ICUBE5: A Conceptual Multidimensional Benchmarking Framework for AI-Native Secure 6G Edge Architectures

Daniel Sanusi *, Chibueze Ikpo, James Uhomoibhi

Posted Date: 3 June 2026

doi: 10.20944/preprints202606.0183.v1

Keywords: 6G networks; AI-native networking; secure edge computing; federated learning; network resilience; trust and governance; sustainable networking; intelligent infrastructure benchmarking

 doi:10.20944/preprints202606.0183.v1

Article

ICUBE5: A Conceptual Multidimensional Benchmarking Framework for AI-Native Secure 6G Edge Architectures

Daniel Sanusi [1,*], Chibueze Ikpo [1] and James Uhomoibhi [2]

[1] Veritas University

[2] Ulster University; j.uhomoibhi@ulster.ac.uk

* Correspondence: d.sanusi@ulster.ac.uk Tel.: +447765221394

Abstract

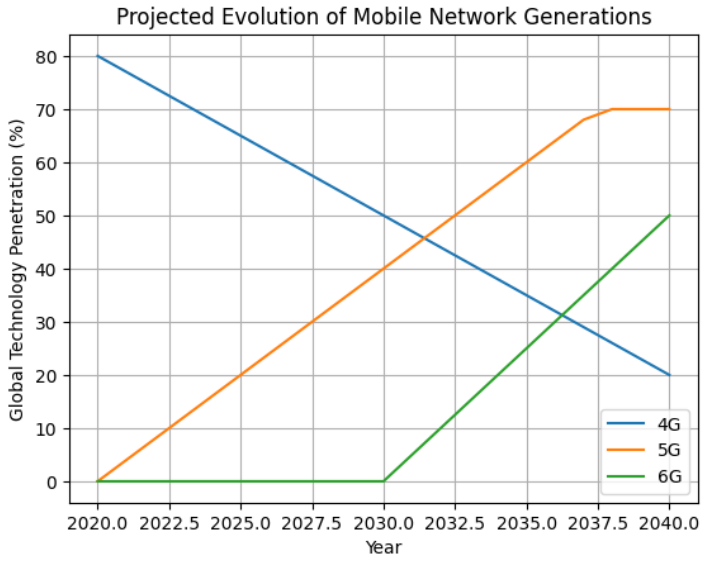
The transition toward 6G envisions network infrastructures that are AI-native, resilient by design, and aligned with emerging regulatory and sustainability expectations. While prior studies have explored AI-driven optimisation, edge intelligence, and secure distributed learning, these dimensions are often treated as isolated enhancements rather than interdependent architectural properties. This paper presents an AI-native safe edge architecture that combines distributed learning, adaptive control, and embedded trust mechanisms into a single cross-layer framework. To allow for systematic evaluation of such systems, we present the Intelligent Capability Unified Benchmarking Engine (ICUBE5), a multidimensional benchmarking construct that measures AI maturity, security resilience, governance alignment, adaptive stability, and sustainability efficiency. Through a comparative illustration of representative architectural archetypes, we demonstrate how cross-layer design choices influence overall infrastructure maturity under adversarial, operational, and regulatory constraints. The proposed framework provides a structured foundation for guiding intelligent 6G deployments and informing future standardisation and policy discussions beyond conventional performance-centric metrics.

Keywords: 6G networks; AI-native networking; secure edge computing; federated learning; network resilience; trust and governance; sustainable networking; intelligent infrastructure benchmarking

1. Introduction

The transition to sixth-generation (6G) wireless technology is reshaping the architectural frameworks of communication networks. Unlike earlier generations, which prioritised throughput, latency, and spectrum efficiency, 6G envisage infrastructures that are AI-native, self-adaptive, robust to adversary disruption, support ultra-low latency and massive connectivity, and are compliant with rising regulatory and sustainability standards [1,2]. Intelligence is no longer only an ancillary optimisation tool; it is becoming an integral part of network functioning. Recent 6G visions further emphasise AI-native orchestration, integrated sensing, distributed intelligence, trust-aware communication, and sustainability-aware infrastructure management as foundational capabilities for future intelligent networking ecosystems [1,2,27].

 doi:10.20944/preprints202606.0183.v1



Graph 1. Evolution of mobile network technologies illustrating the transition from 4G to 5G and projected emergence of 6G after 2030. [1,2].

The incorporation of AI into radio access and core network services has accelerated because of recent developments in edge computing, distributed learning, and federated intelligence [3–6]. At the same time, security structures are shifting towards zero-trust principles, and governance issues such as data sovereignty and algorithmic accountability have grown essential in the conception of infrastructure. However, these developments are usually pursued concurrently. AI optimisation, secure edge computing, governance compliance, and sustainability indicators are usually seen as separate design layers rather than interrelated architectural aspects.

The convergence of artificial intelligence, edge computing, and next-generation communication networks forms the foundation for intelligent network infrastructures capable of supporting future digital ecosystems.

Existing standardisation initiatives and strategic roadmaps, including ITU-R IMT-2030 and the Next G Alliance roadmap, primarily emphasise communication capability, service integration, spectral efficiency, and latency optimisation. However, comparatively fewer studies provide multidimensional benchmarking mechanisms capable of jointly evaluating governance alignment, adaptive resilience, sustainability efficiency, and distributed intelligence maturity in AI-native infrastructures [1,27].

Despite these advances, current 6G research remains fragmented across functional and disciplinary boundaries. AI optimisation, security resilience, governance compliance, and sustainability considerations are often developed in parallel rather than within a unified architectural framework. Consequently, there is limited methodological guidance for understanding how these interdependent capabilities collectively influence the maturity of intelligent network infrastructures.

This fragmentation creates a fundamental challenge: how should AI-native 6G infrastructures be evaluated when intelligence, resilience, trust, stability, and sustainability interact dynamically across layers? Conventional performance-centric metrics are insufficient to capture systemic maturity in such environments.

This article addresses this gap by proposing an AI-native secure edge architecture that integrates distributed learning, adaptive control, and embedded trust mechanisms within a unified cross-layer framework. To enable structured evaluation, we introduce the Intelligent Capability Unified Benchmarking Engine (ICUBE5), a multidimensional benchmarking construct capturing five interdependent capabilities: AI maturity, security resilience, governance alignment, adaptive stability, and sustainability efficiency.

 doi:10.20944/preprints202606.0183.v1

Unlike traditional optimisation metrics, the proposed framework evaluates infrastructure maturity as a composite architectural property. Through a comparative illustration of representative deployment archetypes, we demonstrate how cross-layer design choices influence systemic robustness under adversarial, operational, and regulatory constraints.

The contributions of this article are threefold:

1. We present a unified AI-native secure edge architecture for 6G that embeds intelligence, trust, and governance within network control loops.
2. We introduce the Intelligent Capability Unified Benchmarking Engine (ICUBE5) as a multidimensional evaluation construct for benchmarking heterogeneous intelligent deployments.
3. We provide an illustrative comparative analysis demonstrating how architectural integration affects overall infrastructure maturity.

The remainder of this article is organised as follows. Section 2 reviews related developments in AI-native networking and secure edge architectures. Section 3 presents the proposed cross-layer framework. Section 4 introduces the Intelligent Infrastructure Index. Section 5 provides a comparative architectural illustration. Section 6 discusses deployment implications and future research directions.

2. Related Work and Background

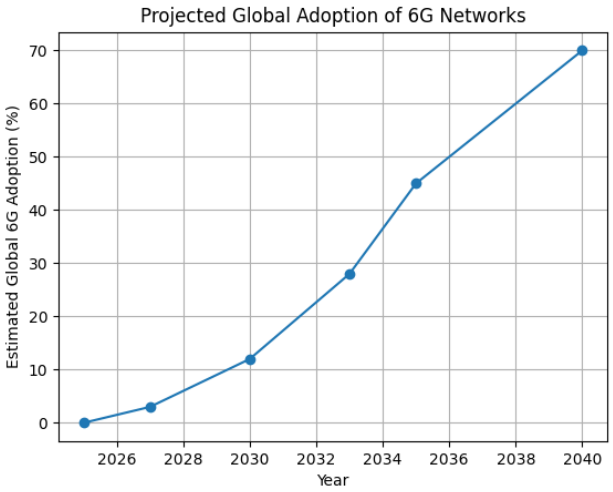
The integration of artificial intelligence into wireless networks has undergone significant evolution over the past decade. Early research focused on applying machine learning techniques to isolated optimisation tasks such as resource allocation, channel estimation, traffic prediction, and interference management [3,4]. These studies demonstrated measurable performance gains in dynamic environments and established the technical feasibility of data-driven control mechanisms in communication systems. Recent studies increasingly emphasise edge intelligence, autonomous orchestration, distributed learning coordination, and adaptive optimisation as central enablers of intelligent 6G infrastructures [4,19,20].

As research matured, attention shifted toward the concept of AI-native networking, in which learning models are embedded within network control loops rather than deployed as external optimisation modules. This shift aligns with emerging 6G visions emphasising autonomous operation, context awareness, and self-optimising radio access networks [1,2]. Distributed and federated learning approaches have further enabled collaborative intelligence across heterogeneous devices and edge nodes, reducing centralised data exposure while maintaining model adaptability [5–7].

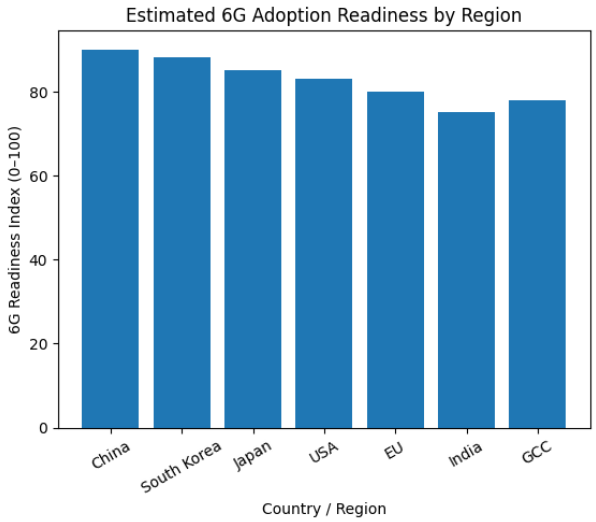
Edge computing is key to this progress. Edge designs reduce latency by moving computer resources closer to end users, enabling real-time adaptation under severe service restrictions. The combination of edge intelligence and federated aggregation approaches allows for scalable AI deployment across large-scale infrastructures while resolving bandwidth and privacy problems.

Parallel to AI integration, security paradigms in communication systems have progressed toward resilience-oriented and zero-trust frameworks [8,9]. Modern network security increasingly incorporates adversarial robustness, anomaly detection within learning pipelines, and continuous authentication models. Furthermore, governance issues such as data sovereignty, explainability, and regulatory compliance are evolving into structural restrictions in infrastructure design rather than external policy overlays [2,10]. Several countries and regions have launched national 6G initiatives and research programmes to accelerate next-generation network deployment [1,27]. Global research roadmaps anticipate the gradual deployment and adoption of 6G networks beginning around 2030, as illustrated in Graph 2.

 doi:10.20944/preprints202606.0183.v1



Graph 2. Projected global adoption trajectory of 6G networks based on industry research roadmaps and deployment forecasts.



Graph 3. Estimated readiness levels for early 6G deployment across leading regions based on national research initiatives, infrastructure investment, and telecommunications development strategies. [1,27].

Table 1. Global 6G development initiatives and expected deployment timelines.

Region	Expected 6G Deployment	Key Drivers
China	2030	Massive R&D investment
South Korea	2030	Telecom leadership
Japan	2030–2031	National 6G strategy
USA	2030	Industry ecosystem
Europe	2031	Research programmes
India	2030–2032	Rapid telecom growth

Sustainability has also emerged as a key problem for next-generation networks. Energy-aware scheduling, carbon-efficient infrastructure planning, and lifetime optimisation methodologies are currently part of 6G research roadmaps. However, sustainability metrics are frequently evaluated separately from intelligence maturity and security resilience, resulting in fragmented evaluation techniques.

 doi:10.20944/preprints202606.0183.v1

Despite these developments, most contemporary systems evaluate AI performance, security robustness, and energy efficiency independently. There are currently few comprehensive benchmarking frameworks that examine intelligence maturity, resilience, governance alignment, adaptive stability, and sustainability efficiency simultaneously. As 6G infrastructures become more AI-native and cross-layer dependent, there is a greater demand for multidimensional evaluation approaches that can capture systemic architectural maturity rather than single-metric optimisation.

The framework proposed in this article addresses this gap by integrating architectural design and structured benchmarking within a unified perspective tailored to AI-native secure edge deployments.

3. AI-Native Secure Edge Architecture

Instead of being introduced as supplementary modules, the suggested architecture sees 6G infrastructure as an AI-native, cross-layer system with learning, control, security, and governance mechanisms integrated. The Intelligence Layer, the Execution Layer, and the Governance and Trust Layer are the three interconnected parts of the tiered system shown in Figure 1.

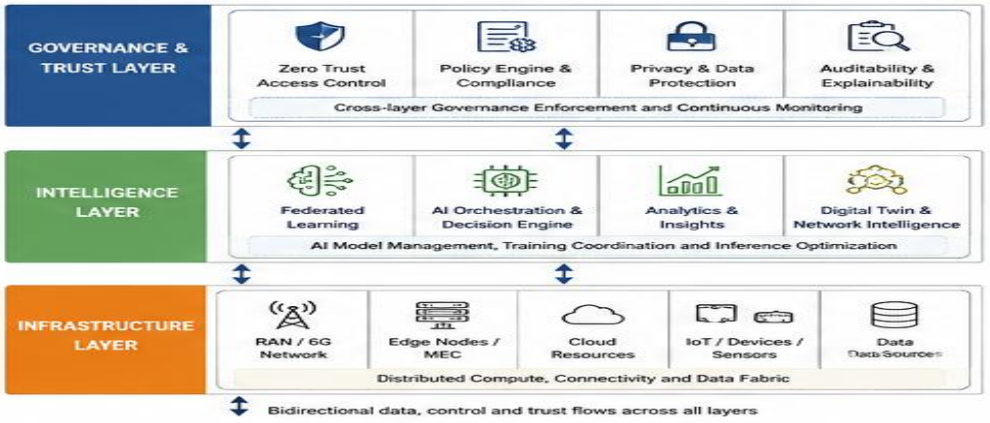


Figure 1. AI-native secure edge architecture for 6G infrastructures illustrating the interaction between intelligence, execution, and governance layers in a cross-layer network design.

3.1. Intelligence Layer

The Intelligence Layer embeds distributed learning capabilities across edge nodes and core network entities. Instead of depending primarily on a centralised model training, learning processes are carried out collaboratively via federated and distributed aggregation systems. Federated learning enables collaborative model training across distributed infrastructures while preserving local data ownership and reducing centralised exposure risks [6–8,28]. Edge devices train models locally on contextual data, while periodic aggregation provides global coherence without disclosing raw data. However, federated learning systems remain vulnerable to adversarial behaviours such as Byzantine attacks, where malicious participants introduce corrupted updates into the aggregation process. Additional threats include model poisoning, gradient leakage, membership inference attacks, stealth backdoor insertion, and adversarial manipulation of distributed model updates [31–33].

 doi:10.20944/preprints202606.0183.v1

Figure 2. Projected 6G deployment timeline and adoption forecast adapted from ITU-R IMT-2030 and Next G Alliance roadmaps.

This layer enables:

- Real-time traffic prediction and adaptive resource allocation
- Context-aware mobility management
- Anomaly detection within network flows
- Continuous policy refinement under dynamic conditions

Crucially, intelligence operates within closed-loop control cycles, allowing network policies to adapt to stochastic traffic variations and environmental uncertainties.

3.2. Execution Layer

The Execution Layer translates learned policies into operational network control actions. It encompasses radio access functions, scheduling mechanisms, routing logic, and orchestration modules. Control decisions generated by the Intelligence Layer are applied through adaptive scheduling, dynamic spectrum allocation, and service prioritisation mechanisms.

To ensure stability, the execution process includes feedback monitoring, which continuously assesses system state factors like latency, congestion, and energy usage. Deviations cause policy modifications in the Intelligence Layer, resulting in a continual adaptive cycle.

This bidirectional interaction ensures that learning is grounded in operational feedback rather than abstract optimisation objectives.

3.3. Governance and Trust Layer

Beyond speed optimisation, AI-native 6G systems must have inbuilt trust and governance limitations. The Governance and Trust Layer implements security verification, adversarial robustness methods, compliance procedures, and data privacy regulations. Recent governance frameworks further emphasise explainability, auditability, transparency, accountability, and trustworthy AI deployment as critical requirements for future intelligent infrastructures [29,30].

Unlike typical perimeter defences, this layer incorporates continuous verification into learning pipelines. Model updates are checked for integrity, anomalous patterns in training signals are identified, and access constraints are dynamically implemented across remote nodes.

Beyond Byzantine attacks, federated intelligence infrastructures remain vulnerable to additional threats, including model poisoning attacks, data poisoning attacks, membership inference attacks, gradient leakage, reconstruction attacks, and stealth backdoor manipulation. To mitigate these risks,

 doi:10.20944/preprints202606.0183.v1

the proposed architecture incorporates continuous trust validation, encrypted aggregation mechanisms, anomaly-aware update filtering, and policy-driven access control enforcement across distributed edge participants.

Governance policies, such as data locality requirements or regulatory constraints, are encoded as operational parameters that shape learning and execution behaviour. As a result, compliance is not externally audited but internally operationalised.

3.4. Cross-Layer Integration

The suggested architecture is distinguished by its interaction between layers. Intelligence drives execution, execution creates feedback that helps to enhance intelligence, and governance limitations shape both processes simultaneously. Energy efficiency and environmental goals are similarly interwoven throughout levels, rather than being considered as separate optimisation aims. To enable coordinated optimisation across learning, execution, and governance mechanisms, a latency-aware secure aggregation framework is introduced.

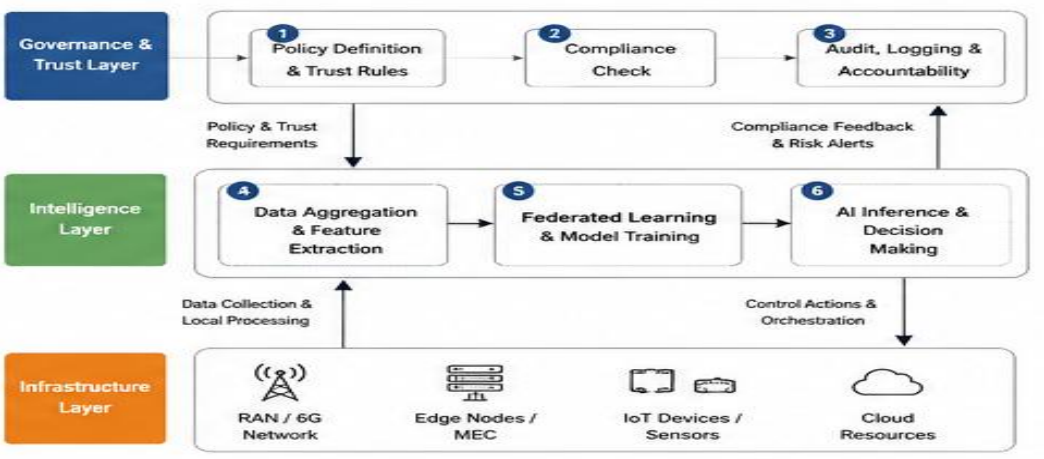


Figure 3. Cross-layer AI-orchestrated data, control, and governance flow across infrastructure, intelligence, and trust layers in the proposed AI-native 6G architecture.

Architectural Layer	Core Functions	Primary ICUBE5 Dimensions
Intelligence Layer	Federated learning, distributed orchestration, adaptive optimisation	AI maturity, adaptive stability
Execution Layer	Scheduling, routing, resource allocation, service coordination	Adaptive stability, sustainability efficiency
Governance & Trust Layer	Policy enforcement, trust validation, compliance auditing	Security resilience, governance alignment

The ICUBE5 framework emerges directly from the measurable operational objectives of the proposed architecture. Each architectural layer contributes distinct infrastructure characteristics that collectively shape multidimensional system maturity across intelligence capability, resilience, governance consistency, adaptive stability, and sustainability efficiency.

This integrated design guarantees that performance, resilience, and compliance improve in sync. Rather than maximising isolated metrics, the architecture promotes systemic maturity across intelligence capability, trust resilience, adaptive stability, and sustainability efficiency.

The following section introduces a structured framework for evaluating this multidimensional maturity through the Intelligent Infrastructure Index.

 doi:10.20944/preprints202606.0183.v1

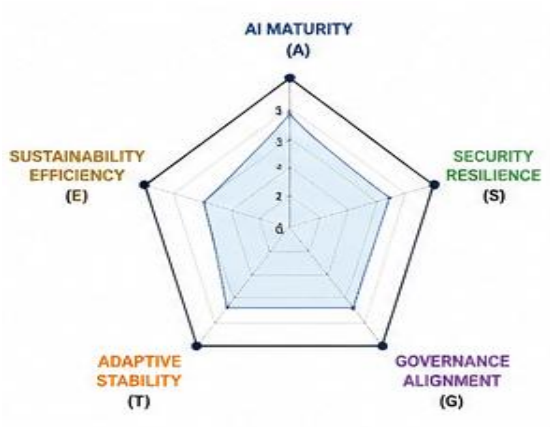
4. ICUBE5: Intelligent Capability Unified Benchmarking Engine

Examining infrastructure maturity requires going beyond conventional performance measurements like throughput, latency, and spectral efficiency as 6G systems move toward AI-native designs. The systemic relationships among embedded intelligence, adversarial resilience, governance alignment, adaptive control stability, and sustainability efficiency are not captured by these metrics, despite their continued usefulness. To overcome this gap, we present the Intelligent Capability Unified Benchmarking Engine (ICUBE5), a multidimensional benchmarking tool for assessing integrated architectural maturity.

Existing 6G evaluation frameworks primarily emphasise communication-centric indicators such as throughput, latency, reliability, and spectral efficiency. However, AI-native infrastructures introduce multidimensional requirements involving governance consistency, adaptive resilience, sustainability optimisation, and distributed intelligence coordination [1,27].

Communication-centric metrics, including throughput, latency, spectral efficiency, and reliability, are the main focus of current 6G assessment frameworks. AI-native infrastructures, however, bring with them new multifaceted needs that include trust-aware orchestration, distributed intelligence coordination, governance consistency, adaptive resilience, and sustainability optimisation. The ICUBE5 framework is therefore proposed as a complementary multidimensional benchmarking methodology intended to evaluate intelligent infrastructure maturity beyond conventional network performance metrics.

The ICUBE5 framework unifies five interdependent capability dimensions, AI maturity, security resilience, governance alignment, adaptive stability, and sustainability efficiency, into a single structured benchmarking model for intelligent 6G infrastructures. It permits the comparative evaluation of diverse 6G installations under varied operational and regulatory restrictions. The conceptual structure of the Intelligent Capability Unified Benchmarking Engine (ICUBE5) is illustrated in Figure 4.



Dimension	Symbol	Measurement Goal	Example Indicators
AI Maturity	A	Capability and effectiveness of AI-native functions	• FL adoption rate • Inference latency • Model accuracy
Security Resilience	S	Robustness against threats and vulnerabilities	• Attack detection • Byzantine tolerance • Recovery time
Governance Alignment	G	Alignment with policies, ethics and regulations	• Explainability • Auditability • Privacy compliance
Adaptive Stability	T	Ability to adapt and maintain stable performance	• Load adaptation • QoS stability • Resource elasticity
Sustainability Efficiency	E	Efficient use of resources with minimal impact	• Energy efficiency • Carbon footprint • Green orchestration

Composite ICUBE5 Score: $S = \sum_{i=1}^{5} w_i \cdot x_i$, where $\sum_{i=1}^{5} w_i = 1$, $0 \le w_i \le 1$

x_i : Normalized score of dimension i (range: 0–5); w_i : Weight of dimension i

Figure 4. ICUBE5 multidimensional benchmarking framework for evaluating AI-native 6G infrastructure across AI maturity, security resilience, governance alignment, adaptive stability, and sustainability efficiency.

4.1. Multidimensional Structure

The ICUBE5 aggregates five bounded dimensions representing core properties of AI-native secure edge infrastructures:

- **AI Maturity (A)** refers to the extent of embedded intelligence, model flexibility, distributed learning integration, and real-time inference capabilities across network levels.

 doi:10.20944/preprints202606.0183.v1

- **Security and Trust Resilience (S)** refers to the effectiveness of adversarial robustness approaches, anomaly detection pipelines, continuous authentication, and model integrity validation.
- **Governance Alignment (G)** is the integration of regulatory compliance, data sovereignty constraints, auditability procedures, and policy-aware control parameters.
- **Adaptive Stability (T)** is the ability of closed-loop control to endure stochastic traffic circumstances, adversarial disturbances, and dynamic workload changes.
- **Sustainability Efficiency (E)** refers to energy-efficient operation, carbon-aware resource allocation, and environmentally sustainable infrastructure design.

To enable comparison across various infrastructures, each dimension is normalised to the interval [0,1]. The ICUBE5 is expressed as:

$$ICUBE5 = w_A A + w_S S + w_G G + w_T T + w_E E$$

Subject to:

$$0 \leq w_i \leq 1$$

and

$$w\_A + w\_S + w\_G + w\_T + w\_E = 1$$

Where:

- A = AI maturity
- S = Security resilience
- G = Governance alignment
- T = Adaptive stability
- E = Sustainability efficiency

Weight coefficients may be determined using expert elicitation, analytic hierarchy process (AHP), entropy-based weighting, or deployment-specific policy prioritisation, depending on operational objectives and regulatory requirements.

4.2. Normalisation and Weighting Strategy

Because of size disparities, normalisation ensures that no one dimension is dominating. Quantitative measurements (such as energy consumption per bit or adversary detection rate) or structured qualitative evaluations (such as governance compliance maturity levels) can be used as indicators for each dimension. The ICUBE5 maintains its interpretability and comparability across many deployments by restricting all dimensions to a comparable period.

The weighting mechanism introduces policy-adjustable benchmarking. For instance, whereas urban smart infrastructure projects may prioritise sustainability and regulatory compliance, mission-critical industrial networks may prioritise stability and resilience. This flexibility preserves structural integrity while enabling context-aware evaluation. The computational workflow used to derive the Intelligent Capability Unified Benchmarking Engine (ICUBE5) score from its multidimensional inputs is illustrated in Figure 5.

Positive-benefit indicators are normalised using:

x′_i = \frac{x_i - \min(x)}{\max(x)-\min(x)}

]

while negative-cost indicators are normalised using:

x′_i = \frac{\max(x)-x_i}{\max(x)-\min(x)}

]

To reduce sensitivity to extreme values, percentile clipping or robust scaling approaches may additionally be incorporated during preprocessing. Furthermore, nonlinear utility growth may be represented through logarithmic or sigmoid transformation functions in cases where marginal infrastructure improvements exhibit diminishing returns.

 doi:10.20944/preprints202606.0183.v1

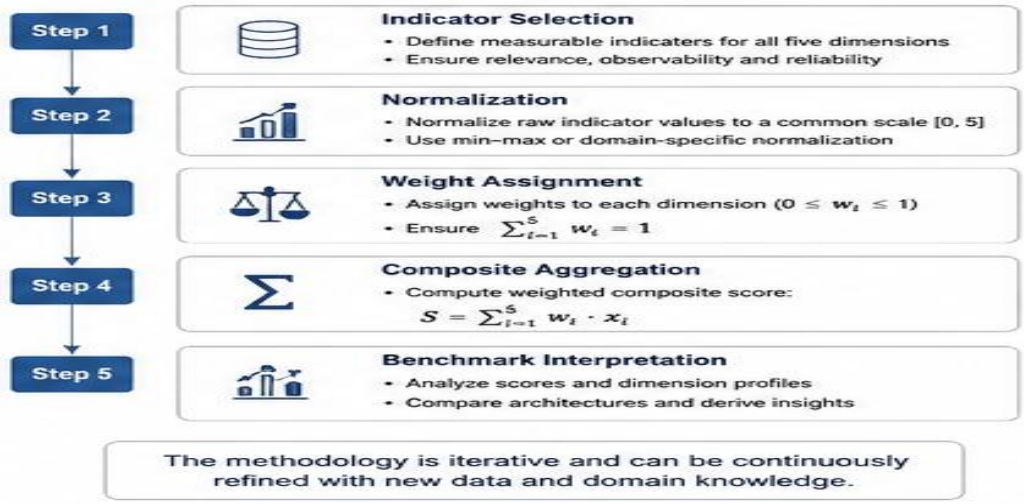


Figure 5. ICUBE5 evaluation methodology comprises indicator selection, normalisation, weight assignment, composite aggregation, and benchmark interpretation.

The procedural computation process of the ICUBE5 framework is further illustrated in Figure 6.

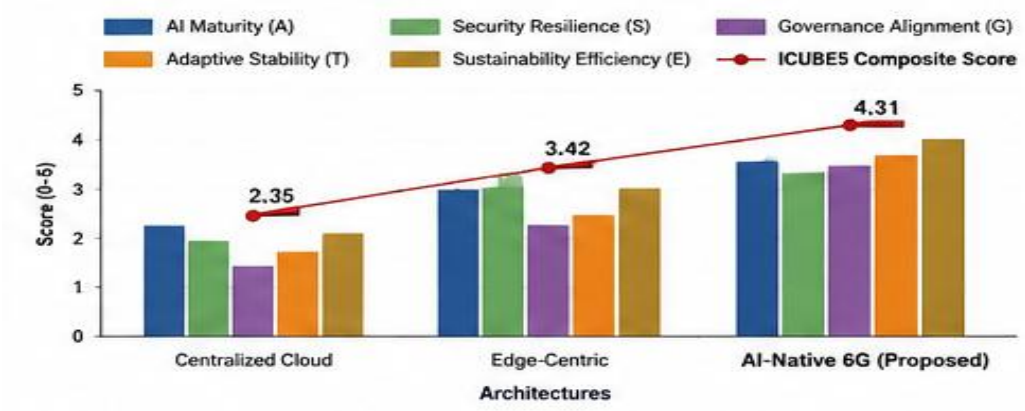


Figure 6. Comparative ICUBE5 score evaluation across centralised cloud, edge-centric, and AI-native 6G architectures.

4.3. Cross-Layer Trade-Off Visibility

A central advantage of the ICUBE5 is its ability to expose cross-layer trade-offs. Enhancing distributed intelligence without corresponding investment in trust validation mechanisms may increase A while degrading S. Similarly, aggressive energy optimisation strategies may improve E but risk destabilising adaptive control loops if not carefully coordinated. By aggregating multidimensional properties, the ICUBE5 makes such systemic interactions visible during benchmarking rather than obscured within isolated KPIs.

Although the present framework evaluates dimensions independently for interpretability, future extensions may incorporate interaction terms between infrastructure indicators. Such extensions may be represented as:

ICUBE5_{ext} = \sum w_ix_i + \sum \lambda_{ij}(x_ix_j)

]

where λ_{ij} represents the interaction strength between infrastructure dimensions. This extension would enable the framework to capture latent dependencies between intelligence maturity, resilience mechanisms, governance constraints, and sustainability optimisation.

 doi:10.20944/preprints202606.0183.v1

4.4. Role in 6G Infrastructure Assessment

As 6G infrastructures become increasingly autonomous and policy-constrained, multidimensional evaluation frameworks will be necessary to guide design and deployment decisions. The ICUBE5 provides a structured foundation for assessing systemic maturity across AI-native secure edge architectures. It supports comparative analysis among heterogeneous deployments and facilitates alignment between technical optimisation and regulatory objectives.

The next section illustrates the application of the ICUBE5 through a comparative analysis of representative architectural archetypes.

5. Comparative Illustration of Architectural Archetypes

The following evaluation is intended as an illustrative analytical benchmarking exercise designed to demonstrate the interpretability and comparative applicability of the ICUBE5 framework under representative architectural scenarios. The resulting scores should therefore be interpreted as structured conceptual assessments rather than empirical deployment measurements.

To demonstrate the interpretability of the Intelligent Capability Unified Benchmarking Engine (ICUBE5), we consider three representative architectural archetypes that reflect common deployment strategies in emerging 6G environments. The purpose of this illustration is not to provide empirical benchmarking results, but to highlight how multidimensional evaluation reveals systemic trade-offs across integrated capabilities.

To illustrate the applicability of the Intelligent Infrastructure Index, a comparative scoring exercise was conducted across three representative infrastructure paradigms: cloud-centric networks, edge-centric architectures, and the proposed AI-native secure edge infrastructure. Each architecture was evaluated across the five infrastructure capability dimensions defined earlier. The resulting scores and computed ICUBE5 values are presented in Table 2. The scores used in this comparative analysis represent illustrative benchmark values derived from infrastructure capability assessments and are intended to demonstrate the application of the proposed ICUBE5 framework.

Table 2. Comparative Evaluation of Infrastructure Architectures Using ICUBE5.

Infrastructure Type	AI	Security	Governance	Stability	Sustainability	ICUBE5
Cloud-centric	0.55	0.45	0.60	0.50	0.40	0.50
Edge-centric	0.65	0.55	0.60	0.65	0.50	0.59
Proposed architecture	0.82	0.75	0.70	0.78	0.72	0.75

For illustration consistency, similar weighting coefficients were employed across all five dimensions during the comparison study.

$w_A = w_S = w_G = w_T = w_E = 0.20$

]

The presented values are derived from structured architectural capability assessments based on distributed intelligence integration, governance embedding, adaptive coordination capability, adversarial resilience mechanisms, and sustainability-aware orchestration characteristics described within each architectural archetype.

The comparative analysis indicates that the proposed AI-native secure edge architecture achieves the highest Intelligent Infrastructure Index score (0.75), reflecting stronger performance across multiple infrastructure capability dimensions. In particular, improvements in AI maturity, security resilience, and adaptive stability contribute significantly to the overall index value. In contrast, traditional cloud-centric architectures exhibit lower security and sustainability performance due to centralised processing constraints.

 doi:10.20944/preprints202606.0183.v1

5.1. Centralised Intelligence Architecture

The first archetype represents a predominantly centralised AI architecture in which model training and decision-making occur within core network entities. Edge nodes perform limited local processing and rely on centralised aggregation for policy updates.

Such architectures may achieve strong AI maturity (A) in terms of global model coherence and centralised optimisation. However, security resilience (S) may be constrained by increased attack surfaces associated with centralised aggregation points. Governance alignment (G) may benefit from simplified compliance monitoring, yet sustainability efficiency (E) may suffer due to increased backhaul communication and energy consumption. Adaptive stability (T) may also be impacted by latency-induced feedback delays.

Under the ICUBE5 framework, this archetype may demonstrate high intelligence maturity but moderate composite maturity due to imbalances across resilience and sustainability dimensions.

5.2. Distributed Edge Intelligence Architecture

The second archetype reflects a distributed edge-centric deployment, where learning and inference are executed locally across multiple edge nodes using federated aggregation. Decision-making loops are shorter, and contextual adaptation is faster.

This architecture may improve adaptive stability (T) and sustainability efficiency (E) by reducing centralised data transfer and enabling localised optimisation. Security resilience (S) may improve through distributed trust verification mechanisms, although coordination complexity increases. Governance alignment (G) may need more complex policy encoding to ensure compliance across diverse nodes.

Within the ICUBE5 framework, this archetype frequently achieves a more balanced maturity profile, but coordination overhead and heterogeneity management are still design problems.

5.3. Governance-Embedded Secure Architecture

The third archetype emphasises embedded governance and adversarial robustness mechanisms integrated directly into learning and control processes. Zero-trust validation, model integrity verification, and policy-aware execution constraints are tightly coupled with distributed intelligence.

This approach may strengthen security resilience (S) and governance alignment (G) substantially, while maintaining competitive AI maturity (A). However, increased verification overhead may influence sustainability efficiency (E), and the complexity of integrated trust pipelines may affect adaptive stability (T) if not carefully engineered.

The ICUBE5 framework reveals how prioritising embedded trust reshapes the overall maturity profile, highlighting the importance of coordinated cross-layer optimisation.

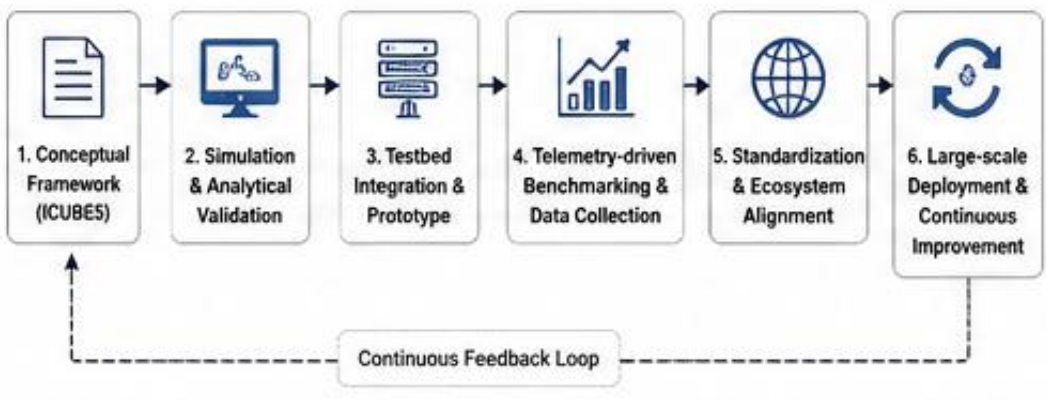


Figure 7. Conceptual future research and deployment pathway for ICUBE5, progressing from theoretical formulation to simulation, testbed validation, telemetry-driven benchmarking, and standardisation alignment.

 doi:10.20944/preprints202606.0183.v1

These five dimensions were selected based on recurring architectural priorities identified in recent 6G roadmaps and AI-native network research. Recent optimisation and adaptive control studies further reinforce the importance of stability-aware orchestration, sensor-aware optimisation, and dynamic reward balancing in intelligent autonomous systems [36,37]. Together, they capture the operational, security, regulatory, adaptive, and sustainability characteristics increasingly recognised as fundamental to future network infrastructures.

5.4. Interpretive Insights

Across the three archetypes, the ICUBE5 exhibits its potential to uncover multidimensional trade-offs that traditional performance measurements would miss. Rather than rating systems only on throughput or latency, the composite evaluation prioritises systemic maturity patterns as indicated by cross-layer integration choices.

Crucially, the model permits stakeholders to alter the weighting parameters in order to achieve their own goals. As an example, though sustainable structures may place a higher priority on energy efficiency, safety-critical designs could prioritise stability and resilience. This flexibility guarantees that benchmarking is policy-aware and deployment-sensitive.

Sensitivity analysis under alternative weighting distributions further indicates that architectures with stronger cross-layer coordination maintain more stable multidimensional maturity profiles across varying deployment priorities. In contrast, fragmented architectures exhibit greater score variability when governance, resilience, or sustainability priorities are adjusted.

These illustrated comparisons demonstrate the need for organised multidimensional evaluation in guiding AI-native 6G architecture growth.

5.5. Comparative Maturity Interpretation

When examined equally across all five dimensions, the distributed edge intelligence architecture often has the best balanced maturity profile, owing to its integration of localised adaptability and distributed resilience mechanisms. Centralised intelligence systems, on the other hand, may show great AI maturity but have vulnerabilities in resilience and sustainability in hostile or heavy-load scenarios. Governance-enabled secure architectures, although improving trust alignment and compliance robustness, may result in increased operational overhead that must be carefully tuned to maintain adaptive stability and energy efficiency.

These distinctions demonstrate that architectural excellence cannot be evaluated using a single performance indicator. Instead, systemic maturity results from coordinated cross-layer design decisions.

5.6. Policy-Adjusted Weighting Scenario

To further illustrate interpretability, consider two deployment contexts:

- In **Safety-Critical Industrial Automation**, higher weights attributed to resilience (S) and adaptive stability (T) would prefer designs with embedded trust and robust control integration.
- **Sustainability-Driven Smart Urban Networks:** Putting more focus on sustainability efficiency (E) and governance alignment (G) may elevate dispersed edge-centric architectures that use energy-efficient coordination mechanisms.

The ICUBE5 allows deployment-sensitive benchmarking without compromising structural integrity by modifying weight parameters while maintaining dimensional normalisation. This flexibility allows regulators, operators, and system designers to match infrastructure evaluation to context-specific goals.

5.7. Implications for Architectural Evolution

The comparison research shows that AI-native 6G progress should not be fuelled exclusively by performance optimisation or isolated resilience improvements. Rather, a single architectural plan that

 doi:10.20944/preprints202606.0183.v1

incorporates intelligence capability, adversarial robustness, policy compliance, adaptive stability, and sustainability concerns determines the maturity of an infrastructure.

Because of this, the ICUBE5 framework facilitates cross-layer collaboration at the first stages of architectural development by acting as both a benchmarking tool and a design guide.

6. Discussion and Deployment Implications

The move to AI-native 6G infrastructures creates new systemic difficulties that go beyond performance optimisation. As intelligence becomes more integrated into network control loops, security enforcement, governance limitations, and sustainability goals must be regarded as structural design factors rather than afterthoughts. The suggested architecture and Intelligent Capability Unified Benchmarking Engine (ICUBE5) offer a single approach to resolving these interconnected objectives.

6.1. Implications for 6G Deployment

Emerging 6G visions highlight autonomous network operation, AI-driven radio access development, and integrated sensing and communication capabilities [1,2]. In these situations, infrastructure maturity will be determined by the coordinated growth of distributed intelligence, adversary resilience, policy compliance, and energy efficiency.

The ICUBE5 framework supports deployment decision-making by enabling comparative benchmarking across heterogeneous architectures. Operators can evaluate trade-offs between centralised optimisation and distributed adaptability. Regulators can assess governance alignment and compliance integration. System designers can detect cross-layer imbalances that are not obvious using traditional KPIs.

Importantly, incorporating governance and trust limitations into architectural design may lower long-term compliance costs while increasing public confidence in AI-powered infrastructures. This proactive integration is consistent with wider worldwide issues on ethical and trustworthy AI deployment in critical systems.

6.2. Standardisation and Policy Alignment

As international authorities develop 6G standards roadmaps, intelligence-native architectures are widely regarded as fundamental design concepts. However, established evaluation procedures for multidimensional maturity are still in their early stages of development.

The ICUBE5 framework provides a structured conceptual platform for future benchmarking standards and cross-domain assessment approaches. While not intended to be a prescriptive standard, it does provide a flexible framework that may adapt to changing governmental aims and regional regulatory demands.

The framework bridges the gap between technological optimisation and governance objectives by allowing for policy-adjustable weighting, facilitating harmonised infrastructure evolution across varied deployment circumstances.

6.3. Limitations and Future Research

Several limitations warrant consideration. First, the ICUBE5 currently represents a formalised conceptual benchmarking framework rather than an experimentally validated operational evaluation engine. The illustrative comparative scenarios are therefore intended to demonstrate interpretability and multidimensional assessment capability rather than empirical performance superiority. The objective of the current work is to establish a multidimensional assessment foundation capable of supporting future empirical benchmarking, executable toolchains, and telemetry-driven infrastructure validation environments. Future studies should look at quantitative validation in real-world testbeds and simulation settings to improve indicator selection and normalisation procedures.

 doi:10.20944/preprints202606.0183.v1

Second, cross-layer interdependencies in AI-native systems provide dynamic feedback effects that static composite weighting may not completely capture. Future research may therefore explore nonlinear aggregation models, adaptive weighting systems, interaction-aware indicators, and telemetry-driven benchmarking mechanisms capable of capturing evolving infrastructure behaviour over time. Future research on adaptive or time-varying weighting systems represents an important direction for improving multidimensional infrastructure evaluation.

Third, research into the integration of sustainability indicators with adversarial robustness and adaptive control stability remains critical, particularly for large-scale heterogeneous deployments.

To overcome these limits, multidisciplinary collaboration amongst fields such as cybersecurity, machine learning, communication systems, and regulatory policy is required.

7. Conclusion

The evolution toward 6G marks a structural transition in communication system design, where intelligence, resilience, governance alignment, and sustainability must be embedded within the architectural fabric of network infrastructures. Treating these properties as isolated optimisation targets is no longer sufficient in AI-native environments characterised by dynamic workloads, adversarial risks, and regulatory constraints.

This article presented a unified AI-native secure edge architecture that integrates distributed learning, adaptive control, and embedded trust mechanisms within a cross-layer framework. To facilitate the systematic evaluation of such systems, we proposed the Intelligent Capability Unified Benchmarking Engine (ICUBE5), a multidimensional benchmarking construct that measures AI maturity, security resilience, governance alignment, adaptive stability, and sustainability efficiency.

We illustrated how cross-layer design decisions impact systemic maturity beyond traditional performance-centric measures by comparing representative 6G architectural paradigms. The suggested approach emphasises the need for coordinated integration across intelligence, trust, and sustainability domains in determining the resilience of next-generation infrastructures.

Multidimensional assessment techniques will play a bigger role in directing architectural choices and coordinating technological optimisation with social and regulatory objectives as 6G standardisation and implementation initiatives pick up speed. The framework proposed in this article contributes a structured conceptual foundation for multidimensional intelligent infrastructure assessment in AI-native 6G systems while highlighting important directions for future empirical validation, executable benchmarking environments, and cross-domain evaluation research.

Author Contributions: Conceptualisation, D.S. and C.I.; methodology, D.S. and C.I.; validation, D.S. and C.I.; formal analysis, D.S.; investigation, D.S. and C.I.; resources, J.U.; data curation, D.S.; writing—original draft preparation, D.S.; writing—review and editing, D.S., C.I. and J.U.; visualisation, D.S.; supervision, J.U.; project administration, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analysed in this study. Data sharing does not apply to this article as the results are based on conceptual modelling and illustrative analysis.

Acknowledgements: The authors wish to thank colleagues at Veritas University and Ulster University. The authors also acknowledge the staff of the MarvLaboratory and CRESTech for their research support and technical contributions that helped shape parts of the analysis.

Conflicts of Interest: The authors declare no conflicts of interest.

 doi:10.20944/preprints202606.0183.v1

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Meaning
6G	Sixth Generation Wireless Networks
AI	Artificial Intelligence
MEC	Multi-access Edge Computing
FL	Federated Learning
KPI	Key Performance Indicator
ICUBE5	Intelligent Capability Unified Benchmarking Engine (5 Dimensions)
RAN	Radio Access Network
ITU	International Telecommunication Union

References

1. International Telecommunication Union (ITU-R), *Framework and Overall Objectives of the Future Development of IMT for 2030 and Beyond (IMT-2030)*, Recommendation ITU-R M.2160, 2023.
2. W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2020.
3. J. Gao, W. Wu, M. Li, C. Zhou and W. Zhuang, "Holistic Network Virtualization and Pervasive Network Intelligence for 6G," *arXiv preprint arXiv:2301.00519*, 2023.
4. Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo and J. Zhang, "Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1738–1762, 2019.
5. Y. Mao, C. You, J. Zhang, K. Huang and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.
6. M. Al-Quraan et al., "Edge-Native Intelligence for 6G Communications Driven by Federated Learning: Trends and Challenges," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 7, no. 3, pp. 957–979, 2023.
7. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proc. AISTATS*, 2017.
8. Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated Machine Learning: Concept and Applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, 2019.
9. K. Ramezanpour and J. Jagannath, "Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the Context of O-RAN," Computer Networks, vol. 217, 109358, 2022.
10. S. Rose, O. Borchert, S. Mitchell and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, 2020.
11. R. Roman, J. Lopez and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.
12. Y. Wang, X. Kang, T. Li, H. Wang, C. K. Chu and Z. Lei, "SIX-Trust for 6G: Toward a Secure and Trustworthy Future Network," IEEE Access, vol. 11, pp. 107657–107668, 2023.
13. H. F. Atlam et al., "Role of Blockchain and AI in Security and Privacy of 6G," in *AI and Blockchain Technology in 6G Wireless Network*, Springer, 2022.
14. A. V. Rial et al., "The Role of AI in 6G MAC," *TechRxiv*, 2023. doi:10.36227/techrxiv.23708310.v2.
15. S. Wang et al., "Adaptive Federated Learning in Resource-Constrained Edge Computing Systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.
16. T. Taleb et al., "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Architecture," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, 2017.
17. Y. Liu et al., "Federated Learning for 6G Communications: Challenges, Methods, and Future Directions," *China Communications*, vol. 17, no. 9, pp. 105–118, 2020.
18. G. Liu et al., "6G Autonomous Radio Access Network Empowered by Artificial Intelligence and Network Digital Twin," *Frontiers of Information Technology & Electronic Engineering*, 2025.

 doi:10.20944/preprints202606.0183.v1

19. J. Park, S. Samarakoon, M. Bennis and M. Debbah, "Wireless Network Intelligence at the Edge," *Proceedings of the IEEE*, vol. 107, no. 11, pp. 2204–2239, 2019.
20. M. J. Neely, *Stochastic Network Optimization with Application to Communication and Queueing Systems*, Morgan & Claypool, 2010.
21. A. Bianzino et al., "A Survey of Green Networking Research," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 1, pp. 3–20, 2012.
22. A. Chorti, "Trust and Physical Layer Security for 6G Cyber-Physical Systems," *Harvard Data Science Review*, 2023.
23. S. H. A. Kazmi et al., "Security of Federated Learning in 6G Era: A Review on Conceptual Techniques and Software Platforms Used for Research and Analysis," *Computer Networks*, vol. 245, 110358, 2024.
24. European Commission High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, European Commission, 2019.
25. GSMA Intelligence, "The Mobile Economy 2024," GSMA Intelligence, 2024. [Online]. Available: https://www.gsmaintelligence.com/research/the-mobile-economy-2024
26. Next G Alliance, Roadmap to 6G: Building the Foundation for North American Leadership in 6G and Beyond, ATIS Next G Alliance, 2022. [Online]. Available: https://nextgalliance.org/wp-content/uploads/2022/02/NextGA-Roadmap.pdf
27. P. Kairouz et al., "Advances and Open Problems in Federated Learning," *Foundations and Trends in Machine Learning*, vol. 14, nos. 1–2, pp. 1–210, 2021.
28. L. Floridi and J. Cowls, "A Unified Framework of Five Principles for AI in Society," *Harvard Data Science Review*, vol. 1, no. 1, 2019.
29. National Institute of Standards and Technology (NIST), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, 2023.
30. E. Bagdasaryan et al., "How To Backdoor Federated Learning," in *Proc. AISTATS*, 2020.
31. L. Zhu, Z. Liu and S. Han, "Deep Leakage from Gradients," in *Proc. NeurIPS*, 2019.
32. M. Nasr, R. Shokri and A. Houmansadr, "Comprehensive Privacy Analysis of Deep Learning," in *IEEE Symposium on Security and Privacy*, 2019.
33. A. Kaplan and M. Haenlein, "Siri, Siri in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence," *Business Horizons*, vol. 62, no. 1, pp. 15–25, 2019.
34. S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed., Pearson, 2021.
35. J. Li, X. Wang, X. Meng and F. L. Lewis, "Optimal Sensor Selection of Linear Quadratic Regulation with Unknown Sensor Noise Covariances," *IEEE/CAA Journal of Automatica Sinica*, 2025.
36. X. Zhou and J. Li, "Inverse Optimal Control for High-order Nonlinear Fully Actuated Systems with Unknown Reward Weights," *International Journal of Robust and Nonlinear Control*, 2026.