Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Agentic Edge Orchestration: A Deterministic Framework for AI-Native Retail Networks

Bhavinkumar Jayswal

Independent Researcher, USA

ARTICLE INFO

Received: 07 Feb 2026

Revised: 08 Feb 2026

ABSTRACT

High performance requirements in today's data-rich environments, such as stores with many sensors and systems that make quick decisions, cannot be fulfilled by old designs that treat connectivity as just a basic infrastructure element focused on being available and cheap. Smart and adaptable in-store technologies, such as Internet of Things devices that monitor the physical store environment, are required to support the digital nervous system. AI processes the raw telemetry, creating predictive models and deriving control actions. Fifth-generation wireless network technology offers deterministic performance, smooth mobility, and logical network isolation through what is called network slicing. These technologies need to converge into integrated federated architectures. Observability is fragmented, control models are centralized, and latency is inconsistent, leading to operational challenges, especially at scale. This article describes foundational attributes of architectures that embed intelligence, essential governance, and resilience into the underlying network infrastructure. Layers organize these attributes, which include physical sensing, differentiated transport, edge intelligence, distributed control, and governance. Further metrics include effective autonomous responses, predictability of latency across the network, and the reduction of operational load. A further aim is to form slf-controlled networks in retail with governance and ethics in mind.

Keywords: Retail Connectivity, Internet of Things Architecture, Artificial Intelligence Networks, 5G Integration, Edge Intelligence

1. Introduction

Retail is shifting from a focus on mere transactions to integrated, cyber-physical stores. These modern environments continuously deliver digital services and foster value co-creation among customers, employees, and physical objects. This represents a significant business model transformation, as demonstrated by the food industry's successful merger of e-commerce and physical stores to create seamless customer experiences [1].

Modern retail relies on real-time data streams to enable capabilities like:

- Inventory accuracy
- Dynamic pricing
- Loss prevention
- Customized marketing and communications
- Energy efficiency
- Actionable insights

Achieving these capabilities requires decision-making speeds that surpass human reaction times.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A variety of technologies support diverse store network needs:

- **Computer vision** analyzes customer behavior and detects security threats.
- **Electronic shelf labels** adjust prices in real time based on demand and competitor pricing.
- **Autonomous robots** handle tasks such as aisle scanning and floor cleaning.
- **Edge analytics** processes video streams locally, preserving bandwidth and minimizing latency.

This cyber-physical system facilitates a bidirectional flow of information between a store's physical and digital components.

However, many retail networks still treat connectivity as a basic utility, optimizing primarily for cost and availability. Modernization requires a new focus, building networks for resilience, reliability, and future technology requirements. As stores adopt more devices and services, scalability becomes essential.

Legacy network designs face several challenges:

- They prioritized Wide Area Network (WAN) access, treating wireless access as "best effort" [2].
- Architectures stress under the increased sensor counts, as operations currently rely heavily on manual, non-scalable configuration.
- Video analytics requires guaranteed bandwidth, which is often unavailable on shared networks.
- Real-time control loops for robotics need latency guarantees that conventional control systems cannot provide.

True modernization demands a fundamental, holistic architectural shift. IoT, AI, and 5G must be viewed as symbiotic and cooperative elements, not as isolated upgrades that create new silos. Only through this deliberate convergence can retail networks evolve into intelligent platforms capable of sensing, reasoning, and acting at an enterprise scale.

2. Structural Limitations of Traditional Architectures

Modern retail applications, especially those using AI-based automation, expose the limitations of legacy networks that focus on average latency. For real-time retail use cases—such as AI inference, robotics, and video analytics—average latency can mask critical, momentary spikes that can disable autonomous systems. Network performance is vital for logistics, with warehouse management systems relying on continuous connections for inventory tracking and transportation management needing real-time distribution visibility [3].

The sensitivity of AI inference workloads to network instability is highlighted by performance modeling. Deep Learning (DL) models run on distributed systems, where the timed arrival of data from previous stages is essential. Latency "jitter" can accumulate, leading to degraded accuracy. Performance modeling is an effective tool for identifying and resolving such bottlenecks before deployment [4]. Furthermore, for safe operation, robots often require a strict latency tolerance, and computer vision systems demand a guaranteed frame rate, which standard networks cannot assure.

Operational visibility is complicated by the collection of telemetry from numerous, disconnected systems. Data is scattered across various sources: devices on the wide area network, port statistics from local area network switches, client tracking from wireless access points, sensor health from IoT platforms, and application transaction logs. Each source often has its own dashboard and alerting mechanism, necessitating manual correlation to determine cause and effect. This siloed view—where the network team sees connectivity issues and the application team sees transaction errors—extends

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

the time and expertise needed to find a root cause, increasing mean time to resolution (MTTR) and overall operational risk, even when customer complaints signal a problem.

While centralization simplifies overall management—with Network Operations Centers controlling thousands of stores from regional or national hubs—it introduces operational rigidity and risk. Centralization means that all policies, settings, and problem resolution are handled centrally. A policy error in the central region can disrupt an entire store, and stores lack the ability to autonomously adapt to changing local conditions. Remote troubleshooting requires internal escalation, diagnosis, and remediation of connectivity issues, which increases response time and the "blast radius" of problems. Issues at one site frequently impact others, prolonging recovery. The diagram below summarizes the fundamental design flaws in older retail networks that obstruct effective support for environments reliant on numerous sensors, AI, and autonomous operations. Each limitation category illustrates how outdated assumptions create significant operational barriers at the enterprise scale.

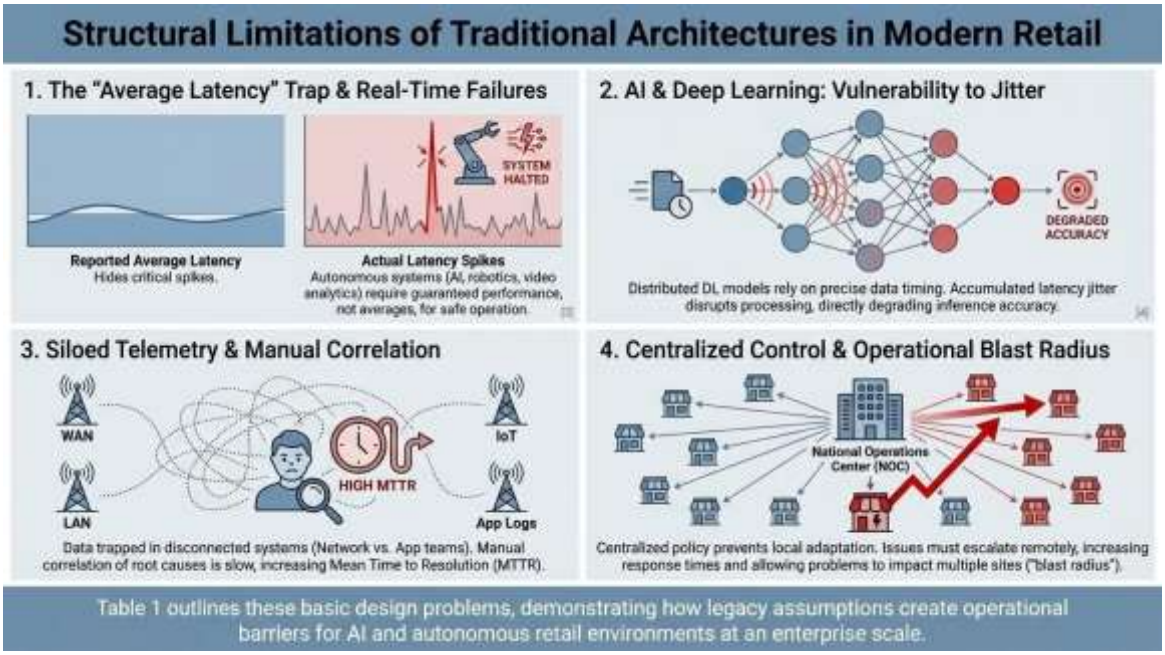

Figure 1: Structural Limitations of Legacy Retail Network Architectures

3. IoT as Physical-Digital Interface

Modern retail network architectures must accommodate the varied demands of diverse Internet of Things (IoT) devices. Traditional network designs, which treat all sensors uniformly, lead to operational complexity and inefficiency because they fail to account for the unique loads each device type imposes.

Effective network management, particularly in heterogeneous environments with multiple vendors using proprietary protocols, requires multi-vendor network observability. Unified observability platforms are crucial for correlating data and providing insights across the infrastructure, which facilitates faster troubleshooting and proactive operations.

IoT devices can be functionally classified based on their tolerance for latency, data criticality, and control coupling:

- **Passive Sensing Devices:** These devices, such as temperature or footfall sensors, generate

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

telemetry at regular intervals. They can tolerate some latency, making best-effort network access suitable for them.

- **Perceptual Systems:** This category includes high-bandwidth, consistent-latency applications like cameras, computer vision sensors, and RFID readers. They are vital for analytics, loss prevention, and inventory management. Retail applications, such as tracking customer movement, analyzing product engagement, facial recognition for personalization/security, and automated inventory, rely on these systems. Variable data delivery can compromise inference accuracy for these applications, necessitating prioritized quality of service.
- **Interactive Actuators and Closed-Loop Control:** This domain involves devices that respond to control signals, such as electronic shelf labels that adjust prices, smart lighting that reacts to occupancy, and digital signage offering contextual information. The closed-loop control domain, particularly for retail robots, requires strict latency and reliability guarantees. Onboard safety and operation depend on the timing of the control loop; network jitter can lead to navigation errors, collisions, or mission failure. Autonomous agents operate on dedicated, low-latency network slices.

Integrated network architectures manage resources efficiently by enforcing policies based on these device classes: prioritizing perceptual systems, offering best-effort access to passive sensors, and utilizing virtual networks or low-latency slices for interactive actuators and autonomous agents. This approach prioritizes business-critical traffic to ensure appropriate service guarantees while balancing cost and performance.

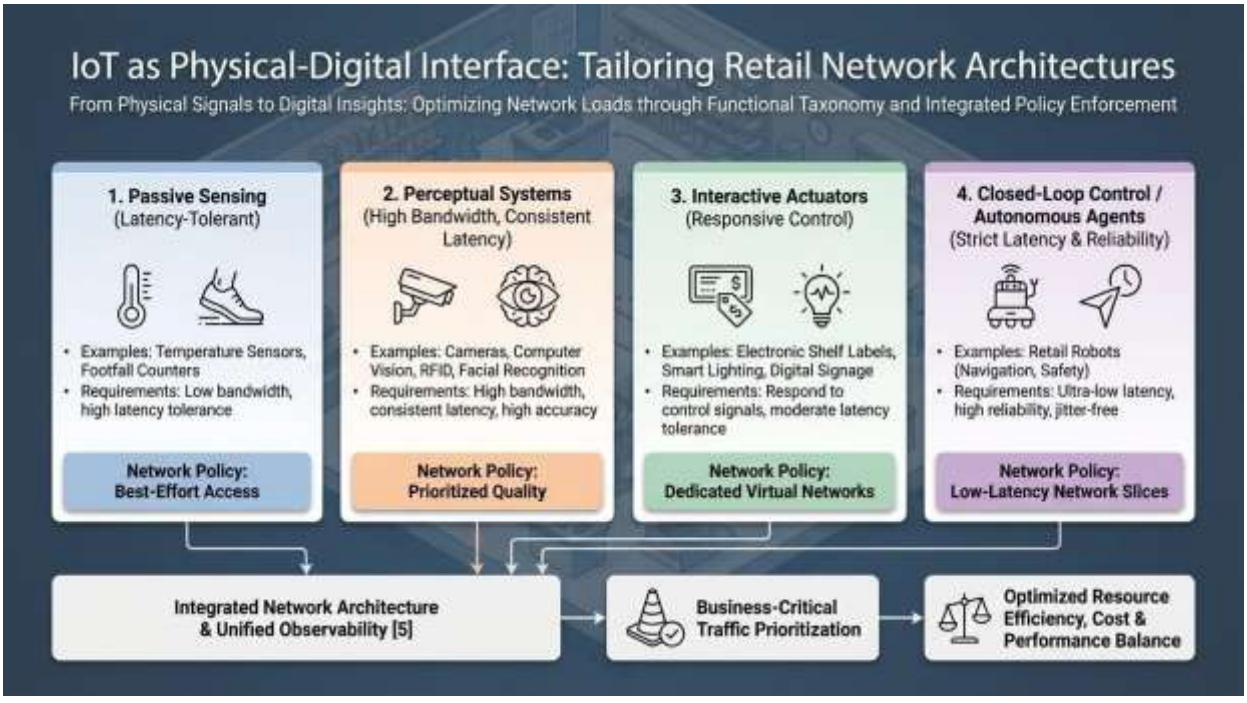

Figure 2: IoT Device Functional Classification and Network Resource Allocation

4. AI-Driven Network Intelligence

AI is transforming network infrastructure from a passive transport layer into an adaptive, continuous control system. This is evident in autonomous retail environments, such as checkout-free stores. Here, computer vision and machine learning identify what customers take, enabling automatic payment

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

without the need for manual scanning. This type of implementation goes beyond simple analytics or reporting.

The true challenge lies not in the algorithms themselves, but in the system architecture. For AI to achieve genuine autonomy, it must be embedded within the control planes and possess an understanding of both business and operational constraints, respecting established governance frameworks. Without this integration, AI serves only in an advisory capacity, requiring human operators to implement the suggested changes, which maintains human bottlenecks and speed limits. True autonomy is only realized when intelligence is directly coupled with control systems.

This embedded intelligence enables systems to sense, predict, and prescribe corrective actions, thereby moving operations from a reactive to an autonomous state.

Key Applications of Embedded AI in Networks:

- **Perceptual Intelligence:** Correlates telemetry data across various infrastructure layers to establish situational awareness through data calibration. It can identify small anomalies that may be symptomatic of larger, systemic problems that are often difficult for humans to detect.
- **Predictive Analytics & Maintenance:** Prevents network failures before they impact the business by identifying underlying patterns in historical data.
  - Machine learning models, trained on error rates, can predict hardware failures.
  - Thermal sensors detect when components exceed their thermal limits.
  - Traffic analysis pinpoints capacity issues.
  - This allows repair and maintenance to be scheduled during downtimes, minimizing service disruption and extending equipment life.
- **Prescriptive Intelligence:** Takes autonomous action to resolve detected problems, closing the control loop at the edge without human involvement. Examples include traffic re-routing, adjusting quality-of-service (QoS) parameters, or activating redundant paths.

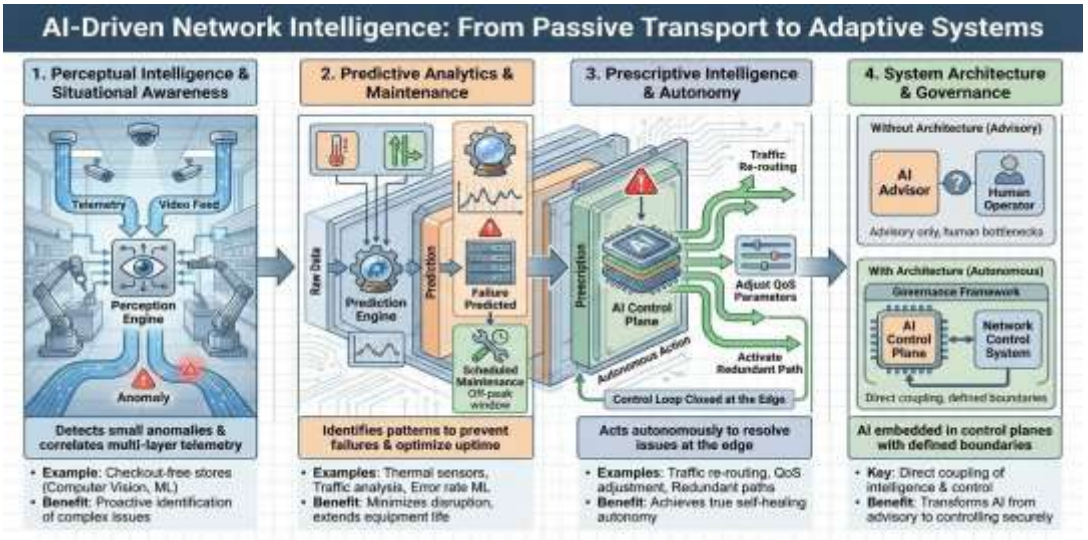

Figure 3: AI-Driven Network Intelligence Control Loop

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

5. 5G in Retail: New Connectivity Paradigms

Fifth-generation (5G) wireless technology introduces significant advances over previous generations, offering capabilities that fundamentally change network assumptions. A key differentiator is 5G's ability to provide deterministic performance guarantees, unlike traditional WLAN. Furthermore, 5G ensures service continuity for mobile users as they traverse different coverage areas.

The Role of Network Slicing

A crucial feature of 5G is network slicing, which allows for the creation of multiple, separate logical networks atop shared physical infrastructure. These slices can be configured with diverse characteristics. For retail environments, automated 5G network slice management is essential, as manually configuring slices across thousands of locations is impractical. Orchestration platforms can automatically scale slices according to application needs, while machine learning can optimize slice parameters based on traffic conditions, and self-healing mechanisms can restore service [9]. This allows for true multi-tenancy within a single deployment. For example, critical applications can utilize low-latency slices with bounded jitter, while guest access can be assigned to lower-priority slices.

Retail 5G Deployment Models

Retail 5G deployments generally fall into three categories:

1. **Public Deployments:** These leverage a carrier's public network, often for redundancy. Stores offload non-mission-critical traffic, such as guest internet access, to the carrier infrastructure to minimize capital expenditure and operational risk.
2. **Private Deployments:** These utilize dedicated on-premise infrastructure. The retailer manages the entire stack, from the radio access network to the core network. Hosting workloads like point-of-sale and inventory robots in-house provides enhanced security and performance predictability.
3. **Hybrid Deployments:** These combine elements of both, using local private networks for fast and secure applications while retaining the flexibility and control of public carrier networks for backup and mobile applications.

Application-Intent-Based Connectivity

Flexible connectivity, powered by technologies like network function virtualization (NFV) and software-defined networking (SDN), offers a significant benefit by enabling retailers to allocate network resources based on the application's specific purpose or intent, rather than its static physical location. This dynamic assignment allows for the creation of distinct, isolated network paths, or "slices," tailored to the needs of different operational systems. For instance, an automated cleaning robot, which requires guaranteed low-latency and reliable connectivity, can be allocated a dedicated, private infrastructure slice. This separation ensures its critical operations are not impacted by the traffic of less-critical systems, such as the public network used by customer-facing mobile applications, thereby enhancing the operational performance and security of the device.

This concept extends to mission-critical business systems, such as terminal point-of-sale (POS) applications, which can also be hosted on their own private network slices. By utilizing network slicing, each POS application is guaranteed an appropriate Service Level Agreement (SLA) for throughput, latency, and reliability, ensuring seamless and fast transaction processing even during peak hours. This ability to dynamically and intentionally allocate resources is the core advantage of these modern deployment models and technologies. By contrasting various approaches in terms of performance reliability, network slicing capabilities, and infrastructure variation, organizations can select the optimal combination to support connectivity that directly aligns with and meets specific operational and business requirements.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 4: Comparison of 5G Deployment Models in Retail Settings

Feature	Public Deployment	Private Deployment	Hybrid Deployment
Infrastructure	Carrier's Public Network	Dedicated On-Premise Infrastructure	Mix of Private & Public Networks
Traffic Focus	Non-Mission-Critical, Guest Access	Mission-Critical Workloads (POS, Robots)	Critical (Private) & Backup/Flexible (Public)
Performance	Best-Effort, Higher Latency Tolerance	Deterministic, Low-Latency, Bounded Jitter	Optimized based on Application Intent
Security & Control	Carrier-Managed Security	High Security, Retailer-Operated	Balanced Security & Control
Key Benefits	Redundancy, Reduced CapEx & Risk	Predictability, Security, Custom Slices	Flexibility, Control, Path Selection

Source: Adapted from [9] and user text.

Figure 4: 5G Network Slicing Architecture for Retail Applications

6. Integrated Reference Architecture

The retail connectivity reference architecture is a system-of-systems approach that integrates IoT, AI, and 5G across five distinct logical layers. This separation of concerns simplifies integration.

The Architecture Layers:

1. **Physical Sensing and Actuation Layer:** This foundational layer includes all IoT devices and mobile assets within the store environment responsible for generating and consuming data signals.
2. **Access and Transport Layer:** This layer ensures connectivity using a variety of technologies, such as wireless local area networks, wired Ethernet, and 5G. The chosen transport method depends on the application's specific requirements for latency tolerance, mobility, and importance.
3. **Edge Intelligence Layer:** This layer enables local computation and AI processing at the store level for near-real-time situational awareness. Key benefits of edge computing include reduced latency and bandwidth consumption. It also supports autonomous operations—even when connectivity is lost—through a distributed control plane and policy-driven orchestration. This layer balances centralized governance with local autonomy, allowing stores to adapt to immediate circumstances while central teams retain visibility and overriding authority.
4. **Governance and Trust Layer:** Providing embedded security, privacy controls, and auditability, this layer is crucial. Key functions include:

- Defining security components through smart network governance frameworks.
- Controlling access and authorization via identity and access management.
- Protecting data with encryption, both in transit and at rest.
- Detecting anomalous behavior with threat detection.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Ensuring compliance with regulations through continuous monitoring.
- Allowing for immediate containment via incident response procedures.

These governance and security functions are integrated across every architectural layer. Policies govern device authentication, transport encryption, and data access control. Furthermore, privacy policies enforce data minimization and purpose limitation. Audit systems log all autonomous decisions, supporting compliance and debugging efforts. Governance is thus an essential, built-in feature of the architecture, rather than an afterthought. If robust security and privacy controls cannot be implemented to protect the system, organizations must prioritize this integrated governance from the outset.

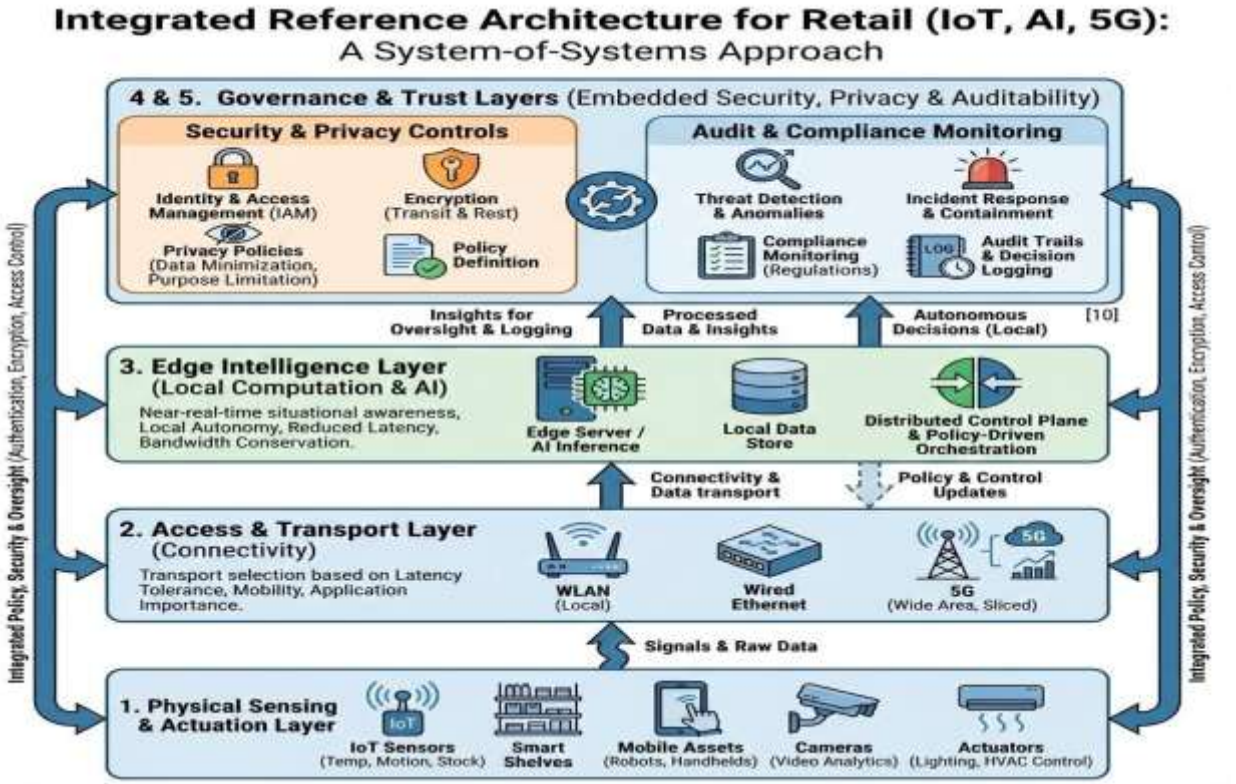

Figure 5: Five-Layer Integrated Reference Architecture

Conclusion

Retail connectivity is undergoing a fundamental transformation driven by technological and business trends, notably the detailed physical visibility provided by IoT devices in store environments. This change is enabled by AI, which converts raw data into actionable predictions and control decisions. While 5G offers reliable performance and service isolation through slicing, the successful integration of IoT, AI, and 5G is crucial.

Current legacy architectures, which treat latency as a static, aggregate metric, are insufficient for modern applications that require bounded predictability. Furthermore, siloed systems hinder comprehensive observability, and centralized models lack the scalability needed for large enterprises.

This article proposes a layered reference architecture designed to integrate physical sensing, various transport methods, edge intelligence, and embedded distributed control and governance.

Journal of Information Systems Engineering and Management
2026, 11(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Key Shifts and Implications:

- **Network Governance:** Governance will become a core element of network design, not an afterthought. New performance metrics must be introduced, such as the responsiveness of autonomous systems and the reduction in human workload they achieve.
- **Privacy and Security:** Increased privacy risks necessitate architectural solutions that enforce data minimization and purpose limitation as a default setting.
- **System Autonomy:** Future retail networks, leveraging ubiquitous sensing and AI, will be self-regulating, operating unless constrained or overruled by human intent.
- **Industry Focus:** Standards bodies will shift their focus from mere protocol efficiency to system autonomy and ethics.
- **Workforce Evolution:** The retail workforce will transition toward roles in oversight, design, and governance.

By embedding intelligence, clear rules, and effective management, this new type of smart infrastructure offers resilience and scalability that traditional networking models lack, profoundly impacting business connectivity beyond the retail sector.

Figure 6: Deployment Model Comparison Matrix

References

1. Chavapol Yensabai, et al., "Digital Retail Shop Services in Cyber-Physical Retail System: A Case Study of Food Business," IEEE Xplore, 2023. Available: https://ieeexplore.ieee.org/document/10044743
2. Versitron, "Future-Proofing Your Retail Network: Key Considerations for Resilience and Reliability," 2023. Available: https://www.versitron.com/blogs/post/future-proofing-your-retail-network-key-

considerations-for-resilience-and-reliability?srsltid=AfmBOoqg5QOoRVF9n4FZMKCA4a2mOoyNqnQVkdYQW8ff5PfjMNk5hC1c

3. Vidushi Sharma, "Impact of Automation on Retail Logistics: AI-Powered Solutions for Efficient Supply Chains," ResearchGate, 2023. Available: https://www.researchgate.net/publication/388757964
4. Max Sponner, et al., "AI-Driven Performance Modeling for AI Inference Workloads," Electronic, 2022. Available: https://cfaed.tu-dresden.de/files/Images/people/chair-pd/Papers/electronics-11-02316.pdf
5. Mahesh Ramachandran, "Unlocking the Power of Multi-Vendor Network Observability with OpsRamp and Aruba: A Collaborative Approach," Ops Ramp. Available: https://blog.opsramp.com/multi-vendor-network-observability
6. Team Trantor, "Computer Vision in Retail: A Step-by-Step Guide to Boosting Sales and Efficiency," Trantor, 2025. Available: https://www.trantorinc.com/blog/computer-vision-in-retail
7. Shashikant Kalsha, "Autonomous Retail: AI and Robotics in Checkout-Free Stores," Qodequay Technologies, 2025. Available: https://www.qodequay.com/autonomous-retail-ai-robotics?srsltid=AfmBOorq1VN_2Rw_3ZyXALDyZ_q1wFTeoBYgLULnoYPtGmHXuDgAc1zN
8. Adam Brykowicz, "5 Ways Predictive Analytics can Prevent Network Failures," ISMSEagle, 2018. Available: https://www.smseagle.eu/2018/01/08/5-ways-predictive-analytics-can-prevent-network-failures/
9. André Perdigão, et al., "Automating 5G network slice management for industrial applications," Computer Communications, 2025. Available: https://www.sciencedirect.com/science/article/pii/S0140366424003384
10. JE-SPIN, "Security Governance Framework: Key Components & Real-World Insights," 2025. Available: https://www.e-spincorp.com/security-governance-framework-components-insights/