**United International Journal of Multidisciplinary Research (UIJMR) An International Peer-Reviewed and Refereed Multidisciplinary Journal**
**ISSN: 3048-6726 Impact Factor:6.934(SJIF)Volume-3, Special Issue-10**

# ARTIFICIAL INTELLIGENCE AS THE ENGINE OF DIGITAL INDIA: SECURE PAYMENTS, EXPLAINABLE DECISIONS AND INCLUSIVE GROWTH

**Ch. Keerthi**
**MCA, TS-SET, UGC-NET**
**Lecturer in Computer Science**
**Girraj Government Degree College (A)**
**Nizamabad, Telangana, INDIA**
**DOI:10.37854/UIJMR.2026.310.162**

**ABSTRACT**

India's journey towards Viksit Bharat @2047 rests on a digital foundation that few countries have attempted at comparable scale. Digital India has produced a public infrastructure anchored on Aadhaar, the Unified Payments Interface (UPI) and DigiLocker, and Artificial Intelligence (AI) is now being layered on this infrastructure to lower costs, protect users and improve governance. This paper brings together evidence from the author's earlier studies on AI-powered payment routing, AI-based fraud detection in Indian digital payments and Explainable AI (XAI) in governance, to show how AI is transforming the Indian economy along four dimensions: efficiency, security, inclusion and accountability. The evidence reviewed indicates that, in reported implementations, AI-based routing can reduce transaction costs by up to 25 percent and raise approval rates by 15–20 percent; that ensemble machine-learning models achieve fraud-detection accuracy of 92–100 percent in experimental and production settings; and that XAI is needed to make AI-assisted decisions in welfare, justice and finance understandable and reviewable by citizens. At the same time, the paper highlights persistent challenges: class imbalance, the adversarial use of generative AI by fraudsters, the digital divide, uneven protection between urban and rural users, data-privacy limits and the opacity of complex models. The paper concludes that AI can accelerate India's economic transformation only if it is deployed as a layered, explainable and inclusive system supported by regulation, capacity building and consumer awareness.

**Keywords:** Digital India; Artificial Intelligence; Economic Transformation; Digital Payments; UPI; Fraud Detection; Payment Routing; Explainable AI; Viksit Bharat @2047.

## 1. Introduction

India is entering the second quarter of the twenty-first century with an ambitious national goal: to become a developed economy by the centenary of its independence in 2047. The Viksit Bharat @2047 vision, elaborated by NITI Aayog (2023), combines economic prosperity, social development, environmental sustainability and good governance. Digital technology is central to this goal. Over the last decade the Digital India programme has created a Digital Public Infrastructure (DPI) anchored on Aadhaar, UPI and DigiLocker, which is one of the most comprehensive digital transformation programmes in the world (PIB, 2024).

Digital infrastructure alone, however, does not transform an economy. What converts connectivity into productivity is the intelligence applied to the data that flows through it. Artificial Intelligence (AI), including machine learning, deep learning and natural language processing, is increasingly used to decide how payments are routed, which transactions are fraudulent, who is eligible for a welfare benefit and how public services are delivered. The Government of India has recognised this through the IndiaAI Mission, launched in March 2024 with a budget of ₹10,371.92 crore (MeitY, 2024), and through the India AI Governance Guidelines published by the Ministry of Electronics and Information Technology (MeitY) on 5 November 2025.

This paper argues that AI is transforming the Indian economy along four mutually reinforcing dimensions: **efficiency** (lower costs and faster processing), **security** (protection of users and trust in digital channels), **inclusion** (extension of benefits to rural, multilingual and low-literacy populations) and **accountability** (decisions that citizens and regulators can understand and challenge).

The objectives of the paper are: (a) to describe Digital India as the infrastructural base of economic transformation; (b) to examine how AI improves efficiency in payment processing; (c) to assess the role of AI in securing digital payments in India; (d) to explain why Explainable AI is essential for accountable digital governance; and (e) to identify

challenges and recommend a way forward. The study is descriptive-analytical and is based entirely on secondary data drawn from government publications, regulatory disclosures, industry reports and peer-reviewed studies, as compiled in the author's earlier papers (Keerthi, 2024; Keerthi, 2025; Keerthi, n.d.).

## 2. Digital India: The Foundation of Economic Transformation

### 2.1 Digital Public Infrastructure

The DPI framework anchored on Aadhaar, UPI and DigiLocker provides the basis on which AI can be integrated into governance and finance (PIB, 2024). Table 1 summarises the scale of this infrastructure. More than 138 crore Aadhaar enrolments, 56.2 crore DigiLocker users, 96.96 crore internet subscribers and 5.84 lakh Common Service Centres (4.63 lakh of them at Gram Panchayat level) show how far digital services have been taken. The UMANG platform offers 2,300 services in 23 languages, and mobile connectivity covers 97.65 percent of villages. At the same time, India's rank of 97th among 193 countries in the UN E-Government Development Index 2024 (United Nations, 2024) is a reminder that the scale of infrastructure and the quality of digital government are not the same thing, and that transparency and accountability must keep pace with expansion.

***Table 1: India's Digital Infrastructure and Payment Indicators***

| **Indicator** | **Current Status** |
|---|---|
| Aadhaar enrolments | 138+ crore (mid-2024) |
| DigiLocker users | 56.2 crore (July 2025) |
| Internet subscribers | 96.96 crore (2024) |
| Common Service Centres (CSCs) | 5.84 lakh (including 4.63 lakh at GP level) |
| UMANG app services | 2,300 services in 23 languages; 8.71 crore registrations |
| Village mobile connectivity | 97.65% of villages covered (May 2025) |
| IndiaAI Mission budget | ₹10,371.92 crore (March 2024) |
| UN E-Government Development Index rank | 97th out of 193 countries (2024) |

| Indicator | Current Status |
|---|---|
| UPI transactions, FY2024-25 | 185.9 billion transactions; value ₹260.6 lakh crore |
| RBI Digital Payment Index | 100 (2017-18) to 493.22 (2024-25) |

*Source: Compiled from PIB (2024); MeitY (2024); United Nations (2024); Medianama (2025); Keerthi (2024).*

### 2.2 UPI and the Digital Payment Revolution

The most visible expression of Digital India is the growth of digital payments. UPI transaction volume increased by 41.7 percent to 185.9 billion in 2024-25, while the value of transactions rose by 30.3 percent to ₹260.6 lakh crore; by the end of FY2024-25, UPI accounted for 84 percent of all transactions on India's retail payment systems (Medianama, 2025). The RBI's Digital Payment Index rose from 100 in 2017-18 to 493.22 in 2024-25, an almost five-fold increase in the adoption of digital payments (Keerthi, 2024). This growth is attributed to the affordability of the internet, increasing financial inclusion and interoperability among banks and payment apps such as Google Pay, PhonePe and Paytm (Business Today, 2024), together with UPI's zero-transaction-cost model for users (Keerthi, 2024).

Financial inclusion programmes such as Jan Dhan Yojana and Digital India have brought hundreds of millions of previously unbanked citizens into the formal financial system. This is a major economic achievement, but it also created a very large population of new digital users who may be more susceptible to fraud because of limited digital literacy (Keerthi, 2024). Growth in digital payments therefore creates a parallel need for intelligent protection, which is where AI enters the picture.

## 3. Artificial Intelligence as an Economic Enabler

### 3.1 Policy and Institutional Framework

The IndiaAI Mission is the government's initiative to develop a world-class AI ecosystem (MeitY, 2024). On 5 November 2025, MeitY released the India AI Governance Guidelines, prepared by a committee chaired by Prof. Balaraman Ravindran of IIT Madras. The guidelines follow a non-regulatory approach that emphasises voluntary safeguards rather than legal enforceability, and they set out principles that include transparency, accountability, safety and reliability, privacy and security, fairness and non-discrimination, human-

centred values, inclusive innovation and digital-by-design governance. The proposed institutional structure includes an AI Governance Group (AIGG), a Technology and Policy Expert Committee (TPEC) and an AI Safety Institute (AISI) (MeitY, 2025; PIB, 2025a). Multilingual capability is supported by the BHASHINI platform, which covers more than 35 Indian languages with over 1,600 AI models (PIB, 2024).

### 3.2 AI Techniques Used in Digital Payments

AI in payments is rarely built on a single algorithm. Institutions typically deploy a layered combination of techniques, each addressing a different part of the problem, from real-time transaction scoring to post-transaction network analysis (Afriyie et al., 2023; Preciado Martínez & Náñez Alonso, 2025). Table 2 summarises the principal techniques and their applications.

***Table 2: AI Techniques Applied in Digital Payments***

| Technique | Core Function | Representative Application |
|---|---|---|
| Supervised machine learning (Random Forest, Logistic Regression, Gradient Boosting) | Classifies transactions as fraudulent or legitimate using labelled historical data | Real-time transaction scoring and authorisation decisions |
| Unsupervised learning / anomaly detection | Flags deviations from normal behaviour without labelled fraud examples | Detecting novel fraud typologies absent from training data |
| Deep learning / neural networks | Models complex, nonlinear relationships across large feature sets | Sequential spending-pattern analysis; routing decisions in under 50 milliseconds |
| Natural language processing (NLP) | Analyses message and website content for deception indicators | Phishing and smishing detection; multilingual fraud-report analysis |

| Technique | Core Function | Representative Application |
|---|---|---|
| Behavioural biometrics | Continuously authenticates users through interaction patterns | Detecting account takeover after login |
| Graph / network analytics | Maps relationships among accounts, devices and beneficiaries | Mule-account and fraud-ring detection (e.g., RBI's MuleHunter.AI) |
| Reinforcement learning | Learns optimal routing strategies through continuous interaction with payment networks | Dynamic selection of payment processors |

*Source: Compiled from Afriyie et al. (2023); Preciado Martínez & Náñez Alonso (2025); Business Standard (2025); Keerthi (2025).*

## 4. AI and Economic Efficiency: Payment Routing Optimisation

### 4.1 From Static Rules to Intelligent Routing

Traditional payment routing is based on static rules and predetermined hierarchies, often described as the waterfall approach, in which a transaction is sent through a fixed sequence of processors or acquiring banks. Such systems frequently produce sub-optimal routing decisions, higher transaction costs and lower approval rates (ClearFunction, 2024). The stakes are high: one commercial estimate expects global payment transaction volume to reach $8.49 trillion by 2025 (Volante Technologies, 2024), and even milliseconds of delay or a fraction of a percentage point in fees can add up to millions of dollars for large merchants (Keerthi, 2025).

AI-powered routing engines examine past transaction data, network performance, cost structures and success probabilities to select the best path for each transaction. The techniques reported include machine-learning models that predict transaction success with 85–95 percent accuracy, neural networks that make routing decisions in under 50 milliseconds, reinforcement-learning methods such as Q-learning and policy-gradient algorithms, and ensemble methods such as random forests and gradient boosting (Keerthi, 2025).

### 4.2 Reported Benefits

Table 3 compares traditional and AI-powered routing on cost. Total transaction cost falls from a range of 2.35–3.65 percent to 1.68–2.48 percent, a reduction of about 28 percent, with penalty charges showing the largest relative fall. The same study reports that average processing time fell from 2.3 seconds to 1.4 seconds (39 percent faster), approval rates rose from 85.2 percent to 91.7 percent, retry success improved from 45 percent to 68 percent, and system uptime increased from 99.2 percent to 99.7 percent (Keerthi, 2025).

***Table 3: Cost Comparison between Traditional and AI-Powered Payment Routing***

| Cost Category | Traditional Routing | AI-Powered Routing | Improvement |
|---|---|---|---|
| Interchange fees | 1.8% – 2.5% | 1.4% – 1.9% | 22% reduction |
| Processing fees | $0.25 – $0.35 | $0.18 – $0.28 | 20% reduction |
| Penalty charges | 0.3% – 0.8% | 0.1% – 0.3% | 62% reduction |
| Total transaction cost | 2.35% – 3.65% | 1.68% – 2.48% | 28% reduction |

*Source: Keerthi (2025), based on industry reports and implementation data.*

Two reported case studies illustrate the scale of the gains. A large e-commerce platform processing 50 million transactions a month reported a 23 percent reduction in total payment-processing costs, an 18 percent improvement in approval rates, a 45 percent decrease in payment-related support tickets and annual savings of $15 million. A digital-wallet provider using AI routing for cross-border payments reported a 31 percent reduction in cross-border transaction costs, a 22 percent improvement in success rates and 60 percent faster settlement (Keerthi, 2025). On the investment side, an illustrative analysis shows an initial outlay of $550,000 against annual savings of $2,000,000, with a typical return-on-investment period of three to six months, and recommends a phased deployment of data analysis, model development, pilot and full rollout.

### 4.3 Significance for the Indian Economy

Beyond the firm level, AI-powered routing contributes to broader economic efficiency by reducing transaction costs across the economy, improving financial inclusion through higher approval rates, strengthening the reliability and resilience of payment systems and supporting the growth of digital commerce (Keerthi, 2025). It should be noted that the routing evidence comes largely from global industry sources and reported implementations rather than from Indian public data. Since UPI is a zero-cost model for users (Keerthi, 2024), the fee-related savings are likely to be most relevant for card, wallet and cross-border payments, whereas the gains in speed, approval rates and reliability are relevant to every payment rail.

## 5. AI and Trust: Security and Fraud Detection in Digital Payments

### 5.1 The Scale of the Fraud Challenge

Rapid expansion of digital payments has been accompanied by a rise in payment fraud, identity theft and cyber-enabled financial crime. Globally, 79 percent of companies reported attempted or actual payment fraud in 2024, compared with 65 percent two years earlier (U.S. Bank, 2026). In India, FICO's analysis estimated losses of about ₹11,000 crore to cyber scams in the first nine months of 2024 alone (FICO, 2024). Table 4 shows UPI fraud value over three fiscal years. Fraud as a share of transaction value remained small, at 0.4–0.5 percent, but the absolute rupee value grew substantially in line with transaction volume (PwC India, 2025).

***Table 4: UPI Fraud Value as a Share of Transaction Value in India***

| Fiscal Year | UPI Fraud Value (₹ crore) | Fraud as % of Transaction Value |
|---|---|---|
| 2022-23 | 573 | 0.4% |
| 2023-24 | 1,087 | 0.5% |
| 2024-25 (April–September, with full-year projection) | 485 (about 970 projected for full year) | 0.4% |

*Source: Adapted from PwC India (2025), based on RBI and NPCI data.*

Reported figures probably understate the problem. A 2025 LocalCircles survey of more than 32,000 UPI users across 365 districts found that one in five families with a UPI user had experienced fraud at least once in the preceding three years, and that

51 percent of victims did not report the incident to any authority (Business Standard, 2025). Under the RBI's banking fraud framework, digital-payment (card and internet) fraud cases fell from 29,082 in FY2023-24 to 13,516 in FY2024-25, and the value defrauded fell from ₹1,457 crore to ₹520 crore, although reclassification of earlier cases following a Supreme Court judgment has also affected overall reported totals (Medianama, 2025).

The threat itself is changing. Over 70 percent of phishing emails are now believed to contain AI elements, and fraudsters increasingly use generative AI to create convincing scam messages, synthetic identities and deepfakes (CoinLaw, 2026). In the Indian setting the main fraud types include fake VPA scams, QR-code manipulation, SIM-swap fraud, fake payment confirmations, social-engineering attacks and fake payment apps, which target users in tier-2 and tier-3 cities with limited digital literacy (Keerthi, 2024).

**5.2 Evidence on the Effectiveness of AI**

Rule-based systems built on static thresholds and manually set red flags cannot match the speed and complexity of modern digital transactions (Preciado Martínez & Náñez Alonso, 2025). AI-based systems, in contrast, learn from past transaction patterns, detect new fraud patterns and can flag anomalies before a transaction is approved (U.S. Bank, 2026). Comparative empirical studies consistently find ensemble methods, especially random forest, to be the most effective. Afriyie et al. (2023) reported 96 percent accuracy and an AUC of 98.9 percent for random forest on a credit-card dataset, while an analysis of more than 565,000 real-world bank transactions reported 95.79 percent accuracy for random forest on fraudulent cases (Preciado Martínez & Náñez Alonso, 2025). Industry-wide analysis suggests that AI-based tools can reach about 92 percent accuracy in production conditions (ZIGRAM, 2026). Together, these sources place accuracy in the range of 92 to 100 percent.

Beyond transaction-level classification, behavioural biometrics continuously validate users through typing rhythm, touchscreen pressure and device handling, helping to stop account takeover even when passwords and one-time passwords are compromised. NLP models scan messages and URLs to warn users of phishing, and graph-based models treat accounts, devices and beneficiaries as nodes to reveal coordinated mule-account networks that transaction-by-transaction screening would miss (Business Standard, 2025).

### 5.3 India's Multi-Layered AI Defence

Indian regulators and payment operators have built a multi-layered defence. NPCI has introduced a centralised fraud-monitoring solution for banks that uses AI/ML models to alert on and decline suspicious transactions, together with device binding, two-factor authentication and daily transaction limits (PIB, 2025b). The RBI's MuleHunter.AI, piloted in two public-sector banks in December 2024, uses AI to identify and block mule-account networks used to launder illegally acquired funds, and exclusive domains such as .bank.in and .fin.in are being introduced to curb phishing (Business Standard, 2025). The RBI has also proposed a Digital Payments Intelligence Platform for real-time analytics across banks, and by March 2025 the Central Payments Fraud Information Registry had been extended to 49 scheduled urban cooperative banks and hundreds of regional rural and district cooperative banks, moving the system from siloed institutional controls to system-wide fraud-intelligence sharing (Medianama, 2025).

### 5.4 Performance of Indian Banks and Fintech Platforms

Table 5 presents reported performance of AI-based fraud detection at five major banks. Reported detection accuracy ranges from 92.8 to 95.1 percent, with false-positive rates between 2.9 and 5.1 percent and processing times of 145–195 milliseconds. Fintech platforms report similar results, with AI accuracy of 94.2 percent for Paytm, 93.7 percent for PhonePe, 95.3 percent for Google Pay and 92.9 percent for Amazon Pay (Keerthi, 2024).

***Table 5: Reported AI Fraud-Detection Performance at Major Indian Banks***

| Bank | Daily Transaction Volume | Detection Accuracy | False Positive Rate | Processing Time |
|---|---|---|---|---|
| State Bank of India | 10 crore | 93.2% | 4.8% | 180 ms |
| HDFC Bank | 4.5 crore | 94.6% | 3.2% | 165 ms |
| ICICI Bank | 3.8 crore | 95.1% | 2.9% | 145 ms |
| Axis Bank | 2.2 crore | 92.8% | 5.1% | 195 ms |
| Kotak Mahindra Bank | 1.8 crore | 94.3% | 3.7% | 158 ms |

*Source: Keerthi (2024), compiled from secondary sources; figures are institution-reported and indicative.*

The same study reports that, across the Indian banking sector, total annual fraud losses fell from ₹8,234 crore before AI adoption (2020-21) to ₹2,647 crore after adoption (2023-24), a reduction of 67.8 percent; false-positive costs fell from ₹1,456 crore to ₹432 crore, and manual review costs from ₹876 crore to ₹298 crore. The economic picture is not one-sided, however: system infrastructure costs rose by 142.3 percent, from ₹234 crore to ₹567 crore (Keerthi, 2024). AI therefore reduces the cost of fraud but requires real investment in technology.

**5.5 UPI-Specific Fraud Types**

Table 6 compares AI and traditional detection rates for fraud types specific to UPI. AI-based systems outperform traditional methods across all six categories, with the largest relative gains in SIM-swap fraud (46.4 percent), fake app downloads (46.5 percent) and QR-code manipulation (42.7 percent).

***Table 6: Detection Effectiveness against UPI-Specific Fraud Types***

| Fraud Type | AI Detection Rate | Traditional Detection Rate | Relative Improvement |
|---|---|---|---|
| Fake VPA scams | 91.4% | 67.8% | 34.8% |
| QR code manipulation | 88.9% | 62.3% | 42.7% |
| SIM swap fraud | 86.2% | 58.9% | 46.4% |
| Fake payment confirmation | 93.7% | 71.2% | 31.6% |
| Social engineering | 89.3% | 64.5% | 38.4% |
| Fake app downloads | 87.6% | 59.8% | 46.5% |

*Source: Keerthi (2024).*

**5.6 The Inclusion Gap**

Protection is not evenly distributed. Table 7 shows that detection effectiveness is highest in urban areas and falls in semi-urban and rural areas in every region, with the lowest rural figure in Northeast

India (76.4 percent). Multilingual AI models are reported to improve fraud-detection performance by 23 percent in non-English-speaking regions (Keerthi, 2024). Since rural users, senior citizens and first-time smartphone users in smaller cities are the most vulnerable groups, this gap is an economic as well as a technical problem: unequal protection can slow the adoption of digital finance among precisely the populations that inclusion policy seeks to reach.

***Table 7: Regional AI Fraud-Detection Performance***

| Region | Urban Areas | Semi-Urban Areas | Rural Areas | Regional Average |
|---|---|---|---|---|
| North India | 94.8% | 89.2% | 82.6% | 88.9% |
| South India | 95.6% | 91.4% | 85.3% | 90.8% |
| West India | 95.2% | 90.8% | 84.1% | 90.0% |
| East India | 93.4% | 87.9% | 79.8% | 87.0% |
| Northeast India | 92.1% | 85.6% | 76.4% | 84.7% |

*Source: Keerthi (2024).*

## 6. Explainable AI and Accountable Digital Governance

### 6.1 Why Explainability Matters

As AI moves into decisions on welfare benefits, credit, court procedures and medical diagnosis, opaque “black-box” models create risks for democratic accountability, citizen confidence and fair outcomes. Explainable AI (XAI) is a set of processes and methods that allow human users to understand and trust the outputs of machine-learning algorithms, and it rests on three ideas: transparency, interpretability and explainability (Arrieta et al., 2020; Keerthi, n.d.). Technical tools include LIME, which explains individual predictions using simpler local models; SHAP, which uses game-theoretic Shapley values to measure feature importance; DeepLIFT, which traces the contribution of neurons in neural networks; inherently interpretable decision trees; and counterfactual explanations that show how a different input would change the outcome (Ribeiro et al., 2016; Lundberg & Lee, 2017).

### 6.2 Constitutional and Regulatory Basis

The constitutional values of justice, liberty, equality and fraternity require that technological systems used by the State be

understandable and answerable to citizens. Article 14, which guarantees equality before the law, implies that citizens should be able to know the basis on which the State takes decisions that affect them, and Article 21, widely interpreted by the Supreme Court to include the right to live with human dignity, could be undermined by opaque algorithms that control access to essential services (Keerthi, n.d.). The India AI Governance Guidelines place transparency and accountability among their core principles, but because the guidelines are voluntary, operationalising explainability for high-stakes government applications will need more specific technical standards (PIB, 2025a).

### 6.3 Sectoral Applications

In welfare distribution under the JAM (Jan Dhan–Aadhaar–Mobile) trinity, an explainable model can show why an applicant is eligible or ineligible, enable appeals and reduce exclusion errors. In the judiciary, where AI is being tested for case management and outcome prediction, XAI is essential. Multilingual explanation is possible through platforms such as BHASHINI (PIB, 2024). Table 8 links the Viksit Bharat @2047 development pillars to AI applications and the explainability each requires.

***Table 8: Viksit Bharat @2047 Development Pillars and XAI Applications***

| Development Pillar | 2047 Target | AI Application | XAI Requirement |
|---|---|---|---|
| Economic | GDP of USD 30–40 trillion | Credit scoring; investment analysis | Loan decision rationale |
| Social | Zero poverty | Welfare targeting; Direct Benefit Transfer | Eligibility explanations |
| Healthcare | Universal coverage | Diagnostic AI; resource allocation | Diagnosis justification |
| Education | Quality for all | Personalised learning (DIKSHA) | Learning-path rationale |

| Development Pillar | 2047 Target | AI Application | XAI Requirement |
|---|---|---|---|
| Environment | Net-zero by 2070 | Climate modelling; resource optimisation | Prediction transparency |
| Agriculture | Farmer uplift | Crop advisory; pest prediction | Advisory reasoning |

*Source: Adapted from NITI Aayog (2023); World Bank (2024), as compiled in Keerthi (n.d.).*

**7. AI-Driven Economic Transformation: An Integrated View**

The three strands of evidence discussed above can be read together as one economic story, in which each dimension supports the others.

**Efficiency.** AI lowers the cost and time of moving money, through smarter routing, higher approval rates and fewer failed or retried payments, and lowers the cost of fraud through fewer false positives and lower manual-review effort (Keerthi, 2024; Keerthi, 2025).

**Security and trust.** Digital payments only grow when users trust them. With 84 percent of retail payment transactions on UPI (Medianama, 2025), AI-based monitoring by NPCI, MuleHunter.AI and bank-level systems has become part of the basic infrastructure of the digital economy rather than an optional add-on.

**Inclusion.** AI can extend protection and services to new users through multilingual models, vernacular alerts and simplified interfaces. The regional gaps in Table 7 show, however, that inclusion has to be designed deliberately and cannot be assumed.

**Accountability.** XAI converts AI from a black box into a system whose decisions can be examined, appealed and audited. This is what allows AI to be used in welfare, justice and finance without weakening constitutional guarantees (Keerthi, n.d.).

Investment trends confirm that markets see this potential. Surveys show that 76 percent of businesses are increasing investment in AI, machine learning and analytics for fraud prevention (SEON, 2025), and market-research projections place the global fraud detection and prevention market at $32.00 billion in 2025 growing to $65.68 billion by 2030 at 15.5 percent annually (Markets and Markets, 2025), or from $35.3 billion in 2025 to $129.4 billion by 2033 at 18.1 percent annually (Grand View Research, 2026). Estimates differ with scope and method, but all point to double-digit growth.

## 8. Challenges

**Technical challenges.** Fraud is rare relative to legitimate activity: one study sample contained only 95 fraudulent transactions among 141,174, which makes class imbalance a persistent problem requiring resampling, cost-sensitive learning or synthetic data (Preciado Martínez & Náñez Alonso, 2025). Models trained on past data are reactive, and fraudsters adapt. Reported growth of AI-based social-engineering attacks has reached at least 61 percent over three years and deepfake fraud attempts are reported to be rising by 2,100 percent (CoinLaw, 2026), which forces institutions to retrain models more often. There is also a trade-off between accuracy and interpretability, since simpler, interpretable models are often outperformed by deep-learning models (Keerthi, n.d.), and routing decisions must be made within milliseconds at very high volume (Keerthi, 2025).

**Social challenges.** The digital divide between urban and rural populations can limit access to AI-based services for marginalised groups. Most victims of some UPI scams were deceived into authorising the fraud themselves, which transaction-level AI screening cannot stop (Business Standard, 2025), and 51 percent of victims do not report incidents. India's multilingual environment requires explanation and fraud-detection systems that work across more than 22 scheduled languages and many dialects (Keerthi, n.d.).

**Institutional and regulatory challenges.** Adoption is uneven: while 86 percent of surveyed companies allocate more than 3 percent of revenue to anti-fraud measures, real-time transaction monitoring had reached only 62 percent of organisations, and small and medium enterprises often lack the capital and technical capacity for sophisticated AI (SEON, 2025). Government departments face capacity constraints in technical expertise (Turing Institute, 2025), legacy systems are hard to integrate, dependence on third-party vendors creates lock-in risk, and privacy laws and competitive concerns restrict the data sharing on which graph-based detection depends. Over-reliance on automation can also produce false positives and spread biases from training data at scale if human oversight is weak.

**Quality of evidence.** Many of the performance figures cited in this paper are institution-reported or compiled from industry sources, and several come from global rather than Indian data. They should be read as indicative of direction and order of magnitude, and independent audit and published evaluation remain necessary.

## 9. Recommendations

Based on the evidence reviewed, the following measures are recommended for policymakers, regulators, financial institutions and educators:

1. **Adopt layered, hybrid detection.** Institutions should combine supervised classification, unsupervised anomaly detection and graph-based network analysis, because each technique has different strengths against different fraud types (Afriyie et al., 2023; Business Standard, 2025).
2. **Develop sector-specific XAI standards.** The India AI Governance Guidelines should be complemented by explainability standards for high-risk applications in welfare, justice, healthcare and finance.
3. **Build multilingual interfaces.** The BHASHINI platform should be used to provide explanations, alerts and fraud education in all major Indian languages and dialects.
4. **Institutionalise audit and citizen response.** The proposed AI Safety Institute should establish procedures for algorithmic audit and for citizens to question and appeal AI-assisted decisions.
5. **Enable privacy-preserving data sharing.** Mechanisms such as the Central Payments Fraud Information Registry, the proposed Digital Payments Intelligence Platform and federated learning should be strengthened so that institutions can share fraud intelligence without exposing sensitive data.
6. **Support smaller institutions and SMEs.** Affordable, shared and cloud-based AI fraud-detection services should be promoted so that smaller banks and businesses can access AI-grade protection without heavy upfront investment.
7. **Invest in consumer awareness and reporting.** Since social engineering continues to succeed, sustained education in local languages and simplified, widely publicised reporting channels are needed alongside technology, with special attention to rural users, senior citizens and first-time smartphone users.
8. **Build capacity and deploy in phases.** Government officials and institutional staff should be trained to understand and communicate AI decisions; AI systems such as routing engines should be introduced through phased deployment, from data analysis and model development to pilot and full rollout.

9. **Prioritise continuous retraining and research.** Detection models must be retrained and monitored continuously, and public–private research under the IndiaAI Mission should focus on defences against generative-AI-enabled attacks and on XAI methods suited to Indian governance contexts.

## 10. Conclusion

Digital India has given the country a public digital infrastructure of unusual scale, and AI is the layer that can turn this infrastructure into economic transformation. The evidence reviewed in this paper shows that AI can make payments cheaper and faster, make digital channels safer, extend protection to a diverse population and, with explainability, make automated decisions accountable to citizens.

The evidence also shows that AI is not a complete or self-sufficient solution. Class imbalance, adversarial adaptation by AI-literate fraudsters, uneven protection between urban and rural users, privacy constraints, unequal adoption across institutions and the opacity of complex models all limit what AI can achieve alone. AI-based security is best understood not as a fixed solution but as one component of a continuing contest between defensive and adversarial uses of the same technology.

For India to realise the promise of Viksit Bharat @2047, technological progress must therefore be matched by transparency, fairness and inclusion. A resilient digital economy will combine layered AI architectures, explainable models, privacy-preserving data sharing, support for smaller institutions, multilingual and rural outreach, and sustained public awareness. If these elements are put in place through the combined effort of government, academia, industry and civil society, AI can help India grow not only faster, but also more securely, more equitably and more democratically.

## References

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal, 6*, Article 100163.

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., … Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities, and

challenges toward responsible AI. *Information Fusion, 58*, 82–115.

Business Standard. (2025, June 26). *1 in 5 UPI users faced fraud; 51% victims didn't report, reveals survey*.

Business Today. (2024, June 1). *Digital payment frauds surge in India as UPI transactions skyrocket: RBI report.*

ClearFunction. (2024). *AI-powered payment routing: Optimizing transactions for speed and efficiency*. ClearFunction Insights.

CoinLaw. (2026). *Digital payment fraud statistics 2026: Alarming trends now.*

FICO. (2024). *India's digital scam epidemic: A threat to its financial resilience.*

Grand View Research. (2026). *Fraud detection and prevention market report, 2026–2033.*

Keerthi, Ch. (2024). Fraud detection and prevention in online payments: Analyzing the role of AI in identifying and mitigating fraudulent activities in digital transactions—An Indian perspective. *International Journal of Multidisciplinary Educational Research, 13*(9/1), 166–183.

Keerthi, Ch. (2025). AI-powered payment routing optimization: Exploring how AI can optimize payment routes to reduce transaction costs and enhance efficiency. *International Journal of Multidisciplinary Educational Research, 14*(3/1), 177–187.

Keerthi, Ch. (n.d.). *Explainable AI and India's Vision 2047: Building transparent decision-making systems for an equitable and sustainable republic* [Manuscript].

Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. *Advances in Neural Information Processing Systems, 30*.

MarketsandMarkets. (2025, July 28). *Fraud detection and prevention market worth $65.68 billion by 2030* [Press release].

Medianama. (2025, May 30). *UPI handles 84% of India's retail payment volume in FY25: RBI.*

Ministry of Electronics and Information Technology. (2024). *IndiaAI Mission*. Government of India.

Ministry of Electronics and Information Technology. (2025). *India AI governance guidelines*. Government of India.

NITI Aayog. (2023). *Viksit Bharat @2047: Vision document*. Government of India.

Preciado Martínez, P. M., & Náñez Alonso, S. L. (2025). Comparative analysis of machine learning models for the detection of

fraudulent banking transactions. *Cogent Business & Management, 12*(1), Article 2474209.

Press Information Bureau. (2024). *Year-end review 2024: Transforming India's digital landscape*. Ministry of Electronics and Information Technology, Government of India.

Press Information Bureau. (2025a). *Empowering governance through digital infrastructure*. Government of India.

Press Information Bureau. (2025b). *Digital payment transactions surge with over 18,000 crore transactions in 2024–25*. Government of India.

PwC India. (2025). *Combating payments fraud in India's digital payments landscape.*

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144).

SEON. (2025, March 5). *SEON 2025 digital fraud report reveals surge in fraud prevention budgets & headcounts* [Press release]. Business Wire.

The Alan Turing Institute. (2025). *AI governance around the world: Country profile—India.*

United Nations. (2024). *E-government survey 2024: Digital government in the decade of action for sustainable development*. United Nations Department of Economic and Social Affairs.

U.S. Bank. (2026). *How treasury departments use AI to detect and prevent fraud.*

Volante Technologies. (2024). *AI in payments: Balancing innovation with practicality in financial services.*

World Bank. (2024). *India development update: Towards a Viksit Bharat*. World Bank Group.

ZIGRAM. (2026). *Digital payment fraud statistics 2025*.