmesh Vora	SmartCard Systems (Expert)
6	Hemant Jeevan Magadum	C-DAC, Thiruvananthapuram
7	Kaushlendra Singh Sisodia	UniConverge Technologies
8	Ramakrishna	Tejari Solutions (Fintech Expert)
9	Neeraj Dhawan	INVAS
10	Nishi Mundra	Vodafone Idea
11	Pranav Singh	IDEMIA
12	Reshmi TR	SETS India
13	Rishabh Kumar	UniConverge Technologies
14	Sanjesh Tripathi	INVAS
15	Suresh V	C-DAC, Pune
16	Vijay Madan	TSDSI – Convener WP
17	Chandrakanta Rathore	TSDSI – Coordinator WP

Annexures

Annexure 1 - Detailed Mapping of AI–NGN Technology for FinTech

The detailed mapping below provides an extended view of the relationship between FinTech requirements, AI technologies, network technologies, and their potential contribution to the evolution of the FinTech ecosystem.

Table 3: Detailed AI–NGN Technology Mapping for FinTech

Requirement / FinTech Area	AI Technologies	How AI Helps	Network Technologies	How Networks Help
Financial Inclusion	NLP, Conversational AI, Multilingual LLMs, AI Assistants	Enables voice banking, local language interaction, financial literacy support, and AI-assisted onboarding.	5G, 6G, Satellite Networks, Edge Computing	Extends financial services to rural and remote areas through reliable and low-cost connectivity.
Personalized Financial Services	Machine Learning, Predictive Analytics, Recommendation Engines	Provides customized lending, investment, insurance, and financial advisory services.	Edge Computing, Cloud-Native Networks	Supports real-time processing and delivery of personalized financial products.
Real-Time Payments & Transactions	AI Transaction Optimization, Fraud Analytics	Optimizes transaction routing, reduces failures, and detects anomalies instantly.	5G URLLC, Edge Computing, Network Slicing	Enables low-latency, highly reliable, and real-time payment processing.
Security, Privacy & Trust	Fraud Detection AI, Behavioural Analytics, Explainable AI (XAI)	Detects fraud, identity theft, suspicious activities, and improves transparency.	Zero Trust Networks, Secure Network Slicing, AI-Native Security	Provides secure communication channels and cyber-resilient infrastructure.
Interoperability	AI-driven API Management, Intelligent Orchestration	Automates integration, workflow coordination, and intelligent service discovery.	Open APIs, Service-Based Architecture, Cloud-Native Networks	Enables seamless communication among banks, FinTech, regulators, and merchants.
Scalability & High Transaction Volumes	AI Resource Optimization, Predictive Capacity Planning	Dynamically allocates resources and predicts traffic demand.	NGN, SDN, NFV, Distributed Cloud	Supports massive transaction volumes while maintaining performance and availability.
SME & Enterprise Services	AI Credit Scoring, Risk Analytics, Intelligent Automation	Improves lending decisions, credit evaluation, and supply-chain finance.	Edge Computing, Private 5G Networks	Enables secure and responsive enterprise financial services.
IoT & M2M Payments	AI Decision Engines, Autonomous Agents	Enables autonomous transaction decisions by devices.	Massive IoT (mMTC), NGN	Provides connectivity for billions of devices and machine-triggered payments.
Regulatory Technology & Supervisory Technology	Generative AI, Intelligent Automation, Anomaly Detection	Automates compliance monitoring, reporting, auditing, and risk assessment.	Secure APIs, Cloud Platforms, Edge Analytics	Enables real-time data exchange and regulatory supervision.

Digital Identity & Authentication	Biometric AI, Face Recognition, Behavioural AI	Automates identity verification and continuous authentication.	Secure Identity Frameworks, Trusted Networks	Enables secure identity sharing and authentication across institutions.
Fraud & Risk Management	Graph AI, Deep Learning, Predictive Analytics	Detects complex fraud patterns and AML risks.	Edge Security, AI-Native Security Networks	Provides real-time threat monitoring and response.
Customer Support & Financial Literacy	Conversational AI, Voice Bots, Generative AI	Provides 24x7 multilingual customer support and financial education.	Mobile Broadband, Edge Computing, NGN	Ensures continuous service delivery even in low-connectivity areas.
Digital Lending	ML-Based Credit Models, Alternative Credit Scoring	Enables instant credit evaluation and loan approval.	Cloud-Native Infrastructure, Edge Analytics	Provides real-time access to financial and behavioural data.
Insurance Technology	AI Underwriting, Computer Vision, Predictive Analytics	Automates underwriting, claims processing, and risk prediction.	IoT Connectivity, Edge Computing	Enables usage-based and real-time insurance services.
Autonomous Commerce	Agentic AI, Multi-Agent Systems	Supports self-executing purchases and autonomous financial decisions.	6G, Distributed Edge Intelligence	Enables real-time communication between autonomous entities.
CBDC (Digital Rupee)	AI Risk Monitoring, Fraud Analytics	Monitors digital currency transactions and financial risks.	Secure NGN Infrastructure, Distributed Networks	Provides scalable and secure infrastructure for CBDC operations.
Autonomous Finance	Agentic AI, Generative AI, Federated Learning	Creates autonomous financial agents for payments, investments, and savings.	6G, Distributed Edge Intelligence, Network Exposure APIs	Enables future autonomous financial ecosystems with real-time intelligence.
Digital Onboarding & e-KYC	Computer Vision, OCR, Face Recognition, Generative AI	Automates identity verification, document validation, fraud detection	5G, Edge Computing, Cloud Networks	Provides real-time identity verification with low latency
Lending & Credit Scoring	ML, Deep Learning, Alternative Credit Models	Evaluates creditworthiness using transaction history, behaviour, and alternative data	Edge Cloud, 5G Networks	Supports real-time data access and loan approvals
Cybersecurity	AI Security Analytics, Threat Intelligence AI	Identifies cyber threats, malware, and abnormal behaviour	Zero Trust Architecture, 6G Security Framework	Provides secure communication and resilient infrastructure
Identity Management	Biometric AI, Behavioural AI	Continuous identity verification and authentication	Secure APIs, Network Authentication Services	Secure identity exchange across institutions
Regulatory Compliance	Generative AI, NLP, Intelligent Automation	Automates compliance monitoring, reporting, and document analysis	Cloud-Native Networks, Secure APIs	Enables secure real-time reporting to regulators
Supervisory Technology	Predictive Analytics, AI Monitoring Systems	Detects systemic risks and compliance violations	Edge Analytics, API Frameworks	Supports real-time regulatory oversight
Interoperability	AI Orchestration, API Intelligence	Automates integration and workflow coordination	Open APIs, Service-Based Architecture, Network Exposure APIs	Enables seamless communication

				among financial platforms
Digital Payments	AI Transaction Routing, Fraud Analytics	Optimizes transaction processing and risk assessment	5G URLLC, Network Slicing	Ensures ultra-low latency and reliable payments
Cross-Border Payments	AI Risk Analytics, Currency Forecasting	Optimizes exchange rates and fraud monitoring	Global NGN Connectivity, API Frameworks	Accelerates international transaction processing
Wealth Management	Robo-Advisors, Predictive Analytics, GenAI	Provides automated investment recommendations	Cloud Infrastructure, Edge Computing	Supports real-time portfolio management
Supply Chain Finance	Predictive Analytics, AI Risk Models	Tracks supply chain risk and payment behaviour	IoT, 5G, Edge Networks	Provides real-time visibility across logistics networks
Embedded Finance	Context-Aware AI, Recommendation Systems	Delivers financial services within non-financial applications	API Ecosystems, 5G Connectivity	Supports seamless integration across platforms
Financial Literacy	Conversational AI, Generative AI Assistants	Provides personalized financial education and guidance	Mobile Broadband, Edge Services	Enables delivery of educational content at scale
Customer Support	AI Chatbots, Voice Bots, LLMs	Offers 24/7 multilingual customer support	5G, Cloud Contact Centres	Ensures uninterrupted service delivery
Smart Contracts & Digital Assets	AI Validation, Automated Compliance	Supports contract monitoring and risk detection	Blockchain Networks, Secure Connectivity	Provides trusted distributed transaction infrastructure
Machine-to-Machine Payments	Agentic AI, Autonomous Decision Engines	Enables autonomous financial decisions by devices	Massive IoT (mMTC), 6G Networks	Supports billions of connected devices and transactions
Autonomous Commerce	Agentic AI, Multi-Agent Systems	Enables self-executing purchases and transactions	6G, Edge Intelligence	Provides real-time communication among autonomous systems
Smart Cities Finance	Predictive AI, Urban Analytics	Supports automated tolls, parking, utilities, and public services	IoT, NGN, Edge Computing	Provides reliable connectivity for city-wide financial services
CBDC (Digital Rupee)	AI Risk Monitoring, Fraud Analytics	Monitors digital currency transactions and risks	Secure NGN Infrastructure	Supports secure and scalable digital currency operations
Dynamic Risk Management	Predictive Analytics, Federated Learning	Predicts credit, market, and operational risks	Edge Computing, Distributed Cloud	Enables real-time risk monitoring across networks
Real-Time Decision Making	Agentic AI, Reinforcement Learning	Enables instant lending, investment, and payment decisions	Edge Intelligence, URLLC	Supports ultra-low latency processing
Future Autonomous Finance	Agentic AI, Generative AI, Federated Learning	Creates autonomous financial agents capable of acting on behalf of users	6G, Distributed Edge Intelligence, AI-Native Networks	Provides real-time, secure, and intelligent infrastructure for autonomous financial ecosystems

Annexure 2 - Identities for Privacy Preserving, Inclusive Trust

2.1. Background

Mix or channels (physical and variety of virtual), identities create a challenge in providing end-to-end trust. This is amplified for digitally naïve people who may find technology too complex, or make simplistic assumptions based on miss selling / social engineering. This note discusses the challenge and suggests possible recommendation to ITU / WTSA to further study and standardize next generation platforms to be more inclusive for all. It further proposes simplified on-boarding in digital realm and protection against fraud using digital means to improve trust in the systems.

2.2. Identity Types and Digital Representation

- i). **Physical Identity:** Identity of entity (people and/or organizations) are frequently associated to ID cards / tokens issued by organizations at national / enterprise level (state ID, driving license, tax ID etc.).
- ii). **Virtual Identity:** Today most of the entities also have addresses in cyber/telecom/meta realm. These cyber identifies may include phone numbers, mail-ID, social media handle, websites, payment/wallet handles, certificates (PKI),etc.

2.3. Physical Workflows and Identity-Based Trust

Workflows may span a mix of physical and digital channels. E.g. purchase of vegetable in physical world followed by payment using mobile app (digital wallet). Hereinafter such workflows spanning physical and digital channels are referred as Phygital workflows.

- i). **BG2C Verification Workflows (Business / Government with Entities):** Most of these workflows are regulated at least on one side (business / governance). The local laws for due-diligence (know-your-customer / employee-verification) and related background checks need to verify the Physical Identity of the entities.
- ii). **C2C Verification Workflows (Entities with Entities):** Many peer-to-peer workflows may be semi-formal or informal. In context of global south, it may span a wide variety – from purchasing a vegetable from a push-cart to a house help to resale of goods / services on platforms like OLX/eBay. Some of these may be regulated while others may be completely unregulated. In many cases, when the platforms utilize virtual identities, the participants may lack awareness and expertise to understand the finer nuances and rely on support from others (e.g. shared phone number for family or group of migrant workers).
- iii). **Authorization Workflows:** For efficient and affordability many of workflows expect authorization by sharing data (e.g. OTP) through one or more virtual identities. This creates a risk – especially if the identity is not under proper control of the end entity (e.g. shared/stolen phone number, compromised mail-ID etc.).
- iv). **Delegation:** Many a times the entity may delegate the responsibility of operating a physical / virtual identity to someone else. In case of organizations, it may be a person or a group of persons. In case of minors or challenged people, delegation may be with parent(s) and/or guardian. In case of banking in India, business-correspondents (BC) act as a bridge between the bank and the customer. Shared device of BC, coupled with delegation from bank to act on its behalf, enables affordable banking for remote areas.
- v). **Registries:** Work-flows may rely on registries (e.g. clinics / doctors / notary) to identify people (possibly their delegation) participating in the workflow and/or to ensure compliance.

Sometimes these registries also provide additional inputs to the workflow (e.g. Credit ratings, Incorporation of Companies, Verified-handles / white-list, Blocked-handles / black-lists etc.)

- vi). **Audit logs:** For many workflows (especially in realm of finance), compliance to local law requires audit logs to be maintained for subsequent settlement and/or dispute resolution.
- vii). **Compliance:** Regulated entities must carry out regular audits of their records with approved third parties.

2.4. Trust, Inclusion and Security Gaps

- i). **Expertise:** Many end users lack the expertise and hence do not on-board to digital platforms.
- ii). **Trust:** Many end users do not trust the platforms. This could be because of hearsay and/or prior experience.
- iii). **Frauds:** Lack of end user awareness, coupled with systems lack of visibility across the channels allow social engineering attacks to be launched in Phygital workflows. Rest of the discussion will use following simple example:

2.5. Illustrative Phygital Fraud Scenario

i). Actors and System Components

- a) Naïve User (NU),
- b) Rogue User (RU),
- c) Alternate Channels like eBay/Olx (AC),
- d) Compromised Digital Handles / burner accounts / cut-outs (CDH),
- e) Payment App (PA) of naïve user.

ii). Fraud Scenario and Attack Flow

Discovery of “naïve user’s digital handle” by rogue element (RG) on ebay/olx workflow – followed by phone calls / social media chat / emails offering to complete the workflow. Subsequent usage of CDH to fleece naïve user. Distracted by the social engineering the naïve user ends up paying to CDH, rather than receiving money.

Once the naïve user realizes about the fraud (possibly after a day or more) they try to dispute with the wallet provider/bank. Unluckily the bank does not have full visibility on Alternate Channel’s platform. Further police/law enforcement get stuck up on physical jurisdiction (e.g. state / country etc.) and in the meantime RU withdraws the cash by relaying through other CDH or moving out of the country to minimize exposure in subsequent audit.

2.6. Emerging Opportunities and Technology Directions

- i). **Privacy:** For the global south, inclusion along with trust and access is paramount. They are willing to trade some of the privacy to get safe, affordable and easy access workflows. Even for developed economies, consent based privacy-preserving mechanism for data sharing can be devised to reduce frauds and improve trust.
- ii). **Service based architecture in 5G and Beyond:** It’s possible for next generation platforms to handle identity as a service for entities (with tokenization / avatars for a. privacy preservation, and b. minimize attacks/leakage in case of data compromise).
- iii). Additional context about the app / digital handle / user location can be provided as an option, based on user’s consent. This helps improve accuracy for “anti-fraud” measure and possibly identify CDH without explicit reporting from owner. E.g.
 - a) Share alternate channels digital handles with Payment App (both parties)

- b) Network service provider exposes additional context about device of PA of RU and NU out-of-band (e.g. API call exposed by Telco). Absence of these context (or consent) should increase rigor for checks and throttle/delay the transactions.
- c) Changes to phone, SIM, other digital handles can be captured in neutral repositories and relative “risk scores” created based for the handles.
- iv). NU have access to digital handles enabled on their physical / virtual identities through repositories.
 - a) This is akin to SSN/PAN/AADAAR based lookup of mobile numbers or surrendered savings with the government / regulator.
- v). NU may create persona’s / avatars to manage interactions with repositories as well as participate in PA transaction flows.
 - a) May be offered as a retail service by enterprises (telco, bank, cloud service provider) with a baseline version supported by government (e.g. for Jan-Dhan account holders). (bullet to be re-examined)

For various business workflows, some of these activities may be periodically repeated (e.g. re-KYC). While in past the communication for these activities happened in physical world using pen and paper with physical presence, digitization implies that many of these workflows are becoming paperless and presence-less (e.g. video KYC over mobile phone).

In financial world, to reduce fraud and ensure compliance with anti-money-laundering etc. the digital workflows will use existing repositories for legal compliance as well as automatically interact with the NU/RU digital personas to minimize risks/frauds for naïve user.

Annexure 3 - Excerpt from RBI Report on QR Codes

3.1 Background

Briefly introduce the relevance of QR codes to digital/mobile payments and state that the following is an excerpt/adaptation from the RBI Committee report.

3.2 Security Challenges in QR Code-Based Payments

As the most important part of e-commerce, mobile payment directly involves the capital of users and related parties. Therefore, payment security is one of the key issues in mobile payment. In case of QR code payments, remote access to the payment system is given through a QR code. The security of this payment mode is divided in three parts:

i). QR Code Security

- a) Generic names like “Verified Merchant” or “Merchant” make it difficult to build trust in the system and result in poor consumer & merchant experience. P2M QR scans should provide meaningful, user-friendly names. This can be accomplished by registering the rightful beneficiary’s name in a central system available via API calls to validate the VPA.
- b) Like UPI, signing requirements for Bharat QR codes may be evaluated to ensure higher security.

3.3 Application-Level Security

The committee recommends following security measures for all issuer apps that scan QR code for payments:

- i). Card credentials or any PII data should not be stored in the device
- ii). RBI guidelines for ‘card not present transactions’ should be adhered
- iii). Merchant name and masked credential must be displayed in the app after scanning a QR, to enable safe transactions
- iv). App should allow users to have deeper understanding of security

3.4 Backend and Infrastructure Security

Networks, Banks and TPAP should ensure very high levels of security at this layer to ensure secure transmission and storage of data. They should continually invest on monitoring and enhancing security at this layer – at the physical, network and application infrastructure.

3.5 Network Connectivity

India has taken a big step towards becoming a less-cash economy by registering a quantum jump in number of digital payments, especially after demonetization. However, along with digital empowerment of every stakeholder, seamless and secure internet connectivity across the country remains a big challenge. There is an increased penetration of smartphone users in India but, not everyone has access to seamless internet connectivity to enable digital payments with ease. Moreover, using an unsecured public WiFi or other connections may lead to data leak and compromise data security, leading to financial frauds.

Annexure 4 – UPI-Enabled ATM Services: Conceptual Framework and System Architecture

4.1 Introduction and Context

To enhance the capabilities and interoperability of ATM services, UPI-enabled cardless cash withdrawal has been introduced as an extension to conventional ATM-based cash withdrawal mechanisms. This Annexure presents the conceptual framework and high-level system architecture associated with UPI-enabled ATM services.

4.2 Interoperable Cardless Cash Withdrawal (ICCW)

The integration of Unified Payments Interface (UPI) with Automated Teller Machines (ATMs) is officially designated as Interoperable Cardless Cash Withdrawal (ICCW). Developed by the National Payments Corporation of India (NPCI), the technical framework bridges ISO 8583 legacy financial messaging protocols (traditionally used for card-based ATM switching) with JSON-based Restful API architectures native to modern UPI switches.

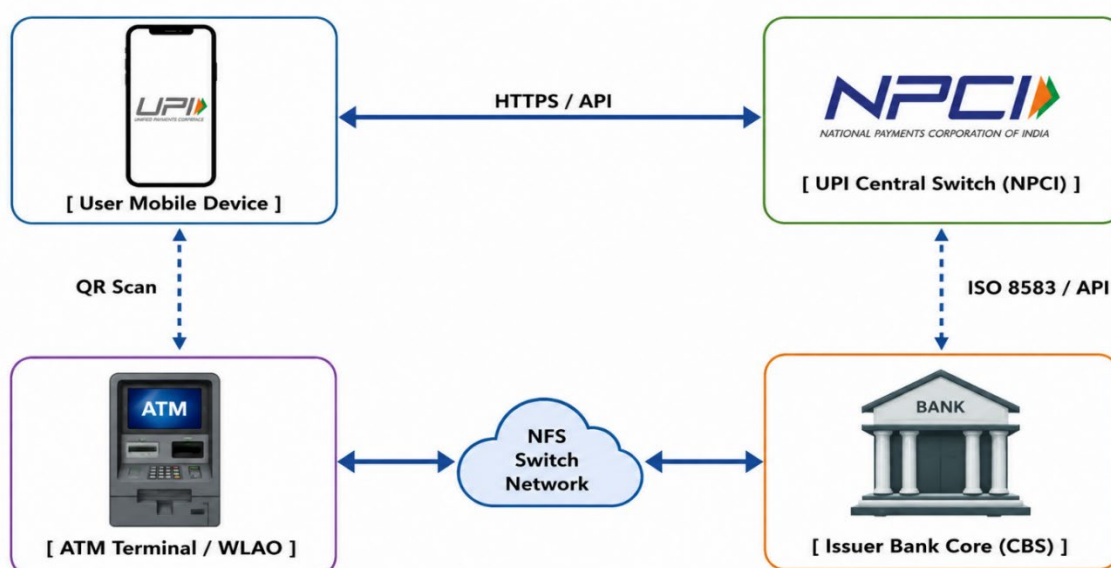


Figure 3: High-Level Architecture of UPI-Enabled ATM Services

4.3 The Ecosystem Intermediary

The system relies on the National Financial Switch (NFS) network. It maps a customer's virtual payment address (VPA) or linked bank account directly to the hardware terminal requests, bypassing physical magnetic-stripe or EMV chip handshakes.

4.4 The Hardware Layer

White Label ATM Operators (WLAOs), such as Hitachi Payment Services, use Android OS-powered ATM architecture. This replaces the older, rigid Windows-based legacy terminal software, allowing for dynamic, screen-generated visual data payloads.

Annexure 5 - Details of Fintech Use Cases

The FinTech use cases can be studied from various perspectives – a. end user (customer, citizen or enterprise); b. incumbent players (banks and related regulated entities); c. tech-innovators or disruptors (who leverage technological breakthrough and agile execution to offer new solutions, some of which may have unknown risks); and d) regulators and government.

The later part of this chapter primarily covers end user and tech-innovator perspective though the incumbent players and regulators play a key role in enabling the use cases.

5.1 Fintech Use case

Following is a broad categorization of the use cases for FinTech:

- i). Customer facing channels: The workflows may be instantiated across various channels like brick-and-mortar Branch, ATM/DBU/Kiosk/PoS, Online (browser), Mobile (App), Agents (BC/FinTech), Social Media etc.
- ii). Loans / Lending – (for retail as well as enterprise)
 - a) Opportunity Discovery, Customer Convenience and Efficiency
 - b) Loans - Collateral and its digitization – over-leverage
 - c) Credit cards –
 - d) Registries like CERSAI, credit reporting agencies etc.
 - e) Exit: Closure / Default (NPA handling)
 - f) Cross vertical / supply chain: TREDS, Warehouse receipts etc.
- iii). Investing – Savings, equity, mutual funds, P2P lending, portfolio management service etc.
 - a) Statements
 - b) Tax reports
- iv). Cross Vertical – Payments and Fund Transfer
 - a) Prepaid instruments like cards,
 - b) Checks, drafts processing
 - c) Bill and utility payments
 - d) Card payments
 - e) UPI / wallets
 - f) Car / bike as transaction anchor using FASTag etc.
- v). Insurance – varied needs – life, health, home/infra, travel, business, supply-chain etc. also includes various sub-activities like KYC, premium processing, claim processing, re-insurance etc. In some cases – Insurance may overlap with other products like investment (e.g. ULIPs) servicing and warranty.
- vi). Channel Network Specific – FinTech ecosystem has multiple channels like card networks (e.g. RuPay, Visa etc.), domestic fund transfers, international fund transfer (SWIFT) etc.
- vii). Forex / Money Exchange / Remittance – these use cases may involve physical currency or cards (both debit and credit) as well as electronic fund transfers. Increasingly this space is being automated with kiosks and digital channels replacing the manned tellers.
- viii). Mixed products – Many of the FinTech services are customized offerings with partnerships across organization. E.g. leasing a car, rewards programs with co-branding for channels / platforms, insurance + investments as ULIPs etc.
- ix). Intra-Enterprise Use Cases
 - a) BCP – business continuity planning
 - b) AAA – Authentication, Authorization and Accounting
 - c) Staff / Partners management – e.g. agents for loan/credit-card leads etc.

- d) Treasury/cash management
- e) Internal audits etc.
- x). Customer Engagement channels – While customers were primarily engaged via brick-and-mortar branches in past, now they are connected in cyber-world through varied channels like plastic cards, NFC wearables, social-media networks, tele-banking, mobile apps etc.
- xi). On-boarding – Background of new customers needs to be verified to ensure that the users are compliant with FATF / AML norms.
- xii). Physical services – FinTech continue to provide few services in physical form. E.g. locker as a service.
- xiii). Customer Safety and Consent Based Data Sharing – FinTech platforms should protect the customers and advise them appropriately. Further using Account Aggregator and similar APIs they should allow them a secure way of sharing their data with third-parties.
- xiv). Advisory and consultant role – Frequently bankers may provide financial advice (e.g. as wealth management service) and in some cases act as consultant to the customers (e.g. for merger / amalgamation / large value purchase etc.), especially if they are providing loans for projects.
- xv). Governance, Risk and Compliance – GRC tools ensure that the banks and related financial organizations optimize their operations while minimizing risks. These tools also monitor / implement controls for Anti Money Laundering, Fraud reduction etc.
- xvi). Grievance and dispute resolution – Fintech solutions should allow easy and efficient mechanism for customers to escalate issues (e.g. dispute transaction) and automate resolution for the same.
- xvii). IT for IT – this category covers a wide gamut technologies enabling the development, deployment and maintenance of FinTech's technology stack.

5.2 Bank Enterprise Architecture

Following section broadly covers the enterprise architecture for a typical bank. Other financial organizations like insurance may have similar architecture

i). Branch / Field Office

Following figure captures the devices and connectivity for a field office

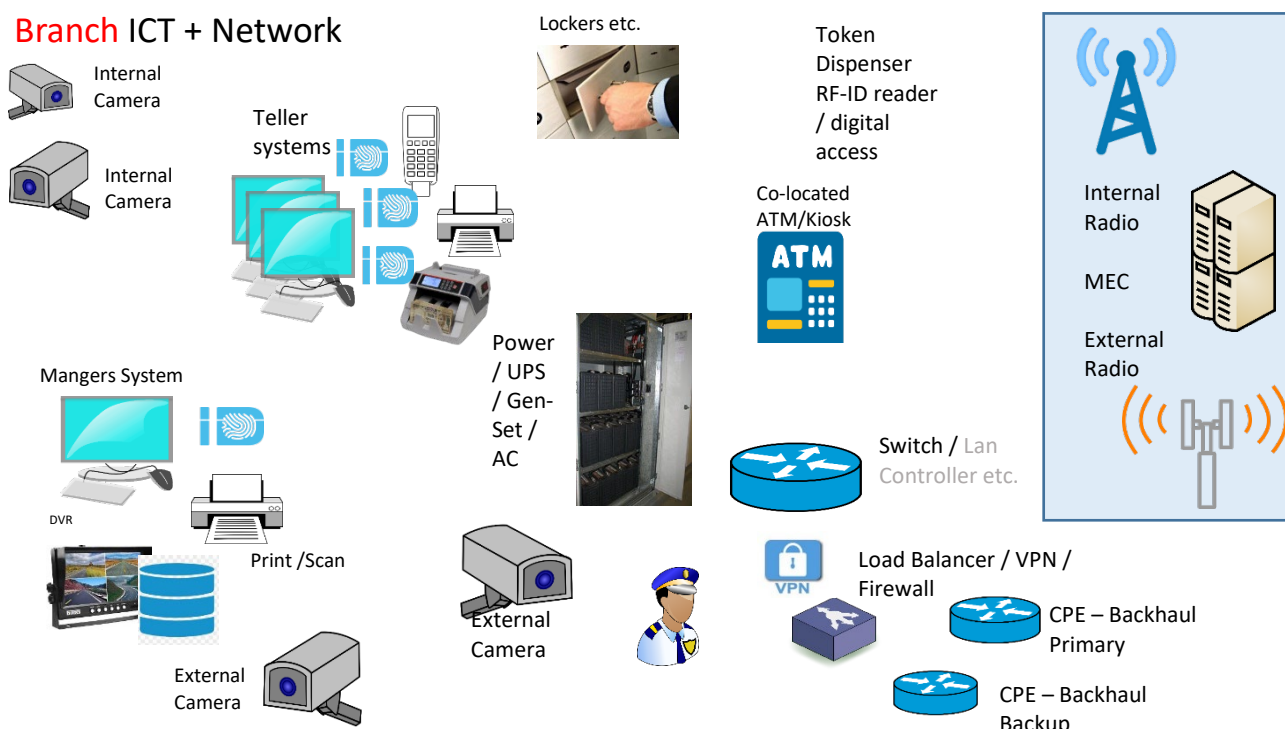


Figure 4: Pilot Structure for including the Bank Branch

ii). Head-office / Centralized components

A typical bank would be headquartered in a physical building with string physical security around it. They may host their primacy data centre (PDC) in their own premise or use a collocated site. For business continuity, the banks would also run a disaster recovery (DR) site in a separate geographic and seismic zone. All the branches and zonal offices connect to the data centres (both PDC and DR) using MPLS links. For cost efficiency, few apps may run out of DR site and replicate / backup to PDC.

In rare cases, the bank may utilize public cloud platforms or services of third party or run their technology stack. This may especially apply for small / neo banks.

Following section captures the large elements within the data centre of the banks

5.3 Core Banking Solution (CBS)

The PDC runs CBS which has a database. Typical transaction involves Double Entry (i.e. debit in one account and credit in another account) and Journals for both the debit and credit. Further the records are replicated to DR site. In essence a single transaction becomes eight record updates in CBS.

5.4 MIS / Data Warehouse / Data Lake

The feeds from various workflows in bank are analysed and presented in MIS dashboard. Big data platforms may be used to expedite the processing and infer the results in close to real time.

5.5 Sandbox – Tech / Workflow

For innovations and partner on-boarding a test environment may be provided in form of a technical sandbox. Parts of it may run within the PDC/DR sites of the banks.

5.6 APIs / Gateways / Registries

Multiple activities in banks business logic would integrate with SMS gateway, CERSAI and Credit Registries, Aadhaar platforms, KYC APIs (e.g. passport verification API), digitized land records etc.

5.7 Transaction Channels for services

The data centre would also integrate with SWIFT, NFS, INFINET, NEFT, RTGS, IMPS, Mastercard, Visa, Rupay and related channels for transactional data flow.

5.8 Usage of public and community cloud

Banks may use community cloud or public cloud based on their IT strategy and related risks.

5.9 Existing FinTech Use Cases and Realization

In context of architecture in the previous section, following use cases are mapped on the technology stacks and challenges / opportunities identified:

- i). User enrolment using Aadhaar and video KYC
- ii). Payment at merchant shop using UPI (present with sound box / dynamic QR)
- iii). Farm loan for purchase of second-hand tractor (for future releases)
- iv). Agents / Business Correspondents as vehicles for Inclusion – cash-based instalment collection against loan (for future releases)

Enrol using Aadhaar and Video KYC – simplified steps

Table 4: FinTech Use Case Realization and Technology Mapping

Goal	Complete customer due-diligence and enrol them as bank customer
Overview	KYC is mandated to minimize fraud risk, implement anti-money-laundering measures and other related requirements. In this case online KYC is done with support of Aadhaar APIs and live video interactions with customer.
Cross Reference	Re-KYC (i.e. KYC at repeated interval), Customer Risk Profile (optional)
Actors	People: Customer, Bank Staff conducting Video interaction, IT: Video Conferencing tool, CBS (Customer Folio), Aadhaar API, SMS Gateway, CERSAI-KYC API
Pre-condition	A. Adult customer with bank's mobile Application release XX or higher installed on their device B. Physical Aadhaar card in possession
Post-condition	Entry created in CBS, CIF# allocated, CERSAI KYC reference number shared with customer
Normal Flow	Initiation 1. Customer selects "Self-Enrolment with Video KYC" by navigation from default/pre-login home screen. 2. Based on risk perception, captcha may be used to minimize bot-based attack before customer moves to next screen. 3. Based on text prompts, customer enters their personal details, including name, date of birth, address, Aadhaar number etc. Note: it may be auto extracted from photo of Aadhaar card or related KYC documents. 4. The customer authorizes bank for Aadhaar enabled verification. 5. Based on text prompt, photo of Aadhaar card (front and back) is uploaded by the app and its clarity is confirmed. The user entered Aadhaar number is verified using text extraction from image.

	6. Aadhaar API is used to trigger an authorization OTP from the customer. 7. Once customer enters the Aadhaar authorization OTP address and other details are matched against KYC fields. Changes if any are flagged to customer and also marked as input for bank staff. 8. Once customer confirms their preferred time for video call – video conferencing tool generates a meeting URL for the configured duration. Video Conference Call and CIF creation 1. Bank staff and customer join the video call at the chosen slot. 2. Bank staff does basic interactions and reverification to ensure that the customer is the real person and not using masks etc. (typically in 2-5 minutes). 3. The aging of customer w.r.t. photo in Aadhaar card is verified by the bank staff. 4. Further key frames from video are extracted and analysed by image processing tool for match with Aadhaar photo. 5. Once the bank staff is convinced, they approve the video-KYC based verification. 6. The CBS system generates the CIF number and populates the fields based on data collected in prior steps 7. CERSAI repository is updated and KYC number generated for the customer
Flow Deviations (normal)	Physical visit by customer to branch or staff to customer's premise may be used in place of video KYC
Flow Exceptions	Various steps may have negative outcomes that needs to be retried or handled as exception – e.g. bad captcha, poor connectivity during video conference, data mismatch with Aadhaar etc.

Annexure 6 – Technology support for existing and Emerging FinTech Use Cases

LPWAN technologies such as NB-IoT, LTE-M, Cat-M1 in telecom domain can work along with LoRa, ZigBee, Wi-SUN, DASH7 and related technologies to provide connectivity for FinTech use cases.

6.1 LORAWAN

LoRa is a wireless modulation technique derived from Chirp Spread Spectrum (CSS) technology. It encodes information on radio waves using chirp pulses - similar to the way dolphins and bats communicate (through Lora uses electromagnetic waves as opposed to sonar waves used by bats and dolphins). LoRa is robust against disturbances and can be received across greater distances (3-10 kms depending on terrain) when compared with Wi-Fi, 4G/5G, or ZigBee. It is ideal for applications that transmit small chunks of data with low bit rates. These features make LoRa well suited for sensors and actuators that operate in low power mode over large geographical spread. LoRaWAN is a Media Access Control (MAC) layer protocol built on top of LoRa modulation.

LoRa can be operated on the license free sub-gigahertz bands, for example, 915 MHz, 868 MHz, and 433 MHz. It also can be operated on 2.4 GHz to achieve higher data rates compared to sub-gigahertz bands, at the cost of range. These frequencies fall into ISM bands that are reserved internationally for industrial, scientific, and medical purposes.

Primary ref: <https://www.thethingsnetwork.org/docs/lorawan/what-is-lorawan/>

Since it works best for low bandwidth non-realtime transactions, LoRa can be used for basic financial transactions like balance enquire and/or fund transfer. Since it utilizes unlicensed spectrum, it is prone to DoS as collision-free environments cannot be guaranteed.

6.2 Wi-SUN

Wi-SUN (Wireless Smart Utility Network) is a wireless communication standard that enables seamless connectivity between smart-grid devices with range of up to 4 kms with data rate up to 300 kbps and 20 msec latency. It is based on the IEEE 802.15.4g standard for the physical layer (PHY) and the IEEE 802.15.4e standard for the MAC layer.

Ref.: <https://www.everythingrf.com/community/what-is-wi-sun>

6.3 WiFi 6 and beyond

Wi-Fi 6/6E (802.11ax) and other forthcoming wireless networking standard like 802.11be has the possibility of enhancing and supplementing connectivity, particularly for mobile-based financial transactions.

Wi-Fi6 provides faster data transfer rates along with low latency, making it suitable for a speedy smart device-based financial transaction such as local shopping. One of the most significant advantages of Wi-Fi6 is its higher connection density, which may be used in remote, concentrated, and congested market areas. This would allow several users to initiate payments/transactions at the same time.

Though Wi-Fi6 assures inbuilt security features, the open and public or free Wi-Fi network pose security risk and may jeopardise financial data.

6.4 Summary Feature List of Advanced LTE, 5G and beyond for Verticals

- i). **Higher Bandwidth:** enables immersive telepresence and XR: Allows leverage of video feeds from camera etc. for edge analytics.
- ii). **Wider coverage:** (using public network): will ensure that field banking would be almost on par with branch-based banking for the majority of the masses.
- iii). **Private Networks:** With the service-based architecture enabling a standards-based split of core network for improved security and orchestration for enterprise networks and their applications. While legacy enterprises may gradually move their existing solutions to such networks, neo-banks and fintech may leverage it for better control and compliance. Scaled to national levels, it provides efficient rails for running PoS/UPI networks etc.
- iv). **Security:** with SIM / eSIM enabled secure communication, telecom networks provide better access control and privacy vis-a-vis ethernet / Wi-Fi networks.
- v). **Lower power:** many of the devices may run off the battery - e.g. PoS, Payment Sound Box, asset-tracker etc. With support for NB-IoT / RedCap devices in telecom networks will provide longer recharge cycles and greener deployments.
- vi). **N3IWF:** Since legacy solutions (including those based on WiFi / Ethernet) cannot be completely replaced, onboarding them in beyond-5G networks will utilize standards-based integration via N3IWF.
- vii). **Novel Architectural Patterns:** integration with multi-access edge, along with service-based architecture in 4G/5G opens up the possibility of new architecture patterns using infrastructure from multiple stakeholders. Some of these patterns would utilize DLT for improved orchestration and audit. They may also be designed to include inbuilt “regulatory controls” to ensure that compliance costs are minimal.



Telecommunications
Standards Development
Society, India

Registered Office Address
C-DOT Campus, Mandi Road, Mehrauli,
New Delhi, India – 110030
www.tsdsi.in

