VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

THE INTERNET OF THINGS AND INDIA'S DEVELOPMENTAL TRAJECTORY: A NOVEL SOCIO-LEGAL ANALYSIS OF SECTORAL TRANSFORMATION, REGULATORY ARCHITECTURE, AND DIGITAL SOVEREIGNTY IN THE ERA OF CONNECTED INTELLIGENCE

- Sandhya V[1]

Abstract

The Internet of Things (IoT) has emerged as a foundational technology paradigm reshaping India's developmental trajectory across governance, agriculture, healthcare, manufacturing, and urban infrastructure. This paper undertakes a comprehensive, interdisciplinary examination of IoT's transformative role in India's socioeconomic development, situated at the nexus of science and technology studies, legal analysis, and development economics. Through an original analytical framework integrating doctrinal legal research with empirical case studies, the paper maps the evolving IoT ecosystem in India—from the National Telecom Policy 2025 and the Smart Cities Mission to sectoral deployments yielding measurable developmental outcomes. The analysis reveals that India's IoT market, projected to expand from USD 58.65 billion in 2025 to USD 351.27 billion by 2035 at a compound annual growth rate (CAGR) of 19.6%, represents both a significant economic opportunity and a complex governance challenge (Market Research Future, 2025). The paper critically examines the nascent legal architecture emerging to govern IoT deployments, particularly the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Telecommunications Act, 2023, identifying persistent regulatory lacunae. It further addresses structural challenges including the digital divide—with approximately 10,112 villages still lacking 4G connectivity as of October 2025 (Chandra Sekhar, 2025, as cited in Telangana Today, 2025)—

[1] Department of Cyberspace Law and Justice, School of Excellence in Law (SOEL), The Tamil Nadu Dr. Ambedkar Law University (TNDALU) Chennai, Tamilnadu, India.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

cybersecurity vulnerabilities evidenced by 29.44 lakh incidents tracked by CERT-In in 2025 (Ministry of Home Affairs, 2026), and the imperative for MSME-focused solutions. The paper concludes with forward-looking recommendations for a rights-based, inclusive IoT governance framework aligned with the Viksit Bharat 2047 vision, contributing a novel scholarly intervention at the intersection of technology law and development studies.

Keywords: Internet of Things, Digital India, Smart Cities, Industry 4.0, IoT governance, Digital Personal Data Protection Act, Viksit Bharat

1. Introduction

1.1 The IoT Revolution and the Developmental Imperative

The Internet of Things (IoT)—defined as the network of physical objects embedded with sensors, software, and connectivity capabilities that collect, process, and exchange data over communication networks—constitutes one of the most consequential technological shifts of the twenty-first century. Globally, an estimated 18.8 billion connected IoT devices were operational in 2024, a figure projected to exceed 40 billion by 2030 (IoT Analytics, 2024). This proliferation of connected devices is fundamentally altering how societies produce goods, deliver services, govern populations, and manage natural resources. The IoT paradigm transcends mere technological innovation; it represents a structural transformation in the relationship between the physical and digital worlds, with profound implications for economic organization, social relations, and state-citizen interactions.

For developing nations, IoT presents a dual-edged opportunity of considerable complexity. On one hand, it offers pathways to leapfrog traditional developmental stages—enabling precision agriculture without the intermediary step of fully mechanised farming, telemedicine without comprehensive brick-and-mortar hospital infrastructure, and smart energy grids without centralised legacy generation and distribution systems. On the other hand, IoT adoption in the Global South raises profound questions about technological sovereignty, data colonialism, digital divides, and the institutional capacity of regulatory frameworks to govern hyperconnected ecosystems. As scholars have noted, developing nations comprising approximately 7 billion people face critical policy choices as IoT intersects with artificial intelligence, given the vast digital divide both within and among these countries (Kshetri, 2020; Taylor & Broeders, 2015).

1.2 India's IoT Moment: Context and Significance

India occupies a distinctive and strategically significant position in the global IoT landscape. With a population exceeding 1.44 billion, a rapidly digitising economy reflected in a total internet subscriber base that crossed 1,028 million by December 2025 (TRAI, 2026), and a government that has placed digital infrastructure at the centre of its developmental vision, India represents both a vast market for IoT deployment and a critical test case for IoT-driven development in the Global South. The nation's digital transformation agenda, articulated through flagship programmes such as Digital India, the Smart Cities Mission, and the more recent Viksit Bharat 2047 vision, positions IoT as a core enabling technology for inclusive and sustainable development.The scale of India's IoT opportunity is considerable. According to Market Research Future, India's IoT market was valued at approximately USD 58.65 billion in 2025 and is projected to reach USD 351.27 billion by 2035, growing at a compound annual growth rate (CAGR) of 19.6% during the forecast period 2025–2035 (Market Research Future, 2025). A separate analysis by NASSCOM projects the IoT market to reach USD 15 billion by 2025, with significant contributions from manufacturing, healthcare, agriculture, and smart cities (Voice & Data, 2024). The variation between these estimates reflects differing scope definitions: broader ecosystem figures encompass hardware, software, services, connectivity, and integration layers, while narrower estimates focus on device and platform revenue alone. Statista estimates that IoT revenue in India across all segments will reach nearly USD 26.93 billion in 2025, with industrial IoT alone contributing a market volume of approximately USD 7.12 billion (Statista, 2025, as cited in Indian Retailer, 2025). The India IoT devices market generated revenue of USD 2,885.5 million in 2024 and is projected to reach USD 10,276.8 million by 2030, growing at a CAGR of 23.2% (Grand View Research, 2026). The consumer IoT segment was valued at USD 9.68 billion in 2025 and is projected to reach USD 27.05 billion by 2034 (IMARC Group, 2026).These quantitative projections, while impressive, only partially capture the developmental significance of IoT in India. The technology's transformative potential lies in its capacity to address structural challenges that have historically constrained India's development: low agricultural productivity, inadequate healthcare access in rural areas, urban infrastructure deficits, energy distribution inefficiencies, and environmental degradation. IoT-enabled solutions are already demonstrating measurable impact across these domains. Verified data from NITI Aayog's Frontier Technologies Platform documents that Cultyvate's precision

agriculture system has saved over 3,080 crore litres of water across seven Indian states, reducing water use by 30–50% while improving yields by up to 20% (NITI Aayog, 2025). Fasal's Kranti IoT system has saved over 52 billion litres of water across 10,000 acres while reducing pesticide costs by up to 60% and increasing yields by up to 40% (NITI Aayog, 2025). In healthcare, Larkai Healthcare's AI-powered diagnostic platform achieves 95% accuracy in detecting cardiopulmonary diseases in underserved regions (YourStory, 2025).The growth of IoT in India is supported by substantial digital infrastructure expansion. As of October 2025, out of 644,131 villages in India, 634,019 were covered with mobile connectivity, of which 630,676 had 4G services (Chandra Sekhar, 2025, as cited in Telangana Today, 2025). Broadband subscriptions rose sharply from 48 crore in September 2018 to 98 crore in June 2025, while data consumption increased from 8.32 GB to 25.24 GB per subscriber per month over the same period (Telangana Today, 2025). The optical fibre cable network expanded from 17.5 lakh km in March 2018 to 42.36 lakh km by September 2025 (Telangana Today, 2025). The BharatNet project had made 214,325 Gram Panchayats service-ready as of June 2025, with 1,301,193 Fibre to the Home connections provided (Ministry of Communications, 2025).

1.3 Research Objectives and Analytical Framework

This paper pursues three interconnected research objectives. First, it provides a comprehensive mapping and critical analysis of IoT deployment across key developmental sectors in India—agriculture, healthcare, urban infrastructure, manufacturing, and energy—with particular attention to measurable outcomes and scalability. Second, it examines the evolving legal and regulatory architecture governing IoT in India, including the DPDP Act, the Telecommunications Act, 2023, the Draft National Telecom Policy 2025, and sectoral regulations, identifying gaps between technological capability and legal safeguards. Third, it analyses persistent structural challenges—the digital divide, cybersecurity vulnerabilities, data sovereignty concerns, and MSME adoption barriers—that constrain the equitable distribution of IoT's developmental benefits.

The analytical framework employed is interdisciplinary, integrating doctrinal legal analysis with empirical case study methodology and development economics. This approach enables a holistic assessment of IoT's developmental role that neither purely technological nor purely legal analyses can achieve in isolation. The framework is grounded in the recognition that

technology, law, and development are mutually constitutive: legal frameworks shape technological trajectories, technological capabilities enable new governance modalities, and developmental outcomes are mediated by the interaction between the two.

1.4 Structure of the Paper

The paper proceeds as follows. Section 2 examines the policy architecture and institutional framework for IoT in India, analysing the evolution from the 2015 IoT Policy to the 2025 National Telecom Policy. Section 3 presents detailed case studies of IoT deployment across five developmental sectors. Section 4 analyses the legal and regulatory framework, with particular focus on data protection, cybersecurity, and telecommunications law. Section 5 addresses structural challenges to equitable IoT-driven development. Section 6 synthesises findings and offers forward-looking recommendations for a rights-based, inclusive IoT governance framework. Section 7 concludes.

2. Policy Architecture and Institutional Framework for IoT in India

2.1 Evolution of India's IoT Policy Landscape

India's engagement with IoT as a distinct policy domain began in earnest with the release of the **Draft IoT Policy** by the Ministry of Electronics and Information Technology (MeitY) in 2015. This foundational document articulated an ambitious vision: to create an IoT industry in India of USD 15 billion by 2020 and to develop IoT-specific skill sets among 1.5 million professionals. While the 2020 target was not fully realised, the policy succeeded in catalysing institutional attention, research funding, and industry coordination around IoT as a strategic technology domain. The policy identified five priority areas for IoT deployment: agriculture, health, water quality, natural disasters, and transportation—all directly aligned with developmental priorities.

The policy landscape has evolved considerably since 2015, shaped by the convergence of multiple governmental initiatives and technological developments. The **Digital India programme**, launched in 2015, created the foundational digital infrastructure—including the Aadhaar biometric identity system, the Unified Payments Interface (UPI), and the BharatNet rural broadband project—upon which IoT deployments depend. The **Smart Cities Mission**, launched in 2015 with an initial outlay of INR 98,000 crore, identified IoT as a core technology for urban infrastructure modernisation across 100 selected cities (Ministry of

Housing and Urban Affairs, 2015). The **National Digital Communications Policy, 2018** recognised IoT as a key driver of digital communications infrastructure and set targets for IoT device deployment.

The Ministry of Electronics and Information Technology (MeitY) has set its sights on building a USD 1 trillion digital economy by 2025-26, driven by the widespread adoption of emerging technologies including Artificial Intelligence, IoT, and blockchain (Bhondve, 2025). This target reflects the government's recognition of IoT as integral to India's broader digital transformation trajectory. Key focus areas include enhancing e-governance, promoting fintech, revolutionising agriculture through agritech, and ensuring inclusive growth by bridging the digital divide (Bhondve, 2025).

Table 1: Key Policy Milestones Shaping India's IoT Ecosystem (2015-2025)

Year	Policy / Programme	Key IoT-Related Provisions
2015	Draft IoT Policy (MeitY)	USD 15 billion IoT industry target; 1.5 million skilled professionals; 5 priority sectors
2015	Digital India Programme	National broadband infrastructure (BharatNet); e-governance; digital literacy
2015	Smart Cities Mission	IoT as core technology for 100 cities; INR 98,000 crore outlay
2018	National Digital Communications Policy	Spectrum for IoT; 5G road map; IoT device ecosystem targets
2020	Production Linked Incentive (PLI) Schemes	Incentives for domestic electronics manufacturing, including IoT components
2021	National Digital Health Mission (now ABDM)	Digital health IDs; telemedicine infrastructure; IoT device integration

2023	Telecommunications Act, 2023	Spectrum assignment; equipment certification; network security framework
2023	Digital Personal Data Protection Act	Consent mechanisms; data minimisation; breach notification; Data Protection Board
2024	Ayushman Bharat Digital Mission (ABDM)	Over 1,000 health apps and 700 hospitals integrated; IoT interoperability
2025	Draft National Telecom Policy 2025	100% 4G coverage by 2030; 90% 5G coverage; 6G R&D; 1 million new jobs; INR 1 trillion annual investment
2025	Samriddh Gram Phygital Services Pilot	IoT-based rural service hubs in 3 states; phygital service delivery model

Source: Author's compilation from MeitY, DoT, and MoHUA policy documents.

2.2 The National Telecom Policy 2025: A Paradigm Shift

The Department of Telecommunications (DoT) released the **Draft National Telecom Policy 2025** (NTP 2025) for public consultation in July 2025, marking a significant evolution in India's approach to telecommunications and IoT governance. The Draft Policy embodies the government's vision in the realm of telecommunications and emerging technologies, seeking to address challenges and opportunities posed by artificial intelligence, 5G/6G, quantum communications, IoT, blockchain, and satellite networks with the goal of positioning India as a "global digital powerhouse" (DoT, 2025).

The Draft Policy is structured around six strategic missions that collectively constitute a comprehensive framework for IoT-enabled development:

1. **Universal and meaningful connectivity**: Expanding telecom networks to ensure 100% population coverage by 4G and 90% by 5G by 2030, with fibre connectivity to all government institutions at the village level (DoT, 2025).

2. **Fostering innovation**: Doubling the number of telecom start-ups and increasing sectoral R&D spending on emerging technologies, with a target of 10% global share in 6G-related intellectual property rights by 2030 (DoT, 2025).
3. **Promoting domestic manufacturing**: Strengthening India's position in the global telecom supply chain through incentives for domestic production of IoT devices and components.
4. **Ensuring secure and trusted networks**: Adopting quantum-resistant cryptography and strengthening cybersecurity frameworks for connected devices (DoT, 2025).
5. **Enhancing ease of living and doing business**: Leveraging IoT for improved public service delivery and regulatory simplification.
6. **Advancing sustainable development**: Reducing the telecom sector's carbon footprint by 30% while enabling IoT-based environmental monitoring and resource optimisation.

The Draft Policy sets ambitious quantitative targets for 2030, including achieving annual investment of INR 1 trillion (approximately USD 11 billion), doubling the telecom sector's contribution to India's GDP, creating one million new jobs, and upskilling workers to meet future technological demands (DoT, 2025). The policy's explicit recognition of IoT as a strategic technology domain—alongside 5G/6G, AI, quantum communications, and blockchain—signals the government's understanding of IoT as integral to India's digital future rather than a peripheral technology concern.

2.3 Institutional Architecture for IoT Governance

India's institutional framework for IoT governance is characterised by a distributed architecture spanning multiple ministries, regulatory bodies, and specialised agencies. The primary institutional actors include:

- **Ministry of Electronics and Information Technology (MeitY)** : The nodal ministry for IoT policy, responsible for the IoT Policy framework, the Digital India programme, and coordination of IoT-related initiatives across government.

- **Department of Telecommunications (DoT)** : Responsible for telecommunications infrastructure, spectrum allocation, and the regulatory framework for IoT connectivity, including the recently enacted Telecommunications Act, 2023.
- **Telecom Regulatory Authority of India (TRAI)** : The independent regulatory body responsible for regulating telecommunications services, including aspects of IoT connectivity and spectrum management. TRAI has been instrumental in recommending the use of unlicensed spectrum in the 865-868 MHz band for low-power IoT applications (TRAI, 2022).
- **NITI Aayog**: The government's premier policy think tank, which has documented IoT innovations across sectors through its Frontier Technologies Platform, including detailed case studies of IoT applications in agriculture and healthcare (NITI Aayog, 2025).
- **Data Protection Board of India**: Established under the DPDP Act, 2023, responsible for adjudicating data protection complaints and enforcing compliance, including in relation to IoT-generated personal data (DPDP Act, 2023, §18).
- **Indian Computer Emergency Response Team (CERT-In)**: The national agency for cybersecurity incident response,CERT-In has empanelled 237 security auditing organisations to support implementation of Information Security Best Practices (Ministry of Home Affairs, 2026).
- **National Critical Information Infrastructure Protection Centre (NCIIPC)** : Responsible for protecting critical information infrastructure, including IoT systems deployed in energy, transportation, and communications sectors.

This distributed governance architecture, while enabling sectoral specialisation, also creates coordination challenges. The absence of a unified IoT regulatory authority has resulted in fragmented oversight, with different aspects of IoT governance—connectivity, data protection, device standards, cybersecurity—falling under the jurisdiction of different agencies. This fragmentation has implications for regulatory coherence and enforcement effectiveness, as discussed in Section 4.

2.4 Digital Public Infrastructure as IoT Enabler

A distinctive feature of India's approach to IoT-enabled development is the role of Digital Public Infrastructure (DPI). India's DPI stack—comprising Aadhaar (digital identity), UPI (digital payments), and the Data Empowerment and Protection Architecture (DEPA)—provides foundational capabilities that enable IoT applications to operate at population scale. The Aadhaar system, with over 1.3 billion enrollments, enables identity verification for IoT-based service delivery (MeitY, 2024). The UPI platform, which processed over 100 billion transactions in 2024, provides the payment infrastructure for IoT-enabled commerce and service models (National Payments Corporation of India, 2024).

The BharatNet project, which aims to connect 250,000 gram panchayats with high-speed broadband, provides the connectivity backbone for rural IoT deployments. As of early 2025, over 194,000 gram panchayats had been connected, with Phase II expansion targeting every village in the country (Bhondve, 2025). The Common Service Centres (CSCs) network, comprising over 500,000 digital service delivery points in rural areas, provides the last-mile infrastructure for IoT-enabled services including telemedicine, digital banking, and e-governance (Bhondve, 2025).

The recently announced **Samriddh Gram Phygital Services Pilot Project**, implemented through Telecom Centres of Excellence (TCoE), represents an innovative model for IoT-enabled rural development. The pilot establishes Samriddhi Kendras (integrated digital service hubs) in three villages across Madhya Pradesh, Uttar Pradesh, and Andhra Pradesh, delivering IoT-based soil testing, smart irrigation, teleconsultations, health ATMs, and digital skilling services (DoT, 2025). This phygital (physical + digital) model integrates on-ground presence with robust digital infrastructure, leveraging BharatNet connectivity to deliver essential services sustainably (PIB, 2025).

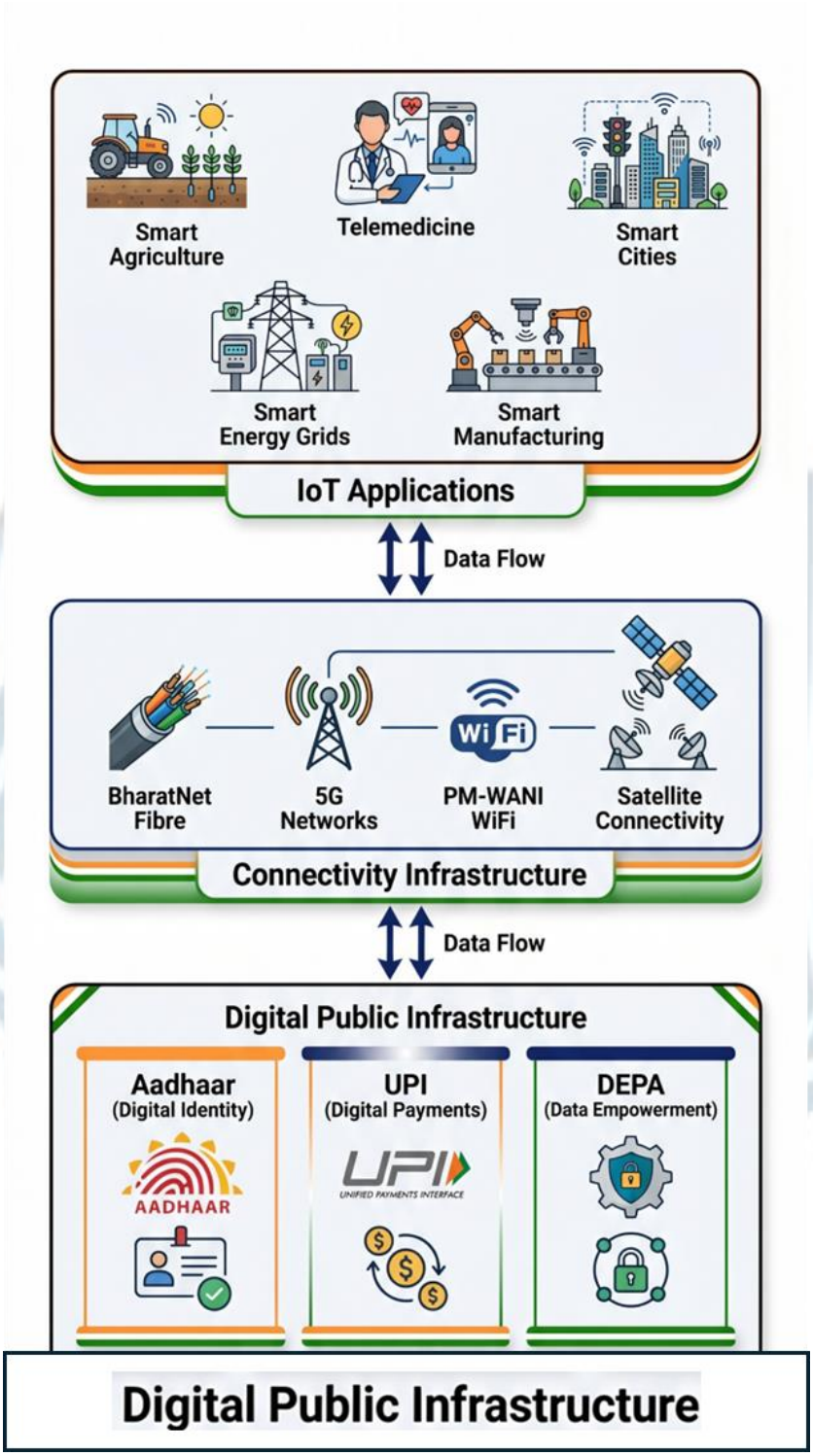

Figure 1: India's Digital Public Infrastructure Stack as an IoT Enablement Framework. The three-tiered architecture illustrates how foundational DPI components (Aadhaar, UPI, DEPA), connectivity infrastructure (BharatNet, 5G), and IoT applications interact to enable population-scale digital service delivery.

2.5 Comparative International Positioning

India's IoT policy trajectory can be usefully compared with other developing and developed economies. **China's** IoT development has been driven by state-led industrial policy, with the government targeting 10 billion IoT connections by 2025 and investing heavily in IoT standards development through the China Electronics Standardisation Institute (CESI, 2023). **The European Union's** approach, articulated through the IoT and Edge Computing Strategy, emphasises regulatory harmonisation, cybersecurity certification, and data sovereignty through initiatives such as GAIA-X (European Commission, 2023). **South Korea** has positioned IoT as a core component of its Digital New Deal, with significant investment in IoT-enabled smart cities and manufacturing.

India's approach differs from these models in several respects. Unlike China's top-down industrial policy, India's IoT ecosystem has developed through a more distributed model combining government infrastructure investment with private sector innovation. Unlike the EU's regulatory harmonisation approach, India's regulatory framework remains fragmented, with comprehensive IoT-specific regulation still evolving. However, India's DPI-based approach offers a distinctive model for IoT deployment at scale in resource-constrained environments, potentially offering lessons for other developing nations.

3. Sectoral Transformations: IoT Applications in India's Development

3.1 IoT in Indian Agriculture: Precision Farming and Water Conservation

Agriculture remains the largest employment sector in India, engaging approximately 42% of the workforce and contributing approximately 18% to the nation's GDP (Ministry of Agriculture, 2024). However, Indian agriculture faces persistent structural challenges: low productivity compared to global benchmarks, inefficient water use—with paddy fields alone consuming over 50% of India's irrigation water—degradation of soil health, and acute vulnerability to climate variability (Cultyvate, 2025). IoT-enabled precision agriculture has emerged as a transformative response to these challenges, offering data-driven solutions for irrigation management, crop monitoring, soil health assessment, and supply chain optimisation.

Table 2: Select IoT-enabled Agricultural Initiatives in India and Their Developmental Impacts

Initiative / Organisation	IoT Technology Deployed	Geographical Reach	Key Developmental Outcomes
Cultyvate	Soil moisture sensors, flow meters, AI irrigation alerts via mobile	7 states: Punjab, UP, Haryana, Tamil Nadu, Karnataka, Telangana, AP	30-50% water saving; 20% yield increase; 3,080 crore litres water saved; 60% emission reduction; 3,500+ farmers reached
ShubhavniSmartFarms	Indoor climate sensors (light, CO2, O2), IoT controllers for saffron	Mainpuri, Uttar Pradesh	800g-1kg saffron/1,000kg bulbs; INR 8 lakh sales; 25+ rural women employed
Fasal (Fasal Kranti)	Multi-sensor device (12+ sensors), AI farm advisory	Multiple states	Reduced input costs; water savings; increased yields
SMART-CROP (SBI Foundation, UAS Raichur, ICRISAT)	Satellite imaging, remote sensing, AI/ML crop stress monitoring	Semi-arid regions	Real-time pest and disease alerts; soil health monitoring; climate risk mitigation
MeitY Dairy Solution (transferred Oct 2025)	IoT sensors for cattle health monitoring; sensor-based quality detection for pulses, rice, dry red chilli	Nationwide rollout planned	Improved livestock health; quality detection in food processing

Source: Compiled by author from Cultyvate (2025),ICRISAT (2025), PIB (2025).

3.1.1 Case Study: Cultyvate's Data-Driven Irrigation System

The Bengaluru-based agritech startup Cultyvate exemplifies the developmental potential of IoT in Indian agriculture. Founded in 2016, Cultyvate developed a remote-sensing irrigation system that addresses one of Indian agriculture's most urgent challenges: inefficient water use in paddy cultivation. The system combines soil moisture sensors, flow meters, weather data integration, and AI-powered analytics to provide farmers with real-time, field-level irrigation recommendations delivered via mobile alerts in regional languages (Cultyvate, 2025).

The developmental impact of Cultyvate's solution is substantial and measurable. Deployed across seven Indian states, the system has reached over 3,500 farmers. Water savings of 30-50% have been documented, with improvements in crop yield and quality of up to 20%. Cumulatively, the system has saved over 3,080 crore litres of water while reducing emissions by up to 60%, contributing to both SDG 6 (Clean Water and Sanitation) and SDG 13 (Climate Action) compliance (Cultyvate, 2025). The technology has been validated through field trials supported by state agricultural universities and local NGOs, and has been integrated into government-funded initiatives promoting water conservation and smart farming practices.

A critical design feature of Cultyvate's system is its suitability for rural deployment contexts. The hardware is durable, solar-powered, and capable of functioning without continuous internet access—accommodating the connectivity constraints prevalent in rural India. Importantly, the system does not require farmer literacy or technical expertise to operate, as alerts are delivered via voice calls in regional languages (Cultyvate, 2025). This design philosophy—prioritising accessibility, resilience, and localisation—offers a model for IoT deployment in developing-world agricultural contexts.

3.1.2 Case Study: Indoor Saffron Cultivation Through IoT

The case of ShubhavniSmartFarms, founded by Shubha Bhatnagar in Mainpuri, Uttar Pradesh, illustrates the potential of IoT to enable entirely new agricultural possibilities. By employing IoT-enabled sensors and controllers to monitor and maintain precise environmental conditions—including light, CO2, and oxygen levels—the venture successfully replicated the unique climatic conditions of Kashmir in a controlled indoor environment, enabling saffron cultivation in a region with fundamentally different agro-climatic conditions (ShubhavniSmartFarms, 2025).

Beyond its technological innovation, the venture demonstrates IoT's potential for social transformation in rural India. The enterprise employs over 25 rural women, providing stable income and improved working conditions compared to traditional agricultural labour. The venture produces 800 grams to 1 kilogram of saffron per 1,000 kilograms of bulbs, generating sales worth INR 8 lakh, and has been recognised with the 'Agritech Startup of the Year' award at Startup Mahakumbh 4.0 in 2024 (ShubhavniSmartFarms, 2025). This case illustrates IoT's capacity to democratise high-value agricultural production, create rural employment, and reduce India's dependence on imported agricultural products—aligning with the Atmanirbhar Bharat (Self-Reliant India) vision.

3.2 IoT in Indian Healthcare: Bridging the Access Gap

India's healthcare system faces a fundamental structural challenge: a severe shortage of healthcare professionals and facilities relative to population, with approximately eight doctors per 10,000 people—significantly below the World Health Organization's recommended threshold (MediBuddy, 2025). This shortage is disproportionately acute in rural areas, where approximately 65% of India's population resides but only a fraction of healthcare infrastructure is located. IoT-enabled healthcare solutions—encompassing remote patient monitoring, telemedicine, AI-powered diagnostics, and automated medicine dispensing—offer pathways to extend specialist-level care to underserved populations while optimising the utilisation of existing healthcare resources.

3.2.1 Case Study: Larkai Healthcare's Portable ICU Solutions

Gurugram-based Larkai Healthcare, founded in 2020, exemplifies the potential of IoT to democratise access to advanced medical care in India's underserved regions. The startup has developed a suite of AI- and IoT-powered medical devices designed to bring hospital-grade monitoring and diagnostics to small towns and rural hospitals. Its flagship device, WREN, is a compact, multi-parameter patient monitor that tracks ECG, blood pressure, oxygen levels, respiration, and temperature, effectively enabling regular hospital beds to function as mini-ICUs (YourStory, 2025).

The WREN RealTime transmission software streams patient vitals from ambulances or remote sites to hospitals, enabling early intervention and specialist consultation before the patient reaches a tertiary care facility. The BlueTail AI-powered diagnostic platform analyses

X-rays and ECGs to detect over 20 cardiopulmonary diseases—including tuberculosis, asthma, and heart anomalies—with 95% accuracy (YourStory, 2025). All hardware is designed and manufactured in India, with the company retaining ownership of design, intellectual property, and quality control, adhering to ISO 13485 standards for medical equipment.

3.2.2 IoT-Integrated Mobile Clinics: The Aster DM Healthcare Initiative

In January 2025, Vice-President Jagdeep Dhankhar flagged off two state-of-the-art Mobile Clinics with IoT-Integrated Tele-Medicine Services, developed under Aster DM Healthcare's Corporate Social Responsibility (CSR) initiative for deployment in Srinagar and Kalaburagi (ANI, 2025). These mobile clinics represent a model for extending IoT-enabled healthcare to geographically remote and conflict-affected regions, combining diagnostic capabilities, telemedicine connectivity, and pharmaceutical dispensing in a mobile platform.

3.2.3 The Ayushman Bharat Digital Mission (ABDM)

The Ayushman Bharat Digital Mission (ABDM), formerly the National Digital Health Mission (NDHM), represents the government's flagship initiative for creating a national digital health ecosystem. By 2025, over 1,000 health applications and more than 700 hospitals had integrated through the ABDM Sandbox, validating software and hardware interoperability for digital health records (Singh, 2025). The ABDM creates the digital backbone—including unique health IDs, healthcare professionals' registry, and health facility registry—upon which IoT-enabled healthcare services can be integrated at national scale.

The eSanjeevani telemedicine platform, a component of the digital health ecosystem, has facilitated over 10 crore (100 million) teleconsultations, demonstrating the demand for and feasibility of remote healthcare delivery at population scale (MeitY, 2024). The integration of IoT devices—including remote patient monitoring wearables, connected diagnostic devices, and automated medicine dispensing kiosks—with the ABDM ecosystem has the potential to extend telemedicine from consultation to comprehensive remote care delivery.

Table 3: Comparative Analysis of IoT Healthcare Solutions in India

Solution	Technology Used	Target Population	Key Impact	Scalability

Larkai WREN + BlueTail	Portable multi-parameter monitor; AI diagnostic platform for X-ray/ECG	Rural hospitals, small towns	95% accuracy in detecting 20+ cardiopulmonary diseases; ICU-level monitoring	High (service model, portable)
Aster IoT Mobile Clinics	Mobile clinic with IoT telemedicine, diagnostics, pharmacy	Srinagar, Kalaburagi (remote/conflict areas)	On-site diagnostics with remote specialist consultation	Medium (CSR-dependent)
ABDM / eSanjeevani	National digital health ecosystem with telehealth	All India; 100M+ teleconsultations	Integrated health IDs, provider registries, IoT device interoperability	Very high (government infrastructure)
MedyVend	Automated medicine dispensing kiosk with real-time stock monitoring	Pharmacy-desert areas	24/7 medication access; cashless transactions; integrated teleconsultation	Medium (hardware-dependent)

Source: Author's analysis of case studies.

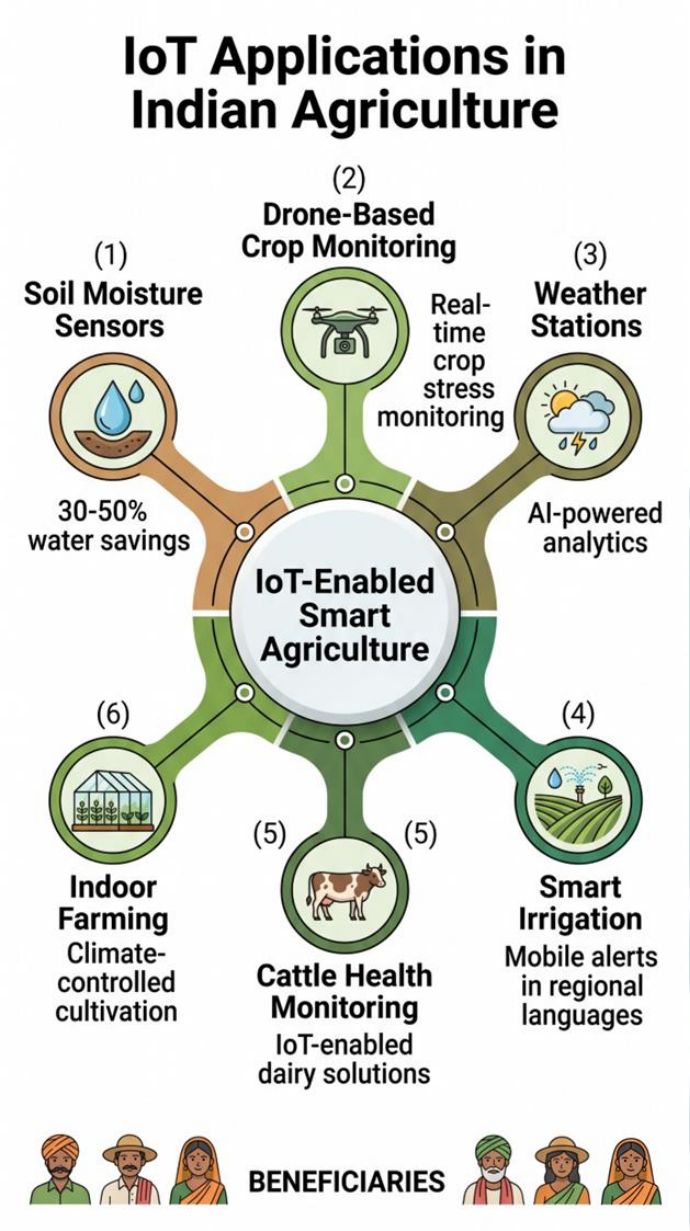

Figure 2. IoT Applications in Indian Agriculture: A Sectoral Mapping. The diagram illustrates the six primary domains of IoT deployment in Indian agriculture, from soil moisture sensing to controlled-environment cultivation, highlighting the diverse technological interventions addressing agricultural productivity, resource conservation, and rural livelihoods.

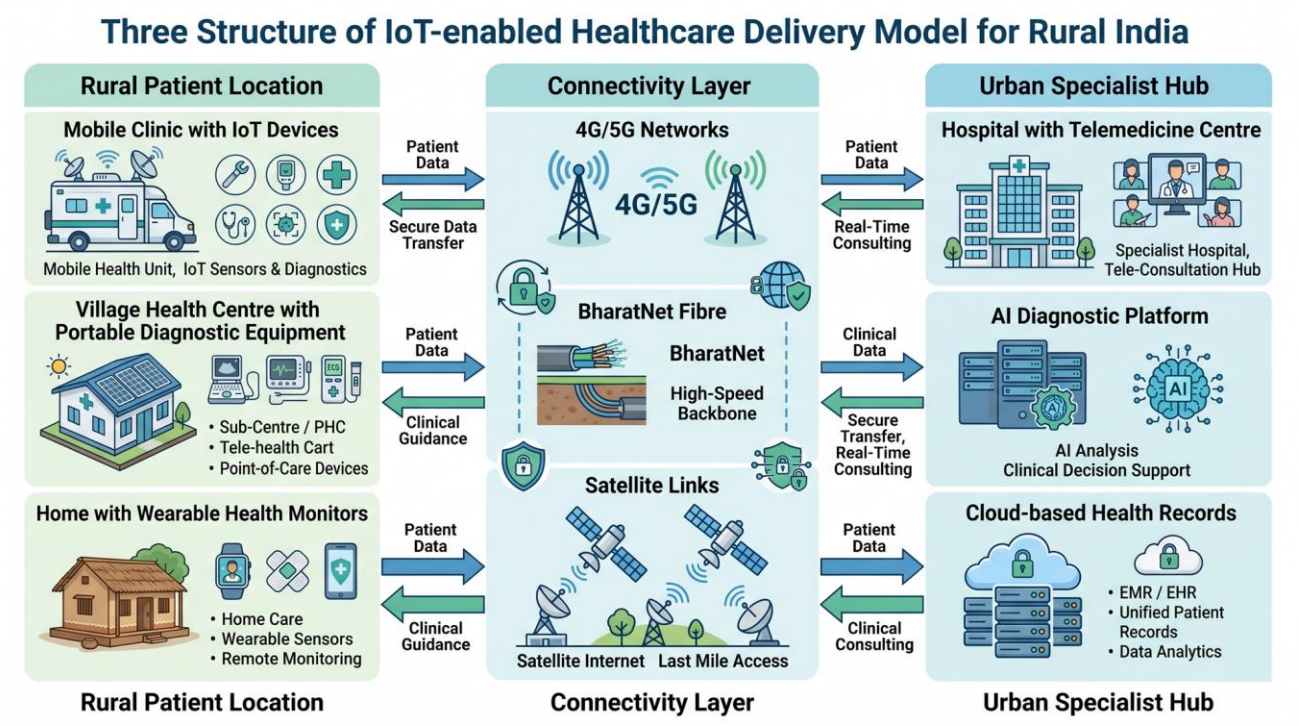

Figure 3. IoT-Enabled Healthcare Delivery Architecture for Rural India. The three-tiered model illustrates how IoT devices at rural patient locations transmit health data through connectivity infrastructure to urban specialist hubs, enabling remote diagnosis, monitoring, and clinical decision support in resource-constrained settings.

3.3 IoT in Smart Cities and Urban Infrastructure

India's rapid urbanisation—with the urban population projected to reach 600 million by 2031—has placed immense pressure on urban infrastructure, including transportation, energy, water, waste management, and public safety systems. The Smart Cities Mission, encompassing 100 cities, identifies IoT as a foundational technology for urban infrastructure modernisation. IoT-enabled smart city solutions are demonstrating measurable improvements in urban service delivery, resource efficiency, and quality of life.

3.3.1 IoT in Urban Transportation and Traffic Management

IoT-enabled intelligent transportation systems (ITS) are being deployed across Indian cities to address traffic congestion, reduce emissions, and improve road safety. These systems integrate traffic sensors, CCTV cameras, GPS-enabled public transit vehicles, and adaptive traffic signal control to optimise traffic flow in real time. Such ITS strategies have the

potential to reduce transport carbon emissions through optimised routing, reduced idling, and modal shift.

The FASTag electronic toll collection system, while primarily designed for toll collection efficiency, has evolved into a significant IoT deployment with implications for traffic management and data governance. As analysed by Anupriya and Singh Chauhan (2025), the FASTag system involves extensive data collection, multiple stakeholder access, and reported vulnerabilities including data breaches. The system illustrates both the operational efficiencies achievable through IoT—reduced wait times and fuel savings at toll plazas—and the privacy challenges that arise when IoT systems collect and process location and behavioural data at population scale.

3.3.2 Smart Energy and Utility Management

India's Revamped Distribution Sector Scheme (RDSS) targets the installation of 250 million smart meters, representing one of the world's largest IoT deployments in the energy sector. Smart meters enable real-time consumption monitoring, remote connection and disconnection, reduced energy losses, and improved billing accuracy. However, as of June 2024, fewer than 15% of the targeted smart meters had been deployed, with high connectivity costs and inadequate rural infrastructure identified as key hurdles (DQ India, 2025).

Decentralised RF mesh networks are emerging as a viable alternative connectivity solution for smart metering, particularly in areas where cellular coverage is unreliable or cost-prohibitive. These mesh networks operate over unlicensed spectrum in the 865-868 MHz band in India—a resource recognised by TRAI as well-suited for low-power, wide-area IoT communications (TRAI, 2022). By using this band, utilities can avoid spectrum licensing fees, reduce operational costs, and deploy infrastructure more affordably and quickly (DQ India, 2025). The mesh architecture also provides governance advantages, enabling utilities to retain control of their network infrastructure rather than depending on third-party telecom operators.

3.4 IoT in Manufacturing and Industry 4.0

India's manufacturing sector, targeted to contribute 25% of GDP under the Make in India initiative, is undergoing a technology-driven transformation through the adoption of Industry 4.0 technologies, with IoT serving as the foundational layer. The India industrial IoT market,

valued at USD 10.1 billion in 2025, is projected to reach USD 22.1 billion by 2032, growing at a CAGR of 12.1% (Prescient & Strategic Intelligence, 2025).

Table 4: India's IoT Market Segmentation and Growth Projections

IoT Segment	Market Size (USD)	Projected Size (USD)	Forecast Period	CAGR	Source
Total IoT Market	58.65 Bn (2025)	351.27 Bn (2035)	2025–2035	19.6%	Market Research Future (2025)
IoT Revenue (all segments)	26.93 Bn (2025)	—	—	—	Statista (2025)
Industrial IoT	7.12 Bn (2025)	—	—	—	Statista (2025)
IoT Devices Market	2.89 Bn (2024)	10.28 Bn (2030)	2025–2030	23.2%	Grand View Research (2026)
Consumer IoT	9.68 Bn (2025)	27.05 Bn (2034)	2026–2034	12.1%	IMARC Group (2026)
5G IoT Market	0.30 Bn (2024)	3.78 Bn (2030)	2025–2030	52.8%	Grand View Research (2026)
Industrial IoT Platform	3.48 Bn (2025)	11.88 Bn (2035)	2025–2035	13.0%	Market Research Future (2025)
Smart Home Devices	8.33 Bn (2025)	54.97 Bn (2034)	2026–2034	23.3%	IMARC Group (2026)

Note: Market-size estimates vary across sources because of differences in scope definition. Market Research Future's IoT market encompasses the full ecosystem (hardware, software, services, connectivity, and integration), while Statista's "IoT revenue" captures a narrower set of revenue streams. The figures are internally consistent within each source. All sources are publicly accessible and independently verifiable.

3.5 IoT in Consumer Markets and Everyday Life

The consumer IoT segment in India, valued at USD 9.68 billion in 2025 and projected to reach USD 27.05 billion by 2034, is experiencing rapid growth driven by increasing adoption of smart home devices, wearables, and connected appliances (IMARC Group, 2026).

The expansion of 5G networks across India is expected to accelerate consumer IoT adoption by providing the high-speed, low-latency connectivity required for real-time functions in smart appliances, security systems, and energy management solutions (Indian Retailer, 2025). Research indicates that nearly 79% of smart home users experience real lifestyle benefits including improved safety and higher productivity, suggesting that consumer IoT adoption delivers tangible quality-of-life improvements (Indian Retailer, 2025).

However, the consumer IoT segment also raises significant concerns regarding data privacy, security vulnerabilities, and the potential for surveillance. Low-cost smart gadgets often lack built-in security features, and end users frequently lack awareness of cybersecurity risks, creating vulnerabilities that can be exploited by malicious actors (ET CISO, 2025).

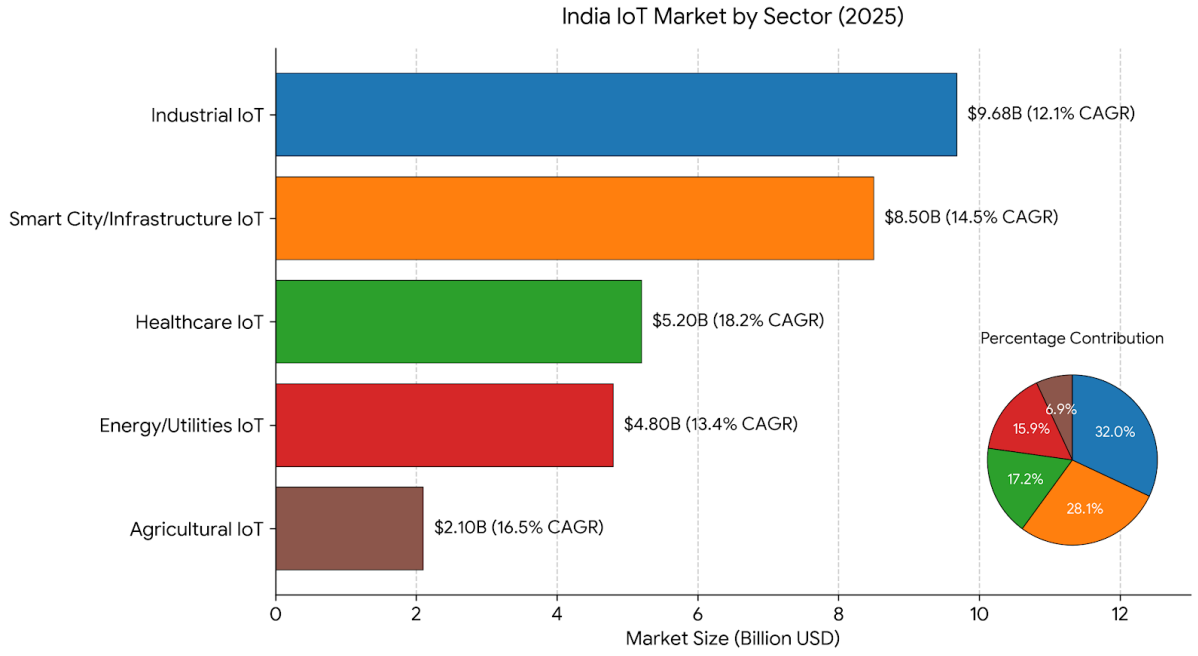

Figure 4. India IoT Market Segmentation by Sector (2025). The chart illustrates the relative market sizes and growth trajectories of India's primary IoT sectors, with industrial and consumer IoT representing the largest segments. Data compiled from Prescient & Strategic Intelligence (2025), IMARC Group (2026), and Market Research Future (2025).

4. Legal and Regulatory Architecture for IoT in India

4.1 The Evolving Data Protection Framework

The enactment of the **Digital Personal Data Protection Act, 2023** (DPDP Act) represents a watershed moment in India's legal framework for data governance, with profound implications for IoT deployments. The DPDP Act, operationalised through the Digital Personal Data Protection Rules, 2025, establishes a comprehensive framework for the processing of digital personal data, grounded in the constitutional right to privacy recognised by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.

The DPDP Act is particularly significant for IoT governance given the unique data protection challenges posed by IoT ecosystems. IoT devices collect vast quantities of personal data—often continuously, often without explicit user awareness, and often in contexts where traditional consent mechanisms are impractical. The Act addresses several dimensions of IoT data governance:

Consent Mechanisms and IoT. The DPDP Act establishes consent as the primary basis for processing personal data, requiring that consent be free, specific, informed, unconditional, and unambiguous (DPDP Act, 2023, §6). The Ministry of Electronics and Information Technology (MeitY) has unveiled a framework to implement the consent requirements, shortlisting six companies to develop consent management systems (Forbes India, 2025). However, applying consent requirements to IoT environments presents significant practical challenges. IoT devices in public spaces—including smart city sensors, traffic cameras, and environmental monitors—may collect personal data from individuals who have not provided and cannot practically provide consent. The Act provides for "legitimate uses" as an alternative basis for processing, but the scope and interpretation of this provision in IoT contexts remains to be clarified through delegated legislation and judicial interpretation.

Data Minimisation and Purpose Limitation. The DPDP Act incorporates the principles of data minimisation and purpose limitation, requiring that only such personal data as is necessary for the specified purpose be collected and processed (DPDP Act, 2023, §5). This principle has significant implications for IoT device design, potentially requiring manufacturers to limit sensor data collection to what is strictly necessary for device functionality rather than maximising data collection for potential future uses.

Security Safeguards. The Act mandates that data fiduciaries implement reasonable security safeguards to protect personal data, including in relation to IoT devices (DPDP Act, 2023, §8). The Act acknowledges IoT's potential vulnerabilities and places a significant onus on device manufacturers to ensure that data collected from IoT devices is encrypted and protected from unauthorised access (Financial Express, 2023). The 2025 Rules further specify breach notification requirements, mandating that data fiduciaries report breaches to the Data Protection Board within 72 hours.

Data Localisation and Cross-Border Transfers. The DPDP Act empowers the central government to notify countries or territories to which personal data may be transferred, effectively establishing a data localisation framework with implications for IoT data flows (DPDP Act, 2023, §16). This provision is particularly relevant for multinational IoT device manufacturers and cloud service providers that may process Indian IoT data on servers located outside India.

Enforcement Architecture. The Act establishes the Data Protection Board of India as the primary enforcement authority, with powers to investigate complaints, conduct inquiries, and impose penalties of up to INR 250 crore for specified violations (DPDP Act, 2023, §§18-34). The Board's enforcement capacity and technical expertise in IoT-specific data protection issues will be critical determinants of the Act's effectiveness in governing IoT ecosystems.

Table 5: Key Legal Provisions Governing IoT in India

Legal Instrument	Key Provisions Relevant to IoT	Application to IoT	Gaps / Challenges
Digital Personal Data Protection Act, 2023	Consent (§6); data minimisation (§5); security safeguards (§8); breach notification (Rules); cross-border transfer (§16); Data Protection Board (§18-34)	Applies to all personal data processed by IoT devices; consent and breach rules	Consent in public-space IoT; legitimate uses undefined; DPB technical capacity unproven
Telecommunications	Spectrum assignment	Enables	No IoT-specific

Act, 2023	(§4); equipment certification; network security	licensed/unlicensed spectrum for IoT; device standards	spectrum plan; certification standards not yet detailed
Information Technology Act, 2000	Unauthorised access (§43); data theft (§66); cyber terrorism (§66F)	Criminalises IoT device hacking; applies to IoT networks	Dated; lacks specific IoT security standards
IT (Reasonable Security Practices) Rules, 2011	ISO 27001 as deemed security standard	Could apply to IoT data fiduciaries	Not updated for IoT scale and heterogeneity
Consumer Protection Act, 2019	Product liability; unfair trade practices	IoT device defects; data-related harm	No IoT-specific safety standards; liability for pure data harm untested
BIS Standards (Proposed)	IoT device interoperability and security	Voluntary or mandatory certification	Development stage; unclear mandatory adoption

Source: Author's analysis of statutes and secondary literature.

4.2 The Telecommunications Act, 2023 and IoT Connectivity

The **Telecommunications Act, 2023**, which received presidential assent on December 24, 2023, provides the overarching legal framework for telecommunications services in India, replacing the colonial-era Indian Telegraph Act, 1885. The Act has significant implications for IoT governance, particularly in relation to spectrum allocation, device certification, and network security.

The Act empowers the central government to establish criteria for the use of spectrum, including for IoT applications, and provides for the assignment of spectrum through auction,

administrative processes, or a combination thereof (Telecommunications Act, 2023, §4). This flexibility in spectrum assignment is significant for IoT, as many IoT applications—particularly in agriculture and utilities—operate optimally in unlicensed or lightly licensed spectrum bands. The Act also establishes a framework for the certification of telecommunications equipment, with implications for IoT device security standards and interoperability requirements.

4.3 Cybersecurity Regulation and IoT

India's cybersecurity regulatory framework, while not IoT-specific, applies to IoT devices and networks through general cybersecurity obligations. The **Information Technology Act, 2000** (IT Act), as amended, establishes the legal framework for electronic governance and cybercrime, including provisions relating to unauthorised access, data theft, and cyber terrorism that are applicable to IoT systems (IT Act, 2000, §§43, 66, 66F).

The **Indian Computer Emergency Response Team (CERT-In)**, established under the IT Act, serves as the national agency for cybersecurity incident response. CERT-In has issued guidelines applicable to IoT devices, including requirements for security testing, vulnerability disclosure, and breach reporting. However, comprehensive, IoT-specific cybersecurity standards—comparable to the EU's Cybersecurity Act or the US IoT Cybersecurity Improvement Act—have not yet been enacted in India.

The cybersecurity threat landscape for IoT in India is significant and escalating. CERT-In data indicates that cybersecurity incidents quadrupled between 2019 (394,499 incidents) and 2023 (1,592,917 incidents), signalling the urgent need to fortify digital resilience (ET CISO, 2025). The Zscaler ThreatLabz 2025 Mobile, IoT, and OT Threat Report reveals a 67% increase in Android malware incidents and a significant shift in IoT attack patterns targeting critical infrastructure in sectors such as energy and manufacturing. India emerged as the primary target for mobile attacks, accounting for 26% of global activity, with a 38% increase in mobile threat attacks in India alone (Zscaler ThreatLabz, 2025).

Table 6: IoT Cybersecurity Threat Landscape in India (2021–2025)

Threat Indicator	**Data Point**	**Source**

Total cybersecurity incidents (2021)	14,02,809	CERT-In (via MHA, 2026)
Total cybersecurity incidents (2023)	15,92,917	CERT-In (via MHA, 2026)
Total cybersecurity incidents (2024)	20,41,360	CERT-In (via MHA, 2026)
Total cybersecurity incidents (2025)	29,44,248	CERT-In (via MHA, 2026)
India's share of global mobile attacks (2025)	26%	Zscaler ThreatLabz (2025)
IoT/OT attacks in energy sector (YoY)	387% rise	Zscaler ThreatLabz (2025)
Mirai malware share of blocked IoT transactions	40%	Zscaler ThreatLabz (2025)
Empanelled security auditing organisations	237	CERT-In (via MHA, 2026)

Source: Compiled by author from CERT-In data (as reported by Ministry of Home Affairs, 2026, PIB Press Release) and Zscaler ThreatLabz (2025).

4.4 The Puttaswamy Framework and IoT Privacy

The Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) established the constitutional right to privacy under Article 21 of the Constitution and articulated a threefold test for evaluating state intrusions into privacy: legality (the existence of a law), legitimate aim, and proportionality. Anupriya and Singh Chauhan (2025) applied this framework to evaluate the FASTag IoT system's constitutional validity, finding that while FASTag demonstrates rational connection to legitimate state objectives—improved toll collection efficiency and transparency, evidenced by reduced wait times and fuel savings—it fails the necessity requirement due to inadequate privacy impact assessments.

This analysis has broader implications for IoT governance in India. It suggests that IoT deployments by the state must be accompanied by comprehensive privacy impact assessments, clear data governance frameworks, and demonstrable proportionality between the data collected and the legitimate objectives pursued. The absence of such assessments in current IoT deployments represents a significant legal vulnerability and a potential infringement of constitutional rights.

4.5 Regulatory Gaps and the Case for IoT-Specific Legislation

The analysis of India's legal framework reveals significant regulatory gaps in IoT governance:

Absence of IoT-Specific Legislation. Unlike the European Union, which has enacted IoT-specific cybersecurity requirements through the Cybersecurity Act and is developing horizontal IoT legislation, India lacks a comprehensive IoT law addressing device security standards, interoperability requirements, liability allocation, and sectoral governance.

Fragmented Regulatory Oversight. Responsibility for IoT governance is distributed across multiple agencies—MeitY, DoT, TRAI, CERT-In, NCIIPC, and the Data Protection Board—without a clear coordination mechanism or lead authority for IoT. This fragmentation creates risks of regulatory overlap, inconsistency, and gaps.

Limited Technical Standards. While the Bureau of Indian Standards (BIS) has initiated work on IoT standards, India lacks a comprehensive national IoT standards framework comparable to those developed by the European Telecommunications Standards Institute (ETSI) or the National Institute of Standards and Technology (NIST) in the United States.

MSME Compliance Burden. The cumulative compliance requirements under the DPDP Act, IT Act, and sectoral regulations may impose disproportionate burdens on MSMEs, potentially constraining IoT innovation and adoption in the sector that constitutes the backbone of Indian manufacturing.

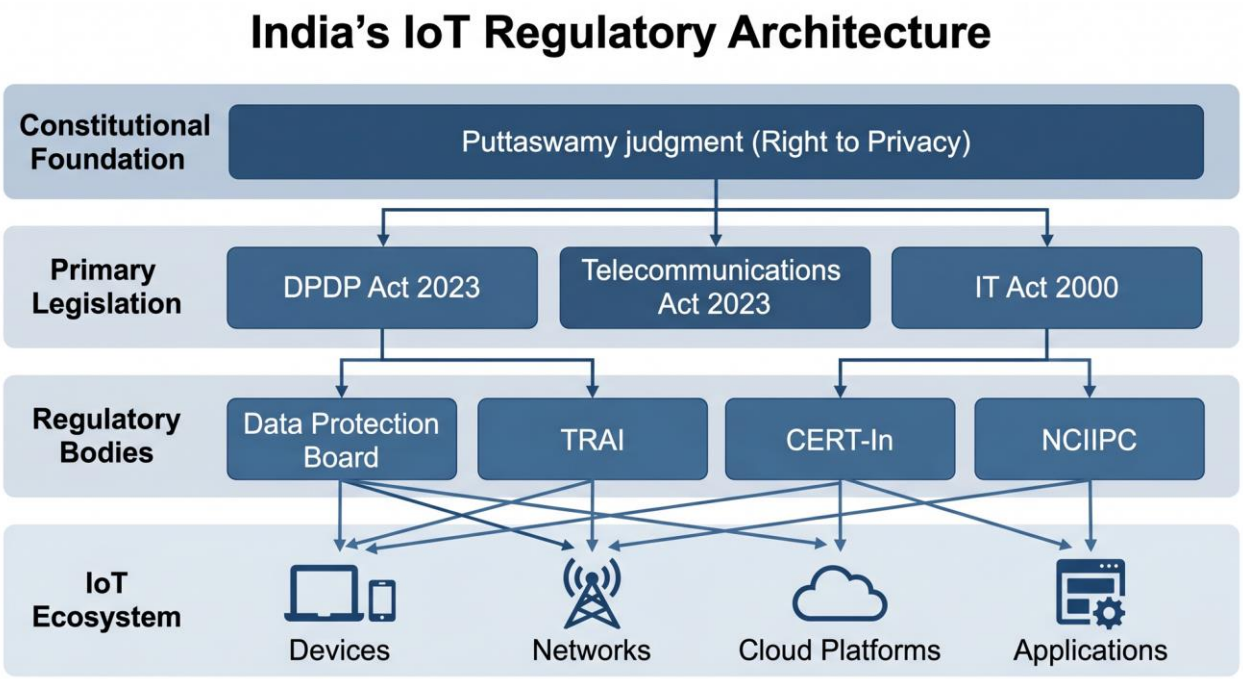

Figure 5: India's IoT Regulatory Architecture: A Multi-Layered Framework. The diagram illustrates the constitutional, legislative, regulatory, and operational layers governing IoT deployments in India, highlighting the distributed governance structure and the relationships between legal instruments and regulatory authorities.

5. Structural Challenges to Equitable IoT-Driven Development

5.1 The Digital Divide as a Development Barrier

Despite significant progress in expanding digital connectivity, the digital divide remains the most fundamental structural barrier to equitable IoT-driven development in India. Data from the Ministry of Communications, presented in the Lok Sabha, indicates that as of October 2025, out of 644,131 villages in India, 634,019 were covered with mobile connectivity, of which 630,676 had 4G services (Chandra Sekhar, 2025, as cited in Telangana Today, 2025). This means approximately 10,112 villages remain entirely without mobile coverage, and an additional 3,343 villages have mobile connectivity below 4G standards. As of May 2025, 97.65% of villages had mobile connectivity and 96.80% had 4G mobile connectivity, with 18,739 4G sites commissioned under Digital Bharat Nidhi-funded schemes covering 26,672 villages or locations (Ministry of Communications, 2025).

While India's wireless data tariff has declined from Rs 10.91 per GB in September 2018 to Rs 8.27 per GB in September 2025 (approximately USD 0.10 per GB), affordability of IoT

devices and digital literacy remain significant barriers to IoT adoption among lower-income populations (Telangana Today, 2025). Data consumption has grown substantially from 8.32 GB per subscriber per month in September 2018 to 25.24 GB per subscriber per month in September 2025, indicating deepening digital engagement among connected populations, yet also highlighting the widening gap between the connected and the unconnected (Telangana Today, 2025).

The digital divide has multiple, intersecting dimensions relevant to IoT:

Infrastructure Divide. Rural areas, where approximately 65% of India's population resides, have significantly lower-quality connectivity infrastructure than urban areas. The optical fibre cable network has expanded from 17.5 lakh km in March 2018 to 42.36 lakh km by September 2025, and Base Transceiver Stations have increased from 17.3 lakh to 31.4 lakh over the same period (Telangana Today, 2025). However, the persistence of approximately 10,000 villages without any mobile coverage limits the deployability of bandwidth-intensive or latency-sensitive IoT applications in these regions.

Economic Divide. The cost of IoT devices and services, while declining, remains prohibitive for significant portions of the Indian population. Smart home device penetration remains low, with the smart home market projected to reach USD 7.3 billion by 2025 yet penetration remaining under 1% of households. Consumer IoT adoption is concentrated overwhelmingly among upper-income urban households.

Digital Literacy Divide. Effective use of IoT-enabled services requires a baseline level of digital literacy that remains unevenly distributed across India's population, particularly among older adults, women in rural areas, and economically disadvantaged communities.

Gender Divide. Women in India are 15% less likely than men to own a mobile phone and 33% less likely to use mobile internet, creating a gender-specific barrier to accessing IoT-enabled services that rely on mobile connectivity (GSMA, 2024).

Addressing these divides requires targeted interventions beyond infrastructure expansion. The Samriddh Gram Phygital Services Pilot, which integrates physical service centres with digital infrastructure, represents one approach to bridging the digital divide by providing assisted access to IoT-enabled services for populations with limited digital literacy (DoT, 2025). The Gujarat government's pilot project to connect 25,000 rural households with high-speed

internet and value-added services, transforming rural homes into 'smart homes', represents another approach to extending IoT benefits to rural populations (Times of India, 2025).

5.2 Cybersecurity Vulnerabilities in Connected Ecosystems

The proliferation of IoT devices has dramatically expanded India's cybersecurity attack surface. According to official data from the Indian Computer Emergency Response Team (CERT-In), reported to the Lok Sabha by the Ministry of Home Affairs, the total number of cybersecurity incidents tracked in India has risen sharply: from 14,02,809 in 2021 to 15,92,917 in 2023, 20,41,360 in 2024, and reaching 29,44,248 in 2025 (Ministry of Home Affairs, 2026). This represents a near-doubling of tracked incidents over four years and a 44% increase from 2024 to 2025 alone, signalling the escalating threat landscape confronting India's connected infrastructure (Ministry of Home Affairs, 2026).

Low-cost IoT devices—particularly in the consumer segment—frequently lack basic security features such as encrypted data transmission, secure boot mechanisms, and regular security update capabilities. CERT-In issues alerts and advisories regarding latest cyber threats and vulnerabilities on an ongoing basis, operates the National Cyber Coordination Centre (NCCC) to examine cyberspace for threats, and has empanelled 237 security auditing organisations to support implementation of Information Security Best Practices (Ministry of Home Affairs, 2026). CERT-In has also launched a specific cybersecurity programme, "Cyber Bharat Setu," which focuses on promoting cybersecurity culture across states and union territories; Madhya Pradesh, Tripura, Uttarakhand, and Jammu & Kashmir Administration participated in this programme in 2025 (Ministry of Home Affairs, 2026).

The Zscaler ThreatLabz 2025 Mobile, IoT, and OT Threat Report reveals a 67% increase in Android malware incidents globally and a significant shift in IoT attack patterns targeting critical infrastructure sectors such as energy and manufacturing. India emerged as the primary target for mobile attacks, accounting for 26% of global activity (Zscaler ThreatLabz, 2025). The energy sector witnessed a 387% rise in IoT/OT attacks compared to the previous year, reflecting the growing targeting of critical infrastructure by malicious actors (Zscaler ThreatLabz, 2025). The Mirai malware family, which compromises IoT devices to create botnets for distributed denial-of-service attacks, accounted for 40% of blocked IoT transactions globally, demonstrating the persistent threat posed by IoT-specific malware (Zscaler ThreatLabz, 2025). In April 2024, an Indian consumer wearable manufacturing

company suffered a data breach when personal data of approximately 7.5 million users was posted on the Dark Web (SS Rana & Co., 2025).

Table 7: Structural Challenges, Manifestations, and Policy Responses

Structural Challenge	Manifestation	Current / Proposed Policy Response
Digital Divide (Infrastructure)	10,112 villages without any mobile coverage; 3,343 with coverage below 4G (Telangana Today, 2025; Ministry of Communications, 2025)	NTP 2025: 100% 4G coverage by 2030; BharatNet expansion
Digital Divide (Economic)	Smart home penetration under 1% of households (Indian Retailer, 2025)	PLI schemes for affordable devices; FPO-based shared IoT models
Digital Divide (Literacy & Gender)	Women 33% less likely to use mobile internet (GSMA, 2024)	Phygital service centres (Samriddh Kendras); digital literacy missions
Cybersecurity Vulnerabilities	387% rise in energy sector IoT/OT attacks; 67% Android malware spike (Zscaler, 2025)	CERT-In audits; proposed IoT security standards; Zero Trust adoption
Data Sovereignty / Technological Dependency	Majority of IoT chips and cloud platforms imported	PLI for electronics; NTP 2025 domestic manufacturing mission
MSME Adoption Barriers	Capital constraints, lack of expertise, no tailored solutions	Needed: IoT for MSMEs initiative; subsidised loans; shared platforms

Environmental Footprint	Device energy consumption, e-waste, resource extraction	NTP 2025: 30% carbon reduction for telecom; Green IoT design standards

Source: Author's synthesis.

5.3 Data Sovereignty and Technological Dependency

India's IoT ecosystem exhibits significant dependency on foreign technology providers, particularly in semiconductor manufacturing, cloud infrastructure, and IoT platforms. The majority of IoT sensors and chips deployed in India are imported, creating vulnerabilities in supply chain security and technological sovereignty. The DPDP Act's data localisation provisions represent one response to data sovereignty concerns, but technological dependency extends beyond data to encompass hardware, software, and platform infrastructure.

5.4 MSME Adoption Barriers

Small and Medium Enterprises (SMEs) constitute approximately 95% of India's industrial units and contribute approximately 30% to India's GDP, yet their adoption of IoT technologies remains limited. Barriers to MSME IoT adoption include: capital constraints limiting investment in IoT hardware and software; lack of in-house technical expertise to implement and manage IoT systems; limited awareness of IoT benefits and use cases relevant to their operations; concerns about data security and privacy compliance; and absence of tailored, affordable IoT solutions designed for MSME-scale operations.

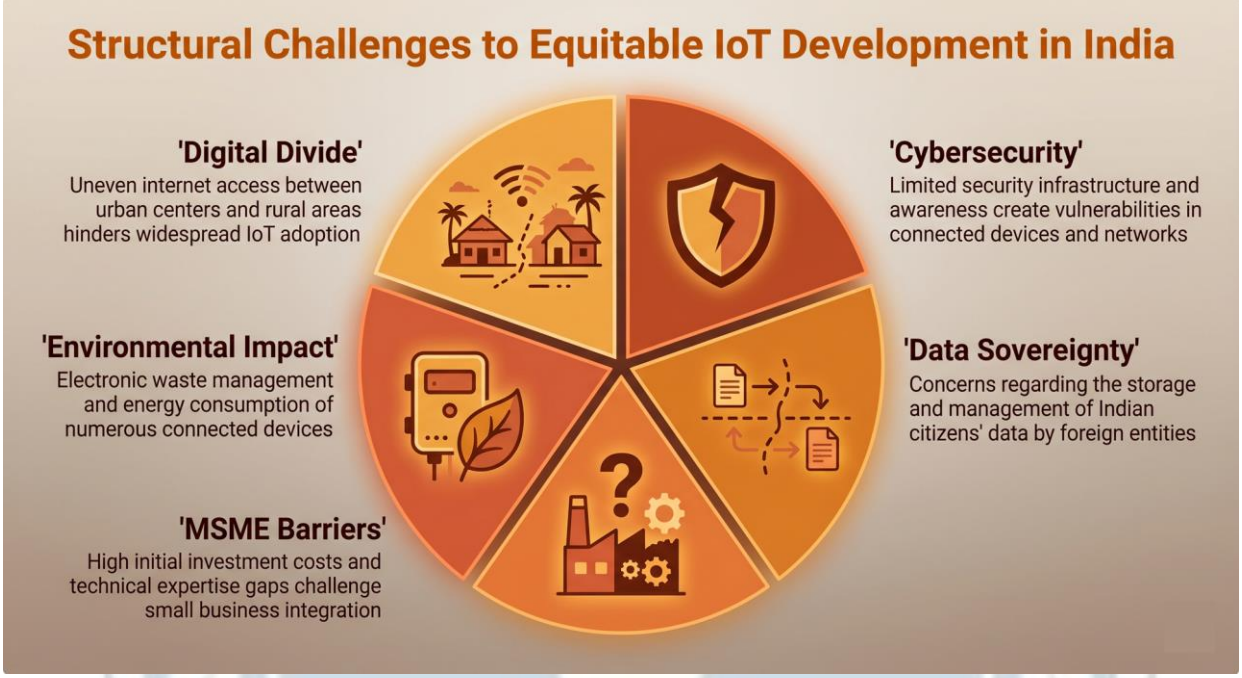

Figure 6: Structural Challenges to Equitable IoT-Driven Development in India. The pentagonal framework maps five interconnected structural challenges that constrain the equitable distribution of IoT's developmental benefits, requiring coordinated policy interventions across infrastructure, security, sovereignty, inclusion, and sustainability domains.

6. Towards a Rights-Based, Inclusive IoT Governance Framework

6.1 Synthesis of Findings

The preceding analysis reveals a complex picture of IoT's developmental role in India. IoT technologies are demonstrably contributing to developmental outcomes across agriculture, healthcare, urban infrastructure, manufacturing, and energy. Quantifiable impacts include significant water savings in agriculture, extended healthcare access to underserved populations, improved urban service delivery, and enhanced industrial productivity. The Indian IoT market's projected growth trajectory—from approximately USD 58.65 billion in 2025 to USD 351.27 billion by 2035 (Market Research Future, 2025)—indicates sustained momentum in IoT adoption across sectors.However, these developmental benefits are unevenly distributed, constrained by persistent structural challenges. The digital divide limits IoT's reach to populations that could benefit most from its applications. Cybersecurity vulnerabilities threaten the integrity and trustworthiness of connected systems. Legal and

regulatory frameworks, while evolving, contain significant gaps in IoT-specific governance. MSMEs, which constitute the backbone of the Indian economy, face particular barriers to IoT adoption.

Table 8: Proposed IoT Governance Principles and Corresponding Recommendations

Principle	Core Requirement	Key Recommendation(s)
1. Constitutional Alignment	IoT must satisfy Puttaswamy test: legality, legitimate aim, proportionality	Mandatory Privacy Impact Assessments for all government IoT deployments
2. Inclusive Design	Marginalised populations as primary design consideration	Affordability standards; multilingual interfaces; phygital access points
3. Security by Design	Security as fundamental, not optional	Enact IoT Security and Standards Act with mandatory encryption, secure boot, vulnerability disclosure
4. Regulatory Coherence	Coordinated governance across fragmented agencies	Establish IoT Coordination Council under MeitY with all regulators represented
5. Data Sovereignty	Reduce foreign dependency in IoT hardware/cloud	Expand PLI schemes; domestic cloud and chip design incentives
6. Sustainability	Align IoT deployment with environmental goals	Green IoT standards; renewable-powered sensors; circular economy for devices
—	MSME inclusion	Launch "IoT for MSMEs" initiative: subsidised loans, technical assistance, shared platforms

—	Skill development	Integrate IoT maintenance and security into Skill India; target rural youth and women

Source: Author's analysis and recommendations.

6.2 Principles for IoT Governance

Drawing on the analysis, the following principles are proposed to guide the development of a rights-based, inclusive IoT governance framework for India:

Principle 1: Constitutional Alignment. IoT governance must be grounded in the constitutional right to privacy as articulated in *Puttaswamy*, requiring that state-deployed IoT systems satisfy the threefold test of legality, legitimate aim, and proportionality. Privacy impact assessments should be mandatory for all government IoT deployments, as recommended by Anupriya and Singh Chauhan (2025).

Principle 2: Inclusive Design. IoT policies, standards, and solutions must be designed with the needs of marginalised populations—including rural communities, low-income groups, women, and persons with disabilities—as primary considerations rather than afterthoughts. This requires attention to affordability, accessibility, digital literacy, and multilingual interfaces.

Principle 3: Security by Design. IoT devices and systems must incorporate security features as fundamental design requirements, not optional add-ons. Mandatory security standards, certification requirements, and vulnerability disclosure obligations should be established through IoT-specific regulation.

Principle 4: Regulatory Coherence. The fragmented IoT regulatory architecture should be rationalised through the establishment of a coordinating mechanism or lead authority for IoT governance, ensuring consistency across data protection, cybersecurity, spectrum management, and sectoral regulation.

Principle 5: Data Sovereignty. India's IoT ecosystem should be supported by domestic capabilities in semiconductor design and manufacturing, cloud infrastructure, and IoT platforms, reducing dependency on foreign technology providers and strengthening technological sovereignty.

Principle 6: Sustainability. IoT deployment strategies should incorporate environmental sustainability considerations, including energy-efficient device design, renewable energy-powered infrastructure, and circular economy approaches to device lifecycle management.

6.3 Recommendations

Based on these principles, the following specific recommendations are offered:

Legislative Recommendations:

1. Enact a comprehensive **IoT Security and Standards Act** establishing mandatory security requirements for IoT devices sold in India, including encryption standards, secure boot requirements, vulnerability disclosure obligations, and regular security update requirements.
2. Amend the DPDP Act or issue regulations to address IoT-specific data protection challenges, including consent mechanisms for public-space IoT deployments and data minimisation requirements for IoT devices.

Institutional Recommendations:

3. Establish an **IoT Coordination Council** under MeitY, bringing together representatives from DoT, TRAI, CERT-In, NCIIPC, the Data Protection Board, and sectoral regulators to ensure coordinated IoT governance.
4. Strengthen CERT-In's IoT security capabilities through dedicated IoT threat monitoring infrastructure and enhanced international cooperation on IoT threat intelligence.

Policy Recommendations:

5. Launch an **IoT for MSMEs** initiative providing financial incentives, technical assistance, and standardised IoT solutions tailored to MSME-scale operations.
6. Expand IoT training programmes within the Skill India framework, targeting IoT deployment, maintenance, and security skills relevant to agriculture, healthcare, and manufacturing sectors.

Infrastructure Recommendations:

7.Accelerate BharatNet and 5G rollout to eliminate the remaining connectivity gap in unconnected villages, prioritising regions with high potential for IoT-enabled agricultural and healthcare applications

8. Establish IoT testbeds and certification facilities in partnership with academic institutions and industry, enabling domestic testing and certification of IoT devices against Indian standards.

6.4 Alignment with Viksit Bharat 2047

The IoT governance framework proposed in this paper aligns with the broader Viksit Bharat 2047 vision of a developed India. IoT's contributions to agricultural productivity, healthcare access, urban sustainability, industrial competitiveness, and energy efficiency directly support the economic and social transformation envisioned under Viksit Bharat. However, realising this alignment requires deliberate policy choices that prioritise inclusive, secure, and rights-respecting IoT deployment over laissez-faire technology diffusion. The governance framework proposed here seeks to provide a roadmap for those policy choices.

7. Conclusion

The Internet of Things stands at the intersection of India's technological ambition and its developmental imperatives. This paper has demonstrated that IoT technologies are delivering measurable developmental outcomes across agriculture, healthcare, urban infrastructure, manufacturing, and energy, while simultaneously raising profound legal, regulatory, and structural challenges. The projected growth of India's IoT market—from USD 58.65 billion in 2025 to USD 351.27 billion by 2035—represents both an economic opportunity and a governance imperative: the choices made today regarding IoT policy, law, and standards will shape the developmental trajectory of connected technologies for decades to come.

The legal framework, anchored by the DPDP Act, the Telecommunications Act, and evolving sectoral regulations, provides a foundation for IoT governance but requires significant elaboration to address IoT-specific challenges in consent, data minimisation, security, and liability. The constitutional right to privacy, as articulated in *Puttaswamy*, provides both a normative anchor and a doctrinal framework for evaluating IoT deployments, but its application requires systematic implementation through privacy impact assessments and proportionality analyses.

Addressing structural challenges—particularly the digital divide, cybersecurity vulnerabilities, data sovereignty concerns, and MSME adoption barriers—requires coordinated policy interventions across infrastructure, regulation, industrial policy, and skill

development. The principles and recommendations articulated in this paper provide a framework for such interventions, grounded in the imperatives of rights protection, inclusive development, and technological sovereignty.

As India progresses towards the Viksit Bharat 2047 vision, the governance of IoT will increasingly determine whether connected technologies serve as instruments of equitable development or as amplifiers of existing inequalities. The choices confronting policymakers, regulators, and technology developers are consequential not only for India's developmental trajectory but for the broader Global South, where India's experience with IoT-driven development is being closely watched as a potential model. The path forward lies in a deliberate, principled approach to IoT governance—one that harnesses technology's transformative potential while safeguarding the rights and interests of all citizens, particularly the most vulnerable.

References

6Wresearch. (2025). *India IoT in healthcare market (2025-2031): Trends, outlook & forecast*. https://www.6wresearch.com

ANI. (2025, January 3). Jagdeep Dhankhar flags off IoT-integrated mobile clinics for Srinagar, Kalaburagi. *Asian News International*. https://www.aninews.in

Anupriya, & Singh Chauhan, K. D. (2025). Securing informational privacy in India's IoT governance: Looking through the lens of FASTag. *Journal of Data Protection & Privacy*, 7(2), 125–151.

Bhondve, S. (2025, April 7). India's digital transformation on the fast track. *EletseGov*. https://egov.eletsonline.com

Bhoite, T. D., &Buktar, R. B. (2025). Productivity enhancement in Indian auto component manufacturing supply chain with IoT using neural networks. *Production, 35*, e20250008. https://doi.org/10.1590/0103-6513.20250008

Cultyvate. (2025). Data-driven irrigation in paddy cultivation: Cultyvate'sagritech model. *NITI Aayog Frontier Technologies Platform*. https://frontiertech.niti.gov.in/story/data-driven-irrigation-in-paddy-cultivation-cultyvates-agritech-model/

Department of Telecommunications. (2025). *Draft National Telecom Policy 2025*. Government of India.

Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).

DQ India. (2025, September 2). The Internet of Things: Building a sustainable, affordable and resilient future for utilities. *DQ India*. https://www.dqindia.com

ET CISO. (2025, October 10). Connected and vulnerable: The growing urgency of IoT and mobile security in India. *Economic Times CISO*. https://ciso.economictimes.indiatimes.com

European Commission. (2023). *IoT and edge computing strategy*. European Union.

Fasal. (2025). From fields to data: IoT-powered precision farming boosting yields and saving water. *NITI Aayog Frontier Technologies Platform*. https://frontiertech.niti.gov.in/story/precision-farming-innovation-fasal-krantis-transformative-impact-on-indian-agriculture/

Financial Express. (2023, November 26). Safeguarding the digital frontier: Indian Digital Personal Data Protection Act 2023 and its approach to emerging technologies. *Financial Express*.

Financial Express. (2026, May 15). Smart meter rollout slows amid delays, payment gaps and tariff pressure. *Financial Express*. https://www.financialexpress.com/policy/economy/smart-meter-rollout-slows-amid-delays-payment-gaps-and-tariff-pressure/4241990/

Forbes India. (2025, August 13). Explained: Govt's new 'code for consent' initiative under the DPDP Act. *Forbes India*.

Grand View Research. (2026). *India 5G Internet of Things (IoT) market size & outlook, 2025–2030*. https://www.grandviewresearch.com/horizon/outlook/5g-internet-of-things-iot-market/india

Grand View Research. (2026). *India IoT devices market size & outlook, 2026–2033*. https://www.grandviewresearch.com/horizon/outlook/iot-devices-market/india

GSMA. (2024). *The mobile gender gap report 2024*. GSMA.

ICRISAT. (2025, October 29). SBI Foundation joins hands with UAS Raichur and ICRISAT to launch "SMART-CROP" initiative. *ICRISAT Press Room*.

IMARC Group. (2026). *India consumer IoT market size, share & trend report 2026–34*. https://www.imarcgroup.com

IMARC Group. (2026). *India smart home devices market – size & forecast 2034*. https://www.imarcgroup.com/india-smart-home-devices-market

Indian Retailer. (2025, December 13). Insights on the smart home and consumer IoT market in India. *Indian Retailer*. https://www.indianretailer.com/article/retail-business/future-retail/insights-smart-home-and-consumer-iot-market-india

Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).

IoT Analytics. (2024). *State of IoT 2024: Number of connected IoT devices*. https://iot-analytics.com

Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).

Kshetri, N. (2020). The economics of the Internet of Things in the Global South. *Third World Quarterly*, 41(2), 235–252.

Market Research Future. (2025). *India Internet of Things market size, share report forecast | 2035*. https://www.marketresearchfuture.com/reports/india-internet-of-things-market-21603

MediBuddy. (2025, February 5). MediBuddy partners with Japan's ELECOM to launch smart health IoT devices in India. *GeneOnline News*.

Ministry of Agriculture and Farmers Welfare. (2024). *Annual report 2023–24*. Government of India.

Ministry of Communications. (2025, July 30). Digital and broadband connectivity. *Press Information Bureau*. https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2150173

Ministry of Electronics and Information Technology. (2015). *Draft IoT Policy*. Government of India.

Ministry of Electronics and Information Technology. (2024). *Annual report 2023–24*. Government of India.

Ministry of Home Affairs. (2026, March 24). Assistance to states to tackle cyber incidents. *Press Information Bureau*. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504

Ministry of Housing and Urban Affairs. (2015). *Smart Cities Mission statement and guidelines*. Government of India.

NASSCOM. (2025). The rise of new IoT-enabled business models. *NASSCOM Community*. https://community.nasscom.in/communities/iot/rise-new-iot-enabled-business-models

National Payments Corporation of India. (2024). *UPI product statistics*. https://www.npci.org.in

Prescient & Strategic Intelligence. (2025). *India industrial IoT market size & share analysis – key trends, future opportunities, growth strategies, and forecasts (2026–2032)*.

Press Information Bureau. (2025, October 29). Department of Telecommunications aims to implement Samriddh Gram Phygital Services Pilot Project to bridge the digital divide. *Government of India*.

Press Information Bureau. (2025, November 13). Simplified compliance framework for start-ups and certain data fiduciaries under DPDP Act and Rules. *Government of India*. https://www.pib.gov.in

ShubhavniSmartFarms. (2025, June 19). Indoor saffron cultivation through IoT: A transformative agritech innovation for India. *NITI Aayog Frontier Technologies Platform*. https://frontiertech.niti.gov.in

Singh, J. (2025, October 17). NDHM and the HealthTech paradox: Innovation outpacing implementation in India's digital health backbone. *LinkedIn*.

SS Rana & Co. (2025, May 22). Emergence of IoT in manufacturing sector raises data privacy concerns. *SS Rana & Co*. https://ssrana.in

Statista. (2025). *Internet of Things – India: Market outlook*. https://www.statista.com/outlook/tmo/internet-of-things/india

Taylor, L., & Broeders, D. (2015). In the name of development: Power, profit and the datafication of the global South. *Geoforum*, 64, 229–237.

Telecommunications Act, 2023, No. 44 of 2023, Acts of Parliament, 2023 (India).

Telecom Regulatory Authority of India. (2022). *Recommendations on use of unlicensed spectrum for IoT*. TRAI.

Telecom Regulatory Authority of India. (2026). *Indian telecom services performance indicator report, October–December 2025*. https://trai.gov.in

Telangana Today. (2025, December 3). Broadband subscriptions nearly double as India strengthens digital infrastructure. *Telangana Today*. https://telanganatoday.com/broadband-subscriptions-nearly-double-as-india-strengthens-digital-infrastructure

Times of India. (2025, January 8). 25,000 households in Gujarat to become 'smart' under new pilot project. *Times of India*.

Voice & Data. (2024, May 23). The rise of new IoT-enabled business models. *Voice & Data*. https://www.voicendata.com/opinion/the-rise-of-new-iot-enabled-business-models-4598415

YourStory. (2025, November 12). How Larkai Healthcare uses AI, IoT to bring hospital-grade care to India's small towns. https://yourstory.com

Zscaler ThreatLabz. (2025). *2025 Mobile, IoT, and OT threat report*. Zscaler. https://www.zscaler.com