RESEARCH INSIGHTS SERIES · MAY 2026

IoT & Edge Computing

Research Insights 2024–2026

95 papers reviewed · 8 domains · Edge AI · IIoT · 5G/6G · Smart Cities

95+	8	35.4%	98%
Papers	Domains	Energy Saved	IDS Accuracy

Atine John Bosco

ICT Consultant · MBCS · ACM · SIM · ITPA

atine.info

Table of Contents

1. Executive Summary
2. The IoT & Edge Computing Landscape 2026
3. Edge AI and Federated Learning
4. Industrial IoT (IIoT) and Smart Manufacturing
5. Smart Cities and Autonomous Systems
6. 5G/6G Integration with IoT
7. IoT Security, Privacy and Zero-Trust
8. Real-Time Processing and Latency Optimisation
9. Sustainable IoT and Energy Harvesting
10. Digital Twins and IoT Convergence
11. Strategic Roadmap and Action Framework
12. References

Executive Summary

The IoT and Edge Computing landscape in 2024–2026 is defined by a fundamental architectural shift: intelligence is migrating from centralised cloud data centres to the network edge, embedded directly within devices, gateways, and local compute nodes. This report synthesises findings from **95 peer-reviewed papers** spanning eight critical domains, revealing a technology ecosystem undergoing rapid maturation.

Key Finding 1: Federated Learning Dominates Edge AI

Federated Learning (FL) has emerged as the **de facto standard** for privacy-preserving AI at the edge. The Energy-Aware Federated Learning (EAFL) framework achieved a **35.4% reduction in energy consumption** while preserving **91.8% model accuracy**, with blockchain security reducing model-poisoning success rates by **72.3%** [?].

Key Finding 2: IDS Accuracy Reaches 98% at the Edge

Adaptive Curriculum Learning combined with Explainable AI (XAI) achieved **98% accuracy** on CIC-IoV-2024 and CIC-APT-IIoT-2024 datasets, and **97% accuracy** on EDGE-IIoT benchmarks, demonstrating production-ready intrusion detection for IoT networks [?].

Key Finding 3: 5G Network Slicing Cuts Latency by 30%

DynamicSlicerNet, a deep reinforcement learning framework for 5G resource slicing, yielded up to **30% latency reduction** and **20% reliability improvement** versus static allocation for IoT-integrated networks [?].

Key Finding 4: LLMs Now Fine-Tunable on Edge Devices

Parameter-efficient techniques (LoRA, Split Federated Learning) now enable **Large Language Model fine-tuning on constrained edge nodes**, opening new frontiers for on-device intelligence without cloud dependency [?].

Key Finding 5: Fog-Blockchain-FL Synergy Emerging

A systematic literature review identified **fog computing + blockchain + federated learning** as a powerful triad for trustworthy IoT applications, providing auditability, tamper resistance, and privacy preservation in unified architectures [?].

Key Finding 6: Green FL Reduces AI Carbon Footprint

Green Federated Learning frameworks targeting client selection, gradient compression, and communication reduction are reducing the energy footprint of distributed AI training at the edge, with up to **40% latency reduction** and **35% resource efficiency improvement** in documented deployments [?].

Key Finding 7: SCOF Secures IIoT Offloading

The Security-Aware Computation Offloading Framework (SCOF) uses federated reinforcement learning with artificial noise channels and differential privacy for secure edge offloading in smart factories, outperforming baselines on runtime, latency, and energy metrics [?].

The IoT & Edge Computing Landscape 2026

Market Context and Scale

The Internet of Things ecosystem has grown to encompass an estimated **18–20 billion** connected devices globally as of 2026, with projections suggesting over **30 billion** devices by 2030. Edge computing has emerged as the critical enabler for managing this scale, processing data closer to where it is generated rather than routing everything to centralised cloud infrastructure.

The Three-Tier Edge Architecture

Modern IoT deployments operate on a **three-tier architecture**:

- **Device Layer**: Sensors, actuators, embedded systems with local inference
- **Edge/Fog Layer**: Gateways, micro-data-centres, MEC nodes for real-time processing
- **Cloud Layer**: Centralised storage, model training, orchestration and analytics

The research consensus in 2024–2026 is that **80% of IoT data** should be processed at the edge layer to meet latency, bandwidth, and privacy requirements [?].

Convergence Themes

The dominant convergence theme across the 95 reviewed papers is the integration of **Federated Learning** with edge architectures. Rather than treating FL as a standalone privacy technique, researchers are embedding it into comprehensive stacks that combine:

- **Blockchain** for model provenance, auditability, and tamper resistance
- **5G/6G radio management** for bandwidth-efficient model aggregation
- **Reinforcement Learning** for dynamic resource allocation and offloading decisions
- **Explainable AI (XAI)** for interpretable security and anomaly detection
- **Digital Twins** for simulation-driven optimisation of edge deployments

Key Technology Readiness Levels

navyTechnology	TRL	Status 2026
Federated Learning	7–8	Production deployments in IIoT and healthcare
lightgray Edge AI Inference	8–9	Widely deployed on MCUs and edge GPUs
5G Network Slicing	7–8	Commercial deployments in smart cities
lightgray Blockchain-FL Fusion	5–6	Pilot deployments, standardisation underway
Green FL	4–5	Research prototypes, early commercial interest
lightgray LLM on Edge (LoRA)	5–6	Emerging, constrained to mid-range hardware

Digital Twin + IoT	6–7	Industrial pilots in manufacturing
lightgray 6G + Edge AI	3–4	Research phase, 2030 horizon

Edge AI and Federated Learning

The Federated Learning Revolution

Federated Learning has undergone a fundamental transformation from a privacy-preservation technique into a comprehensive distributed intelligence framework. The 2024–2026 research corpus reveals three generations of FL deployment at the edge:

FL Generation 1: Baseline Algorithms

FedAvg, FedProx, FedNova remain the foundation of edge FL. Research confirms that FedNova shows superior convergence properties, while FedProx improves resilience to client dropout in resource-constrained IoT environments. Gradient compression achieves ∼35% communication overhead reduction at the cost of ≈3% absolute accuracy loss [?].

FL Generation 2: Energy-Aware and Secure FL

The Energy-Aware Federated Learning (EAFL) framework represents the state-of-the-art in 2025, achieving:

- 35.4% reduction in energy consumption
- 91.8% model accuracy preservation
- 72.3% reduction in model-poisoning attack success rates (via integrated blockchain)

Validated in simulated 5G-edge IoT network environments [?].

FL Generation 3: LLMs and Split Federated Learning

The frontier of edge FL in 2025–2026 is enabling Large Language Model (LLM) fine-tuning on constrained edge nodes through:

- LoRA (Low-Rank Adaptation): Reduces trainable parameters by >90%
- Split Federated Learning (SFL): Partitions model layers between device and edge server
- Parameter-Efficient Fine-Tuning (PEFT): Adapts pre-trained models with minimal compute

Reviews identify these as the leading practical strategies for on-device LLM deployment [?].

Blockchain-FL Integration

The combination of blockchain with federated learning addresses the fundamental trust problem in distributed ML: how can participants verify that model updates are authentic and that the aggregated model has not been tampered with?

Key findings from the systematic review by Javed et al. (2025) [?]:

- **Smart contracts** automate FL round management and reward distribution
- **On-chain model hashes** provide immutable audit trails for regulatory compliance

- **Decentralised aggregation** eliminates single points of failure and central server trust
- Standards gaps remain: interoperability between FL frameworks and blockchain platforms requires urgent standardisation

The fog computing + blockchain + FL triad (reviewed in [?]) is identified as a **powerful architecture** for IoT applications requiring both privacy and accountability, particularly in healthcare, finance, and critical infrastructure.

Industrial IoT (IIoT) and Smart Manufacturing

Industry 4.0 to Industry 5.0 Transition

The IIoT research landscape in 2024–2026 is characterised by a transition from **Industry 4.0** (automation and data exchange) to **Industry 5.0** (human-robot collaboration, sustainability, resilience). Edge computing is the critical enabler of this transition, providing the real-time processing capabilities required for collaborative robotics, predictive maintenance, and adaptive manufacturing.

SCOF: Security-Aware Computation Offloading

The **SCOF framework** (Peng et al., 2024) [?] represents a breakthrough in secure IIoT edge computing:

- Uses **Federated Reinforcement Learning** for adaptive offloading decisions
- Employs **artificial noise channels** to protect data in transit
- Integrates **differential privacy** for local computation protection
- Outperforms baselines on runtime, latency, and energy metrics in smart factory simulations

Real-Time Anomaly Detection

Haldikar et al. (2024) [?] demonstrated that combining edge computing with federated learning for real-time anomaly detection in IIoT environments delivers:

- Improved detection performance compared to cloud-only approaches
- Data privacy preservation through local model training
- Reduced latency for time-critical manufacturing alerts

The review by Sah et al. (2025) [?] identifies key challenges for FL at the IIoT edge:

- **Heterogeneity**: Diverse hardware capabilities across factory floor devices
- **Energy constraints**: Battery-powered sensors with limited compute budgets
- **Strict confidentiality**: Proprietary manufacturing data cannot leave the facility
- **Real-time requirements**: Sub-millisecond response times for safety-critical systems

Intelligent Transport Systems

Lakhan et al. (2024) [?] demonstrated that **Augmented CNN with Federated Scheduling (ACNN/AFLSS)** for vehicular intelligent transport systems achieves better accuracy and runtime than baselines, showing the practical gains of coordinated edge training and offload policies in mobility contexts.

Satellite-Assisted IIoT Edge Computing

Research on **Federated Deep Recurrent Q-Learning** for task partitioning and resource allocation in satellite mobile-edge-computing-assisted IIoT [?] demonstrates that:

- Deep recurrent networks capture temporal dependencies in offloading decisions
- Federated training preserves enterprise data confidentiality
- Satellite-assisted MEC extends edge capabilities to remote industrial sites

Smart Cities and Autonomous Systems

Urban Intelligence Architecture

Smart city deployments in 2024–2026 are converging on a **distributed intelligence model** where edge nodes perform local analytics, FL aggregates insights across the city, and blockchain provides auditability for public-sector accountability.

DynamicSlicerNet: 5G Slicing for Smart Cities

Mahesh & Bhargava (2024) [?] demonstrated that **DynamicSlicerNet** – a deep reinforcement learning framework for dynamic 5G resource slicing – achieves:

- **Up to 30%** latency reduction versus static allocation
- **Up to 20%** reliability improvement for IoT-integrated city services
- **≈50%** communication overhead reduction via edge-local model training

Privacy-Preserving Urban AI

Shompa (2025) [?] proposed a **Decentralised Federated Learning with Blockchain** architecture for privacy-preserving edge AI in smart cities, addressing the fundamental tension between urban data analytics and citizen privacy:

- **No raw data leaves local edge nodes** – only model gradients are shared
- **Blockchain records** every FL round for regulatory auditability
- **Decentralised aggregation** prevents any single party from controlling city-wide AI

Autonomous Systems Integration

The integration of IoT with autonomous systems (vehicles, drones, robots) requires ultra-low latency processing that only edge computing can provide. Key research findings:

Resource Orchestration Performance Gains

OptiAllocRL and AdaptiveQoSDL frameworks reported:

- **Up to 40%** latency reduction in edge resource orchestration
- **25%** throughput increase for concurrent IoT workloads
- **Up to 50%** packet loss reduction (AdaptiveQoSDL)
- **Up to 35%** improvement in end-to-end delay [?]

5G/6G Integration with IoT

5G as the IoT Nervous System

Fifth-generation networks are not merely a connectivity upgrade – they represent a fundamental re-architecture of how IoT devices communicate, compute, and collaborate. The three key 5G capabilities enabling IoT advancement are:

- **eMBB (Enhanced Mobile Broadband)**: High-bandwidth video and sensor data from dense deployments
- **URLLC (Ultra-Reliable Low-Latency Communication)**: Sub-millisecond latency for autonomous systems and industrial control
- **mMTC (Massive Machine-Type Communications)**: Simultaneous connectivity for millions of IoT devices per km^2

EAFL in 5G-Edge Networks

Rahmati (2025) [?] validated the **Energy-Aware Federated Learning** framework specifically in **5G-enabled IoT network** environments, demonstrating that 5G's low-latency characteristics enable more frequent FL aggregation rounds, improving both model convergence speed and energy efficiency.

The Road to 6G

The systematic review by Ahmad & Jeon (2025) [?] identifies **6G as the ultimate enabler** for convergence ICT, projecting:

- **Terahertz (THz)** communication bands enabling **1 Tbps** peak throughput
- **AI-native air interfaces** with built-in FL for over-the-air model aggregation
- **Integrated sensing and communication (ISAC)** enabling environment-aware edge AI
- **Joint design of FL protocols with radio resource management** as a critical research priority

IoT + LLM + FL in Advanced Networks

Yang et al. (2025) [?] identify the convergence of **IoT + LLMs + Federated Learning** in advanced networked systems as a transformative paradigm, where 5G/6G provides the bandwidth and latency characteristics needed for:

- Real-time LLM inference at edge nodes
- Federated fine-tuning of LLMs across distributed IoT deployments
- Privacy-preserving natural language interfaces for smart city services

IoT Security, Privacy and Zero-Trust

The Threat Landscape

IoT networks face a unique and expanding threat surface. Unlike traditional enterprise IT, IoT devices are often resource-constrained, deployed in physically accessible locations, and operate with minimal human oversight. The 2024–2026 research corpus documents an accelerating arms race between attackers and defenders.

State-of-the-Art IDS: 98% Accuracy

Narkedimilli et al. (2025) [?] demonstrated that **Adaptive Curriculum Learning + XAI Ensemble** achieves:

- **98%** accuracy on **CIC-IoV-2024** and **CIC-APT-IIoT-2024** datasets
- **97%** accuracy on **EDGE-IIoT** benchmark datasets
- **Explainability**: XAI components provide interpretable attack attribution
- Suitable for deployment on edge nodes with constrained compute budgets

Privacy-Preserving Primitives

Li et al. (2024) [?] conducted a comprehensive survey of federated learning data security and privacy-preserving techniques for edge IoT, identifying the following as essential primitives:

- **Differential Privacy (DP)**
- **Homomorphic Encryption (HE)**
- **Secure Multi-Party Computation (SMPC)**
- **Byzantine-Resilient Aggregation**
- **Gradient Perturbation**
- **Secure Aggregation Protocols**
- **Trusted Execution Environments (TEE)**
- **Noise Injection Mechanisms**

Zero-Trust for IoT

The zero-trust security model – "never trust, always verify" – is gaining traction as the appropriate security posture for IoT deployments. Key principles applied to edge IoT:

Zero-Trust IoT Architecture Principles

1. **Micro-segmentation**: Each IoT device operates in its own network segment
2. **Continuous verification**: Device identity and behaviour validated at every interaction
3. **Least-privilege access**: Devices granted only the minimum permissions required
4. **Encrypted communications**: All device-to-edge and edge-to-cloud traffic encrypted
5. **Behavioural analytics**: AI-driven anomaly detection for compromised device identification

AI-Driven Security in 5G Edge Stacks

Surveys map the following as key enablers for scalable security across 5G/edge IoT landscapes [?]:

- **AI-driven Intrusion Detection Systems (IDS)** with real-time response
- **Blockchain-AI hybrids** for tamper-evident security event logging
- **Privacy-preserving learning** for threat intelligence sharing without data exposure

Real-Time Processing and Latency Optimisation

The Latency Imperative

Many IoT applications – autonomous vehicles, industrial safety systems, surgical robotics, smart grid management – have latency requirements measured in milliseconds or microseconds. Cloud computing, with round-trip times of 50–200ms, cannot meet these requirements. Edge computing brings processing within **1–10ms** of the data source.

Latency Reduction Achievements 2024-2026

- **30%** latency reduction: DynamicSlicerNet 5G slicing [?]
- **40%** latency reduction: OptiAllocRL resource orchestration [?]
- **35%** end-to-end delay improvement: AdaptiveQoSDL [?]
- **50%** communication overhead reduction: FedEdgeAI-style approaches [?]
- **35%** communication reduction: Gradient compression in FL [?]

Task Offloading and Scheduling

Reinforcement learning-based offloading frameworks have emerged as the dominant approach for dynamic task allocation between IoT devices and edge servers:

RL-Based Offloading Strategies

- **Federated Deep Q-Learning**: Optimises task partitioning for satellite-assisted MEC IIoT [?]
- **SCOF (Federated RL + DP)**: Secure offloading for smart factory edge nodes [?]
- **ACNN/AFLSS**: Augmented CNN with federated scheduling for vehicular ITS [?]
- **Multi-agent RL**: Distributed edge orchestration for heterogeneous IoT workloads

Edge Architecture Performance

Veeramachaneni (2024) [?] documented the performance characteristics of modern edge computing architectures:

- **Up to 40% latency reduction** through local processing versus cloud offloading
- **$\sim$35% resource efficiency improvement** in edge-native deployments
- **Decentralised era**: Edge architectures enabling peer-to-peer IoT communication without cloud intermediaries

Sustainable IoT and Energy Harvesting

The Green Imperative

IoT's explosive growth carries a significant energy cost. With billions of devices transmitting data continuously, the aggregate energy consumption of IoT networks is becoming a material contributor to global carbon emissions. The 2024–2026 research corpus documents a growing "Green IoT" movement focused on energy-aware architectures, sustainable FL, and hardware-software co-design for efficiency.

Green Federated Learning: Key Levers

Thakur et al. (2024) [?] identify the primary levers for energy reduction in distributed IoT learning:

- **Client selection algorithms**: Choose energy-efficient participants for each FL round
- **Gradient compression**: Reduce communication energy through sparse updates
- **Early stopping and adaptive rounds**: Terminate training when convergence plateaus
- **Asynchronous FL**: Decouple device participation from synchronous round constraints
- **Model pruning and quantisation**: Reduce inference energy on edge hardware

Energy-Aware Edge Models for 5G IoT

The study by Zenodo (2025) [?] on energy-aware edge computing models for sustainable 5G-enabled IoT networks documents:

- **Dynamic voltage and frequency scaling (DVFS)** for edge compute nodes
- **Sleep scheduling** for IoT devices during low-activity periods
- **Energy harvesting integration** from solar, vibration, and RF sources
- **Carbon-aware workload scheduling** aligned with renewable energy availability

EAFL Energy Performance

The Energy-Aware Federated Learning (EAFL) framework [?] achieved **35.4% energy consumption reduction** while maintaining **91.8% model accuracy** – demonstrating that energy efficiency and model performance are not fundamentally in conflict when architecture is designed holistically.

Digital Twins and IoT Convergence

The Digital Twin Paradigm

A digital twin is a real-time virtual replica of a physical asset, process, or system, continuously updated with live IoT sensor data. The convergence of digital twins with edge computing and AI is enabling a new generation of **predictive and prescriptive** industrial applications.

Digital Twin + Edge AI Architecture

The emerging architecture for digital twin deployments integrates:

- **IoT sensors**: Continuous data streams from physical assets
- **Edge compute nodes**: Local twin processing for real-time response
- **Federated Learning**: Privacy-preserving model updates across twin instances
- **Cloud synchronisation**: Periodic state synchronisation for historical analytics
- **Simulation engines**: What-if scenario modelling for predictive maintenance

Current Limitations and Research Gaps

While digital twin + IoT convergence is a prominent research direction, the 2024–2026 corpus reveals important limitations:

Research Gaps in Digital Twin + IoT

- **Standardised performance metrics**: No consensus on how to measure digital twin fidelity or IoT integration quality
- **Quantitative benchmarks**: Insufficient cross-study numeric results for direct comparison
- **Energy harvesting integration**: Limited empirical evidence on energy harvesting effectiveness in twin deployments
- **Scalability**: Most twin deployments remain at pilot scale; enterprise-wide deployments face orchestration challenges
- **Security**: Twin synchronisation channels represent new attack surfaces requiring dedicated security frameworks

Industrial Applications

Despite these gaps, digital twin deployments are advancing in specific verticals:

- **Smart manufacturing**: Real-time equipment health monitoring and predictive maintenance
- **Smart grid**: Virtual replicas of power distribution networks for fault prediction
- **Smart buildings**: HVAC, lighting, and occupancy optimisation through building twins
- **Healthcare**: Patient digital twins for personalised treatment optimisation

- **Urban infrastructure**: City-scale twins for traffic, utilities, and emergency response

Strategic Roadmap and Action Framework

IoT & Edge Maturity Model

Five-Level Edge AI Maturity Model

1. **Level 1 – Connected**: IoT devices transmit raw data to cloud; no edge processing
2. **Level 2 – Processed**: Edge gateways perform basic filtering and aggregation
3. **Level 3 – Intelligent**: Edge nodes run ML inference for local decision-making
4. **Level 4 – Federated**: FL enables privacy-preserving collaborative learning across edge nodes
5. **Level 5 – Autonomous**: Self-optimising edge AI with blockchain governance and LLM interfaces

6-Point Action Framework for ICT Leaders

Action 1: Adopt Federated Learning for Privacy-Critical IoT

Deploy FL frameworks (FedAvg/FedProx baseline, EAFL for energy-constrained environments) for any IoT use case involving sensitive data. Integrate blockchain for model provenance and auditability from day one.

Action 2: Invest in 5G Network Slicing Capabilities

Leverage DynamicSlicerNet-style deep RL for 5G resource management to achieve the documented 30% latency and 20% reliability improvements for IoT-integrated services.

Action 3: Implement Zero-Trust IoT Security

Deploy adaptive curriculum learning + XAI-based IDS (targeting 98% accuracy) combined with differential privacy, Byzantine-resilient aggregation, and micro-segmentation for comprehensive IoT security posture.

Action 4: Embed Green FL in AI Strategy

Apply client selection algorithms, gradient compression, and asynchronous FL to reduce IoT AI energy consumption. Target the 35.4% energy reduction benchmark demonstrated by EAFL as a deployment KPI.

Action 5: Pilot Digital Twin Deployments

Begin digital twin pilots in highest-value asset categories (manufacturing equipment, energy infrastructure). Establish standardised KPIs for twin fidelity and edge synchronisation performance before scaling.

Action 6: Prepare for 6G and LLM-at-Edge

Monitor 6G standardisation (ITU-R IMT-2030) and invest in edge hardware capable of running LoRA-fine-tuned LLMs. The IoT + LLM + FL convergence will define the competitive landscape of the next decade.

References

[1] Adu-Manu, K. S., Kyeremanteng, P. S., & Ofori, P. (2025). *Federated Learning at the Edge: Enhancing Privacy and Efficiency in Distributed AI Systems*. IntechOpen. https://doi.org/10.5772/intechopen.1011986

[2] Rahmati, M. (2025). *Energy-aware federated learning for secure edge computing in 5G-enabled IoT networks*. *Journal of Electrical Systems and Information Technology*. https://doi.org/10.1186/s43067-025-00203-2

[3] Yang, H., Liu, H., Yuan, X., et al. (2025). *Synergizing Intelligence and Privacy: A Review of Integrating Internet of Things, Large Language Models, and Federated Learning in Advanced Networked Systems*. Preprints. https://doi.org/10.20944/preprints202504.2082.v1

[4] Valdez Solis, W., Parra-Ullauri, J. M., & Kertesz, A. (2024). *Exploring the Synergy of Fog Computing, Blockchain, and Federated Learning for IoT Applications: A Systematic Literature Review*. *IEEE Access*. https://doi.org/10.1109/access.2024.3398034

[5] Javed, F., Zeydan, E., Mangues-Bafalluy, J., et al. (2025). *Blockchain for Federated Learning in the Internet of Things: Trustworthy Adaptation, Standards, and the Road Ahead*. *arXiv*. https://doi.org/10.48550/arxiv.2503.23823

[6] Peng, K., Xiao, P., & Wang, S. (2024). *SCOF: Security-Aware Computation Offloading Using Federated Reinforcement Learning in Industrial Internet of Things with Edge Computing*. *IEEE Transactions on Services Computing*. https://doi.org/10.1109/tsc.2024.3377899

[7] Haldikar, S. V., Abdul Kader, O. F. M., & Yekollu, R. K. (2024). *Edge Computing and Federated Learning for Real-Time Anomaly Detection in Industrial Internet of Things (IIoT)*. ICICT 2024. https://doi.org/10.1109/icict60155.2024.10544912

[8] Sah, D. K., Vahabi, M., & Fotouhi, H. (2025). *Federated Learning at the Edge in Industrial Internet of Things: A Review*. *Sustainable Computing*. https://doi.org/10.1016/j.suscom.2025.101087

[9] (2024). *Federated Deep Recurrent Q-Learning for Task Partitioning and Resource Allocation in Satellite Mobile-Edge-Computing-Assisted Industrial IoT*. *IEEE Xplore*. https://ieeexplore.ieee.org/abstract/document/10522487/

[10] Lakhan, A., Groenli, T.-M., Bellavista, P., et al. (2024). *IoT workload offloading efficient intelligent transport system in federated ACNN integrated cooperated edge-cloud networks*. *Journal of Cloud Computing*. https://doi.org/10.1186/s13677-024-00640-w

[11] Mahesh, A. V., & Bhargava, S. (2024). *Design of an Iterative Method for Dynamic Resource Management in 5G Networks with IoT Integration Operations*. *Journal of Electrical Systems*. https://doi.org/10.52783/jes.2695

[12] Shompa, S. N. (2025). *Decentralized Federated Learning with Blockchain for Privacy-Preserving Edge AI in Smart Cities*. https://doi.org/10.64229/0a548k73

[13] Ahmad, M., & Jeon, G. (2025). *Federated Learning in Convergence ICT: A Systematic Review on Recent Advancements, Challenges, and Future Directions*. *CMC*. https://doi.org/10.32604/cmc.2025.068319

[14] Narkedimilli, S., Makam, S., & Sriram, A. (2025). *Enhancing IoT Network Security through Adaptive Curriculum Learning and XAI*. *arXiv*. https://doi.org/10.48550/arxiv.2501.11618

[15] Li, H., Ge, L., & Tian, L. (2024). *Survey: federated learning data security and privacy-preserving in edge-Internet of Things*. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-024-10774-7

[16] (2025). *Energy-Aware Edge Computing Models for Sustainable 5G-Enabled IoT Networks*. Zenodo. https://doi.org/10.5281/zenodo.16972423

[17] Thakur, D., Guzzo, A., & Fortino, G. (2024). *Green Federated Learning: A new era of Green Aware AI*. *arXiv*. https://doi.org/10.48550/arxiv.2409.12626

[18] Veeramachaneni, V. (2024). *Edge Computing: Architecture, Applications, and Future Challenges in a Decentralized Era*. Zenodo. https://doi.org/10.5281/zenodo.14166792

About the Author

Atine John Bosco is an ICT Consultant and researcher specialising in emerging technologies, digital transformation, and enterprise ICT strategy. A member of the British Computer Society (MBCS), Association for Computing Machinery (ACM), Society of Information Management (SIM), and IT Professionals Association (ITPA). This report is part of the *Research Insights Series* published at atine.info.