TRANSFORMA INSIGHTS

The Intelligent Last Mile: How networks must leverage AI to address the evolving needs of IoT

White Paper

July 2026

Sponsored by:

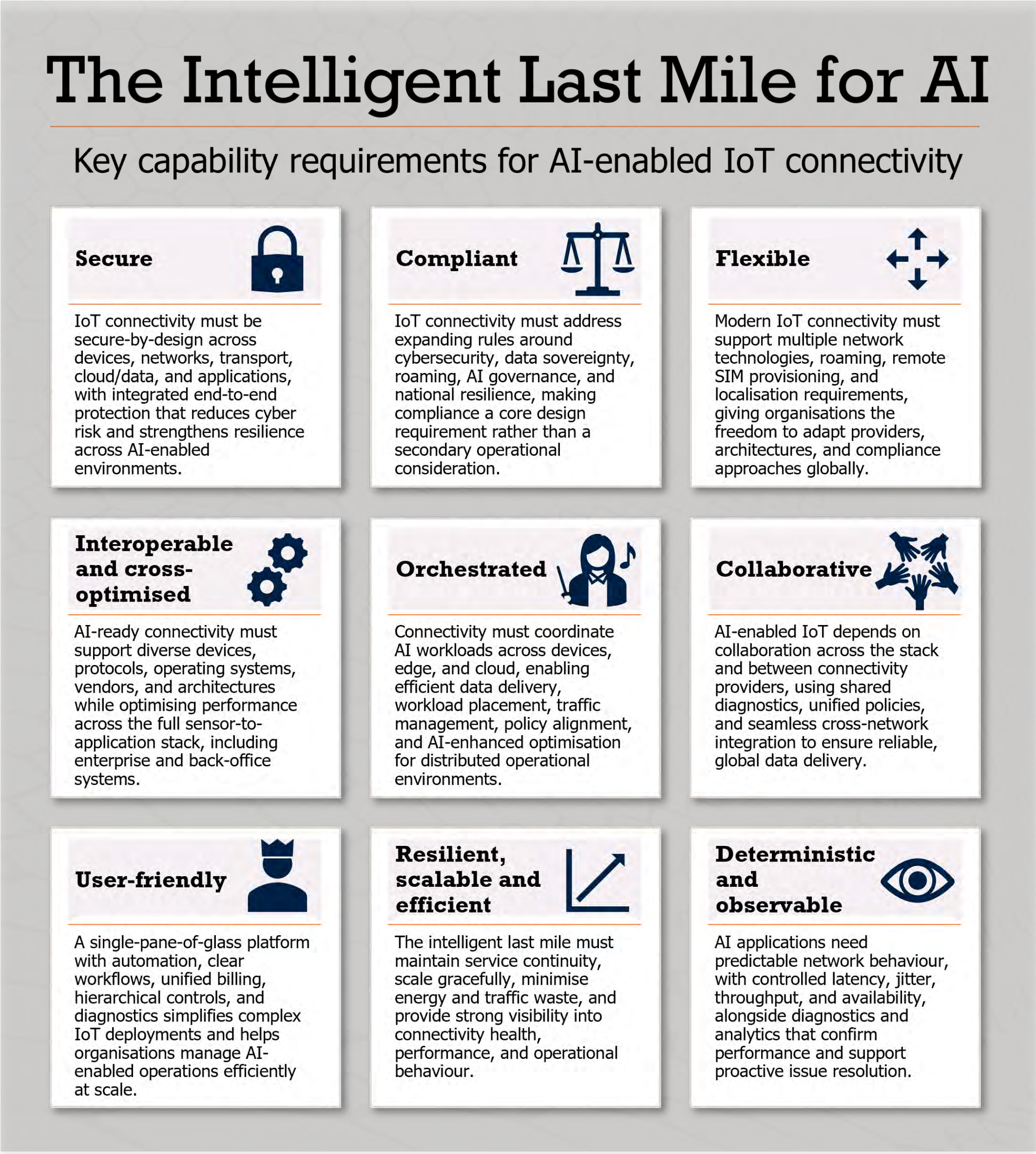
TATA COMMUNICATIONS

Executive Summary

This report outlines how the convergence of Artificial Intelligence and the Internet of Things is reshaping data requirements, infrastructure needs, and operational models. AI's dependence on real-world data elevates the role of connected devices, while the rise of AIoT is accelerating the shift of intelligence toward the edge. This creates increased pressure on connectivity to manage larger data volumes, stricter latency demands, and more complex regulatory and security environments. At the same time, organisations seeking to monetise AI are turning to IoT to create tangible services and improved efficiency, reinforcing the strategic value of optimised connectivity.

The report finds that IoT connectivity must evolve significantly to meet these new requirements. Next-generation solutions must be designed to be secure across all layers, compliant with fast-moving regulatory frameworks, and flexible enough to operate across global networks and multiple technologies. They must also support deep interoperability across heterogeneous device fleets, orchestrate distributed AI workloads between edge and cloud environments, and enable collaboration across the IoT stack and between connectivity providers. In addition, platforms must become more user-friendly through unified management, automation, and operational simplification. These capabilities collectively define the "Intelligent Last Mile" required for AI-enabled IoT systems.

The sections of the report examine: the growing interdependence of AI and IoT; the challenges of delivering data for AI; the functional requirements of the Intelligent Last Mile, including security, compliance, flexibility, interoperability, orchestration, collaboration, usability, resilience, scalability, efficiency, determinism, and observability; and a worked example showing how these principles apply to connected cars.



AI: a driver of demand for IoT

Artificial Intelligence (AI) and the Internet of Things (IoT) are two of the most impactful and far-reaching technology developments of our time. The need to support AI's inexhaustible thirst for data is driving greater value in IoT, as is AI's application to numerous use cases involving connected devices.

IoT is where AI interfaces with the physical world

The rise of artificial intelligence is tightly connected to the expansion of the Internet of Things. IoT supplies the real-world data that AI systems depend on, enabling uses ranging from predictive maintenance to smart infrastructure. It is the "eyes and ears" of AI. It also provides the mechanisms through which AI-driven decisions are executed, including driverless cars, autonomous robotics, industrial automation, and adaptive energy systems.

Because IoT bridges physical environments and digital platforms, it is positioned to support many of the most influential applications of AI. Adding AI to connected devices strengthens their value, and many organisations are embedding advanced capabilities directly into hardware to enhance functionality and open new service models. Adoption of AI within IoT devices is expected to increase rapidly, influencing product planning, software design, and market structure.

As AI and IoT continue to converge, demand for dependable and scalable connectivity will grow. This convergence also introduces new compliance and governance requirements. Rules related to sovereignty, data location, and sector-specific oversight determine how IoT data can be gathered, transmitted, and processed. Connectivity strategies must therefore meet performance expectations while aligning with these evolving constraints. In many contexts, AI must be operated within national boundaries, supported by distributed network nodes that manage processing at the appropriate points to balance latency and scalability.

AI workloads will also require compute resources positioned across multiple layers, including device-level processing, edge sites, and cloud environments. Coordinating data storage and processing across these locations calls for more sophisticated orchestration.

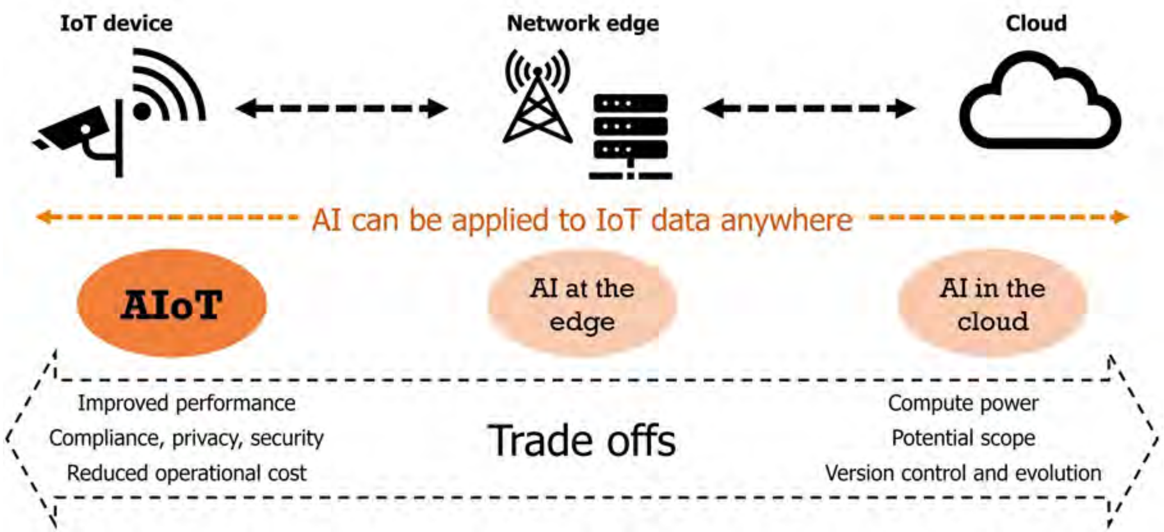
Given these trends, IoT connectivity providers play a central role in enabling an AI ecosystem that is inherently distributed and dependent on scalable compute. Meeting these requirements demands flexible, scalable architectures built on cloud-native principles.

AIoT: the next paradigm

As well as the synergistic ways in which AI and IoT interact as noted above, increasingly these two technologies are deployed together and the term 'AIoT' has come to the fore.

When we refer to 'AIoT' we mean specifically the deployment of AI use cases on board IoT devices. Applying AI to IoT data on board the source IoT devices can bring significant benefits, including improved performance, enhanced compliance, privacy and security and potentially reduced operational costs. In contrast, applying AI to IoT data in cloud locations allows for access to the greater compute power that is typically available in edge locations, as well as simplified AI application management. In many cases, AIoT (i.e. AI deployed on board IoT devices) does not exist in isolation and often AIoT devices may generate data that is further processed using potentially more sophisticated AI algorithms either in cloud or edge locations (or both).

Figure: AIoT: The convergence of AI and IoT
[Source: Transforma Insights, 2025]



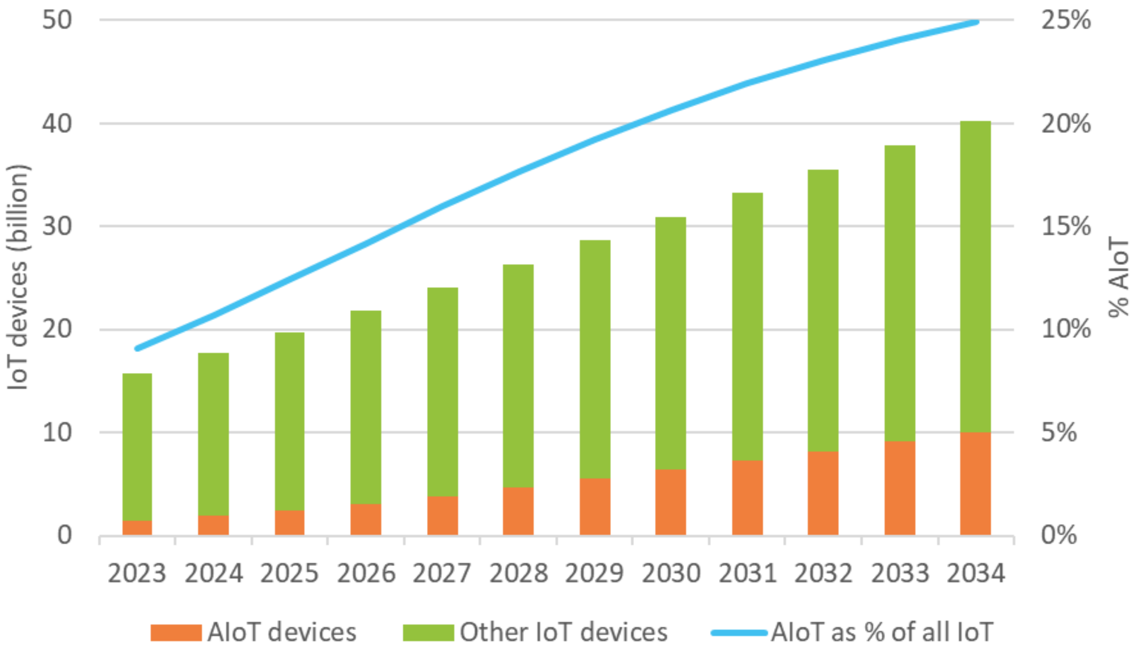
AI: a driver of demand for IoT

The potential for AIoT is significant. Transforma Insights forecasts that total AIoT connections will grow from 1.9 billion at the end of 2024 to exceed 10 billion at the end of 2034. This is a more than 5-fold growth in 10 years.

For context, we forecast a total of 40 billion IoT devices at the end of 2034, up from 18 billion at the end of 2024. Accordingly, as illustrated below, we forecast that 11% of IoT devices will have onboard AI in 2024, rising to 25% in 2033. The rate of growth of AIoT penetration of IoT devices slows towards the end of the forecast period, primarily due to the AIoT penetration of key IoT applications reaching saturation.

Figure: AIoT device share of IoT

[Source: Transforma Insights, 2025]



IoT as a mechanism for monetising AI

Many organisations are investing heavily in advanced models and automated analytics, yet many struggle to turn these deployments into measurable commercial returns. AI programmes often begin as experimental initiatives without clear pathways to productisation, resulting in high development costs and limited adoption. Fragmented data, unclear ownership, and integration challenges also slow progress, making it difficult to embed intelligence directly into workflows or customer-facing offerings. As a result, companies frequently see value in improved insights but not in sustained revenue growth or meaningful operational transformation.

The combination of AI with connected devices presents a more direct route to monetisation. When intelligence is embedded in equipment, infrastructure, or consumer hardware, it creates opportunities for new service-based business models. These may include performance optimisation services, remote diagnostics, predictive maintenance, or pay-as-you-use frameworks. By grounding AI in real-time operational data, organisations can build offerings that deliver tangible outcomes rather than abstract analytics, making it easier to justify pricing and demonstrate clear value to customers.

Pairing AI with IoT also supports differentiation and efficiency gains. Devices that adapt, learn, or automate complex tasks can reduce operating costs while enhancing user experience and product capability. These improvements strengthen loyalty, raise switching barriers, and support premium positioning in competitive markets. At the same time, better utilisation of assets and streamlined operations help companies realise internal savings. The integrated use of AI and IoT therefore enables both improved financial performance and stronger competitive advantage, addressing many of the monetisation challenges that standalone AI efforts struggle to overcome.

An example: AI-enabled video analytics

One particularly prominent IoT use case that is set to draw heavily on AI and edge computing is video analytics. The use of video monitoring solutions has unlocked significant improvements, from round-the-clock surveillance for security purposes to object detection, gesture detection, facial recognition, and motion tracking across industries to gain real-time business insights and prescriptive analysis.

Using video analytics, businesses can unlock greater value by analysing spatial and temporal information, provide instant alerts in the event of anomaly detection, and take actions in real-time. Transforma Insights sees this as a key enhancement and in some cases replacement for traditional IoT sensors. There is a growing range of video analytics solutions that can replace functions that would historically have been handled by sensors, in most cases enabled by AI.

The challenge of delivering IoT data for AI

The provision of IoT connectivity is becoming increasingly complex. In part this is due to the growing demand for the delivery of large volumes of data, with low latency, in a compliant and secure manner. In part this is driven by the accelerating demands of AI, but it applies also more broadly across all aspects of connectivity for IoT.

The data wave

The growth of AI, as well as the increasing use of IoT for critical systems, drives an increasing volume of data with greater demands for low latency and local data management:

- Volume of data – Device fleets produce rising quantities of information as sensing capabilities increase and applications demand richer inputs. High-frequency sampling, video streams, and complex telemetry contribute to sustained growth that challenges transmission, storage, and processing capacity.
- Latency – Time-sensitive applications depend on rapid data movement. Automated control, operational safety systems, and real-time analytics require pathways that minimise delay. Latency becomes a defining factor for system quality as AI models rely on immediate context.
- Requirements for local data management – Local processing is increasingly necessary for performance, resilience, and compliance. Edge compute supports rapid inference and reduces backhaul demand. Jurisdictional and sector-specific rules also require data to be stored and processed within defined geographic or organisational boundaries.

In particular, the increasing use of 5G should drive larger volumes of data and the ability to support low latency connectivity, necessitating local data management.

Security and compliance rules

Security consistently ranks as one of the top challenges when deploying IoT. There are numerous examples of security breaches and the threat landscape continues to become ever more challenging. Threats range from device tampering and credential theft to network intrusion and manipulation of data streams. The importance of security becomes ever more pronounced with the increasing integration of AI for automated and critical systems.

IoT devices have always been somewhat more vulnerable to hacking by virtue of being deployed in unattended environments, and often deployed in complex combinations of technologies and stakeholders, all of which represent a potential weak point in the security chain. The widespread deployment of IoT in various consumer and enterprise applications opens up more hacking opportunities, and IoT is being used in increasingly critical systems. The scale of deployments continues to rise, with Transforma Insights predicting that IoT connections will grow from 16 billion IoT devices in 2023 to 41 billion in 2034. The diversity of IoT also represents a challenge, necessitating enterprise security specialists to understand the security risks of a wider range of devices than simply phones, PCs and other IT infrastructure. The challenges have increased in recent years with the evolution in IoT devices; for instance, there is an ongoing trend for IoT devices to become increasingly constrained in terms of processing, memory, and power, reducing their ability to support robust security features and updates.

Global regulatory frameworks – particularly related to security – continue to expand and diverge. Data sovereignty shapes where information is allowed to reside. Restrictions on permanent roaming influence how cross-border devices are provisioned and managed. Cybersecurity mandates require stronger controls on authentication, encryption, and device integrity. AI oversight introduces requirements related to risk classification, transparency, and operational assurance. Together, these factors create a fragmented compliance landscape that organisations must navigate when delivering IoT data.

Complexity of the stack

The technology landscape for IoT continues to evolve at pace, with new network technologies, protocols, operating systems and functions coming on stream with unerring regularity. While for the most part the evolution provides increasingly sophisticated tools for delivering IoT, the complexity of the stack can be daunting for enterprises looking to deploy IoT. For instance:

The challenge of delivering IoT data for AI

- Connectivity – Device estates rely on a mix of communication modes that range from low-power networks to terrestrial broadband and satellite links. Each option has distinct characteristics related to coverage, throughput, and reliability. Coordinating these modes within a unified framework increases operational complexity.
- Operating systems – A wide variety of embedded operating systems supports different hardware profiles and application needs. Ensuring secure updates, managing long-term maintenance, and achieving interoperability across this diversity add to system complexity.
- Protocols – Multiple data exchange protocols coexist across industries and use cases. They differ in reliability, efficiency, and security features. Harmonising these protocols and maintaining compatibility over time requires sustained engineering effort.

Other challenges

Beyond those noted above there are numerous other challenges with delivering IoT data:

- Power management - Many devices operate in remote or constrained environments, where power efficiency is essential. Data transmission is often the most energy-intensive function, creating tensions between data needs, device longevity, and operational cost.
- Reliability and resilience – IoT solutions must operate across varied physical environments, from industrial sites to public infrastructure. Ensuring consistent performance despite intermittent connectivity, harsh conditions, or hardware degradation adds significant engineering challenges.
- Lifecycle and fleet management – Large deployments require coordinated provisioning, monitoring, diagnostics, and retirement of devices. As AI capabilities evolve, devices may also need new inference models or updated firmware, increasing the importance of scalable and secure over-the-air management.
- Interoperability – Growing diversity across vendors, platforms, and standards increases the risk of fragmentation. Achieving seamless integration across components and ecosystems becomes essential for reliable data flow and successful AI outcomes.

The ‘Intelligent Last Mile’ for AI

In order to support the growing demands of AI, as well as IoT more broadly, connectivity needs to evolve to be ultra-efficient, compliant, secure, and flexible. In this section we address the key capability requirements of an IoT connectivity solution.

Secure

The best mechanism for addressing the growing security threat is to adopt a ‘Secure-by-Design’ approach which considers all elements of the IoT application holistically, as well as giving careful consideration of the overall approach to security.

When discussing IoT security, we refer to the protection measures across the various components involved in IoT deployments, which are complex and include devices, networks, platforms, applications, and enterprise systems. There are five main security layers:

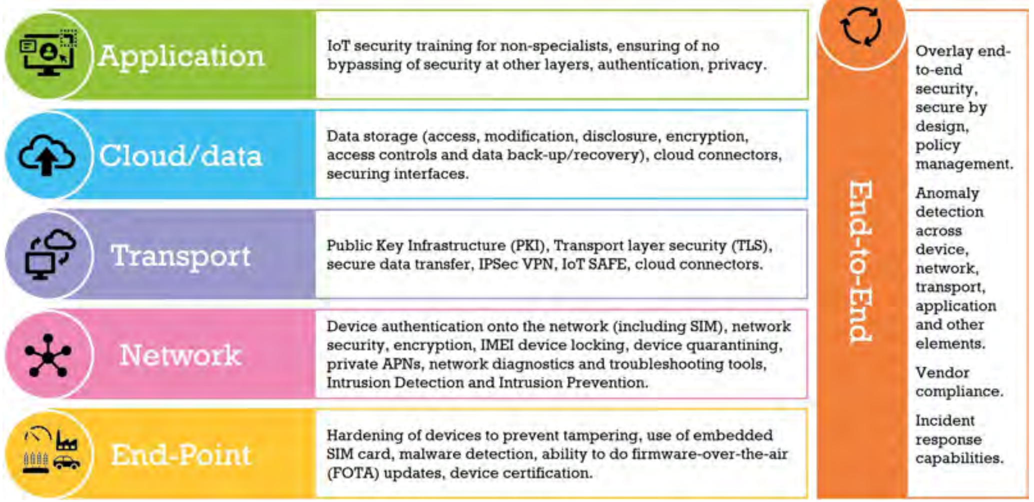
- End Point: The primary focus is securing the device itself. Hardening the device to prevent tampering is crucial, including the use of embedded SIM cards (eSIMs) that cannot be removed. Devices should also support Firmware Over-The-Air (FOTA) updates, which require adequate network technologies, storage, and processing capabilities. Detecting malware is essential at this layer. Securing the credentials by storing them in GSMA standardized IoT SAFE (IoT SIM Applet For Secure End-to-End Communication) on the SIM/eSIM further strengthens security at the end-point level.
- Network: Network security is generally robust, particularly on mobile networks, but vulnerabilities still exist. IoT applications often span multiple networks, including the public internet, increasing the risk of exploits. Key security measures include device and SIM authentication, network encryption, private APNs, network diagnostics, IMEI locking, quarantining devices, DNS white-listing, DoS/DDoS protection, and the deployment of Intrusion Detection and Prevention Systems (IDS/IPS).
- Transport: Network layer security may be insufficient alone. Transport Layer Security (TLS) is often required, particularly by cloud providers, to secure data delivery. Typical measures include IPsec VPNs and private global backbones. IoT SAFE, a GSM Association initiative, uses the SIM card for secure end-to-end communication, ensuring mutual authentication and TLS.
- Cloud/Data: Security measures are necessary regardless of whether data is stored in the cloud or on-premises. This includes preventing unauthorized access, encryption, access controls, and data backup/recovery. Cloud security for IoT also involves managing credentials, access control, and device SDKs, as well as addressing vulnerabilities in interfaces, APIs, and potential data breaches. Zero Trust Network Access (ZTNA) implementation further protects the data in cloud by allowing access to only authenticated and authorized endpoints and by creating micro-segmentation of the cloud application that divides network into small, isolated zones to enforce strict, granular access and improving the breach containment.
- Application: Application security is critical as many vulnerabilities arise from poorly built applications. Developers must prioritize security, ensuring authentication and data privacy are integrated into the application design.

Additionally, we identify a sixth aspect: End-to-End security. This considers the entire system, integrating all layers to optimize protection. This includes secure application design, anomaly detection across layers, third-party vendor compliance, and robust incident response capabilities to manage cyber threats effectively. These layers of IoT security are presented in the chart below.

The IoT security landscape is evolving rapidly. The nature and scale of the threats are changing, as is the regulation that is being introduced to cope with it. Approaches from providers of IoT connectivity are also evolving, and ideally should embrace the multi-level model presented in the previous section, including consideration of end-to-end security.

Figure: Layers of IoT security

[Source: Transforma Insights, 2026]



The 'Intelligent Last Mile' for AI

Compliant

Regulatory compliance has long been part of IoT through device certification and safety requirements. However, as IoT increasingly supports critical infrastructure and sensitive applications, regulations are expanding in scope and complexity, particularly around security, data sovereignty, and AI. Compliance is therefore becoming a core element of IoT connectivity rather than a secondary concern.

Recent years have brought major regulatory developments covering security, data management, permanent roaming, national resilience, and AI.

Security regulations have evolved from voluntary guidelines to mandatory standards. In the UK, the 2018 Code of Practice for Consumer IoT Security was replaced in 2024 by the Product Security and Telecommunications Infrastructure Act, requiring measures such as banning default passwords, providing software updates, and implementing vulnerability disclosure policies. Similar approaches are emerging globally. In the US, the IoT Cybersecurity Improvement Act of 2020 introduced minimum security standards for federal IoT devices, while NIST's Cybersecurity Framework 2.0 added stronger supply chain risk guidance. Additional US initiatives include consumer disclosure requirements and the Cyber Trust cybersecurity label.

Data management and sovereignty rules are also reshaping IoT. The EU Data Act establishes rules for access, sharing, and international transfer of IoT-generated data while strengthening transparency and privacy protections. It also requires IoT providers to make generated data available to device owners for their own use or sharing with third parties.

Permanent roaming and eSIM regulation remain significant challenges. Many countries restrict continuous roaming by foreign devices due to tax, registration, and security concerns. Emerging eSIM and KYC requirements add further complexity, with non-compliance risking disconnection of IoT fleets. Providers are responding with compliance tools, multi-IMSI solutions, and eSIM localisation.

Alongside these broad frameworks, many sectors face vertical-specific regulations covering areas such as eCall systems, environmental monitoring, energy efficiency, and supply chain transparency.

AI regulation is also developing rapidly. Although relatively little legislation is fully in force, activity is increasing worldwide. The EU AI Act is the most advanced framework, while many countries have issued AI strategies, codes of practice, and guidelines.

Finally, geopolitical tensions are driving national resilience regulations aimed at protecting critical infrastructure. Examples include the EU's NIS2 Directive and US restrictions on equipment from certain foreign vendors.

Together, these developments show that IoT systems must increasingly be designed to meet evolving regulatory requirements and geopolitical risks, even though the practical impact of many new rules is still emerging.

Flexible

The mechanisms for delivering global (cellular-based) IoT connectivity have evolved significantly in the last decade. The prevailing approach then was to use a plastic removable SIM card connected via roaming to a largely undifferentiated 2G or 4G network. Since then there have been numerous technological developments including the soldered SIM card and the associated remote SIM provisioning for managing the connectivity, and the increasing availability of network technologies optimised for various aspects of IoT, including NB-IoT, LTE-M, and 5G Standalone (5G SA). The profusion of different technologies is certainly helpful for addressing the needs of IoT, but it does present some complexity. Helping enterprises to choose between the technologies on offer, and providing the freedom to switch, is a critical aspect of intelligence in the IoT last mile.

The most recent development in managing cellular-based connectivity is the arrival of the SGP.32 'IoT' standard for remote SIM provisioning. This builds on a couple of previous standards, expanding the capabilities and driving more flexibility for adopters. Nominally this change means that every enterprise customer with SGP.32-capable devices is dramatically more footloose than they were previously, with the ability to 'at the click of a button' move some or all of their connections from one network to another. And, furthermore, it enables greater abilities to comply with localisation requirements in markets – or for networks – that prohibit permanent roaming. As such the flexibility provided by SGP.32 is on another level compared to previous approaches, where there was inevitably a greater level of 'lock-in' with the connectivity provider. However, we should note, SGP.32 is not in itself a 'magic wand' and there is more to managing IoT connections than just managing the eSIM profile, for instance related to the provision of end-to-end SLAs, or APN management.

Furthermore, we should note that SGP.32 does not necessarily represent the only approach that might be taken to delivering multi-network connectivity. Roaming still has a place, as does the use of multi-IMSI technology, or even the earlier RSP technologies. Ideally an IoT connectivity proposition should offer the full suite and the flexibility to select between them as appropriate for the customer.

Interoperable and cross-optimised

A truly holistic 'last mile' for AI incorporates a wide variety of deployment environments, including in-building, highly remote, and globally distributed. It also includes a highly heterogeneous fleet of devices each with their own capabilities and requirements, for instance for processing, power consumption or data throughput. As such, the broad spectrum of IoT deployment types needed for supporting AI harnesses a wide range of operating systems, protocols, and architectures (including deployments in cloud or edge environments). As such, the provision of the intelligent last

The 'Intelligent Last Mile' for AI

mile must be sufficiently interoperable to manage devices with a wide range of characteristics, and which therefore make use of different network technologies, protocols, operating systems and architectures. Furthermore, it must also be interoperable between the various vendors of devices, networks, and other functions including such capabilities as eSIM management.

Similarly, Transforma Insights sees an increasing focus on the cross-optimisation of the various functions of an IoT solution from sensor to gateway to network to cloud to application. There is an increasing recognition that any solution needs to give careful consideration to the requirements and capabilities of all of the other constituent elements of the application from 'device-to-cloud' (or, probably more accurately, sensor-to-application). Additionally it would include integration with ERP/CRM and other back-office systems.

Orchestrated

A next-generation connectivity proposition must be designed to support AI workloads that span devices, edge environments, and central cloud platforms. As applications depend on rapid decision cycles, richer contextual data, and increasing autonomy, the network becomes a key determinant of how information is transported and where computation takes place. Local inference often requires proximity to the data source to minimise latency and reduce transport overhead, while larger-scale training and aggregation continue to rely on central facilities. Supporting this distribution requires a connectivity layer that can deliver data efficiently and predictably across all tiers of the architecture.

The expansion of edge processing places new emphasis on close coordination between local compute and network behaviour. Connectivity must provide stable performance for time-critical inference, maintain synchronisation with cloud-based models, support selective upstreaming of relevant outputs, and adapt to varying network conditions. This demands flexible traffic management, intelligent routing, and the ability to operate across heterogeneous networks. It also requires seamless integration with operational systems such as billing, business rules, and policy frameworks, ensuring that data flows, service tiers, and device behaviours align with commercial models and organisational controls. These supporting components play a critical role in orchestrating workloads across edge and cloud environments.

AI can itself enhance the effectiveness of this architecture by improving how connectivity is delivered and managed. Predictive anomaly detection helps identify issues before they affect performance, while adaptive quality-of-service mechanisms use AI-driven insights to allocate bandwidth, prioritise sensitive traffic, and optimise routing decisions. This enables the network to respond proactively to changing conditions and maintain consistent data delivery for distributed workloads. When combined with integrated policy management, business logic, and billing systems, an intelligent last mile proposition supports large-scale orchestration, operational efficiency, and stable performance across the full lifecycle of AI-enabled IoT solutions.

Collaborative

An Intelligent Last Mile must increasingly support a more collaborative operating model because AI-driven systems depend on coordinated behaviour across the entire IoT stack. As data is collected, processed, and acted upon across devices, edge platforms, orchestration layers, and cloud environments, no single component can operate in isolation. Collaborative capabilities include shared diagnostics, open APIs, unified policy frameworks, and cooperative management models that improve data flow and overall service quality.

Effective "North–South" collaboration (i.e. through the stack with other components) ensures that connectivity works in concert with device management, security frameworks, data platforms, and AI engines. This alignment helps guarantee that data is available when required, policies are applied consistently, and AI workloads receive the network conditions they need for stable performance.

Collaboration is also essential at the connectivity layer itself, where "East–West" partnerships between network providers play an increasingly important role. AI applications depend on predictable, uninterrupted access to data from globally distributed device fleets. Achieving this footprint requires seamless integration across cellular operators, satellite networks, and short-range technologies. Coordinated roaming, multi-technology handover, and shared quality-assurance frameworks ensure that devices remain reachable and able to exchange data regardless of location or movement. This collaboration also creates resilience by providing alternative pathways when coverage or local conditions change.

AI intensifies the need for these collaborative models because its effectiveness depends on holistic visibility and coordinated operation across all data paths. Distributed inference, dynamic workload shifting, and selective data movement rely on strong alignment between connectivity providers and platform ecosystems. Collaborative mechanisms enable consistent enforcement of policies, harmonised service behaviours, and unified monitoring across heterogeneous networks. By supporting both vertical and horizontal cooperation, the connectivity layer becomes a foundation for reliable global delivery of AI-enabled IoT services.

User-friendly

Another key facet of an IoT connectivity capability relates to its user-friendliness, given the complexity of deployments. A unified experience built around a single-pane-of-glass (SPOG) platform allows users to manage devices, connectivity, policies, and AI-related data paths from one environment, reducing friction and the risk of configuration errors. Centralised billing, consolidated support channels, and unified fault resolution simplify administration by removing the need to navigate multiple suppliers or interfaces. Hierarchical management functions ensure that organisations

The 'Intelligent Last Mile' for AI

can assign permissions, segment estates, and delegate responsibilities in a structured way, supporting both scale and governance.

Ease of use is further enhanced by intuitive interfaces, guided workflows, and automation that reduce manual intervention. Automated provisioning, policy enforcement, diagnostics, and lifecycle management allow teams to focus on outcomes rather than operational overhead. Clear visualisations of performance, data flows, and workload distribution help users understand how AI and connectivity interact, enabling faster decision-making and efficient troubleshooting. By reducing operational burden and making complex tasks accessible, a user-friendly connectivity proposition accelerates deployment, supports wider adoption, and ensures that AI-enabled IoT solutions deliver consistent value.

Resilient, scalable and efficient

An intelligent last mile must tolerate network disruptions, variable signal quality, and hardware faults. Built-in resilience mechanisms such as multi-path routing, adaptive quality-of-service, local buffering, and autonomous failover ensure that essential data continues to flow even under adverse conditions. This supports continuous AI operation and avoids gaps in training or inference inputs.

Furthermore, as device fleets grow and AI models demand richer data, the connectivity layer, including particularly the underlying Connectivity Management Platform, must scale without introducing delays or congestion. Scalable architectures support high device densities, dynamic bandwidth allocation, and elastic resource management across radio, core, and cloud layers. This ensures consistent performance as data volumes and application demands increase.

Efficiency is essential for reducing cost and prolonging device life. An intelligent last mile should optimise energy consumption, data transmission patterns, and use of network resources. Techniques such as adaptive reporting, compression, and edge pre-processing reduce unnecessary traffic while maintaining data quality for AI workloads.

Deterministic and observable

AI applications often depend on predictable behaviour from the network. Deterministic performance requires tight control over latency, jitter, throughput, and availability. Features such as prioritised traffic classes and deterministic scheduling enable devices to deliver data within defined bounds, supporting real-time inference and reliable actuation.

Delivering data for AI requires clear visibility into the performance, health, and behaviour of the connectivity layer. Observability features include device diagnostics, network analytics, data-path tracing, and anomaly detection. These capabilities allow operators to identify issues early, tune performance, and validate that data flows meet application requirements.

Connected Cars: applying the Intelligent Last Mile concepts

Connected cars reflect almost every challenge and requirement described in the intelligent last mile model, making them a strong illustration of why next-generation IoT connectivity must be secure, compliant, flexible, interoperable, orchestrated, collaborative, user-friendly, resilient, scalable, efficient, deterministic, and observable.

Security sits at the core of connected-car deployments because vehicles host mission-critical systems and produce safety-relevant data. End-point protection is essential for in-vehicle telematics units, sensors, and gateways, including hardened hardware, embedded SIMs, and authenticated firmware updates. Network security also plays a substantial role as vehicles frequently move between public and private networks, exposing them to evolving threats. Measures such as traffic filtering, private APNs, SIM-based authentication, and anomaly detection help maintain protection. Transport-layer encryption, secure backhaul, and IoT SAFE-based mechanisms ensure integrity for data moving between the vehicle, cloud services, and OEM platforms. Cloud and application security are critical for safeguarding telematics platforms, infotainment apps, and remote services. End-to-end protection integrates these layers to defend against increasingly sophisticated automotive cyber-risks.

Compliance is a major consideration because connected-car services must navigate a dense landscape of regulations that govern safety, data, connectivity, and increasingly AI. Automotive deployments interact with multiple regulatory domains described in the text, including security rules such as the UK Product Security and Telecommunications Infrastructure Act, supply-chain and cybersecurity requirements such as NIST's Cybersecurity Framework 2.0, and data sovereignty obligations influenced by the EU Data Act. Vertical rules such as eCall add sector-specific constraints. Permanent-roaming restrictions affect global vehicle fleets, requiring careful management of eSIM localisation, KYC obligations, and profile provisioning. As vehicles generate sensitive personal, behavioural, and location data, compliance becomes inseparable from connectivity design.

Flexibility is essential because carmakers deploy globally and must support diversified technologies across markets. The arrival of SGP.32 remote SIM provisioning introduces meaningful new abilities for fleet operators to switch networks dynamically, localise connectivity for compliance, and select partners based on service quality. Automotive deployments also rely on varying network technologies, from LTE-M for telematics to 5G SA for high-bandwidth sensor data. Roaming, multi-IMSI approaches, and legacy RSP standards all continue to play roles in maintaining broad, resilient coverage. A flexible connectivity model enables vehicles to adapt to service availability, regulatory environments, and performance requirements throughout their lifecycle.

Interoperability and cross-optimisation are crucial because vehicles integrate a complex mix of sensors, gateways, embedded operating systems, protocols, and cloud applications. Connected-car platforms must operate across different network technologies, chipset vendors, and device management frameworks. Furthermore, cross-optimisation between sensor, gateway, network, edge compute, and cloud environments determines how efficiently vehicles can support AI-enabled features such as predictive maintenance, driver assistance, or real-time hazard detection. Connectivity must align with enterprise systems such as fleet platforms, CRM tools, and diagnostics engines to ensure coordinated behaviour across all layers.

Orchestration is a defining requirement as vehicles increasingly rely on distributed AI models that operate across in-vehicle processing units, edge nodes, and cloud platforms. Real-time inference for ADAS and vehicle-to-everything (V2X) functions demands stable, low-latency connectivity, while cloud-based analytics and model training require periodic transfer of richer datasets. Connectivity must therefore support intelligent workload placement, with traffic management, selective upstreaming, and stable synchronisation of models across environments. Integration with billing, business rules, and policy frameworks ensures that data flows and service tiers align with commercial and operational priorities. AI-driven improvements to anomaly detection and dynamic

Connected Cars: applying the Intelligent Last Mile concepts

QoS further enhance consistency and safety across the fleet.

Collaboration is fundamental for connected-car deployments because vehicles rely on coordinated behaviour across the entire technology stack. North–South collaboration ensures that connectivity works seamlessly with vehicle OSs, security systems, telematics platforms, and cloud-AI engines. East–West collaboration is equally important, as vehicles move across borders and network footprints. A unified approach between cellular operators, satellite providers, and short-range systems supports seamless service continuity, predictable access to telematics, and robust fallback options. Such coordination also supports harmonised policies, diagnostics, and performance standards across heterogeneous networks.

User-friendliness directly influences the operational efficiency of automotive programmes. OEMs and fleet operators require single-pane-of-glass platforms to manage millions of vehicles, administer connectivity policies, localise eSIMs, and oversee diagnostics across global markets. Unified billing, a single point of contact for support, consolidated fault management, and hierarchical controls simplify operations at scale. Easy-to-use interfaces, guided workflows, and automation reduce the complexity of managing distributed fleets and help operations teams maintain performance while deploying advanced AI-enabled services.

Resilience, scalability, efficiency, determinism, and observability are indispensable in the automotive environment. Resilience ensures vehicles maintain connectivity even when encountering coverage gaps, network failures, or adverse conditions, using features such as multi-path routing, local buffering, and autonomous failover. Scalability supports global fleets and growing data demands as AI models evolve. ,Efficiency helps manage energy use in battery-powered components and reduces operational costs by optimising data reporting. Deterministic behaviour supports safety-critical applications that depend on predictable performance. Observability gives OEMs and operators detailed insight into device health, network quality, anomaly patterns, and data flows, enabling proactive management and accelerating diagnostics.

Vehicle Security Operations Center (VSOC) helps with security in connected cars by providing 24/7, real-time monitoring and threat detection across the entire vehicle ecosystem, including cloud services and in-vehicle networks. VSOCs integrated with AI models would evolve from manual monitoring systems into proactive security ecosystems capable of protecting against sophisticated automotive cyberattacks.

Tata Communications: Transforming IoT with AI & ML applications

Tata Communications MOVE™ (hereafter referred to as MOVE) is increasingly leveraging advanced Artificial Intelligence (AI) and Machine Learning (ML) technologies to strengthen and differentiate its Connectivity Management Platform (CMP) offering. Some of the initiatives MOVE is utilizing AI&ML for are as below:

1) One of the key areas where MOVE is harnessing AI and ML is in enabling precise location intelligence for IoT devices that are constrained by hardware limitations. Many low-end or cost-optimized IoT devices do not support GPS due to constraints related to power consumption, form factor, or component cost. Traditionally, this has limited the ability of enterprises to accurately track and monitor such devices, particularly across global supply chains. MOVE addresses this challenge by employing AI-powered location inference models that use alternative network signals and contextual data to determine device location with a high degree of accuracy. Through continuous training and refinement of these models, MOVE enables its asset-tracking customers to not only locate their devices globally but also to derive predictive insights. For example, by correlating historical movement patterns, network behaviour, and logistics data, the AI models can generate accurate predictions for expected delivery times and destination arrival. This enhanced visibility enables enterprises to improve supply-chain planning, proactively manage delays, reduce losses, and deliver better service to their end customers—all without requiring expensive GPS-enabled hardware.

2) MOVE CMP is building an Intelligent Connectivity, powered by AI and ML, to deliver seamless and resilient network access for IoT devices operating across multiple geographies. In a typical global deployment, IoT devices may encounter multiple mobile networks, each offering different levels of coverage, performance, and quality of service (QoS). MOVE's Intelligent Connectivity capability enables devices to dynamically switch between available mobile networks ensuring best connectivity.

3) Software-over-the-Air (SOTA) updates remotely to IoT devices often fail due to various reasons viz. device may be out of network, the device may be in sleep mode, or simply because of provisioning or data balance issues. MOVE CMP is significantly improving SOTA update success rate by introducing AI and ML models to predict the best window of availability for every IoT device connected.

In addition to the above initiatives, MOVE CMP is gearing up with AI and ML to enable enterprises define how their devices should behave in every situation and automatically orchestrates the right connectivity service, not only based on footprint and quality expectations, but also on cost, timing, multi-modal connectivity availability, and dynamic conditions.

This report was produced by Transforma Insights in collaboration with sponsors Tata Communications

TRANSFORMA INSIGHTS

Learn more.

TATA COMMUNICATIONS
move™

Learn more.