International Journal of
Telecommunications &
Emerging Technologies

ISSN: 2455-0345
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJTET

https://journalspub.com/journal/IJTET/

Review IJTET

Emerging Trends and Challenges in Telecommunications: A Review of 5G/6G, Softwarization, Edge Intelligence, IoT Security, and Enabling Technologies

Gaurav Singh[1], Sameer Gupta[1], Karan Gupta[1,*]

Abstract

Telecommunications research over the last decade has accelerated from the deployment and optimization of 5G to early explorations of 6G, driven by demands for extreme data rates, ubiquitous low-latency connectivity, massive device density and novel services such as extended reality (XR) and holographic communications. This review synthesizes recent developments across six interlocking technology areas: radio access and physical-layer advances (5G/6G), network softwarization (SDN/NFV), edge and cloud–native architectures, artificial intelligence for wireless networks, IoT security and privacy, and trust technologies (incl. blockchain). This research identifies cross-cutting trends – notably the shift from hardware-centric to software- and data-centric network design, the rise of edge intelligence, and security as a first-class design constraint. It critically evaluates open research challenges (spectrum and coexistence, trustworthiness of AI, orchestration across cloud-edge-device, scalable security for massive IoT) and outline opportunities for future work including explainable AI in networking, energy-efficient 6G design, and standardization of edge–native network slices. Two illustrative figures (taxonomy and trend plot) summarize the topic relationships and research momentum. This article cites recent surveys and representative works to provide a compact guide for researchers entering the field.

Keywords: 5G/6G, network softwarization, edge intelligence, IoT security, AI for wireless, blockchain-enabled trust

INTRODUCTION

The telecommunications landscape has been transformed by the twin forces of massive mobile broadband and pervasive sensing. The commercialization of 5G has shifted attention from raw capacity to flexible, service-oriented networks that can meet heterogeneous service level requirements. At the same time, research communities are already exploring 6G concepts – ultra-high-rate, extremely low-latency, integrated sensing-communications, and pervasive intelligence. Alongside advances in the radio and physical layer, network softwarization (SDN, NFV), edge computing, and AI-driven network optimization have emerged as critical enablers. Security, privacy and trust technologies (including blockchain-inspired approaches) are rising to

***Author for Correspondence**
Karan Gupta
E-mail: papersjournals66@gmail.com

[1]Research Scholar, Department of Computer and Information Technology, Ludhiana, Punjab, India

Received Date: November 04, 2025
Accepted Date: November 08, 2025
Published Date: December 31, 2025

Citation: Gaurav Singh, Sameer Gupta, Karan Gupta. Emerging Trends and Challenges in Telecommunications: A Review of 5G/6G, Softwarization, Edge Intelligence, IoT Security, and Enabling Technologies. International Journal of Telecommunication and Emerging Technologies. 2025; 11(2): 38–43p.

prominence as these systems become more distributed and multi-stakeholder. This review organizes recent literature and synthesizes directions across these domains, highlighting both technological successes and continuing gaps [1–4].

SCOPE AND METHODOLOGY

This review selects recent high-impact surveys and systematic reviews across six thematic areas (5G/6G physical access; SDN/NFV; edge/cloud architectures; AI for wireless; IoT security; blockchain and trust). This research prioritized comprehensive survey articles, IEEE/ACM reviews, and highly-cited systematic analyses from 2015–2024 to capture both the established foundations and the newest trends. Representative papers are cited per section to guide the reader to deeper treatments. While not exhaustive, the article aims to provide a compact synthesis and to identify open problems amenable to short- and medium-term research [5].

5G AND THE PATH TO 6G: KEY DEVELOPMENTS AND CHALLENGES

5G research and deployment focused on three usage categories – enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine-type communications (mMTC). Research surveyed early in the 5G lifecycle highlighted radio techniques (massive MIMO, millimeter wave), spectrum management and densification as enablers for eMBB, while URLLC and mMTC demanded new scheduling and protocol adaptations. Security and privacy emerged as major cross-cutting concerns due to network softwarization and heterogeneous stakeholders. More recently, conceptual and survey work on 6G emphasizes additional frontiers: terahertz communications, integrated sensing and communications, native AI functionality in the network plane, and stringent energy and sustainability constraints. The literature also documents a growing need for standardization and cross-domain orchestration as heterogeneity increases [6].

Open Challenges

Spectrum sharing at higher bands, energy-efficient terahertz design, joint design of sensing and communications, privacy-preserving radio analytics, and securing softwarized RAN components.

NETWORK SOFTWARIZATION: SDN AND NFV EVOLUTION

Software-defined networking (SDN) and network function virtualization (NFV) promised to separate control and data planes and to implement network functions in software on commodity servers – enabling agility, programmable slices and rapid service innovation. Foundational surveys show SDN/NFV's transformative potential and the many system-level challenges (performance, orchestration, reliability, and resource management). Recent work has focused on integrating SDN/NFV with mobile core and RAN functions, scaling orchestration across multi-domain operators, and reconciling real-time radio constraints with virtualized, cloud–native implementations. Performance overheads, deterministic latency guarantees for URLLC, and multi-tenancy isolation remain practical hurdles (Figure 1).

Open Challenges

Real-time NFV for RAN, scalable multi-domain orchestration, policy-driven slicing that ensures isolation and performance guarantees [7].

EDGE AND CLOUD–NATIVE ARCHITECTURE

Edge computing brings computation and storage closer to devices to reduce latency and preserve bandwidth – critical for XR, connected vehicles, and industrial IoT. Reviews of edge computing in IoT and 5G document architectures (MEC, fog, cloudlet), orchestration concerns, and security implications. Edge–native design raises interesting trade-offs: where to place intelligence (device, edge, cloud), how to manage mobility and session continuity, and how to guarantee privacy under constrained device resources. Emerging research also examines edge-assisted model training and federated learning mechanisms that exploit a nearby compute while maintaining data locality [8, 9].

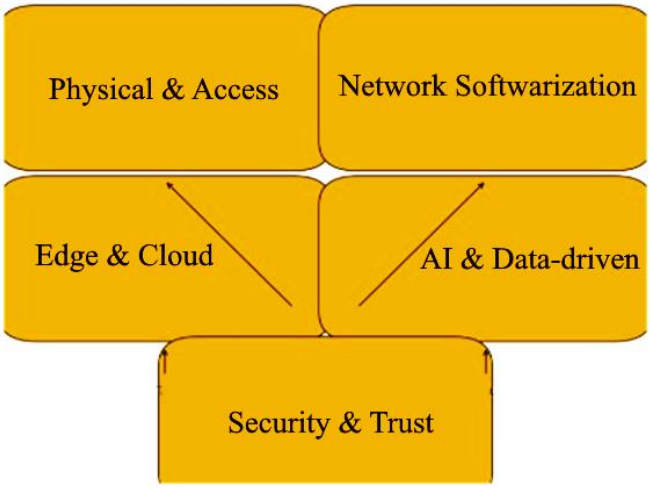

Figure 1. Taxonomy of key technologies (Physical & Access, Network Softwarization, Edge & Cloud, AI & Data-driven, Security & Trust) (see embedded Figure 1).

Open Challenges

Seamless edge–cloud orchestration, mobility-aware service placement, resource-efficient federated learning, and standardized APIs for edge services.

ARTIFICIAL INTELLIGENCE FOR WIRELESS NETWORKS

Machine learning (ML) and AI are reshaping network planning, resource allocation, beamforming, and anomaly detection. Surveys show increasing use of supervised, unsupervised, and reinforcement learning across the protocol stack, including PHY-layer learning for channel estimation and MAC-layer scheduling. A notable recent trend is "wireless for ML" and "ML for wireless" convergence – designing wireless protocols that are ML-aware (task-oriented communication) and developing ML techniques tailored to wireless constraints (low-latency, energy limits, distributed data). Concerns include data availability, label scarcity, model explainability, and robustness against adversarial examples in operational networks (Figure 2).

Open Challenges

Explainability and verification of learned policies, online continual learning under non-stationary channels, privacy-preserving distributed training, and standards for ML model lifecycle in telecom networks.

IOT SECURITY AND PRIVACY

Large-scale IoT deployment exposes networks to new attack surfaces: device compromise, botnets, insecure default configurations, and fragile update mechanisms. Systematic surveys highlight the taxonomy of IoT threats, vulnerability patterns, and security solutions spanning lightweight cryptography, anomaly detection, and edge-enforced access control. Because IoT devices are resource-constrained, security solutions need to be efficient and scalable. The interplay between edge computing and IoT security is promising nodes can offload heavy security processing and provide local trust anchors – but this creates new trust and orchestration problems.

Open Challenges

Secure device lifecycle management at scale, bootstrapping trust for device onboarding, secure OTA updating in poor-connectivity contexts, and privacy-preserving telemetry for network monitoring [10–14].

BLOCKCHAIN AND TRUST TECHNOLOGY IN TELECOMMUNICATIONS

Blockchain and distributed ledger technologies (DLTs) attract interest for decentralized identity, secure roaming, SLA settlement and spectrum access coordination. Surveys indicate potential for

blockchain-based marketplaces and service settlement models in telecoms, but also note scalability, latency and regulatory obstacles. Blockchain is often complementary rather than a panacea – best applied where tamper-evidence and decentralization yield clear business value (e.g., multi-operator revenue sharing, spectrum registries). Integration with softwarized orchestration and identity frameworks is an active research area.

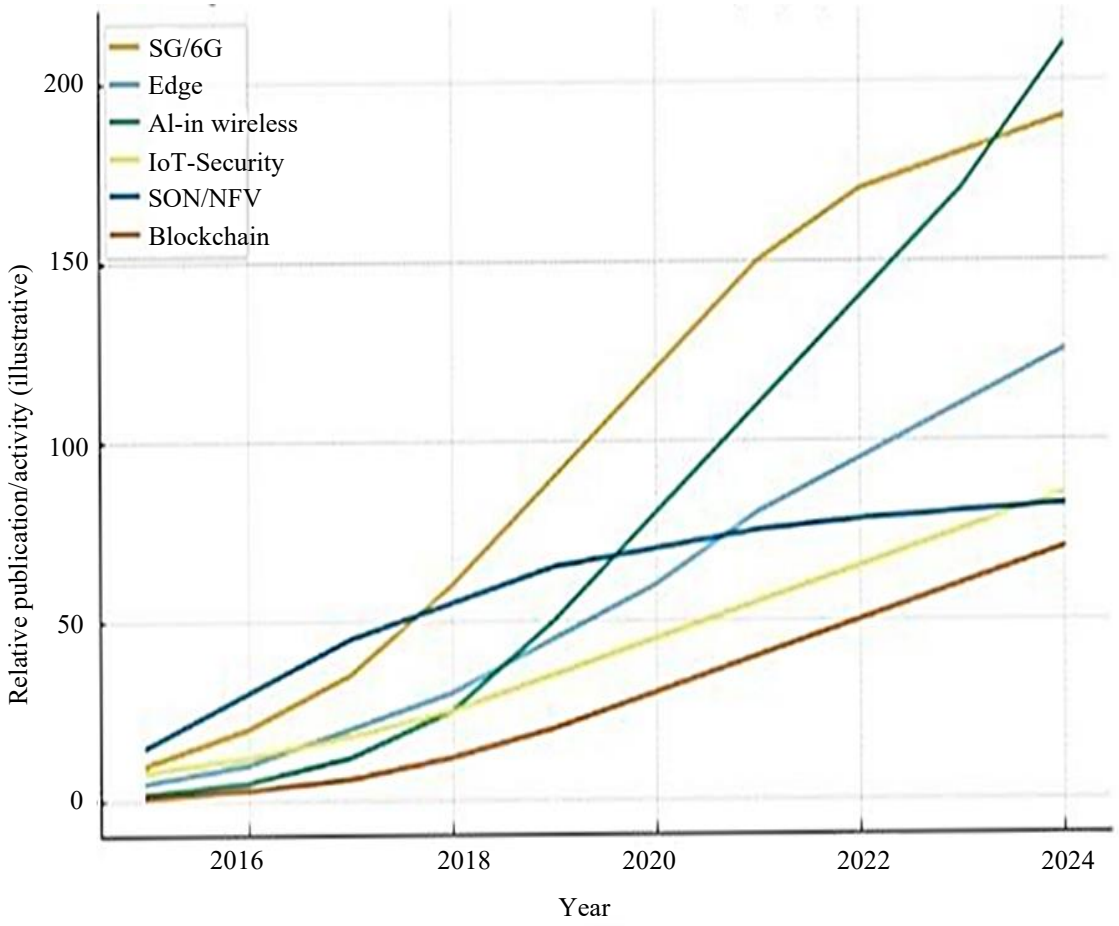

Figure 2. Illustrative trend of research activity by topic (2015–2024) showing rising momentum in AI-for-wireless and continued growth of 5G/6G, edge, IoT-security and blockchain.

Open Challenges

High-throughput, low-latency DLTs for telecom use cases, privacy-preserving ledger designs, economic models for blockchain adoption, and interoperability with telco OSS/BSS.

CROSS-CUTTING ISSUES: SECURITY, STANDARDIZATION, SUSTAINABILITY

Three cross-cutting themes demand attention

- *Security-by-Design:* Softwarization and open interfaces increase attack surfaces; thus, security must be embedded across RAN, core, and orchestration layers. Surveys on 5G security provide frameworks for threat modeling and defense-in-depth.
- *Standards and Multi-Stakeholder Governance:* Interoperability across vendors and operators remains essential. 3GPP, ETSI (NFV/MEC), IEEE and industry consortia are shaping interoperable building blocks; however, rapid research innovation strains standardization cycles.
- *Sustainability and Energy:* Future networks must balance capacity against energy budgets. Research is increasingly prioritizing energy-aware protocol design, hardware efficiency, and life-cycle sustainability – especially important for dense small-cell and terahertz deployments. (Emerging surveys and editorials emphasize sustainability as a research priority.)

OPPORTUNITIES AND RESEARCH DIRECTIONS

Based on the literature synthesis, following promising directions are recommended.

- *Explainable and Verifiable AI for Networks:* Frameworks that provide guarantees (safety envelopes) for learned controllers.
- *Edge-Native Orchestration Standards:* APIs and abstractions to allow portable, migration-capable services across multiple edge providers.
- *Federated/Partitioned Learning in Mobile Settings:* Methods to handle non-iid data, straggler devices and communication constraints.
- *Secure-by-Design Softwarized RANs:* Combining formal verification and runtime attestation for VNFs and RAN software.
- *Scalable DLT Designs for Telecom Functions:* Hybrid on-chain/off-chain architectures for SLA and identity with measurable performance.
- *Green 6G Design:* Research on energy-adaptive beamforming, sleep modes, and cross-layer energy management.

CONCLUSIONS

Telecommunications research in the 2015–2024 window shows a decisive shift from purely physical-layer capacity engineering towards integrated systems that place software, data and trust at the core. SDN/NFV have made operator networks programmable, while edge computing and AI are enabling new low-latency, context-aware services.

Security and privacy remain critical bottlenecks, especially for large-scale IoT. Looking forward, 6G research, explainable AI, and sustainable network design represent fertile ground. Interdisciplinary collaboration – linking communication theory, systems engineering, machine learning, and security – is essential to realize ambitious visions responsibly.

REFERENCES

1. Panwar N, Sharma S, Singh AK. A survey on 5G: The next generation of mobile communication. Phys Commun. 2016;18:64–84.
2. Jawad AT, Maaloul R, Chaari L. A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges. Comput Netw. 2023;237:110085.
3. Kreutz D, Ramos FM, Verissimo PE, Rothenberg CE, Azodolmolky S, Uhlig S. Software-defined networking: A comprehensive survey. Proc IEEE. 2014;103(1):14–76.
4. Yi B, Wang X, Li K, Huang M. A comprehensive survey of network function virtualization. Comput Netw. 2018;133:212–62.
5. Sha K, Yang TA, Wei W, Davari S. A survey of edge computing-based designs for IoT security. Digit Commun Netw. 2020;6(2):195–202.
6. Kong L, Tan J, Huang J, Chen G, Wang S, Jin X, et al. Edge-computing-driven Internet of Things: A survey. ACM Comput Surv. 2022;55(8):1–41.
7. Hellström H, da Silva JM Jr, Amiri MM, Chen M, Fodor V, Poor HV, et al. Wireless for machine learning: A survey. Found Trends Signal Process. 2022;15(4):290–399.
8. Kulin M, Kazaz T, De Poorter E, Moerman I. A survey on machine learning-based performance improvement of wireless networks: PHY, MAC and network layer. Electronics. 2021;10(3):318.
9. Hassan WH. Current research on Internet of Things (IoT) security: A survey. Comput Netw. 2019;148:283–94.
10. Sadhu PK, Yanambaka VP, Abdelgawad A. Internet of Things: Security and solutions survey. Sensors. 2022;22(19):7433.
11. Khan R, Kumar P, Jayakody DN, Liyanage M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Commun Surv Tutor. 2019;22(1):196–248.
12. Al-Matari NY, Zahary AT, Al-Shargabi AA. A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks. Sci Rep. 2024;14(1):30990.

13. Krichen M, Ammi M, Mihoub A, Almutiq M. Blockchain for modern applications: A survey. Sensors. 2022;22(14):5274.
14. Evgenieva E, Vlahov A, Ivanov A, Poulkov V, Manolova A. A comprehensive survey of 6G simulators: Comparison, integration, and future directions. Electronics. 2025;14(16):3313.

