

TOWARDS INTELLIGENT 6G-IOT ECOSYSTEMS: A SYSTEMATIC REVIEW OF ENABLING TECHNOLOGIES, NETWORK ARCHITECTURES, SECURITY, AND EMERGING APPLICATIONS

Muhammad Ali¹, Hafiz Muhammad Umer Mayal², Tanveer Hussain^{*3}, Sawera Farrukh⁴

^{1,2,*3}Department of Computer Science, NCBA&E (Alhamra University), Rahim Yar Khan, 64200, Pakistan

⁴Khwaja Fareed University of Engineering & Information Technology (KFUEIT), Rahim Yar Khan, Pakistan

¹muhammadali.ryk@outlook.com, ²tanveerryk541@gmail.com, ^{*3}umarmayal97@gmail.com

⁴sawerafarrukh99@gmail.com

DOI: <https://doi.org/10.5281/zenodo.23338563>

Keywords

6G; Internet of Things; terahertz communication; reconfigurable intelligent surfaces; integrated sensing and communication; artificial intelligence; edge computing; network security; privacy

Article History

Received: 01 July 2026

Accepted: 29 September 2026

Published: 13 October 2026

Copyright @Author

Corresponding Author: *

Tanveer Hussain

Abstract

Research on sixth-generation (6G) wireless systems is increasingly shaped by the needs of large-scale, intelligent Internet of Things (IoT) deployments. Yet the literature remains dispersed across physical-layer technologies, network architecture, artificial intelligence, security, and application-specific studies. This systematic review brings these strands together and examines how 6G is being positioned to support future IoT ecosystems. The review searched IEEE Xplore, Scopus, Web of Science, ScienceDirect, and Google Scholar for peer-reviewed work published from 2023 to 2026. The screening process identified 120 records and retained 38 studies for the final thematic analysis. The evidence was organized around enabling technologies, integrated space-air-ground-underwater networking, edge intelligence and network slicing, resource management, security and privacy, and application domains including healthcare, industrial IoT, autonomous mobility, and extended reality. Across the reviewed studies, proposed 6G targets commonly include terabit-per-second peak rates, microsecond-level latency, very high connection density, and AI-native control. These capabilities, however, depend on unresolved issues such as terahertz propagation, scalable reconfigurable surfaces, trustworthy AI, post-quantum security, interoperable non-terrestrial networking, and sustainable deployment. The review therefore treats 6G-IoT not as a single technology upgrade, but as a tightly coupled communication-computing-sensing ecosystem whose success will depend on coordinated progress across several technical and governance layers.

"© 2026 by the Author(s). Published by IJAR under CC BY 4.0. Unrestricted use allowed with credit to the author."

INTRODUCTION:-

Wireless communication has advanced through a sequence of generations, but each transition has been driven by more than a demand for higher data

rates. The shift from 4G to 5G, for example, introduced service categories for enhanced mobile broadband, ultra-reliable low-latency communication, and massive machine-type

communication. Even so, emerging IoT systems are beginning to expose limits that cannot be addressed by bandwidth alone. Large populations of sensing devices, autonomous machines, immersive interfaces, and distributed AI services require communication, computation, sensing, positioning, and security to work as a coordinated system rather than as separate network functions [1]-[5].

This is the context in which 6G-enabled IoT has emerged as a major research direction. The literature describes 6G as an AI-native and highly distributed network environment that extends beyond terrestrial cellular infrastructure. Terahertz links, reconfigurable intelligent surfaces, integrated sensing and communication, non-terrestrial networks, edge intelligence, and semantic communication are repeatedly proposed as complementary building blocks [10]-[19]. For IoT, their importance lies in the possibility of supporting dense device populations while moving decision-making closer to the physical processes being observed or controlled.

At the same time, many published visions rely on ambitious design targets that remain research objectives rather than routinely demonstrated

operating points. Proposed benchmarks include peak rates approaching 1 Tbps, microsecond-scale local latency, connection densities on the order of ten million devices per square kilometer, and reliability suitable for safety-critical services [8], [12], [13]. These figures are useful as directional targets, but they also highlight the scale of the engineering challenge. Performance must be achieved under severe propagation constraints, heterogeneous hardware, limited device energy, mobility, and an attack surface that expands as intelligence is distributed throughout the network [6], [17], [25].

The purpose of this review is therefore to examine 6G-IoT as an integrated research problem. Rather than discussing individual radio technologies in isolation, the paper connects the physical layer with network architecture, resource management, security, and application requirements. It also identifies points where the literature is relatively mature and areas where claims still depend on simulation, conceptual frameworks, or early prototypes. This perspective is intended to be useful to researchers entering the field as well as practitioners who need a clearer view of the dependencies between candidate 6G technologies

Table 1. Indicative comparison of 5G and proposed 6G capabilities for IoT applications

Metric	5G IoT	Proposed 6G IoT
Peak data rate	Up to 20 Gbps	Up to 1 Tbps
Latency	Millisecond scale	Microsecond-scale target
Device density	About 10^6 devices/km ²	About 10^7 devices/km ²
Spectrum	Sub-6 GHz and mmWave	Sub-6 GHz, mmWave, THz, and optical bands
AI integration	Primarily assisted/overlay functions	AI-native control and optimization
Energy objective	Improved device and network efficiency	Ultra-high efficiency; battery-less IoT explored
Coverage	Predominantly terrestrial	Integrated satellite, UAV, terrestrial, and other non-terrestrial links
Representative applications	Smart devices and industrial automation	XR, digital twins, autonomous systems, dense sensing

2. Systematic Literature Review Methodology

A systematic review procedure was used to reduce ad hoc study selection and to make the evidence-gathering process traceable. The review focused on peer-reviewed work that directly addressed the relationship between 6G communication and IoT, including enabling technologies, architectures, optimization, security, and application-level implications. The procedure followed the staged screening logic commonly used in systematic reviews in engineering and computer science.

2.1 Search Strategy

Searches were conducted in IEEE Xplore, Scopus, Web of Science, ScienceDirect, and Google Scholar. These sources were chosen to cover both communication-engineering venues and broader computing literature. Search strings combined terms such as “6G Internet of Things,” “6G IoT networks,” “6G wireless communication and IoT,” “6G enabling technologies,” “AI-driven 6G IoT,” and “6G network architecture for IoT.” The formal inclusion window was 2023-2026 so that the synthesis would emphasize recent developments in a rapidly changing field.

2.2 Eligibility Criteria and Screening

Studies were considered eligible when they were peer-reviewed journal or conference papers, addressed 6G together with IoT or a directly relevant enabling layer, and contributed to technology, architecture, security, optimization, or applications. Non-peer-reviewed material, duplicate records, papers unrelated to either 6G or IoT, and studies without sufficient technical relevance to the review questions were excluded. Screening proceeded from duplicate removal to title and abstract review and then to full-text assessment. This sequence helped separate broad 6G surveys from papers that contained material directly useful for understanding 6G-enabled IoT.

2.3 Study Selection

The search initially returned 120 records. The PRISMA-style flow used in the study shows 95 records remaining after deduplication, 62 papers retained after title and abstract screening, 45 papers taken forward to full-text assessment, and 38 studies included in the final review. These 38 studies form the main evidence base for the thematic synthesis presented in the following sections.

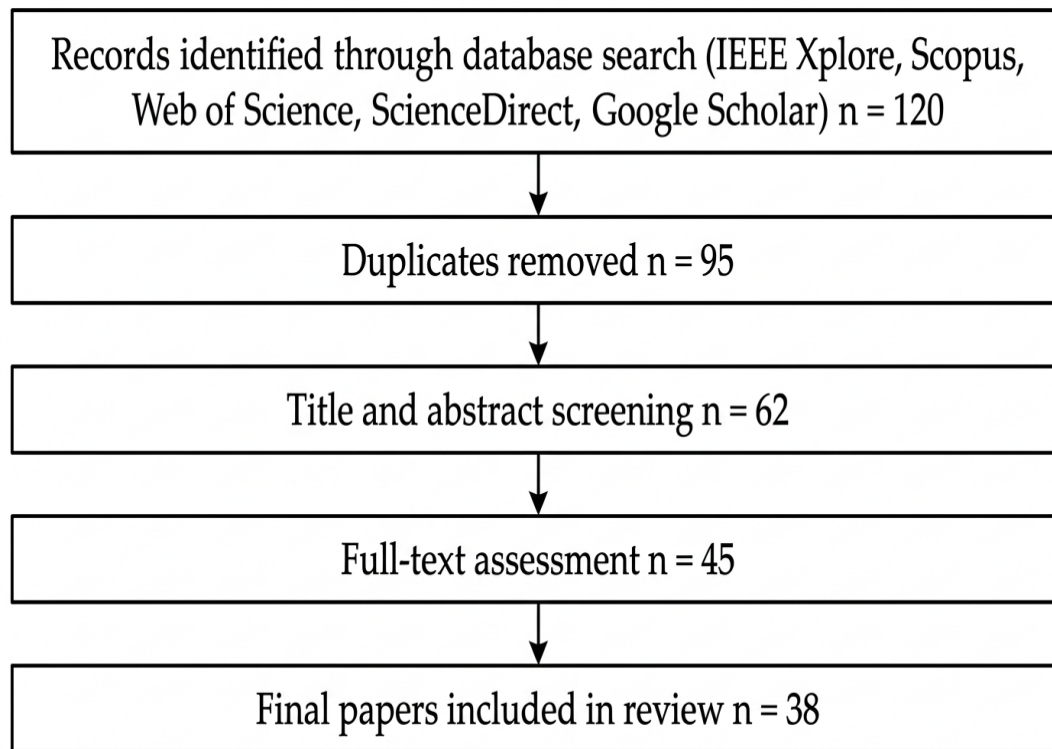


Figure 1. PRISMA-based study selection process used for the systematic literature review.

3. Literature Review and Thematic Synthesis

3.1 6G Vision, Requirements, and Research Landscape

The reviewed literature consistently presents 6G as a broader systems transition rather than a simple extension of 5G. In addition to higher capacity, the proposed architecture combines communication with sensing, positioning, computation, and machine intelligence [12]-[16]. This shift is particularly relevant to IoT because many future applications depend on rapid interaction between physical environments and digital decision systems. A sensor reading may need to be interpreted at the edge, combined with contextual information from neighboring devices, and acted upon within a tight

control loop rather than merely uploaded to a remote cloud.

Several performance targets recur across the literature: terabit-class peak data rates, substantially lower latency than 5G, connection densities approaching ten million devices per square kilometer, high reliability, and markedly improved energy efficiency [8], [12], [13]. Coverage is also treated differently. Instead of assuming a terrestrial cellular footprint, many 6G proposals integrate low-Earth-orbit satellites, unmanned aerial vehicles, high-altitude platforms, and terrestrial networks to provide continuity across remote and difficult environments [18], [19], [23].

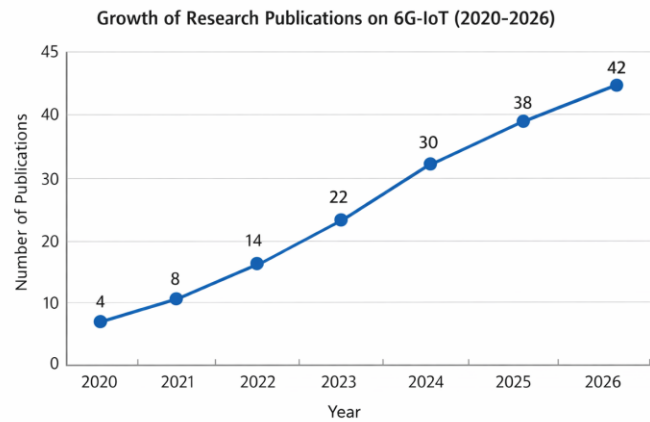


Figure 2: Growth of research publications on 6G-IoT from 2020 to projected 2026.

The publication trend shown in Figure 2 reflects the rapid expansion of interest in 6G-IoT. More importantly, the research agenda has broadened over time: early work concentrated on vision and radio technologies, whereas recent studies

increasingly examine edge intelligence, security, digital twins, and network-level orchestration. This wider scope suggests that future progress will depend on integration across disciplines rather than isolated improvements in a single communication metric.

3.2 Key Enabling Technologies for 6G IoT

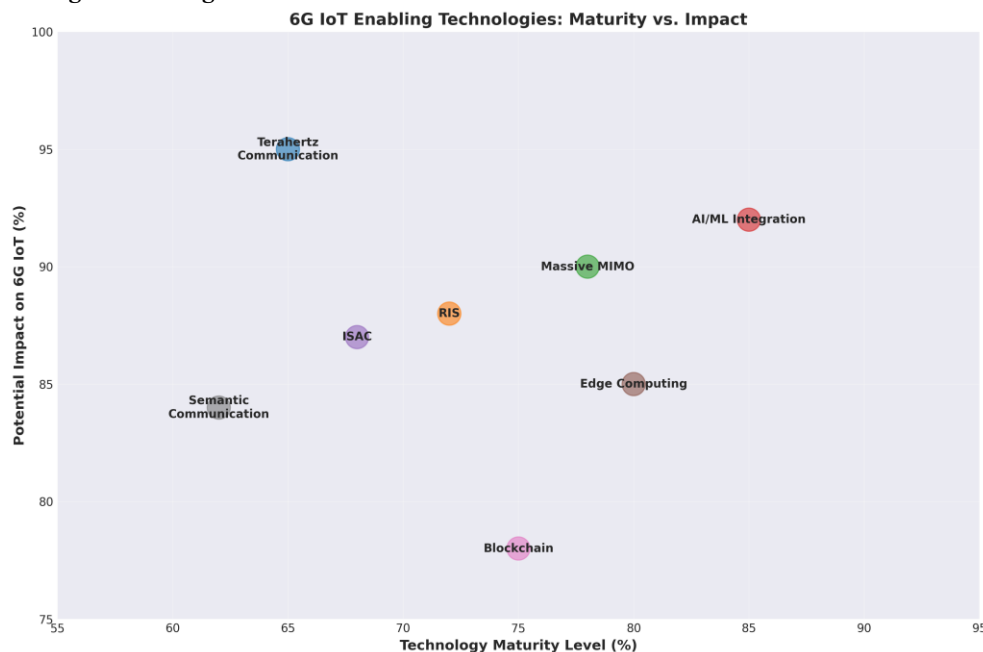


Figure 3. Relative maturity and expected impact of major 6G-IoT enabling technologies as presented in the source study.

3.2.1 Terahertz Communications

Terahertz (THz) communication, typically discussed in the 0.1-10 THz range, is attractive because it offers large amounts of underused spectrum and can support very high short-range data rates [17]. For dense IoT environments, this capacity could benefit applications that generate data volumes far beyond those of conventional sensors, including high-resolution digital twins, machine vision, and immersive interfaces. The advantage, however, comes with demanding propagation conditions. Free-space loss, blockage, atmospheric absorption, hardware limitations, and narrow frequency windows can sharply reduce link range and reliability [10], [17].

Consequently, THz communication is unlikely to function as a universal replacement for lower-frequency links. The more plausible role identified in the literature is as one layer in a multi-band network, supported by highly directional beamforming, adaptive carrier selection, and intelligent surfaces. For IoT design, this implies that link selection should depend on device capability, distance, mobility, and application urgency rather than on a single preferred spectrum band.

3.2.2 Reconfigurable Intelligent Surfaces

Reconfigurable intelligent surfaces (RIS) attempt to make the propagation environment itself controllable. Arrays of low-power reflecting elements can adjust the phase and, in some designs, the amplitude of incident waves so that energy is redirected toward intended receivers [36]. This is appealing for IoT deployments in factories, buildings, and dense urban areas where obstruction and poor coverage are common. RIS may also reduce the transmit-power burden on constrained devices by improving the effective channel rather than asking the device to transmit more strongly.

The practical difficulties are substantial. Channel estimation becomes more complicated when the propagation path includes a large programmable surface, and joint optimization of beamforming and surface configuration can become computationally expensive as the number of elements grows. The reviewed work therefore places strong emphasis on

learning-based control and simplified optimization, but scalability and real-time adaptation remain open problems [13], [36].

3.2.3 Integrated Sensing and Communication

Integrated sensing and communication (ISAC) uses shared radio resources for both data transfer and environmental sensing. This contrasts with conventional systems in which radar-like sensing and communication are designed separately. For IoT, the attraction is clear: a network could communicate with devices while also estimating position, motion, or environmental structure, reducing duplicated hardware and spectrum use [14]. Such capability is relevant to autonomous transport, industrial monitoring, smart spaces, and digital-twin systems. The central research issue is the trade-off between the two functions. A waveform that is optimal for communication is not necessarily optimal for sensing resolution, and resource allocation must account for both goals. Robust ISAC designs therefore require joint waveform, beam, scheduling, and processing strategies that can adapt to changing application priorities.

3.2.4 Artificial Intelligence and Machine Learning

Artificial intelligence is treated in recent 6G literature as part of the network architecture rather than as an optional optimization layer [15], [24], [31], [37]. Learning models are proposed for channel estimation, traffic prediction, spectrum assignment, beam management, network slicing, anomaly detection, and mobility-aware resource allocation. Edge and federated learning are especially relevant to IoT because they allow computation to remain close to devices and can reduce the need to centralize raw data [26].

This tighter integration also creates new dependencies. AI models require computational resources, training data, update mechanisms, and security controls. They may fail under distribution shift or adversarial manipulation, and their decisions can be difficult to interpret in safety-critical settings [2], [6]. As a result, AI-native networking should be evaluated not only for average performance gains but also for robustness,

explainability, communication overhead, and recovery when a learned policy becomes unreliable.

Table 2. Major enabling technologies for 6G-enabled IoT

Technology	Main opportunity	Key challenge	Representative IoT role
Terahertz communication	Very large bandwidth and high short-range data rates	Severe path loss, blockage, absorption, hardware constraints	Digital twins, high-rate sensing, immersive services
Reconfigurable intelligent surfaces	Programmable propagation and improved coverage	Channel estimation and large-scale phase control	Coverage extension, lower device transmit power
Integrated sensing and communication	Shared spectrum and hardware for sensing and data transfer	Communication-sensing trade-offs and waveform design	Environmental sensing, autonomy, positioning
AI/ML integration	Adaptive control, prediction, and autonomous optimization	Compute overhead, robustness, explainability, adversarial risk	Edge intelligence, slicing, resource management
Blockchain	Distributed trust and auditable transactions	Latency, scalability, storage, and energy overhead	Device identity, trusted transactions, decentralized access control

3.3 Network Architecture and Infrastructure

3.3.1 Space-Air-Ground-Underwater Integrated Networks

A recurring architectural theme is the integration of communication resources across space, air, ground, and underwater environments. The aim is to reduce the coverage boundaries created by terrestrial-only infrastructure and to support IoT services in rural, maritime, disaster, agricultural, and industrial settings [18], [23]. Satellites can provide wide-area reach, UAVs and high-altitude platforms can supply flexible regional coverage, terrestrial cells can deliver low-latency access where infrastructure exists, and

specialized links can extend connectivity into underwater environments.

The value of such integration depends on orchestration. Each domain has different propagation delay, bandwidth, mobility, energy, and reliability characteristics, so the network must choose paths and processing locations dynamically. A unified service view therefore requires abstraction, network slicing, and policy mechanisms that can hide infrastructure heterogeneity from applications without ignoring the physical differences that determine performance.

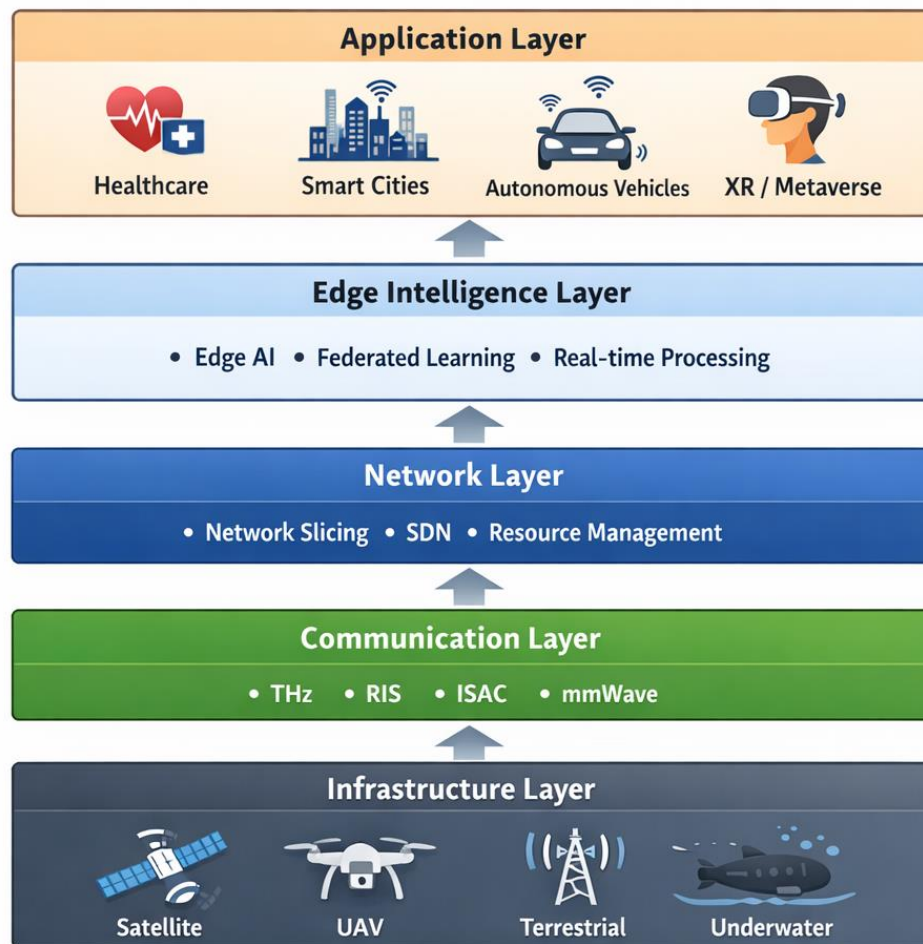


Figure 4. Layered architecture of a 6G-enabled IoT ecosystem, linking infrastructure, communication, networking, edge intelligence, and applications.

3.3.2 Satellite-UAV-Terrestrial and Non-Terrestrial Networks

Satellite-UAV-terrestrial integration is one of the most practical routes toward broader 6G coverage. Low-Earth-orbit satellites can extend connectivity to regions where terrestrial deployment is uneconomical, while UAVs can provide temporary or demand-driven coverage. Terrestrial access remains important for low-latency and high-capacity services. Together, these layers create a flexible non-terrestrial network (NTN) fabric for IoT systems that must operate across large or difficult geographic areas [18], [19], [23].

NTN integration also introduces challenges that are less prominent in conventional cellular IoT. Propagation delay and Doppler shift vary across links, handover decisions become more complex, and backhaul capacity may change as satellites and aerial nodes move. Edge-cloud coordination, predictive mobility management, and software-defined network functions are therefore central to proposed architectures. Digital twins have also been suggested as a way to test routing and reconfiguration strategies before applying them to the physical network [35].

3.3.3 Edge Computing and Network Slicing

Edge computing moves storage, inference, and control closer to IoT devices, reducing the delay and backhaul load associated with sending every data stream to a centralized cloud [5], [26]. In a 6G setting, the edge is expected to operate at several levels, from compute resources colocated with access points to regional edge servers and centralized cloud platforms. The challenge is deciding what should be processed locally and what should be escalated, especially when device energy, model size, privacy, and deadline constraints vary.

Network slicing complements this model by creating logical networks with different service characteristics on shared infrastructure. An industrial control slice may prioritize latency and reliability, a video-analytics slice may prioritize throughput, and a low-power sensing slice may prioritize energy conservation. AI-based orchestration can adjust these allocations as demand changes, although the control system itself must remain stable and predictable when traffic conditions depart from the training data [24], [37].

3.4 Resource Management and Optimization

3.4.1 Energy Efficiency

Energy efficiency is a system-level requirement rather than a device-only concern. Dense IoT deployments increase the number of radios, processors, and edge nodes that must remain available, while many end devices operate with small batteries or are placed where maintenance is difficult. The literature therefore combines low-power protocols with energy harvesting, simultaneous wireless information and power transfer, ambient backscatter, sleep scheduling, and AI-assisted resource control [27], [38].

Reported simulation results in the reviewed studies indicate that dynamic slicing and learning-based allocation can reduce power consumption under particular workloads. These gains should be interpreted in the context of the underlying models and baselines, but they show why energy-aware scheduling is becoming a first-class design objective. In practical deployments, the most useful strategies are likely to be those that jointly account for communication energy, computation energy, device lifetime, and the energy cost of the infrastructure providing the service.

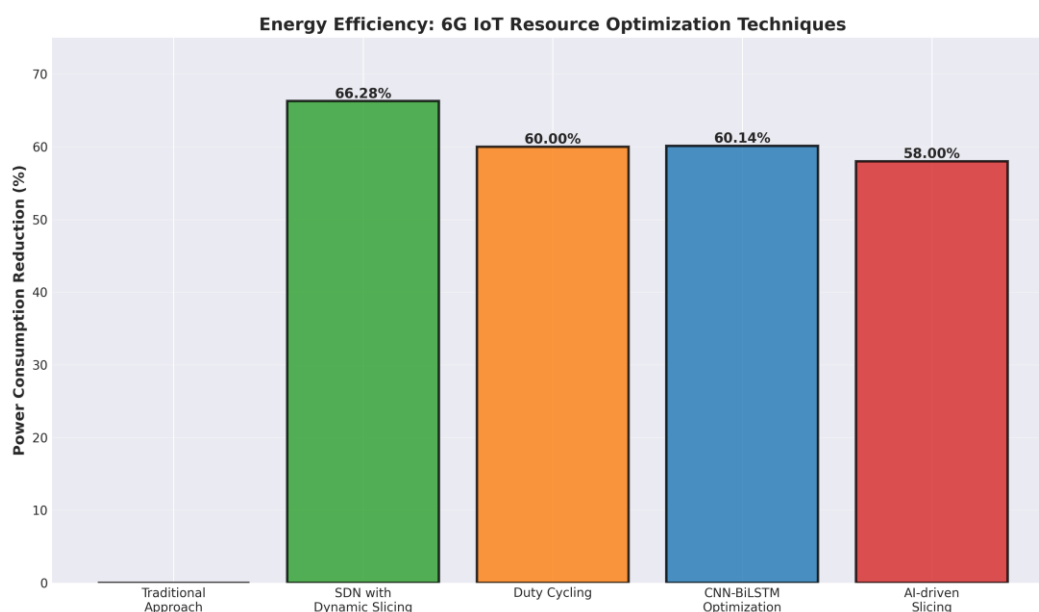


Figure 5. Energy-efficiency comparison of selected 6G-IoT resource-optimization techniques in the source study.

3.4.2 Spectrum Management and Dynamic Resource Allocation

6G proposals span sub-6 GHz, millimeter-wave, terahertz, and optical bands. This broad spectrum palette increases available capacity but also makes allocation more complex because each band has different range, blockage sensitivity, hardware requirements, and regulatory constraints [9], [30]. Cognitive access, non-orthogonal multiple access, sparse code multiple access, and learning-based spectrum prediction are among the approaches discussed for improving utilization in dense IoT networks.

Resource allocation must also react to time-varying channels, traffic, mobility, and energy availability. Deep reinforcement learning and multi-agent methods are frequently proposed because they can learn policies without requiring a closed-form model of every network interaction [13], [31]. Their promise is strongest in high-dimensional problems where conventional optimization is too slow for repeated real-time decisions. Their limitation is equally important: learned policies need reliable training, safeguards against unstable behavior, and evaluation under conditions not seen during training.

3.5 Security, Privacy, and Trust in 6G IoT

3.5.1 Expanding Cybersecurity Risks

The 6G-IoT attack surface is expected to grow because intelligence, sensing, and computation are distributed across many more devices and network layers. Existing IoT weaknesses such as insecure credentials, outdated firmware, denial-of-service attacks, and compromised gateways will remain relevant, while AI-native control introduces model poisoning, adversarial examples, inference attacks, and model theft [2], [6], [25]. Novel radio technologies may also create new physical-layer attack opportunities that are not fully covered by current threat models.

Security therefore needs to be designed as a continuous process rather than as a perimeter around a trusted network. The literature emphasizes behavioral anomaly detection, secure boot and update mechanisms, continuous identity

verification, resilient routing, and security monitoring across edge and cloud layers. AI can contribute to threat detection, but security models themselves must be protected from manipulation and should not become a single point of failure.

3.5.2 Privacy-Preserving Architectures

6G-enabled sensing and precise positioning can reveal more about users and environments than conventional connectivity systems. Privacy-by-design is therefore essential. Federated learning is frequently proposed because it allows model training to use distributed data without routinely moving raw records to a central server. Differential privacy, secure multi-party computation, and homomorphic encryption provide additional mechanisms for limiting information exposure, although each introduces computational or accuracy trade-offs [6], [26].

The main architectural question is not whether privacy mechanisms exist, but where they should be applied and how their cost should be managed on constrained devices. A practical privacy design must consider data sensitivity, device capability, latency tolerance, and the risk created by metadata such as location and communication patterns.

3.5.3 Zero-Trust, Blockchain, and Post-Quantum Security

Zero-trust architectures are well suited to a network in which devices, edge nodes, satellites, and services may belong to different administrative domains. Instead of granting implicit trust based on network location, access decisions are continuously tied to identity, context, and observed behavior. Blockchain is also discussed as a mechanism for decentralized identity and auditable transactions, particularly where no single authority is universally trusted [33]. The trade-off is overhead: consensus, storage, and transaction latency can be difficult to justify on highly constrained IoT nodes.

A longer-term concern is cryptographic migration. Current public-key systems may become vulnerable to sufficiently capable quantum computers, so 6G infrastructure is expected to require cryptographic agility and support for post-quantum algorithms [6].

The challenge is especially acute for IoT because devices can remain deployed for many years and may not be easy to update after installation. Hybrid

transition strategies and lightweight post-quantum implementations therefore deserve early attention rather than late retrofit.

Table 3. Security issues, mitigation directions, and deployment constraints in 6G-enabled IoT

Security area	Representative threats	Mitigation direction	Implementation constraint
AI-native networking	Adversarial inputs, poisoning, model theft	Robust training, validation, adversarial defenses	Compute cost and detection delay
IoT devices	Weak credentials, unpatched firmware	Secure boot, automated updates, strong identity	Limited memory, energy, and update logistics
Cryptographic migration	Future quantum attacks	Post-quantum algorithms and cryptographic agility	Standardization and migration overhead
Distributed edge	Compromised or malicious edge nodes	Zero-trust access and continuous verification	Added control traffic and privacy management
Novel communication media	THz/VLC-specific interception or manipulation	Physical-layer authentication and waveform-level protection	Incomplete channel and attack characterization

3.6 Applications and Use Cases

3.6.1 Healthcare and Telemedicine

Healthcare is often cited as a high-value 6G-IoT domain because clinical monitoring combines continuous sensing with strict requirements for privacy, reliability, and timely response. Wearable and bedside sensors can stream physiological measurements to nearby edge nodes for rapid analysis, while wider-area connectivity can link remote clinics to specialist services [5], [29]. Low-latency communication is also relevant to teleoperation and augmented clinical interfaces, although such applications require end-to-end safety engineering that extends well beyond the radio link.

The strongest contribution of 6G in this setting may be the ability to coordinate sensing, edge analytics, and secure connectivity across heterogeneous devices. Federated learning can support collaborative model development without routinely centralizing patient data, while network slicing may help separate critical clinical traffic from lower-priority services. Regulatory compliance, explainability, fail-safe operation,

and cybersecurity remain essential conditions for adoption.

3.6.2 Smart Cities and Industrial IoT

Smart-city and industrial IoT systems illustrate the scale problem that motivates 6G research. Urban sensing platforms may combine traffic, environmental, energy, and infrastructure data, while factories can contain dense networks of machines, cameras, robots, and condition-monitoring sensors. These environments benefit from local processing, deterministic communication, and flexible resource allocation because the value of data often depends on how quickly it can be converted into an operational decision [5], [9].

In industrial settings, predictive maintenance and closed-loop control are especially important. Edge intelligence can detect abnormal equipment behavior close to the data source, while high-reliability slices can protect time-critical control traffic. The main deployment challenge is integration with existing industrial systems, where legacy protocols, safety certification, and

long equipment lifecycles can slow adoption even when the communication technology is available.

3.6.3 Autonomous Vehicles and V2X Communication

Autonomous mobility requires vehicles to combine onboard sensing with information received from infrastructure, neighboring vehicles, and remote services. 6G vehicle-to-everything (V2X) proposals aim to support cooperative perception, hazard notification, map updates, and coordinated maneuvering across a wider coverage area [18], [23]. Non-terrestrial connectivity may also help maintain service in regions with limited terrestrial infrastructure. The benefit of connectivity should not be confused with dependence on connectivity. Safety-critical vehicle functions must remain robust when links degrade or disappear. Research is therefore needed on graceful degradation, confidence-aware sensor sharing, authenticated messages, and latency bounds that reflect the full sensing-computation-communication chain rather than radio transmission alone.

3.6.4 Extended Reality, Holographic Services, and Digital Twins

Extended reality and holographic communication are among the applications most often used to illustrate the capacity ambitions of 6G. High-resolution volumetric media can demand sustained high throughput and very low interaction delay, particularly when rendering is split between user devices and edge servers [14], [18]. Digital twins create a related requirement: continuous data from physical assets must be synchronized with a computational model closely enough for monitoring, prediction, or control.

These applications are useful stress tests because they expose the need for coordination across bandwidth, latency, compute placement, sensing, and synchronization. They also show why headline peak data rates alone are insufficient; consistent service quality and resource orchestration are more important than an isolated best-case link speed.

4. Research Gaps and Future Directions

4.1 Technical and Deployment Gaps

The reviewed literature reveals a clear gap between attractive architectural visions and evidence from large-scale, heterogeneous deployments. THz channel models still require broader measurement campaigns across indoor, outdoor, mobile, and obstructed environments [17]. RIS research needs scalable channel estimation and control methods that remain effective when surfaces contain very large numbers of elements. ISAC must handle the practical tension between sensing accuracy and communication performance, while AI-native control requires stronger evidence of robustness under distribution shift and adversarial conditions.

A second gap concerns integration. Many studies evaluate one technology under controlled assumptions, but future IoT services will combine several technologies at once. A network may need to decide among terrestrial, aerial, and satellite links while allocating edge compute, configuring an intelligent surface, protecting private data, and meeting an application deadline. Cross-layer experimental platforms and reproducible benchmarks are therefore needed to test interactions that are hidden when each component is studied in isolation.

Table 4. Representative studies in the reviewed literature and the limitations highlighted in the source manuscript

Ref.	Study	Year	Focus	Main contribution	Reported limitation
[1]	Ferrag et al.	2023	AI security	Generative-AI-based cyber-threat detection for 6G-IoT	High computational complexity

Ref.	Study	Year	Focus	Main contribution	Reported limitation
[4]	Akbar and Ahmed	2024	Network challenges	Technical challenges and future requirements of 6G	Limited IoT-specific analysis
[5]	He and Zhang	2025	Edge intelligence	Edge intelligence for more efficient 6G-IoT	Requires advanced edge infrastructure
[6]	Kaur and Singh	2025	Cybersecurity	Explainable-AI-driven cyber defense for 6G-IoT	Scalability challenges
[8]	Islam et al.	2025	Network optimization	KPI, tool, and AI-model survey for 6G optimization	Limited experimental evaluation
[10]	Dogra et al.	2023	Wireless evolution	Overview of beyond-5G and 6G technologies	Broad survey focus
[11]	Chamola et al.	2023	IoT applications	Applications and challenges of 6G-enabled IoT	Limited architectural analysis
[12]	Tataria et al.	2023	Network vision	Vision, requirements, and design targets	Primarily conceptual
[13]	Chowdhury et al.	2023	Enabling technologies	THz, AI, edge computing, and other 6G enablers	Implementation challenges
[15]	Liu et al.	2024	AI networking	AI-enabled architectures for smart IoT communication	Model-training overhead
[18]	Giordani et al.	2024	Applications	Emerging 6G use cases and technologies	Limited real-world validation
[19]	Ahmad et al.	2024	IoT architecture	Architecture for integrating IoT with 6G	Infrastructure complexity
[26]	Zhou et al.	2024	Edge intelligence	Edge-intelligence techniques for IoT in 6G	Deployment challenges
[33]	Chaudhary et al.	2024	Blockchain security	Blockchain-based security for 6G-IoT	Scalability issues
[38]	Park et al.	2025	Energy efficiency	Energy-efficient communication for massive 6G IoT	Limited practical validation

4.2 Standardization, Sustainability, and Equity

6G standardization will require coordination across organizations that traditionally focus on different parts of the technology stack. Radio access, non-terrestrial networking, sensing, AI control, security, and spectrum policy cannot be standardized independently if services are expected to operate end to end [3], [27]. Interoperability will be particularly important for IoT, where low-cost devices may

remain in service for long periods and where fragmented implementations can create both performance and security problems.

Sustainability and equitable access are equally important. A denser, more computationally intensive network could increase energy use even if individual links become more efficient. Research therefore needs lifecycle-aware energy metrics, renewable-energy integration, repairable hardware,

and realistic accounting of the energy consumed by edge and AI workloads [27], [38]. At the policy level, global coverage should not become synonymous with global affordability; infrastructure cost, spectrum access, and deployment incentives will shape whether 6G narrows or widens existing connectivity gaps.

4.3 Research Priorities and Roadmap

The next phase of 6G-IoT research should place greater weight on measurable end-to-end evidence.

Priority areas include experimentally grounded THz models, scalable RIS control, joint ISAC optimization, robust and explainable AI, communication-efficient federated learning, post-quantum migration for constrained devices, and cross-domain orchestration for terrestrial and non-terrestrial links. Benchmarking should report not only throughput and latency, but also energy, reliability, security overhead, model robustness, and performance under failure or mobility.



Figure 6. Research roadmap from core technology development through standardization and testing toward wider 6G-IoT deployment.

The roadmap in Figure 6 captures the transition from core technology development to standardization, testing, and eventual deployment. The dates should be read as planning horizons rather than guaranteed milestones. Progress will depend on whether proposed technologies can be integrated into interoperable systems and validated outside narrow simulation settings. In that sense, the central research question is shifting from “Can each technology work?” to “Can these technologies work together reliably, securely, and efficiently at IoT scale?”

5. Conclusion

6G-enabled IoT is best understood as a convergence of communication, sensing, computing, and machine intelligence. The reviewed literature points to a network that is more distributed, more programmable, and more closely coupled to physical environments than 5G. Terahertz communication can provide exceptional local capacity; RIS can reshape difficult propagation environments; ISAC can combine connectivity

with sensing; edge intelligence can shorten decision loops; and non-terrestrial networking can extend service beyond conventional cellular footprints.

None of these capabilities is sufficient on its own. Their value depends on how well they can be integrated under practical constraints of energy, mobility, security, cost, and interoperability. The 38 studies included in this review show substantial progress in defining the 6G-IoT research agenda, but they also reveal persistent gaps in real-world validation, trustworthy AI, scalable optimization, post-quantum security, and sustainable deployment. Future work should therefore move beyond isolated performance demonstrations and evaluate complete end-to-end systems under realistic operating conditions.

If that shift occurs, 6G could provide a useful foundation for intelligent IoT services in healthcare, industry, mobility, smart environments, and immersive applications. The decisive measure of success, however, will not be whether a network reaches a headline peak rate. It will be whether it can deliver dependable, secure, energy-conscious,

and accessible connectivity to the diverse devices and applications that future IoT ecosystems are expected to support.

REFERENCES

- [1] M. A. Ferrag, M. Debbah, and M. Al-Hawawreh, "Generative AI for cyber threat-hunting in 6G-enabled IoT networks," *IEEE Access*, vol. 11, pp. 45321–45338, 2023.
- [2] B. D. Son, N. T. Hoa, T. V. Chien, W. Khalid, and M. A. Ferrag, "Adversarial attacks and defenses in 6G network-assisted IoT systems," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 1, pp. 210–233, 2024.
- [3] M. Yang et al., "From 5G to 6G: A survey on security, privacy, and standardization pathways," *IEEE Access*, vol. 12, pp. 12211–12240, 2024.
- [4] M. S. Akbar and A. Ahmed, "On challenges of sixth-generation (6G) wireless networks," *Journal of Network and Computer Applications*, vol. 226, pp. 104040, 2024.
- [5] Q. He and Y. Zhang, "Integrating IoT and 6G: Applications of edge intelligence," *IEEE Internet Computing*, vol. 29, no. 4, pp. 56–65, 2025.
- [6] N. Kaur and S. K. Singh, "Securing the 6G-IoT environment: A framework for explainable AI-driven cyber defense," *Sensors*, vol. 25, no. 3, pp. 854, 2025.
- [7] M. M. Saeed et al., "A comprehensive survey on 6G security: Physical connection and service layers," *Journal of Telecommunications and Information Technology*, vol. 2025, pp. 112–135, 2025.
- [8] M. M. Islam, K. Hasan, and S. H. Jeong, "Performance evaluation and optimization for 6G networks: A survey of KPIs, tools, and AI models," *ICT Express*, vol. 11, no. 4, pp. 399–415, 2025.
- [9] A. Soliman, "The future of Internet of Things and multimodal language models in 6G networks: Opportunities and challenges," *IEEE Access*, vol. 13, pp. 15521–15540, 2025.
- [10] A. Dogra, R. K. Jha, and S. Jain, "A survey on beyond 5G and 6G wireless communication," *IEEE Access*, vol. 11, pp. 12450–12482, 2023.
- [11] V. Chamola et al., "6G for Internet of Things: Applications, challenges, and future directions," *IEEE Internet of Things Journal*, vol. 10, no. 11, pp. 9876–9895, 2023.
- [12] H. Tataria et al., "6G wireless systems: Vision, requirements, challenges, insights, and opportunities," *Proceedings of the IEEE*, vol. 111, no. 3, pp. 349–382, 2023.
- [13] M. Z. Chowdhury et al., "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 1347–1373, 2023.
- [14] S. Dang et al., "What should 6G be?" *Nature Electronics*, vol. 6, pp. 23–29, 2023.
- [15] Y. Liu et al., "AI-enabled 6G networks for smart IoT applications," *IEEE Network*, vol. 38, no. 2, pp. 95–101, 2024.
- [16] X. You et al., "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Science China Information Sciences*, vol. 67, no. 4, pp. 141301, 2024.
- [17] S. Mumtaz et al., "Terahertz communication for 6G: Challenges and opportunities," *IEEE Vehicular Technology Magazine*, vol. 19, no. 1, pp. 72–80, 2024.
- [18] M. Giordani et al., "Toward 6G networks: Use cases and technologies," *IEEE Communications Magazine*, vol. 62, no. 2, pp. 84–90, 2024.
- [19] A. Ahmad et al., "6G and the Internet of Things: Vision, architecture, and future trends," *IEEE Access*, vol. 12, pp. 55321–55345, 2024.
- [20] J. Rodriguez, "6G networks: Smart connectivity for IoT and cyber-physical systems," *IEEE Communications Standards Magazine*, vol. 8, no. 2, pp. 23–29, 2024.

-
- [21] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?," IEEE Vehicular Technology Magazine, vol. 19, no. 2, pp. 24–33, 2024.
- [22] M. Latva-aho and K. Leppanen, "Key drivers and research challenges for 6G ubiquitous wireless intelligence," IEEE Access, vol. 11, pp. 11233–11247, 2023.
- [23] S. Chen et al., "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Network, vol. 37, no. 6, pp. 134–142, 2023.
- [24] T. Huang et al., "AI-driven network architecture for 6G IoT ecosystems," IEEE Communications Magazine, vol. 62, no. 5, pp. 40–46, 2024.
- [25] M. Al-Rakhami and M. Al-Amri, "Security challenges in 6G-enabled Internet of Things," IEEE Access, vol. 11, pp. 80321–80340, 2023.
- [26] Z. Zhou et al., "Edge intelligence for Internet of Things in 6G networks," IEEE Internet of Things Journal, vol. 11, no. 2, pp. 1890–1902, 2024.
- [27] S. Zhang et al., "6G wireless networks: Vision, requirements, architecture, and key technologies," IEEE Vehicular Technology Magazine, vol. 18, no. 4, pp. 28–41, 2023.
- [28] H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," IEEE Access, vol. 11, pp. 21910–21930, 2023.
- [29] S. Dang, O. Amin, B. Shihada, and M. S. Alouini, "What should 6G be? Key enabling technologies and research directions," IEEE Communications Surveys & Tutorials, vol. 26, no. 2, pp. 1554–1596, 2024.
- [30] J. G. Andrews et al., "What will 6G be?," IEEE Journal on Selected Areas in Communications, vol. 42, no. 3, pp. 587–598, 2024.
- [31] H. Zhang et al., "Machine learning for 6G-enabled IoT networks," IEEE Wireless Communications, vol. 31, no. 1, pp. 44–51, 2024.
- [32] R. W. Heath et al., "An overview of signal processing techniques for 6G communications," IEEE Journal of Selected Topics in Signal Processing, vol. 18, no. 2, pp. 123–138, 2024.
- [33] A. Chaudhary et al., "Blockchain-based security for 6G Internet of Things," IEEE Internet of Things Journal, vol. 11, no. 7, pp. 6542–6556, 2024.
- [34] P. Yang et al., "Semantic communications for 6G IoT systems," IEEE Network, vol. 38, no. 4, pp. 120–127, 2024.
- [35] H. Yu et al., "Digital twin-enabled 6G networks for smart IoT services," IEEE Communications Magazine, vol. 63, no. 1, pp. 72–79, 2025.
- [36] Y. Sun et al., "Reconfigurable intelligent surfaces for 6G IoT networks," IEEE Wireless Communications, vol. 31, no. 3, pp. 90–97, 2024.
- [37] T. Taleb et al., "AI-native networking for 6G: Vision and architecture," IEEE Network, vol. 39, no. 1, pp. 34–41, 2025.
- [38] S. Park et al., "Energy-efficient massive IoT communications in 6G networks," IEEE Internet of Things Journal, vol. 12, no. 2, pp. 1650–1662, 2025.