

6G-Enabled Intelligent IoT: Emerging Architectures, AI-Native Networking, Digital Twins, and Security Challenges

Ravi Ranjan, Assistant Professor, Department of Electronics and Communication Engineering, Supaul College of Engineering, under the Department of Science, Technology and Technical Education, Bihar, India ranjan92.ravi@gmail.com

Naveen Kumar, Assistant Professor, Department of Electronics and Communication Engineering, Supaul College of Engineering, under the Department of Science, Technology and Technical Education, Bihar, India naveen6064@gmail.com

Dr. Achyuta Nand Mishra, Associate Professor, Department of Electronics and Communication Engineering, Supaul College of Engineering, under the Department of Science, Technology and Technical Education, Bihar, India an.mishra53@gmail.com

Pavan Kumar Shukla, School of Engineering and Technology, CGC University Mohali, Punjab, India pavanfec@gmail.com

Abstract: The convergence of sixth-generation (6G) wireless communication, artificial intelligence (AI), edge intelligence, and the Internet of Things (IoT) is transforming the conventional connectivity-oriented IoT paradigm into an intelligent, autonomous, and context-aware cyber-physical infrastructure. Unlike previous generations, 6G is being conceived not merely as a higher-capacity communication system but as an AI-native platform capable of jointly optimizing communication, computation, sensing, control, and intelligence. This evolution is particularly significant for IoT environments, where billions of heterogeneous devices, sensors, actuators, autonomous machines, vehicles, robots, and cyber-physical assets will generate highly dynamic and geographically distributed data. This paper presents a comprehensive analysis of 6G-enabled intelligent IoT, emphasizing emerging architectures, AI-native networking, network and system digital twins, distributed intelligence, semantic communications, reconfigurable intelligent surfaces, integrated sensing and communication, and security mechanisms. A multidimensional taxonomy is developed according to communication technologies, intelligence placement, learning paradigms, architectural layers, digital-twin functions, and security mechanisms. The paper critically examines centralized, edge, federated, distributed, and multi-agent intelligence architectures and discusses the roles of deep learning, reinforcement learning, federated learning, generative AI, and explainable AI in autonomous network optimization. Particular attention is devoted to digital twins as closed-loop environments for network monitoring, prediction, experimentation, and control. Security challenges are analyzed across device, edge, radio access, AI-model, digital-twin, orchestration, and application layers, including adversarial machine learning, model poisoning, privacy leakage, identity attacks, zero-day attacks, and supply-chain vulnerabilities. Comparative analyses of technologies, datasets, simulation platforms, and performance indicators are provided. Representative applications in smart manufacturing, intelligent transportation, healthcare, agriculture, energy, robotics, and smart cities are examined, followed by an illustrative case study of an AI-native 6G smart-factory ecosystem. Finally, unresolved challenges involving scalability, synchronization, explainability, energy efficiency, interoperability, security, standardization, and trustworthy autonomy are identified. The paper concludes with a research agenda centered on self-evolving AI-native networks, secure digital-twin ecosystems, semantic intelligence, quantum-resistant security, integrated sensing-computing-communication, and sustainable 6G-IoT infrastructures.

Keywords: 6G; Internet of Things; AI-native networking; edge intelligence; digital twin; federated learning; O-RAN; semantic communication; integrated sensing and communication; network slicing; cybersecurity; reconfigurable intelligent surfaces.

1. Introduction

The Internet of Things has progressively evolved from a connectivity paradigm for sensor networks into a distributed cyber-physical ecosystem in which physical objects continuously sense, communicate, compute, and act upon their environment. The transition from machine-to-machine communication toward intelligent IoT has been supported by cloud computing, mobile edge computing, artificial intelligence, software-defined networking, and 5G connectivity. However, the scale and heterogeneity expected in future IoT deployments expose limitations in architectures designed primarily around centralized cloud intelligence and conventional communication objectives. Future IoT systems are expected to simultaneously support massive device populations, autonomous machines, high-resolution sensing, immersive applications, distributed robotics, intelligent transportation, industrial automation, remote healthcare, and machine-to-machine decision-making. Consequently, communication quality alone is insufficient to characterize system performance. The network must increasingly understand application context, infer system state, predict future conditions, and autonomously select communication and computational actions.

The emergence of 6G addresses this broader requirement by envisioning a network in which communication, computing, sensing, artificial intelligence, and control are integrated rather than developed as independent technological layers. Current international standardization work under the ITU-R IMT-2030 framework identifies 6G as an evolution toward capabilities supporting enhanced mobile broadband, massive communication, immersive communication, hyper-reliable and low-latency communication, ubiquitous connectivity, and AI-

assisted sensing and communication. In March 2026, the ITU reported that its technical expert group had agreed on unified IMT-2030 performance requirements, representing an important stage in the standardization process. For IoT, the significance of 6G extends beyond increased data rates. Terahertz and sub-terahertz communication, advanced millimeter-wave systems, reconfigurable intelligent surfaces (RIS), integrated sensing and communication (ISAC), non-terrestrial networks, edge intelligence, semantic communications, network slicing, and AI-native control are expected to create a fundamentally different IoT environment. Recent literature characterizes this evolution as a move toward an AI-native network in which AI is embedded across multiple layers rather than being deployed merely as an external optimization component [1], [2]. A recent 6G-IoT review similarly identifies edge intelligence, artificial intelligence, and advanced radio technologies as central components of the emerging IoT architecture [3].

An important distinction must therefore be made between **AI-enabled networking** and **AI-native networking**. In the former, conventional network infrastructure remains dominant while machine learning is introduced to optimize selected functions such as resource allocation, traffic prediction, or anomaly detection. In an AI-native architecture, by contrast, network intelligence becomes an intrinsic design principle. Network functions are expected to expose data and control interfaces to AI agents; AI models participate in orchestration and optimization; and network operation increasingly becomes closed-loop, adaptive, and autonomous. This distinction is particularly important for IoT because the number of devices and the diversity of traffic patterns make static optimization increasingly impractical.

Digital twins provide another fundamental component of this transformation. A network digital twin creates a synchronized computational representation of physical network infrastructure and its operating state. It enables operators and autonomous controllers to observe, simulate, predict, and optimize network behavior without directly experimenting on the live infrastructure. Recent research has proposed native digital-twin architectures specifically for 6G networks, emphasizing real-time monitoring, modeling, intelligent orchestration, and lifecycle management [4]. Other studies have investigated generative-AI-enabled wireless digital twins in which foundation models and generative models support physical-digital modeling, synchronization, network slicing, and policy optimization [5].

Security becomes correspondingly more difficult. A highly autonomous 6G-IoT network does not merely transmit data; it learns from data and may autonomously modify network configurations. An adversary capable of poisoning training data, manipulating model updates, compromising an edge device, or falsifying digital-twin state could therefore influence network decisions without directly attacking conventional communication channels. Open and disaggregated architectures such as O-RAN further expand the attack surface because multiple vendors, open interfaces, virtualized network functions, AI models, and third-party applications coexist within the same operational ecosystem. O-RAN research groups have consequently identified AI/ML security, quantum security, and cross-domain AI as important areas for 6G evolution [6].

Against this background, this paper investigates the emerging 6G-enabled intelligent IoT ecosystem from an integrated systems perspective. Rather than treating 6G radio technologies, AI, digital twins, IoT, and cybersecurity independently, the paper examines their interactions and resulting architectural consequences. The principal contributions are fourfold: first, a multidimensional taxonomy of 6G-IoT intelligence architectures is developed; second, AI-native networking and digital-twin methodologies are analyzed as mechanisms for closed-loop autonomous operation; third, security and privacy risks are mapped across the complete architecture; and fourth, a research agenda is proposed for trustworthy, sustainable, interoperable, and self-evolving 6G-IoT systems.

The remainder of the paper progresses from technological motivation and taxonomy toward architectures, algorithms, comparative evaluation, applications, implementation tools, security limitations, and future research. This progression reflects the central argument that the future intelligent IoT should be understood not simply as an IoT system connected through 6G, but as an integrated communication-computation-sensing-intelligence-control ecosystem.

2. Background and Motivation

The transition toward 6G-enabled intelligent IoT is driven by the simultaneous growth of connectivity demand, computational complexity, data volume, and application autonomy. Traditional IoT architectures commonly follow a hierarchical pattern in which sensing devices collect information, gateways perform limited processing, and cloud platforms provide large-scale storage and analytics. This model has been effective for applications with

moderate latency requirements, but its limitations become apparent when decisions must be made within milliseconds or microseconds, data cannot leave the local environment, or system behavior changes faster than centralized optimization can respond.

5G introduced major improvements through enhanced mobile broadband, ultra-reliable low-latency communication, massive machine-type communication, network slicing, edge computing, and virtualization. Nevertheless, many IoT workloads remain constrained by energy availability, spectrum resources, heterogeneous protocols, mobility, and limited computational capabilities at the device level. Future applications will generate multimodal data comprising images, video, vibration, radio measurements, environmental measurements, location information, and machine telemetry. Transmitting all such data to centralized cloud platforms is inefficient. Instead, the network must determine which information is relevant, where it should be processed, what level of fidelity is required, and when an action must be taken.

This requirement motivates **edge intelligence**. Edge intelligence moves portions of the learning and inference pipeline toward devices, gateways, edge servers, and radio access networks. A generic distributed learning problem can be represented as $[\min_{\mathbf{w}} F(\mathbf{w}) = \sum_{k=1}^K p_k F_k(\mathbf{w}),]$ where (K) represents participating IoT nodes, (F_k) is the local loss function at node (k) , (p_k) is the aggregation weight, and $(\mathbf{w})$ represents model parameters. Federated learning extends this formulation by allowing devices to train locally and exchange model parameters rather than raw observations. This approach is particularly relevant for privacy-sensitive IoT applications and has been extensively studied for edge-IoT security and 6G systems [7], [8].

However, distributed intelligence creates its own complexity. IoT data are highly non-independent and identically distributed. A manufacturing robot, autonomous vehicle, wearable sensor, and agricultural sensor may observe completely different statistical distributions. Device availability changes dynamically, wireless channels fluctuate, and energy constraints vary across nodes. Conventional federated averaging may therefore converge slowly or produce models that are biased toward dominant participants. Recent research has consequently explored personalized federated learning, clustered federated learning, hierarchical aggregation, asynchronous learning, split learning, and federated reinforcement learning.

The motivation for AI-native 6G becomes stronger when the network itself becomes part of the learning system. Consider a smart factory containing hundreds of mobile robots, machine-vision cameras, wireless sensors, augmented-reality devices, and industrial controllers. The optimal communication configuration depends on machine positions, production schedules, electromagnetic conditions, workload, interference, battery state, and application priority. A static network configuration cannot efficiently adapt to these variables. AI-native control can instead infer network state and dynamically optimize beamforming, spectrum, computing placement, routing, slicing, and power allocation.

Another major motivation is the emergence of **integrated sensing and communication**. Conventional communication systems treat sensing as an external application, whereas ISAC allows radio signals and infrastructure to simultaneously provide connectivity and environmental perception. In a 6G-IoT environment, a base station could communicate with autonomous vehicles while simultaneously estimating their position, velocity, and surrounding objects. Such integration can reduce hardware duplication and enable contextual network optimization. It also changes the nature of security: radio measurements become valuable sensing data and can themselves reveal sensitive information.

RIS technology further modifies the communication environment. Instead of treating wireless propagation as uncontrollable, RIS uses programmable electromagnetic surfaces to manipulate signal reflection and transmission. Machine learning can jointly optimize RIS configurations, beamforming, user association, and resource allocation. Reviews of ML-based RIS-IoT systems indicate that RIS can improve connectivity, reliability, latency, and coverage but also introduces substantial optimization complexity and hardware-control challenges [9].

Semantic communication provides another conceptual shift. Traditional systems attempt to transmit symbols reliably, whereas semantic communication aims to transmit information relevant to the receiver's task. In an autonomous transportation application, for example, a vehicle may not require every pixel of a camera frame if the communication objective is obstacle avoidance. A semantic system could prioritize object locations, velocities, and hazard classifications. Recent surveys identify semantic extraction, semantic encoding, task-oriented transmission, and AI-based resource allocation as important components of future wireless systems [10].

Digital twins complement these technologies by providing a computational environment where network and application behavior can be reproduced. A digital twin can incorporate topology, radio conditions, device states, traffic flows, AI models, application requirements, and control policies. The twin may then evaluate candidate decisions before deployment. This creates a closed loop, quality of this loop depends on synchronization fidelity, modeling accuracy, latency, and uncertainty estimation. A stale or inaccurate twin may produce decisions that are worse than those generated without a twin. Consequently, digital-twin synchronization should be treated as a first-class systems problem rather than simply a data-replication task [4], [11].

These developments collectively establish the motivation for an integrated 6G-IoT architecture. The central challenge is no longer whether individual technologies are technically feasible; rather, it is how they can coexist within an architecture that remains scalable, secure, explainable, energy efficient, and interoperable.

3. Taxonomy / Classification

The technological diversity of 6G-enabled intelligent IoT requires a multidimensional taxonomy. A classification based solely on communication technology is insufficient because the most consequential changes arise from the interaction among connectivity, computation, intelligence, sensing, digital twins, and security. The proposed taxonomy therefore classifies the ecosystem along six dimensions: communication substrate, intelligence placement, learning paradigm, digital-twin scope, control autonomy, and security mechanism.

Table 1. Multidimensional taxonomy of 6G-enabled intelligent IoT

Dimension	Major classes	Representative technologies	Principal objective
Communication	Sub-6 GHz, mmWave, sub-THz/THz, NTN	Massive MIMO, beamforming, satellite, UAV	Connectivity
Intelligent placement	Device, edge, RAN, cloud	TinyML, MEC, AI-RIC, cloud AI	Distributed intelligence
Learning	Supervised, unsupervised, RL, FL, MARL	CNN, Transformer, PPO, FedAvg	Prediction and optimization
Communication paradigm	Conventional, semantic, goal-oriented	Semantic encoders, task-oriented transmission	Reduce redundant information
Physical environment	Conventional, RIS-assisted	Intelligent surfaces	Propagation control
Sensing	Separate sensing, ISAC	Radar-communication integration	Context awareness
Digital twin	Device, factory, network, city	DT, NDT, simulation platforms	Prediction and experimentation
Control	Human-assisted, semi-autonomous, autonomous	SON, AI agents, closed-loop control	Network autonomy
Security	Cryptographic, AI-based, privacy-preserving	PKI, ZTA, FL, XAI, PQC	Trust and resilience
Orchestration	SDN, NFV, O-RAN, intent-based	SMO, RIC, network slicing	Dynamic management

At the communication level, 6G-IoT can be divided into terrestrial and non-terrestrial connectivity. Terrestrial networks include advanced cellular systems, mmWave, and sub-terahertz communication, while non-terrestrial networks incorporate satellites, high-altitude platforms, and unmanned aerial systems. The distinction is important because IoT devices may move across heterogeneous domains. An agricultural sensor may communicate through terrestrial infrastructure when available and switch to satellite connectivity in remote regions. A truly intelligent network therefore requires cross-domain orchestration rather than isolated optimization.

The second dimension concerns the location of intelligence. Device-level intelligence is appropriate for low-latency decisions and privacy-sensitive applications but is constrained by computation and energy. Edge intelligence provides greater computational capacity while retaining geographical proximity. RAN-level intelligence allows network conditions to participate directly in decision-making. Cloud intelligence offers large

models and extensive computational resources but introduces latency and dependency on backhaul connectivity. Consequently, future systems are expected to adopt hierarchical intelligence rather than a single preferred location. The third dimension concerns learning. Supervised learning remains useful when labeled datasets exist, whereas unsupervised and self-supervised methods become important for anomaly detection and representation learning. Reinforcement learning is particularly suitable for dynamic resource allocation because it directly models sequential decisions. Multi-agent reinforcement learning becomes relevant when multiple network controllers or IoT devices interact. Federated learning addresses privacy and data-locality requirements, while split learning and collaborative learning provide alternatives when model size or device resources make conventional FL impractical.

Digital twins create a fourth classification axis. A **device twin** represents an individual physical asset; an **application twin** represents a cyber-physical process; a **network twin** models communication infrastructure; and a **system-of-systems twin** integrates multiple domains. Network digital twins have received increasing attention as mechanisms for real-time network analysis, emulation, and control [11], [12]. The most advanced architecture is therefore not simply a collection of independent twins but a federated twin ecosystem capable of representing relationships among devices, networks, applications, and physical environments.

A fifth axis concerns autonomy. Conventional IoT networks rely on operator configuration. Self-organizing networks automate selected functions. AI-native networks extend autonomy to policy generation, optimization, anomaly response, and service orchestration. The highest level involves self-evolving systems capable of modifying their own models and policies under constrained governance. Such autonomy introduces a fundamental tension: increasing autonomy can improve responsiveness while simultaneously making validation and accountability more difficult.

Finally, security mechanisms can be classified as preventive, detective, corrective, and adaptive. Preventive mechanisms include identity management, encryption, secure boot, and zero-trust access. Detective mechanisms include anomaly detection, intrusion detection, behavioral analytics, and model monitoring. Corrective mechanisms involve isolation, reconfiguration, rollback, and fail-safe control. Adaptive security uses AI and closed-loop orchestration to dynamically respond to changing threats. The taxonomy demonstrates that security cannot be attached as a final layer; it must be integrated into every architectural component.

Table 2. Learning paradigms for intelligent 6G-IoT

Paradigm	Strength	Limitation	Suitable applications
Centralized ML	Global model quality	Privacy, latency, bandwidth	Cloud analytics
Edge ML	Low latency	Limited resources	Industrial control
Federated learning	Data locality	Communication overhead, poisoning	Healthcare, smart homes
Reinforcement learning	Sequential optimization	Exploration risk	Resource allocation
Multi-agent RL	Distributed coordination	Training instability	RAN/IoT orchestration
Split learning	Low device computation	Communication dependence	Resource-constrained IoT
Self-supervised learning	Reduced labeling	Training complexity	Sensor representation
Generative AI	Data/model generation	Hallucination, security	Twin construction, network automation

This taxonomy leads naturally to the architectural question: how can these heterogeneous technologies be organized into a coherent operational system?

4. Core Concepts and Methodologies

4.1 AI-Native Networking

AI-native networking treats intelligence as a fundamental network capability. Instead of applying independent machine-learning models to isolated optimization problems, AI functions are integrated into network control, orchestration, resource allocation, security, and service management. An AI-native network can observe network state, construct contextual representations, generate candidate policies, evaluate their consequences, and deploy selected actions.

4.2 Federated and Distributed Intelligence

Federated learning is particularly important for IoT because it enables distributed model training without centralizing raw data. Recent research therefore emphasizes secure aggregation, robust aggregation, personalized FL, hierarchical FL, and differential privacy. Surveys of FL security in 6G identify threats involving malicious clients, poisoning, inference, Byzantine behavior, and compromised aggregation infrastructure [8], [13]. The implication is important: FL should not automatically be interpreted as a secure mechanism. It protects raw data locality but does not inherently prevent model leakage or malicious updates.

4.3 Semantic Communications

Semantic communications introduce a task-oriented interpretation of network traffic. Rather than maximizing bit-level fidelity, the system attempts to maximize task performance. For example, an industrial monitoring system may transmit a compressed representation of a machine vibration signal rather than the complete waveform when the objective is fault classification. Semantic communication can therefore reduce communication overhead, but its effectiveness depends on shared semantic models between transmitter and receiver. Model mismatch, domain shifts, ambiguity, and security manipulation remain unresolved challenges [10].

4.4 Digital Twins

Digital twins provide the virtual environment required to integrate AI, simulation, and control. A useful digital twin should contain at least four elements: physical-state representation, data synchronization, computational modeling, and control interfaces. The twin can perform descriptive, predictive, prescriptive, and experimental functions. Recent 6G research proposes native network digital twins capable of representing large-scale networks and supporting intelligent orchestration [4]. Other work identifies digital twins as a mechanism for reducing the cost of network experimentation and supporting autonomous operation [11]. Generative AI further extends the concept by enabling synthetic scenarios, model generation, and policy-level interaction with the twin [5], [14].

4.5 Integrated Sensing and Communication

ISAC transforms communication infrastructure into a sensing platform. For intelligent IoT, this is valuable because the network can infer environmental state without requiring separate sensing infrastructure. Applications include localization, industrial monitoring, autonomous vehicles, human activity recognition, and robotic coordination.

5. System Architecture

A comprehensive 6G-IoT architecture should be viewed as a layered but dynamically interconnected system rather than a strict protocol stack. Figure 1 is therefore proposed as a conceptual architecture containing seven functional planes.

At the device layer, sensors, actuators, robots, cameras, vehicles, wearables, and industrial controllers generate physical observations. Lightweight AI models can perform preprocessing, anomaly detection, semantic extraction, and event filtering. TinyML techniques are particularly useful where devices operate under strict energy and memory constraints.

The access layer provides connectivity through advanced 6G radio technologies. Massive MIMO and beamforming provide spatial multiplexing, while RIS can manipulate propagation conditions. ISAC allows communication infrastructure to simultaneously support sensing. Non-terrestrial connectivity provides additional coverage for geographically isolated IoT deployments.

The edge layer contains compute nodes positioned near users and devices. These nodes host AI inference, federated-learning clients, digital-twin components, caching systems, and real-time control functions. O-RAN

architectures can introduce programmable RAN intelligence through near-real-time and non-real-time RIC functions. O-RAN's open interfaces enable greater programmability but also introduce additional security dependencies [6], [15].

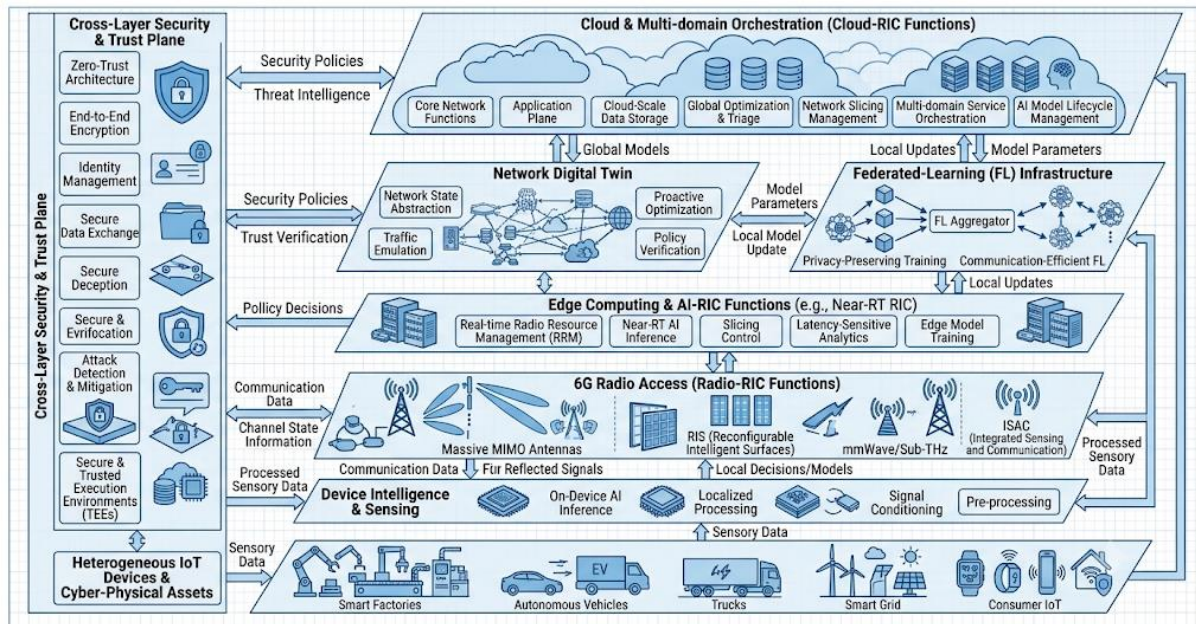


Figure 1: Proposed AI-native 6G-IoT architecture.

The intelligence layer contains learning models and orchestration engines. A hierarchical model may operate as follows:

1. Devices perform local sensing and inference.
2. Edge nodes aggregate local context.
3. Federated learning produces shared models.
4. Digital twins simulate candidate policies.
5. AI agents select actions.
6. Network orchestration deploys approved actions.
7. Devices provide feedback.
8. The twin and models are updated.

6. Comparative Analysis

The convergence of technologies in 6G-IoT creates substantial benefits but also produces trade-offs. No individual architecture simultaneously minimizes latency, energy consumption, communication overhead, privacy risk, computational cost, and implementation complexity. Consequently, architectural selection should depend on application requirements.

Table 3. Comparison of intelligence architectures

Architecture	Latency	Privacy	Scalability	Computation	Communication overhead	Main limitation
Cloud AI	High	Low-moderate	High	High	High	Backhaul dependence
Edge AI	Low	Moderate-high	Moderate	Moderate	Moderate	Edge resource limits
Federated AI	Low-moderate	High	High	Distributed	High model traffic	Non-IID data
Split learning	Low-moderate	High	Moderate	Low device load	Moderate	Split-layer dependence

Multi-agent AI	Low	High	High	High	Moderate	Coordination complexity
Digital-twin-assisted AI	Low after optimization	Moderate-high	High	Very high	High during synchronization	Twin fidelity

The comparison indicates that edge AI is attractive for latency-sensitive applications but does not automatically solve privacy concerns. Federated learning improves data locality but introduces communication and security overhead. Digital twins improve experimentation and policy validation but require substantial computation and synchronization bandwidth. Multi-agent approaches provide scalability for decentralized environments but create difficult convergence and coordination problems.

Table 4. Comparison of enabling 6G technologies

Technology	Primary benefit	IoT contribution	Major limitation
Massive MIMO	Spatial multiplexing	High device density	Processing complexity
mmWave/sub-THz	High bandwidth	High-data-rate sensing	Propagation loss
RIS	Propagation control	Coverage and reliability	Configuration complexity
ISAC	Joint sensing/communication	Context-aware IoT	Signal-processing complexity
NTN	Ubiquitous coverage	Remote IoT	Propagation delay
O-RAN	Programmability	Intelligent RAN control	Expanded attack surface
Semantic communication	Reduced data transmission	Task-oriented IoT	Shared semantic model
Digital twin	Prediction and experimentation	Autonomous optimization	Synchronization burden
Federated learning	Privacy-preserving AI	Distributed learning	Poisoning/non-IID data
Generative AI	Scenario/model generation	Intelligent automation	Hallucination and governance

The literature increasingly supports a combined rather than isolated deployment strategy. Digital twins can provide safe environments for reinforcement learning; federated learning can supply distributed models; O-RAN can expose control interfaces; semantic communication can reduce the data exchanged; and ISAC can supply additional contextual information. Their combined use, however, creates multiplicative complexity.

An important research gap therefore concerns **cross-technology co-design**. Much of the existing literature optimizes individual components—for example, RIS beamforming or FL aggregation—under simplified assumptions. Real deployments must simultaneously address radio conditions, computing resources, application deadlines, security constraints, model uncertainty, and physical processes. Future benchmarks should consequently evaluate integrated systems rather than isolated algorithms.

7. Applications

7.1 Smart Manufacturing

Smart manufacturing is one of the most compelling applications because factories contain dense concentrations of sensors, machines, robots, cameras, controllers, and human operators. A 6G network can provide deterministic connectivity while AI models analyze vibration, acoustic, thermal, and visual signals. Digital twins can represent machines and production lines, allowing predictive maintenance policies to be evaluated before physical implementation.

For example, a digital twin of a robotic assembly line could receive vibration data from motors and joint sensors. An AI model detects deviations from normal behavior and predicts remaining useful life. The network then dynamically prioritizes traffic from the affected machine while the digital twin evaluates alternative maintenance

schedules. Such a system goes beyond predictive maintenance because communication, computation, and physical maintenance decisions are jointly optimized.

7.2 Intelligent Transportation

Connected autonomous vehicles require extremely low latency and high reliability. 6G-IoT can combine vehicle-to-everything communication, ISAC, edge AI, semantic communication, and digital twins. Rather than transmitting complete sensor streams, vehicles could transmit task-relevant semantic information such as detected pedestrians, road hazards, trajectories, and confidence values.

At the infrastructure level, road-side digital twins can maintain representations of traffic conditions. Reinforcement learning can optimize traffic signals and routing, while federated learning allows vehicles to collaboratively train perception models without sharing raw sensor data.

7.3 Smart Healthcare

Healthcare IoT involves wearables, implantable devices, medical imaging, hospital equipment, and remote monitoring. 6G connectivity can support low-latency monitoring and distributed intelligence. Federated learning is particularly relevant because patient data are highly sensitive. Hospitals or edge devices can collaboratively train models while retaining raw patient records locally.

However, healthcare introduces strict reliability and accountability requirements. AI decisions should therefore be accompanied by confidence measures, provenance information, and interpretable explanations. Fully autonomous control is inappropriate for many clinical scenarios; human oversight must remain part of the architecture.

7.4 Smart Agriculture

6G-IoT can integrate soil sensors, weather stations, drones, autonomous agricultural machinery, satellite imagery, and irrigation systems. Edge intelligence can classify crop conditions locally, while digital twins represent field-level environmental conditions. AI models can optimize irrigation according to soil moisture, weather forecasts, crop stage, and water availability.

Non-terrestrial networks may be particularly useful in rural regions where conventional cellular coverage is limited. Semantic communication can reduce the transmission of redundant agricultural imagery by prioritizing disease symptoms, crop stress indicators, or irrigation anomalies.

7.5 Smart Energy

Future power grids will contain distributed renewable generation, electric vehicles, storage systems, smart meters, and intelligent controllers. AI-native 6G networks can dynamically manage communication resources according to grid conditions. Digital twins can simulate load changes and renewable-generation fluctuations before control actions are deployed.

The principal challenge is cybersecurity. A compromised communication or AI system could influence grid operations. Therefore, secure identity, anomaly detection, trustworthy AI, and resilient control mechanisms are essential.

Table 5. Application requirements

Application	Latency	Reliability	Intelligence requirement	Digital-twin value	Security criticality
Manufacturing	Very low	Very high	High	Very high	Very high
Autonomous transport	Very low	Extremely high	Very high	Very high	Extremely high
Healthcare	Low	Extremely high	High	High	Extremely high
Agriculture	Moderate	High	High	High	High

Smart grid	Low	Extremely high	Very high	Very high	Extremely high
Smart city	Moderate	High	High	Very high	High

8. Tools, Technologies and Implementation

The implementation of intelligent 6G-IoT research requires multiple simulation, emulation, machine-learning, and digital-twin platforms. No single platform adequately represents the entire stack.

Table 6. Representative tools and datasets

Tool/dataset	Category	Primary use
ns-3	Network simulator	Protocol and wireless evaluation
OMNeT++	Network simulation	Distributed communication studies
MATLAB/Simulink	Numerical/system simulation	PHY and control modeling
NVIDIA Sionna	Wireless ML framework	Differentiable communication simulation
DeepMIMO	Dataset/framework	MIMO/beamforming research
RadioMapSeer	Dataset	Radio-map learning
DeepSense 6G	Dataset	Multimodal sensing/communications
EdgeCloudSim	Edge simulator	MEC evaluation
CloudSim Plus	Cloud simulation	Resource allocation
OpenAirInterface	Experimental platform	5G/6G prototyping
O-RAN Software Community	Open RAN	RAN experimentation
Kubernetes	Container orchestration	Edge/cloud deployment
Docker	Containerization	Reproducible deployment
PyTorch	AI framework	Deep learning
TensorFlow	AI framework	Deep learning/FL
Flower	FL framework	Federated-learning experiments
NVIDIA FLARE	FL framework	Enterprise FL
SUMO	Traffic simulator	Vehicular IoT
CARLA	Autonomous-driving simulation	V2X/AV research
Gazebo/ROS 2	Robotics	Robot-IoT integration

Recent 6G AI surveys identify datasets such as DeepMIMO, RadioMapSeer, DeepSense 6G, ViWi, Sionna-associated datasets, and several emerging 6G channel datasets as important resources for machine-learning research [16]. Their value is substantial because AI-based networking cannot be evaluated meaningfully without realistic data. However, many existing datasets are limited in scale, environment diversity, temporal variability, or cyberattack representation.

A robust experimental methodology should therefore combine real traces, simulation, emulation, and hardware-in-the-loop testing. For example, a research system may generate wireless data using Sionna or MATLAB, emulate network behavior using ns-3, model vehicles using SUMO/CARLA, train AI models using PyTorch, and deploy orchestration components through Kubernetes.

Digital twins require another layer of tooling. A twin platform should support state ingestion, model execution, synchronization, visualization, simulation, and control APIs. The implementation should distinguish between **offline twins**, used primarily for design and simulation, and **runtime twins**, which maintain synchronization with live systems.

Reproducibility is another major concern. AI-native network experiments often depend on hyperparameters, random seeds, traffic patterns, channel models, topology assumptions, and hardware characteristics. Future

research should therefore publish code, configuration files, datasets, model checkpoints, and evaluation scripts whenever possible.

9. Performance Evaluation

Performance evaluation for 6G-enabled intelligent IoT must extend beyond conventional communication metrics. Throughput, spectral efficiency, latency, packet loss, and reliability remain essential, but they do not fully capture AI-driven systems. Model accuracy, convergence rate, inference latency, energy consumption, twin synchronization error, security resilience, and decision quality should also be measured.

Table 7. Recommended performance metrics

Category	Metrics
Communication	Throughput, spectral efficiency, latency, packet loss
Reliability	Availability, outage probability, deadline success
AI	Accuracy, F1-score, convergence rounds, regret
Edge	CPU/GPU utilization, inference latency
FL	Communication rounds, model accuracy, convergence
Digital twin	Synchronization error, fidelity, update latency
Security	Detection rate, false-positive rate, attack success
Energy	Joules/task, device lifetime
Sustainability	Energy/bit, carbon intensity
Application	Task completion, production loss, clinical utility

Pareto optimization is more appropriate than single-objective optimization for many 6G-IoT scenarios. A system may seek a set of non-dominated configurations balancing accuracy, latency, energy, security, and cost.

Evaluation should also consider statistical robustness. AI-based network optimization may perform exceptionally well under one topology or traffic distribution but degrade significantly under distribution shifts. Therefore, experiments should include multiple environments, device populations, channel conditions, workload levels, and attack scenarios.

Digital-twin experiments additionally require a comparison between the twin and physical system. A twin should not be considered accurate simply because it reproduces historical data. Its predictive capability under previously unseen conditions is more meaningful. Accordingly, evaluation should include temporal extrapolation, topology changes, device failures, mobility, and adversarial conditions.

Federated-learning evaluation requires reporting not only global accuracy but also client-level performance. A model achieving high average accuracy may perform poorly for minority clients. Metrics such as worst-client accuracy, fairness gaps, convergence variance, communication volume, and attack resilience should therefore accompany global metrics.

Security evaluation must similarly move beyond binary detection accuracy. Attack success rate, time to detection, time to mitigation, false positives, false negatives, and recovery time are particularly important in cyber-physical environments. A system that detects an attack after a safety-critical actuator has already responded cannot be considered operationally secure even if its final detection accuracy is high.

10. Challenges and Limitations

The first major challenge is scalability. Future IoT systems may involve billions of devices distributed across heterogeneous terrestrial and non-terrestrial networks. Centralized intelligence cannot efficiently process all observations, while completely decentralized intelligence introduces coordination overhead. Hierarchical intelligence is therefore promising but requires dynamic decisions regarding where computation and learning should occur.

The second challenge is data heterogeneity. IoT data are inherently non-IID, multimodal, noisy, incomplete, and temporally correlated. Federated-learning models can become biased when some devices have significantly more data or more representative observations than others. Personalization can alleviate this problem, but personalized models increase management complexity.

Third, AI itself becomes an attack surface. Adversarial examples can manipulate predictions, poisoning attacks can alter training, backdoor attacks can activate hidden behaviors, and inference attacks can expose private information. Research on edge learning for 6G-IoT has categorized threats including backdoors, adversarial examples, poisoning, Sybil attacks, Byzantine attacks, inference attacks, and dropping attacks [17]. The challenge is amplified because AI models may directly control network resources.

Fourth, digital-twin synchronization remains unresolved. A digital twin must be sufficiently current to support decisions, yet frequent updates consume network and computational resources.

Fifth, explainability becomes increasingly important as autonomous systems gain control authority. A black-box model that reallocates critical network resources or modifies an industrial control policy may be difficult to validate. Explainable AI should therefore be integrated with uncertainty estimation, policy constraints, and audit mechanisms.

Sixth, energy consumption remains a fundamental concern. AI models, digital twins, edge GPUs, and high-frequency communication can substantially increase energy use. The assumption that 6G will automatically improve sustainability is therefore questionable. Energy efficiency must be optimized at the system level, including computation, communication, cooling, and device lifecycle.

Seventh, interoperability is unresolved. IoT ecosystems contain multiple communication protocols, vendors, data models, cloud platforms, AI frameworks, and operational technologies. O-RAN improves openness but also requires careful interoperability testing and security governance. The expanding O-RAN security work illustrates that open interfaces introduce new threat considerations [15], [18].

Eighth, 6G security must address quantum threats. Long-lived IoT devices may remain deployed for many years, making cryptographic migration difficult. Research examining quantum-empowered FL and 6G-IoT security has emphasized the need to investigate quantum-safe mechanisms alongside distributed learning [19].

Finally, the existing literature has an important methodological limitation: many proposed architectures remain conceptual. Simulation results often rely on idealized channel models, simplified traffic, small device populations, or assumed attack scenarios. The transition from simulation to operational deployment remains a major research challenge.

11. Future Research Directions

The first major research direction is **self-evolving AI-native networking**. Future networks should be capable of adapting not only parameters but also models, policies, and architectures. This requires continual learning, meta-learning, neural architecture adaptation, and safe reinforcement learning. However, self-evolution must occur within formally constrained boundaries.

The second direction is **generative-AI-enabled network intelligence**. Generative models can assist in scenario generation, network configuration, synthetic data generation, digital-twin construction, and natural-language interaction with network infrastructure. Recent work has already examined generative AI for wireless network digital twins and identifies transformer- and diffusion-based approaches for physical-digital modeling and policy optimization [5]. The key research challenge is preventing hallucinated configurations from reaching operational systems. Generative models should therefore be coupled with deterministic validation engines.

The third direction is **decision-aware digital twins**. Current digital-twin research frequently focuses on synchronization and fidelity. Future work should instead determine how much fidelity is actually necessary for a given decision. A manufacturing control decision may require millisecond-level machine-state accuracy but not detailed modeling of unrelated network components. Adaptive fidelity could significantly reduce computational overhead.

The fourth direction is **semantic-native 6G-IoT**. Semantic communication should evolve beyond compression toward shared knowledge models between devices, networks, and applications. Knowledge graphs, foundation

models, task-oriented learning, and multimodal representations could enable machines to exchange concepts rather than raw data.

The fifth direction is **trustworthy federated intelligence**. Future FL systems should combine robust aggregation, differential privacy, secure aggregation, decentralized identity, Byzantine resilience, and explainable learning. Research should also investigate cross-domain FL involving vehicles, satellites, edge servers, and terrestrial networks.

The sixth direction is **AI security by design**. Security should become part of model development rather than an afterthought. Every AI model should have provenance, versioning, robustness testing, adversarial evaluation, rollback capability, and runtime monitoring.

The seventh direction is **post-quantum 6G-IoT security**. Because IoT devices have long lifetimes and constrained computational resources, post-quantum cryptography must be designed specifically for embedded environments. Hybrid cryptographic architectures may provide transitional compatibility.

The eighth direction is **integrated communication-computation-sensing-control optimization**. Future research should avoid optimizing radio, computing, sensing, and control independently.

The ninth direction is **6G-IoT foundation models**. Large multimodal models could potentially learn joint representations of network telemetry, radio measurements, device states, application semantics, and physical environments. However, the computational and energy costs of such models require specialized edge architectures, model compression, sparsity, distillation, and hardware acceleration.

The tenth direction concerns **standardized benchmarks**. The absence of standardized end-to-end benchmarks remains a major limitation. Future benchmarks should include realistic device populations, mobility, non-IID data, channel variability, cyberattacks, energy constraints, digital-twin fidelity, and application-level outcomes.

Recent research on AI-driven digital-twin networks emphasizes twin creation, synchronization, prediction, decision-making, and feedback as a connected lifecycle rather than independent functions [20]. This lifecycle perspective should become central to future 6G-IoT research.

Table 8. Proposed future research agenda

Research direction	Current limitation	Required advancement	Expected impact
Self-evolving AI	Static models	Continual/meta-learning	Autonomous networks
GenAI networking	Hallucination	Verified generation	Automated orchestration
Adaptive DT	High synchronization cost	Decision-aware fidelity	Lower overhead
Semantic IoT	Shared-context requirement	Knowledge-centric models	Reduced traffic
Secure FL	Poisoning/privacy	Robust + private FL	Trustworthy learning
PQC IoT	Resource constraints	Lightweight PQC	Long-term security
Foundation models	High compute	Edge-efficient models	General intelligence
ISAC	Joint optimization complexity	Unified sensing/communication	Context-aware IoT
Multi-agent AI	Coordination instability	Safe MARL	Distributed autonomy
Benchmarking	Fragmented evaluation	Standard testbeds	Reproducibility

12. Conclusion

The convergence of 6G, AI, edge computing, digital twins, and IoT is transforming cyber-physical systems into distributed intelligence platforms where communication, sensing, computing, learning, and control are closely integrated. AI-native networking can optimize resources, computing placement, energy, routing, and security, while federated learning enables distributed intelligence with improved data locality. Digital twins further support monitoring, prediction, simulation, and closed-loop optimization, although synchronization, uncertainty, and computational costs remain challenges. Meanwhile, the expanding attack surface requires security-by-design approaches covering devices, networks, AI models, edge platforms, and digital-twin environments. Future

research must jointly address communication, computation, sensing, intelligence, security, and physical control. Ultimately, 6G-enabled intelligent IoT should provide **adaptive, autonomous, privacy-preserving, energy-efficient, interoperable, and trustworthy cyber-physical infrastructures**, supported by standardized benchmarks, realistic testbeds, robust architectures, and interdisciplinary research.

References

- [1] M. Sheraz, T. C. Chuah, Y. L. Lee, M. M. Alam, et al., "A Comprehensive Survey on Revolutionizing Connectivity Through Artificial Intelligence-Enabled Digital Twin Network in 6G," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3384272.
- [2] A. Comprehensive Survey, "A Comprehensive Survey on Emerging AI Technologies for 6G Communications: Research Direction, Trends, Challenges, and Opportunities," International Journal of Intelligent Networks, vol. 6, pp. 113–150, 2025, doi: 10.1016/j.ijin.2025.06.001.
- [3] Aarti, S. Gowroju, and S. I. Ansarullah, "A comprehensive review of developments and challenges in the 6G internet of things," Discover Networks, vol. 1, art. no. 13, 2025.
- [4] "Native Design for 6G Digital Twin Network: Use Cases, Architecture, Functions, and Key Technologies," IEEE Internet of Things Journal, vol. 12, no. 15, pp. 29135–29151, 2025, doi: 10.1109/JIOT.2025.3553500.
- [5] "Wireless Network Digital Twin for 6G: Generative AI as a Key Enabler," IEEE Wireless Communications, vol. 31, no. 4, pp. 24–31, 2024, doi: 10.1109/MWC.002.2300564.
- [6] O-RAN Alliance, "First Research Reports Published by O-RAN nGRG Address the Use Cases, AI/ML and Security Aspects of 6G Mobile Networks," 2023.
- [7] H. Li, L. Ge, and L. Tian, "Survey: federated learning data security and privacy-preserving in edge-Internet of Things," Artificial Intelligence Review, vol. 57, art. no. 130, 2024, doi: 10.1007/s10462-024-10774-7.
- [8] S. H. A. Kazmi, F. Qamar, R. Hassan, K. Nisar, and M. A. Al-Betar, "Security of federated learning in 6G era: A review on conceptual techniques and software platforms used for research and analysis," Computer Networks, vol. 245, art. no. 110358, 2024, doi: 10.1016/j.comnet.2024.110358.
- [9] S. K. Das, F. Benkhelifa, Y. Sun, H. Abumarshoud, Q. H. Abbasi, M. A. Imran, and L. Mohjazi, "Comprehensive review on ML-based RIS-enhanced IoT systems: basics, research progress and future challenges," Computer Networks, art. no. 109581, 2023, doi: 10.1016/j.comnet.2023.109581.
- [10] Y. Liu, X. Wang, Z. Ning, M. Zhou, L. Guo, and B. Jedari, "A survey on semantic communications: Technologies, solutions, applications and challenges," Digital Communications and Networks, vol. 10, no. 3, pp. 528–545, 2024, doi: 10.1016/j.dcan.2023.05.010.
- [11] S. M. Raza, R. Minerva, N. Crespi, M. Alvi, M. Herath, and H. Dutta, "A comprehensive survey of Network Digital Twin architecture, capabilities, challenges, and requirements for Edge-Cloud Continuum," Computer Communications, vol. 236, art. no. 108144, 2025, doi: 10.1016/j.comcom.2025.108144.
- [12] "Navigating the Digital Twin Network landscape: A survey on architecture, applications, privacy and security," High-Confidence Computing, vol. 4, no. 4, art. no. 100269, 2024.
- [13] "Federated Learning for Enhanced Cybersecurity and Trustworthiness in 5G and 6G Networks: A Comprehensive Survey," IEEE Open Journal of the Communications Society, vol. 6, pp. 3094–3130, 2024, doi: 10.1109/OJCOMS.2024.3449563.
- [14] F. Naem, M. Ali, G. Kaddoum, Y. Faheem, Y. Zhang, M. Debbah, and C. Yuen, "A Survey on GenAI-Driven Digital Twins: Toward Intelligent 6G Networks and Metaverse Systems," IEEE Open Journal of the Communications Society, vol. 6, pp. 10365–10402, 2025, doi: 10.1109/OJCOMS.2025.3641307.
- [15] O-RAN Alliance, "O-RAN Study on Security for Artificial Intelligence and Machine Learning in O-RAN," technical report, updated 2024–2025.
- [16] "A Comprehensive Survey on Emerging AI Technologies for 6G Communications: Research Direction, Trends, Challenges, and Opportunities," including discussion of DeepMIMO, RadioMapSeer, Sionna, DeepSense 6G, ViWi and emerging 6G datasets, 2025.
- [17] "Edge Learning for 6G-enabled Internet of Things: A Comprehensive Survey of Vulnerabilities, Datasets, and Defenses," IEEE Communications Surveys & Tutorials, 2023/2024.
- [18] "Security and Privacy in O-RAN for 6G: A Comprehensive Review of Threats and Mitigation Approaches," IEEE Communications Surveys & Tutorials, vol. 28, pp. 5159–5195, 2026, doi: 10.1109/COMST.2026.3669743.
- [19] D. Javeed et al., "Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions," Future Generation Computer Systems, vol. 160, pp. 577–597, 2024, doi: 10.1016/j.future.2024.06.023.
- [20] "Bridging the gap: A comprehensive survey on AI-driven digital twin networks for future wireless systems," Journal of King Saud University Computer and Information Sciences, 2026, doi: 10.1007/s44443-026-00522-y.
- [21] "Federated Learning for 6G Security: A Survey on Threats, Solutions, and Research Directions," IEEE Communications Surveys & Tutorials, 2026, doi: 10.1109/COMST.2026.3663434.
- [22] "Roadmap for Integrating Open RAN and AI for Intrusion Detection Systems in 6G Networks," in Proc. 15th International Conference on Information and Communication Technology Convergence (ICTC), 2024, doi: 10.1109/ICTC62082.2024.10826894.
- [23] "Native Network Digital Twin Architecture for 6G: From Design to Practice," IEEE, 2024.
- [24] "A comprehensive survey on digital twin for future networks and emerging Internet of Things industry," Computer Networks, vol. 244, art. no. 110350, 2024.
- [25] "A contemporary survey of recent advances in federated learning: Taxonomies, applications, and challenges," Internet of Things, vol. 27, art. no. 101251, 2024.
- [26] "Navigating the future of wireless networks: A multidimensional survey on semantic communications," ICT Express, vol. 10, no. 4, pp. 747–773, 2024.
- [27] ITU-R, "IMT-2030: Technical requirements for the 6G future," International Telecommunication Union, Mar. 17, 2026.
- [28] "AI-Native Use Cases in 6G," in Proc. 7th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), 2025, doi: 10.1109/ICHORA65333.2025.11017221.