

Internet of Things in India: Advantages and Delimitations over the Next Decade (2025–2035)

¹Siddharth Bahuguna and ²Prof. (Dr.). Prasad Rao P.V.V.

¹*Research Scholar, Faculty of Management & Commerce, Jagannath University, Delhi NCR, Bahadurgarh, Haryana*

²*Research Supervisor & Vice Chancellor, Jagannath University, Delhi NCR, Bahadurgarh, Haryana*

Received: 14th July, 2026; Revised: 05th August 2026; Accepted: 20th August, 2026; Available Online: 10th September 2026

ABSTRACT

Over the past few years, the Internet of Things (IoT) has moved from being a promising idea to becoming one of the quiet engines behind India's digital economy showing up in smart city control rooms, factory floors, farm fields, and hospital wards alike. This paper takes a qualitative, documentary approach to asking what IoT is likely to mean for India over the next ten years, roughly 2025 to 2035, and what might get in the way. Drawing on the Technology–Organization–Environment (TOE) framework and Rogers' Diffusion of Innovation model as interpretive lenses, the study works through Scopus-indexed journal articles, government policy documents, and industry market reports, sorting the evidence into two broad themes and then into finer sub-themes. What emerges is a fairly clear picture on the upside: expanding 5G networks, early domestic chip-making efforts, the Smart Cities Mission, and growing demand from agriculture, healthcare, and the energy sector all point toward genuine, multi-fold market growth by the mid-2030s. But the same body of literature keeps returning to the same handful of sticking points: cybersecurity gaps, a data-protection law that is still being phased in, a shortage of trained people, high upfront costs, devices that don't talk to each other well, a rural–urban connectivity gap, and a growing e-waste problem nobody has quite figured out how to handle. Taken together, the evidence suggests India's IoT decade won't unfold evenly. Large firms and government-backed urban projects will likely move first and fastest, while smaller businesses, farms, and rural communities lag behind unless someone deliberately works to close that gap. The paper ends with what this means in practice for researchers, policymakers, and industry and is upfront about where a review built entirely from secondary sources has to draw its own boundaries.

Keywords: *Internet of Things; India; smart cities; Industry 4.0; digital transformation; data protection; technology adoption; qualitative review*

How to cite this article: Bahuguna S, Prasad Rao PVV, Internet of Things in India: Advantages and Delimitations over the Next Decade (2025–2035) *Int J Drug Deliv Technol.* 2026;16(84s): 1240-1247; DOI: 10.25258/ijddt.16.84s.134

Source of support: Nil.

Conflict of interest: None

1. INTRODUCTION

The Internet of Things, at its core, is a fairly simple idea: everyday objects—sensors, machines, appliances fitted with the ability to collect data and exchange it over a network, largely without a person having to type anything in (Ashton, 2009; Atzori, Iera, & Morabito, 2010). Kevin Ashton coined the phrase back in the context of supply-chain sensors, and in the years since, the concept has grown well beyond that original use case. It now sits at the centre of how many countries think about digital transformation—not just as a manufacturing tool, but as a way of running cities, extending healthcare, and reaching communities that older infrastructure never quite got to.

India is a useful, if complicated, case to look at closely. Programmes such as the Smart Cities Mission and Digital India, an expanding 5G network, and early attempts at building domestic semiconductor capacity have all pushed IoT toward the centre of the country's modernisation plans (Government of India, Ministry of Housing and Urban Affairs, 2015). At the same time, India's sheer size, its uneven infrastructure, and a data-protection law that only

recently came into force mean the barriers here look somewhat different from what smaller or more evenly developed economies tend to face.

The numbers give some sense of scale, even if they don't agree with each other. India's IoT market was worth somewhere around USD 1.5–1.6 billion in 2025–2026 by more conservative estimates, and different market-research firms expect it to grow anywhere from about USD 3.6 billion to over USD 69 billion by the mid-2030s, depending on how broadly they define the market and what methodology they use (Grand View Research, 2025a, 2025b; IMARC Group, 2026; Ken Research, 2026; Orion Market Research, 2025). That spread is wide enough that the exact figures matter less than the direction they all point in: strong, sustained growth, driven mainly by manufacturing, connected vehicles, precision farming, and city infrastructure.

None of this optimism is uncontested, though. A fairly substantial body of India-specific academic work keeps flagging the same obstacles: weak cybersecurity, unclear regulation, high costs, poor interoperability between

*Author for Correspondence: Siddharth Bahuguna

devices, and a shortage of people who actually know how to build and manage these systems (Bajaj, Almugari, Tabash, Alsyani, & Saleem, 2021; Desingh & Baskaran, 2022; Mital, Chang, Choudhary, Papa, & Pani, 2018; Narwane, Gunasekaran, & Gardas, 2022). This paper tries to bring both sides of that conversation together. It asks, first, what advantages IoT is realistically expected to bring to India over the next decade, sector by sector; second, what structural, regulatory, organisational, and social factors are likely to slow that down or spread it unevenly; and third, pulling the first two together, what shape India's IoT diffusion is likely to take by 2035.

The rest of the paper is organised as follows. Section 2 sketches out the policy backdrop. Section 3 works through the literature, both conceptual and sector-specific. Section 4 lays out the methodology, including where the study deliberately draws its boundaries. Section 5 presents the findings on advantages and delimitations. Section 6 pulls these together into a decade-scale outlook, and the paper closes with implications, policy suggestions, limitations, future research directions, and a conclusion.

2. BACKGROUND: INDIA'S DIGITAL AND IOT POLICY LANDSCAPE

It's hard to talk about where India's IoT sector is headed without first accounting for the digital-infrastructure programmes already in place. The Smart Cities Mission, launched in 2015, has by now set up Integrated Command and Control Centres in 100 cities, rolled out IoT-linked traffic and surveillance systems, installed more than 84,000 CCTV cameras for public safety, and put over 17,000 kilometres of water pipelines under SCADA-based leak monitoring (Government of India, Ministry of Housing and Urban Affairs, 2015). None of this needs to be built from scratch against an existing base that later IoT projects can simply plug into.

Something similar is happening in the energy sector. Under the Revamped Distribution Sector Scheme (RDSS), India has sanctioned roughly 198 million prepaid smart meters, which on its own creates a huge addressable base for connectivity modules, meter-data platforms, and analytics tools (Ken Research, 2026). The National Smart Grid Mission frames this kind of grid modernisation as central to cutting transmission losses, managing demand more flexibly, and folding renewable energy into the grid (Kappagantou & Daniel, 2018).

On the connectivity side, the ongoing 5G rollout should lower latency and let far more devices connect at once, which matters a lot for industrial and automotive IoT specifically. Early domestic chip-design work including what's reported to be India's first commercial IoT-focused chip, said to cost around thirty percent less than comparable imports points to a slow but real push toward hardware self-sufficiency (IMARC Group, 2026).

The most consequential recent shift, though, is regulatory. The Digital Personal Data Protection Act, 2023 was finally put into operation through the Digital Personal Data Protection Rules, 2025, notified by the Ministry of

Electronics and Information Technology on 13 November 2025, with compliance phased in through 13 May 2027 (Government of India, Ministry of Electronics and Information Technology, 2025). This paper treats that as a genuinely important development, but not a settled one; it reshapes several of the concerns raised in earlier literature (discussed in Section 3.9) without fully resolving them just yet.

3. LITERATURE REVIEW

3.1 Conceptual Foundations of the Internet of Things

Most definitions of IoT converge on the same basic idea: a network of physical objects fitted with sensors, software, and connectivity, able to exchange data with other devices and systems over the internet (Atzori et al., 2010). Ashton's (2009) original framing was about replacing manual, error-prone data entry with machines that could report on themselves. Since then, the literature has settled into describing IoT as a layered systemsensing, network/connectivity, edge or gateway processing, data platforms, and finally the application layer where raw signals actually become something useful (Atzori et al., 2010).

3.2 Technology Adoption Theory: TOE and Diffusion of Innovation

Two theoretical frameworks show up again and again in the Indian IoT-adoption literature. The Technology–Organization–Environment (TOE) framework (Tornatzky & Fleischer, 1990) argues that whether a technology gets adopted depends on three things working together: the technology itself (how much advantage it offers, how well it fits existing systems, how complex it is), the organisation (its size, resources, and whether leadership actually backs the change), and the environment (regulation, competitive pressure, industry norms). Rogers' (2003) Diffusion of Innovation model adds a time dimension innovators, early adopters, early majority, late majority, laggards explained by how much relative advantage, compatibility, complexity, trial ability, and observability an innovation has. Some Indian studies applying structural equation modelling to IoT adoption have leaned on related behavioural models too, including the Theory of Reasoned Action, the Theory of Planned Behaviour, and the Technology Acceptance Model, to test which explanation of adoption intention actually holds up (Mital et al., 2018). This paper uses TOE and DOI together as a lens for organising the findings in Section 5, mostly because the Indian literature keeps pointing to organisational and environmental issues not technological ones as the real sticking points.

3.3 IoT in Indian Smart Cities and Urban Governance

Smart-city IoT research in India tends to spend more time cataloguing barriers than celebrating adoption. Mishra, Rani, Saha, Hezam, Pamucar, Marinovic, and Pandey (2022) used a fuzzy multi-criteria decision-making approach to rank fifteen barriers to IoT adoption in smart-city waste management, and found that weak standardisation, unclear regulatory direction, and thin

policy guidance outranked purely technical issues like network coverage. That's a telling result even in an area where the government has put in considerable subsidy and effort, it's institutional friction, not technology, that seems to hold things back.

3.4 IoT in Industrial Automation and Manufacturing

Manufacturing-sector research on Indian IoT usually gets framed under the Industry 4.0 umbrella, alongside cloud computing, big-data analytics, and AI as a package of complementary technologies. Mital et al.'s (2018) broader adoption study found that despite recognised potential, Indian IoT use stays concentrated in a fairly narrow set of applications rather than spreading widely across firms and sectors which fits neatly with what Diffusion of Innovation theory would predict at this stage: early adopters moving first, everyone else still watching.

3.5 IoT in Indian Agriculture and Food Supply Chains

Agriculture is arguably where IoT's social payoff could be largest, given how much of India's economy and employment still runs through it. Narwane et al. (2022) identified twenty-four adoption factors specific to IoT in India's agricultural and food supply chain, grouped them into technological, social, economic, and organisational categories, and used the DEMATEL method to work out which ones actually cause which. Interoperability gaps, sustainability worries, low trust, weak security, and network limitations came out as the five most influential causes once again, organisational and trust issues outweighing anything purely about the hardware.

3.6 IoT in Indian Healthcare and Telemedicine

In healthcare, most of the research centres on remote patient monitoring and telemedicine as ways of reaching people who don't have easy access to a hospital. Dahiya (2022) built and tested an IoT-based remote-monitoring setup for chronic and cardiovascular patients, motivated partly by WHO estimates that a large share of India's population lives with some chronic condition requiring ongoing monitoring; the design deliberately built in protocol-conversion and authentication features specifically to address the trust and security concerns that keep coming up elsewhere in this literature. A related study on subscription-based remote health monitoring (Kirubakaran, Gunasekaran, Dolly, Jagannath, & Peter, 2023) makes a similar point from a different angle that cost and sustainable access, not what the devices can technically do, are what actually limits how far telehealth can scale.

3.7 IoT in Energy, Utilities, and the Smart Grid

India's energy sector is an interesting case because strong top-down policy support (through the National Smart Grid Mission) sits alongside real resistance further down the chain, at the level of utilities and individual consumers. Kappagant and Daniel (2018) went through the technical, socio-economic, and awareness-related challenges facing smart-grid rollout in India and concluded that the real bottleneck isn't generation or transmission technology it's whether consumers actually accept the system. Archana

(2022), using exploratory factor analysis and Fuzzy-TISM on survey data from 221 respondents, found seventeen distinct barriers to consumer acceptance of smart-grid technology, which collapsed into six underlying factors; the biggest of these were the absence of supportive government policy and the lack of any clear monetary benefit for the consumer.

3.8 Digital Divide and Rural Connectivity

One thing that keeps qualifying the sector-specific findings above is that national adoption statistics tend to smooth over a fairly stark rural–urban gap. Shruthi, Ithita, and Chaudhari (2021) put urban broadband penetration at around 93%, against roughly 29.3% in rural areas, and traced the gap to unreliable electricity, affordability, difficult terrain for deployment, and low digital literacy. A separate study covering the COVID-19 period (Indu, Thadikaran, & Chellaswamy, 2022) found the gap narrowed slightly during the pandemic, mostly out of necessity, but concluded the underlying infrastructure and literacy problems were still largely unresolved. Because IoT needs steady connectivity and reliable power to function at all, this divide is a real structural constraint and it compounds, rather than simply sits alongside, the organisational barriers described in the sector studies above.

3.9 Cybersecurity, Data Privacy, and Regulatory Literature

IoT's architecture lots of different devices from lots of different vendors, often running outdated firmware with weak encryption and inconsistent authentication is well documented as expanding the attack surface considerably compared with a conventional, centralised IT system. For a long time, this technical exposure sat alongside a regulatory gap: India simply didn't have a comprehensive statutory data-protection law, something pre-2023 literature raised repeatedly as a barrier to institutional and consumer trust. That gap has now, at least on paper, been addressed. The Digital Personal Data Protection Rules, 2025 set up a Data Protection Board of India, mandatory breach notification, and a phased compliance schedule running to May 2027 (Government of India, Ministry of Electronics and Information Technology, 2025). But because the rules are phased, several of the obligations that matter most for IoT specifically device telemetry, inferences drawn from sensor data, cross-border transfers of industrial data won't be fully enforceable until the final stage. That leaves a multi-year stretch where the regulatory picture is better than it was, but still incomplete.

3.10 Environmental Sustainability and E-Waste

A smaller but growing strand of research looks at the environmental cost of all this connected hardware. Mor, Sangwan, Singh, Singh, and Kharub (2021) studied e-waste awareness in Indian educational institutions and found that even engineering students people who might reasonably be expected to know better had limited understanding of how e-waste is generated and processed, despite growing institutional talk about extended producer responsibility. As IoT adds more sensors, gateways, and

connected devices into circulation every year, this suggests end-of-life device management is a problem that's more likely to get worse before anyone gets around to fixing it.

3.11 Research Gap

Three gaps stand out across this literature. Most Indian IoT research stays within a single sector agriculture, healthcare, energy, waste management with very little attempt to pull the threads together into one picture. A lot of the empirical work also predates the DPDP Rules notified in November 2025, so the standard line about India “lacking” data-protection law needs updating rather than repeating. And decade-scale, forward-looking synthesis is rare; most studies rank barriers at a single point in time rather than asking where things are headed. This paper tries to address all three by pulling sectors together, updating the regulatory picture, and framing the whole thing as a ten-year outlook rather than a snapshot.

4. RESEARCH METHODOLOGY

4.1 Research Design and Philosophical Stance

This is a qualitative, interpretive study built around documentary and thematic analysis of secondary sources not primary surveys, interviews, or experiments. That choice follows fairly naturally from an interpretivist stance: making sense of where India's IoT sector is heading over a decade is more a matter of synthesising and interpreting what's already been found than testing a hypothesis with new numbers. Given that the goal here is a forward-looking, cross-sector picture of a landscape that's still shifting, triangulated secondary evidence read through an established adoption-theory lens offers more interpretive reach than a study confined to one firm or one sector could.

4.2 Data Sources and Selection Criteria

Three kinds of secondary data went into this review. The main body came from peer-reviewed journal articles on IoT adoption, barriers, applications, or theory in the Indian context, drawn mostly from Scopus-indexed journals Technological Forecasting and Social Change, Smart Agricultural Technology, the International Journal of Health Planning and Management, IEEE Access, the Journal of Electrical Systems and Information Technology, Strategic Planning for Energy and the Environment, and Procedia CIRP, among others. Alongside these sit official government and regulatory documents, including Smart Cities Mission material and the Digital Personal Data Protection Rules, 2025. Market-intelligence reports round out the third category, used only for descriptive market-sizing context rather than as evidence in their own right.

A source was included if it addressed IoT, smart-city, or related digital-infrastructure adoption specifically within India, or if it offered foundational theoretical grounding with broader applicability core IoT definitions, TOE, or DOI, for instance. Sources published between 2009 and 2026 were eligible, with a deliberate lean toward 2018–2026 material to keep things current; the older theoretical references (Ashton, 2009; Rogers, 2003; Tornatzky & Fleischer, 1990) were kept specifically for definitional and

theoretical grounding. Anything addressing IoT purely outside the Indian context without clear theoretical relevance was left out, as was promotional or vendor material without an identifiable study or named author behind it.

4.3 Thematic Analysis Procedure

Coding happened in two stages. First, each source was sorted into one of two broad buckets advantage/opportunity or delimitation/barrier based on what it was mainly arguing or finding. From there, sub-themes were built up inductively from whatever patterns kept recurring: on the advantage side, economic/market, urban infrastructure, industrial, agricultural, healthcare, energy, and regulatory-foundation themes; on the delimitation side, cybersecurity, regulatory lag, workforce/skill gaps, cost and interoperability, the digital divide, sustainability/e-waste, and uneven diffusion. These sub-themes are what structure Section 5. Throughout, TOE and DOI worked as sensitising concepts a lens applied while coding, not a rigid checklist imposed on the data beforehand which is fairly standard practice in qualitative documentary work.

4.4 Trustworthiness and Rigor

Three things were done to keep this trustworthy. Triangulating across academic, government, and industry sources meant no single type of evidence carried the whole argument. Cross-checking older barrier-focused studies (mostly 2018–2022) against the most recent regulatory change the DPDP Rules notified in November 2025 guarded against simply repeating claims that have since been overtaken by events, particularly the older line about India having no comprehensive data-protection law. And deliberate effort went into noting complicating evidence rather than smoothing it over for instance, flagging that the DPDP Rules' phased rollout still leaves several IoT-relevant provisions unenforced for now, rather than treating the law's existence as a solved problem.

4.5 Scope and Delimitations of the Study

This review is bounded in three deliberate ways, worth stating plainly rather than leaving implicit. Geographically, it sticks to India-specific literature and doesn't attempt a systematic cross-country comparison. Temporally, it looks ahead to 2025–2035; earlier material is used only where it helps with definitions or theory. And methodologically, it works from publicly available secondary and documentary evidence only no new survey, interview, or firm-level financial data was collected, and the market-size figures are presented as rough ranges rather than firm predictions, given how much the commercial reports disagree with each other, as noted in Section 1.

4.6 Ethical Considerations

Since this is a documentary study with no human participants, it didn't require the usual consent or ethics-board process. Even so, a few things mattered ethically: sources are attributed properly and paraphrased rather than lifted verbatim; market-intelligence figures are flagged clearly as promotional material with acknowledged

variability, not treated as neutral fact; and nothing claimed here goes further than what the underlying sources actually support.

5. FINDINGS AND THEMATIC DISCUSSION

5.1 *Advantages of IoT in India: A Decadal Outlook*

5.1.1 Economic Scale and Market Expansion

Despite disagreeing on the specifics, market-intelligence estimates line up on one point: India's IoT sector is set for sustained, high double-digit growth through the mid-2030s, pushed along by industrial digitalisation, smart metering, and a steadily rising number of connected devices (Grand View Research, 2025a; IMARC Group, 2026; Ken Research, 2026; Orion Market Research, 2025). Seen through a Diffusion of Innovation lens, this looks like a market moving out of its early-adopter phase and into early-majority territory most visibly in industrial and urban-infrastructure applications, where the case for adoption is clearest and fits best with what firms already have in place.

5.1.2 Smart Urban Infrastructure and Governance

The Smart Cities Mission has already built up a fair amount of groundwork Integrated Command and Control Centres, IoT-linked traffic and surveillance systems, SCADA-monitored water networks, all spread across 100 cities that later IoT projects can build on rather than start from zero (Government of India, Ministry of Housing and Urban Affairs, 2015). In TOE terms, this counts as a genuinely favourable environment: established regulatory backing and inter-agency coordination that lowers the bar considerably for the next round of municipal IoT projects.

5.1.3 Industrial Automation and Connectivity Acceleration

As 5G networks spread and domestic chip-design efforts mature, hardware costs and network latency should both come down, which in turn should speed up industrial and automotive IoT adoption (Grand View Research, 2025b; IMARC Group, 2026). That directly improves the technological side of the TOE equation both the relative advantage and the fit with existing systems for manufacturing and logistics firms weighing whether IoT investment is worth it.

5.1.4 Agricultural and Healthcare Transformation

Precision-irrigation sensors, livestock and cold-chain monitoring, and remote patient-monitoring devices sit among the highest-value applications here, given how directly they speak to India's rural resource management and healthcare-access problems (Dahiya, 2022; Narwane et al., 2022). But these are also the two domains facing the heaviest compounding barriers, which Section 5.2 gets into so their near-term growth prospects are genuinely more uncertain than the industrial or urban picture above.

5.1.5 Energy and Utility Modernisation

Smart-metering rollout under the RDSS, together with the broader National Smart Grid Mission, positions IoT as central to cutting transmission losses, managing demand

more flexibly, and integrating renewable energy (Kappagantu & Daniel, 2018; Ken Research, 2026). This sector is a good illustration of a mismatch within the TOE framework: strong policy-level support sits next to comparatively weak readiness at the consumer and utility levels a tension picked up again in Section 5.2.

5.1.6 A Maturing Regulatory Foundation

For the first time, India now has an enforceable, internationally comparable data-protection framework through the Digital Personal Data Protection Rules, 2025 something a good deal of earlier IoT literature flagged as simply missing (Government of India, Ministry of Electronics and Information Technology, 2025). Once fully phased in by May 2027, this has real potential to turn what has long been a barrier into something closer to an advantage, by giving institutions and consumers more reason to trust how their IoT-generated data is handled.

5.2 *Delimitations and Persistent Challenges*

5.2.1 Cybersecurity Exposure

IoT's spread-out architecture, mixed device standards, and in plenty of real deployments outdated firmware together mean the attack surface keeps growing faster than security practice can keep up. This isn't confined to one sector: it shows up in waste management (Mishra et al., 2022), agriculture (Narwane et al., 2022), and healthcare (Dahiya, 2022; Kirubakaran et al., 2023) alike, which suggests cybersecurity is less a sector-specific problem than a general one running underneath all of them.

5.2.2 Regulatory Implementation Lag

The DPDP Act and Rules exist now, but full compliance is staggered out through May 2027, and enforcement capacity, IoT-specific guidance, and clarity on cross-border data flows are all still works in progress rather than settled matters (Government of India, Ministry of Electronics and Information Technology, 2025). That leaves a multi-year stretch where the regulatory side of TOE's environmental context is only partly favourable, even though the framework technically exists.

5.2.3 Workforce and Skill Shortages

A shortage of people who understand IoT architecture, data analytics, and cybersecurity comes up again and again across sector studies healthcare, agriculture, waste management as a major reason deployments stall at the pilot stage instead of scaling up (Mishra et al., 2022; Narwane et al., 2022). In TOE terms, this is an organisational constraint that doesn't just go away because the technology or the regulation improves.

5.2.4 Cost and Interoperability

High upfront costs for sensors, connectivity, and systems integration, combined with a lack of shared interoperability standards across vendors, tend to hit small and medium enterprises harder than the large, well-funded organisations that can absorb these costs more easily (Narwane et al., 2022). The energy sector tells a similar

story from the consumer side: Archana (2022) found that what actually held Indian consumers back from accepting smart-grid technology wasn't unfamiliarity with the tech, but the absence of clear monetary benefit and supportive government policy.

5.2.5 The Rural–Urban Digital Divide

IoT needs steady connectivity and reliable power to function, which runs straight into India's well-documented broadband gap roughly 93% penetration in urban areas against about 29.3% in rural ones (Shruthi et al., 2021). COVID-19 narrowed that gap somewhat (Indu et al., 2022), but the underlying infrastructure and literacy problems are still largely there, which means the applications with arguably the highest social value precision agriculture, rural telemedicine are also the ones operating in the least favourable connectivity conditions of any domain covered here.

5.2.6 Environmental Sustainability and E-Waste

Every new wave of sensors, gateways, and connected devices adds to a growing pile of hardware that eventually has to be disposed of somehow, and end-of-life device management remains an under-addressed problem. Given that even engineering students show limited awareness of e-waste practices (Mor et al., 2021), there's little reason to expect this constraint to resolve on its own if anything, it looks set to get worse before any deliberate policy response catches up.

5.2.7 Uneven Adoption Across Application Areas

Structural-equation-model evidence suggests Indian IoT adoption is still concentrated in a fairly narrow set of applications rather than spread broadly (Mital et al., 2018), which lines up with what Diffusion of Innovation theory would predict at this stage early-majority diffusion tends to lag well behind the early adopters. That's a useful check on the market-growth numbers cited in Section 5.1.1: the aggregate figures may be hiding a fair amount of unevenness across sectors, firm sizes, and regions.

6. SYNTHESIS: INDIA'S IOT TRAJECTORY, 2025–2035

Put the advantage and delimitation findings side by side, and read through TOE and DOI, and a fairly consistent picture emerges: India's IoT decade probably won't be one of even, market-wide adoption. It looks more like a two-speed process. Large enterprises, government-backed smart-city projects, and well-funded industrial and automotive applications are best placed to capture near-term growth they benefit from a favourable technological environment (better connectivity, falling hardware costs) and a favourable regulatory environment (established sponsorship, smart-city precedent to build on). Agriculture, rural healthcare, and small-enterprise manufacturing arguably where the social payoff would matter most come out worse on all three TOE dimensions: weaker organisational readiness in terms of skills and capital, a less developed technological environment because of the rural digital divide, and thinner policy support relative to the flagship urban programmes.

The DPDP framework's phased rollout through 2027 sits right in the middle of this decade and matters a great deal. How well it's actually enforced, and whether its provisions get extended clearly to IoT-specific device telemetry, inferences drawn from sensors, cross-border industrial data will largely decide whether cybersecurity and privacy stay a persistent weak spot or turn into something India can actually compete on by 2035. Much the same goes for rural connectivity investment: how far programmes like BharatNet actually reach will determine whether agriculture and rural healthcare IoT move past pilot projects and into the kind of early-majority adoption already visible in cities and factories.

On the whole, the evidence supports cautious optimism with a fairly firm condition attached: India's overall IoT market growth is well supported and likely to happen in some form, but how that growth gets distributed across sectors, firm sizes, and regions depends a lot more on deliberate work building organisational capacity, following through on regulation than on technological momentum carrying things forward by itself.

7. THEORETICAL AND PRACTICAL IMPLICATIONS

On the theoretical side, this review backs up the idea that IoT adoption in India is best understood as a socio-technical issue rather than a purely technological one. The fact that organisational factors (skills, cost, capital) and environmental factors (regulatory maturity, policy incentives, connectivity) rather than what the devices themselves can do keep showing up as the real constraints across independent sector studies gives some empirical weight to using the TOE framework in emerging-economy IoT settings, and suggests future adoption research should give institutional and infrastructural readiness at least as much weight as technical capability.

Practically, four things stand out. Policymakers should push out sector-specific guidance under the DPDP Rules for IoT device and telemetry data well before the 2027 deadline, rather than letting the interim period drift into a de facto regulatory gap. Industry should focus on interoperability standards and financing models that bring IoT within reach of small and medium enterprises and farmers, not just large industrial players. Educational institutions should build out IoT-specific training covering architecture, analytics, and cyber security to close the skills gap before it starts holding back the growth that market analysts are currently projecting. And rural connectivity investment needs to happen alongside agricultural and healthcare IoT programme design, not after it, given how much the digital divide compounds everything else discussed in Section 5.2.5.

8. POLICY RECOMMENDATIONS

- Issue IoT-specific guidance under the DPDP Rules covering device telemetry, sensor-derived data, and cross-border industrial data transfer, well ahead of the May 2027 compliance deadline.

- Set minimum interoperability and security-by-design standards for IoT devices used in publicly funded smart-city, smart-grid, and healthcare programmes, to cut down on vendor fragmentation.
- Extend the financing and subsidy support currently available mostly to large industrial adopters to small and medium enterprises and farmer collectives, to address the cost gap identified in Section 5.2.4.
- Plan rural broadband and reliable-power investment (BharatNet and similar programmes) alongside agricultural and healthcare IoT rollout, rather than treating connectivity and application deployment as two separate problems.
- Build out extended producer responsibility enforcement and public awareness specifically around IoT device disposal, before e-waste volumes reach the scale already seen in general ICT hardware.
- Fund IoT-specific vocational and higher-education programmes in partnership with industry, aimed squarely at the architecture, analytics, and cybersecurity skills gaps identified across the sector studies reviewed here.
- Device-level empirical research on IoT-specific e-waste volumes and disposal practices, building on the general ICT e-waste literature discussed in Section 3.10 but focused on IoT hardware specifically.
- Mixed-methods work combining this paper's qualitative synthesis with quantitative structural equation modelling, to test which matters more organisational or environmental TOE factors in actual Indian IoT adoption decisions.

11. CONCLUSION

Over the next decade, India's IoT story looks set to be one of real opportunity running up against equally real constraints. The opportunity spans smart urban infrastructure, industrial digitalisation, agriculture, healthcare, and energy; the constraints show up as cybersecurity gaps, a regulatory framework still being phased in, workforce shortages, cost and interoperability problems, a persistent rural–urban divide, and an e-waste question nobody has quite answered yet. Read through TOE and Diffusion of Innovation, the evidence points toward an uneven, two-speed diffusion path cities, industry, and large firms moving well ahead of rural areas, agriculture, and small enterprises. The recent move to operationalise the Digital Personal Data Protection framework is a meaningful step toward closing a gap this literature has flagged for years, even if it hasn't fully proven itself yet. In the end, how fast and how fairly IoT spreads across India by 2035 will probably come down less to whether the technology is available it largely already is and more to whether the institutions, skills, connectivity, and security practices needed to support it get built at the same pace.

REFERENCES

- Archana. (2022). Smart grid technology acceptance barriers: Indian consumers perspective. *Strategic Planning for Energy and the Environment*, 42(1), 79–100.
- Ashton, K. (2009). That 'Internet of Things' thing. *RFID Journal*, 22(7), 97–114.
- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805.
- Bajaj, P., Almagari, F., Tabash, M. I., Alsyani, M., & Saleem, I. (2021). Factors influencing consumer's adoption of internet of things: An empirical study from Indian context. *International Journal of Business Innovation and Research*, 24(3), 315–338.
- Dahiya, N. (2022). IoT driven healthcare system for remote monitoring of patients. *Voyager*, 12, 40–48.
- Desingh, V., & Baskaran, R. (2022). Internet of Things adoption barriers in the Indian healthcare supply chain: An ISM-fuzzy MICMAC approach. *International Journal of Health Planning and Management*, 37(1), 318–351.

9. LIMITATIONS OF THE STUDY

Being a qualitative review built from secondary sources, this study doesn't generate new primary evidence, and it's only as good as the sources it draws on India's market and regulatory situation is moving fast enough that some of the figures here may well look dated before the decade this paper covers is over. The market-size estimates cited vary a fair amount across commercial firms, given how differently they define scope and methodology, which is why they're presented here as rough ranges rather than firm forecasts. The review is also confined to India-specific literature and doesn't attempt cross-country comparison, and the thematic coding while structured through a clear two-stage process and guided by established adoption theory remains an interpretive exercise rather than something statistically validated, which is normal for qualitative documentary work but different from what multi-rater content analysis would offer.

10. DIRECTIONS FOR FUTURE RESEARCH

- Primary, cross-sector survey research testing the TOE and DOI ideas discussed here against real firm-level and household-level adoption data, once the DPDP Rules reach full compliance in 2027.
- Longitudinal tracking of the rural–urban IoT adoption gap specifically, rather than general internet-connectivity tracking, to see whether agricultural and healthcare IoT actually follows the same path as urban industrial IoT or falls structurally behind.
- Comparative work placing India's regulatory and adoption trajectory alongside other large emerging economies that have recently brought in their own data-protection regimes.

- Government of India, Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025.
- Government of India, Ministry of Housing and Urban Affairs. (2015). Smart Cities Mission.
- Grand View Research. (2025a). India industrial internet of things market size & outlook, 2030.
- Grand View Research. (2025b). India 5G internet of things (IoT) market size & outlook, 2030.
- IMARC Group. (2026). India Internet of Things market size, share & forecast, 2034.
- Indu, Thadikaran, G. B., & Chellaswamy, K. P. (2022). Bridging digital divide in India: Positive outlook amid COVID-19. *Prabandhan: Indian Journal of Management*, 15(6), 46–56.
- Kappagantu, R., & Daniel, S. A. (2018). Challenges and issues of smart grid implementation: A case of Indian scenario. *Journal of Electrical Systems and Information Technology*, 5(3), 453–467.
- Ken Research. (2026). India Internet of Things market share, companies & trends report, 2025–2032.
- Kirubakaran, S. J., Gunasekaran, A., Dolly, D. R. J., Jagannath, D. J., & Peter, J. D. (2023). A feasible approach to smart remote health monitoring: Subscription-based model. *Frontiers in Public Health*, 11, 1150455.
- Mishra, A. R., Rani, P., Saha, A., Hezam, I. M., Pamucar, D., Marinovic, M., & Pandey, K. (2022). Assessing the adaptation of Internet of Things (IoT) barriers for smart cities' waste management using Fermatean fuzzy combined compromise solution approach. *IEEE Access*, 10, 37109–37130.
- Mital, M., Chang, V., Choudhary, P., Papa, A., & Pani, A. K. (2018). Adoption of Internet of Things in India: A test of competing models using a structured equation modeling approach. *Technological Forecasting and Social Change*, 136, 339–346.
- Mor, R., Sangwan, K. S., Singh, S., Singh, A., & Kharub, M. (2021). E-waste management for environmental sustainability: An exploratory study. *Procedia CIRP*, 98, 193–198.
- Narwane, V. S., Gunasekaran, A., & Gardas, B. B. (2022). Unlocking adoption challenges of IoT in Indian agricultural and food supply chain. *Smart Agricultural Technology*, 2, 100035.
- Orion Market Research. (2025). India Internet of Things (IoT) market size, share & trends analysis report, 2026–2035.
- Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.
- Shruthi, K. A., Ihita, G. V., & Chaudhari, S. (2021). A survey on rural internet connectivity in India. *arXiv preprint arXiv:2111.10219*.
- Tornatzky, L. G., & Fleischer, M. (1990). *The processes of technological innovation*. Lexington Books.