Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

(Review Article)

Check for updates

Architectural enhancements, challenges and future trends in real-time IoT applications over 5G networks

Precious Nowamagbe [1,*], Samuel Oluwatosin Akande [2], Goodness Damilare Atolagbe [3], Bankole Adefemi [4], Adeniyi Joshua Boluwade [5], Christopher Chibuike Nzekwe [6] and Izunna Norbert Agu [7]

[1] *University of Port Harcourt, Marketing, Port Harcourt, Rivers State, Nigeria.*
[2] *University of Lagos, Computer engineering, Akoka, Lagos, Nigeria.*
[3] *University of Ilorin, Mechanical Engineering, Ilorin, Kwara State, Nigeria.*
[4] *Federal University of Technology Minna, Process/Chemical Engineering, Minna, Niger State, Nigeria.*
[5] *University of Lagos, Electrical and Electronics Engineering, Akoka, Lagos, Nigeria.*
[6] *Ulster University, International Business/Finance/Economics, United Kingdom*
[7] *University of Lagos, Electrical and Electronics Engineering, Akoka, Lagos, Nigeria.*

Global Journal of Engineering and Technology Advances, 2025, 23(03), 167-179

Publication history: Received on 23 April 2025; revised on 08 June 2025; accepted on 11 June 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.23.3.0185

Abstract

The introduction of real-time Internet of Things (IoT) applications has introduced unprecedented demands on communication systems, which require ultra-low latency, high reliability, and massive device connectivity. Fifth-generation (5G) wireless networks represent a foundational shift in network architecture, offering advanced capabilities such as ultra-reliable low-latency communication (URLLC), mobile edge computing (MEC), and network slicing to support time-sensitive IoT services at scale. This review critically examines how these architectural enhancements enable real-time IoT deployment across domains, with inclusion of autonomous transportation, industrial automation, remote healthcare, and smart energy systems.

While 5G provides a robust framework, its real-world adoption has faced technical constraints related to interoperability, spectrum management, energy efficiency, and cybersecurity. The paper synthesizes existing research on these challenges, and highlight persistent integration gaps and trade-offs that must be navigated to achieve deterministic performance in complex environments. In response, future research directions are proposed, including AI-driven orchestration, blockchain-based trust models, and emerging sixth-generation (6G) technologies. This work provides a comprehensive foundation for scalable, secure, and latency-guaranteed designs of real-time IoT systems in the 5G era and beyond.

Keyword: 5G Networks; Internet of Things (IoT); Real-Time Systems; Edge Computing; Ultra-Reliable Low-Latency Communication (URLLC); Network Slicing; Sixth-Generation (6G)

1. Introduction

The Internet of Things (IoT) describes a system of physical objects, which range from industrial sensors to wearable health monitors, embedded with electronics, software, and connectivity, enabling them to collect, process, and exchange data over digital networks [1]. These devices increasingly operate not in isolation but as interconnected nodes in distributed, cyber-physical network. It is especially critical for these kinds of systems to be able to make and enact decisions rapidly, since mistakes in application fields such as industrial automation, autonomous cars or telemedicine may lead to serious problems 2].

* Corresponding author: Precious Nowamagbe

Fortunately, the performance issues seen in older mobile networks are being met by 5G wireless networks. The document introduces the basic service types: enhanced mobile broadband (eMBB), massive machine-type communications (mMTC) and ultra-reliable low-latency communications (URLLC) [3]. The capabilities are meant to interact and help each other to drive the flexibility and growth of digital infrastructures. With ultra-fast latency for processing millions of devices and more support for different sizes of devices than ever before, 5G is the base needed to include real-time IoT in sensitive environments [4].

The convergence of 5G and IoT is thus central to a new wave of intelligent, adaptive, and decentralized systems. By leveraging mobile edge computing, software-defined network slicing, and optimized protocol stacks, 5G enables the dynamic, context-aware behavior expected from real-time IoT applications [5].

1.1. Motivation

With 5G, new network architecture has been developed to help real-time data-dependent applications grow and work with optimal speed [6]. Yet, using these features for IoT devices that require quick responses has uncovered problems in their design and operation that have not been addressed enough [7]. To achieve smart mobility, smart manufacturing and remote medical support using software, networks must behave deterministically, offer very low latency and remain reliable, things today's infrastructure does not always provide [8].

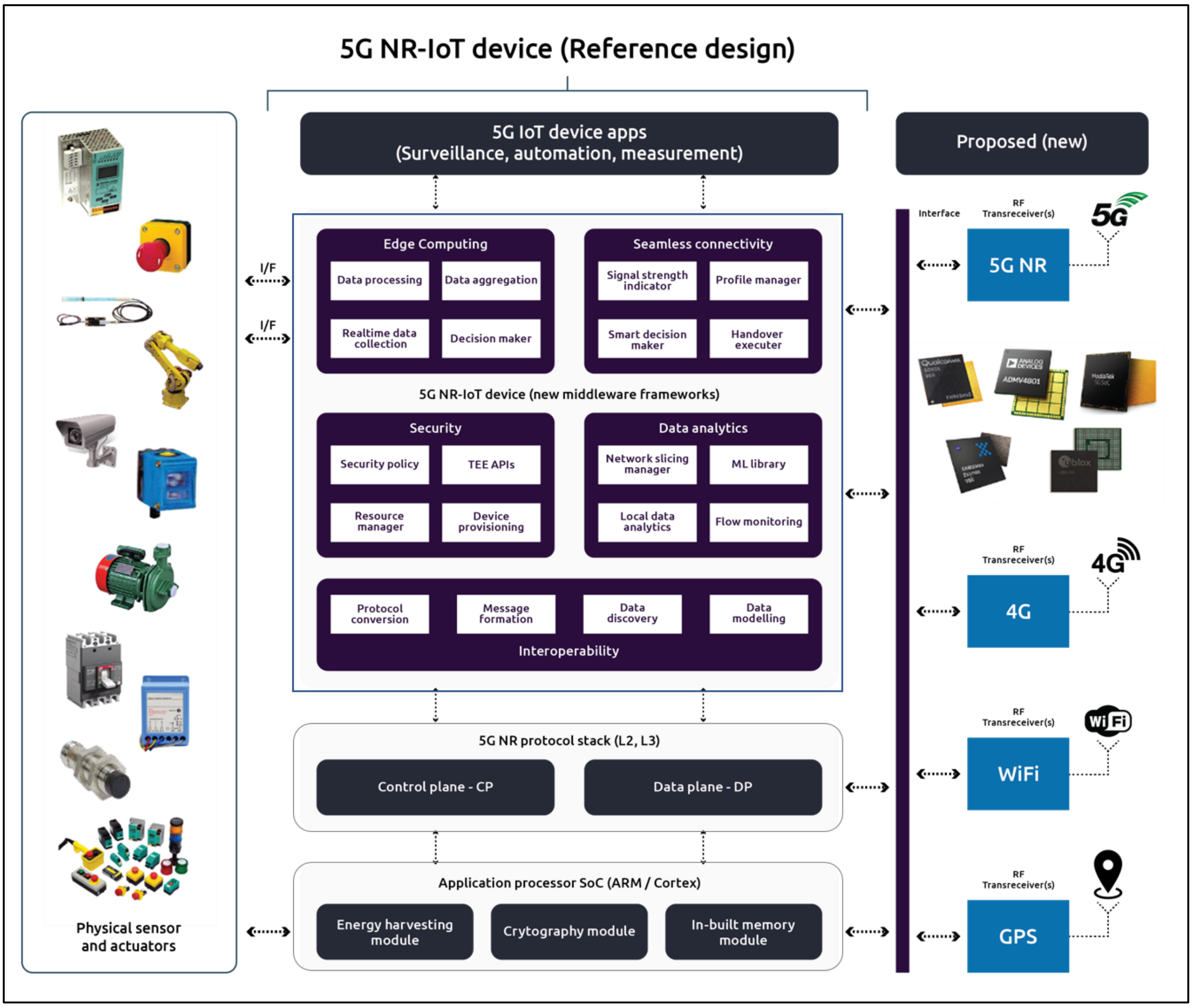
The design of network slicing, MEC and URLLC aims to offer strict control over latency, bandwidth and how networks isolate different types of services [9]. Yet, putting them to use in integration and mixed-vendor settings raises serious doubts. Part of these issues are power consumption in confined gadgets, enabling through various networking pieces, handling virtual services throughout their life and detecting risks in networks arranged in different systems [7].

1.2. Objectives

This paper is motivated by the need for a comprehensive and critical review of how 5G's architectural mechanisms function not as standalone innovations, but as a cohesive system for enabling real-time IoT. This work aim to identify the technical bottlenecks, unresolved gaps, and integration challenges that must be addressed to realize scalable, secure, and latency-guaranteed IoT services over 5G networks [6].

The aim of this paper is to critically examine how the architectural components of fifth-generation (5G) networks enable, constrain, or reshape the deployment of real-time Internet of Things (IoT) applications. Rather than addressing individual technologies in isolation, this review evaluates how mechanisms such as ultra-reliable low-latency communication (URLLC), mobile edge computing (MEC), and network slicing function as an integrated framework to meet the performance, reliability, and scalability demands of time-sensitive IoT systems.

This work contributes by synthesizing recent advances from both academic research and industry practice to evaluate the extent to which current 5G architectures align with the operational requirements of real-time IoT. Particular emphasis is placed on identifying implementation bottlenecks, architectural limitations, and unresolved challenges that hinder deployment in practical, heterogeneous environments. The analysis further highlights emerging directions for technical innovation, providing a foundation for future work in designing scalable, secure, and latency-guaranteed IoT infrastructures over 5G networks.



Adapted from Capgemini, "A View on 5G NR-IoT Devices: Reference Design Architecture," 2022 [34].

Figure 1 Architecture of a 5G NR-IoT device, showing middleware frameworks, edge intelligence modules, security layers, and interoperability support

2. Architectural enhancements in 5g for iot

2.1. Network Slicing

Network slicing is a fundamental enabler within the 5G system architecture that allows a single physical network to be logically divided into multiple, independently managed virtual networks, each tailored to specific service requirements. Unlike traditional networks that apply uniform treatment to diverse traffic types, network slicing provides differentiated resource allocation and quality-of-service guarantees per slice. This is especially significant for real-time IoT systems, where traffic sensitivity to latency, jitter, and reliability can vary drastically across applications [3], [9].

In mission-critical scenarios, a slice configured for ultra-low-latency and high-reliability communication can be reserved exclusively for connected vehicles exchanging collision-avoidance data at road intersections. Within the same physical infrastructure, another slice can concurrently support municipal surveillance systems or public environmental sensors, which do not require sub-millisecond responsiveness. This level of service differentiation ensures that high-priority applications remain unaffected by background or delay-tolerant traffic [10].

Network slicing operates at both the core and radio access layers, leveraging software-defined networking and network function virtualization for dynamic instantiation, scaling, and lifecycle management [3], [11]. The ability to orchestrate and reconfigure slices in response to service demand is particularly advantageous in large-scale IoT deployments, where devices may differ in their connectivity profiles and performance constraints. However, the real-world realization of network slicing introduces several challenges, including cross-slice isolation, end-to-end service assurance, and the complexity of coordinating virtual functions across multi-domain environments [12].

2.2. Ultra-Reliable Low-Latency Communication (URLLC)

Ultra-reliable low-latency communication (URLLC) is a cornerstone of the 5G architecture, engineered to support applications where communication failures or delays are intolerable. It targets use cases that require end-to-end latencies in the sub-millisecond range and reliability levels exceeding 99.999%, ensuring that mission-critical operations can proceed without disruption. These guarantees are particularly important in systems where mechanical or safety-critical actions depend on near-instantaneous data exchange, such as industrial robotic coordination, autonomous navigation, or remote surgical procedures [13].

To achieve this performance level, URLLC uses several design improvements at the physical and protocol layers. For this purpose, they employ compact transmission, allow uplink without a grant, use prioritization and have powerful error correction. Having multiple routes for sending data and multiple antennas is often done to overcome fading and interference when connecting devices in difficult radio environments. The purpose of these features is to maintain limited delay and certain behavior when the user is on the go or if the network becomes busy [14].

Although URLLC greatly enlarges possibilities for instant applications over wireless networks, using it means dealing with certain disadvantages. Restricting how the schedule is built and requiring the system to always be on time reduces the amount of data that each user can send and cuts the number of users who can use the system at the same time. Besides, linking URLLC into shared wireless spectrum and common IoT networks requires base station roles to be carefully coordinated with schedulers and localized computers.

2.3. Mobile Edge Computing (MEC)

Mobile edge computing (MEC) is a major component in the 5G network architecture, designed to mitigate the latency and bandwidth limitations of centralized cloud systems. In scenarios demanding immediate responsiveness, such as predictive maintenance in industrial automation or real-time navigation in autonomous vehicles, MEC enables localized data processing, thereby reducing the reliance on distant cloud servers and minimizing communication delays. This proximity not only enhances the system's responsiveness but also alleviates the burden on core network infrastructure by decreasing backhaul traffic [16].

MEC also leverage local environmental data to support context-aware services which enables applications to adapt dynamically to changing conditions. For instance, in smart city implementations, MEC can process data from various sensors to optimize traffic flow and manage energy distribution efficiently [17].

However, MEC incorporation into expansive IoT ecosystems has introduced challenges, which include the orchestration of distributed services, ensuring data consistency across edge nodes, and maintaining robust security protocols to protect sensitive information processed at the edge.

2.4. Massive MIMO and Beamforming

Massive multiple-input multiple-output (MIMO) and beamforming are integral to the 5G architecture, significantly enhancing wireless communication's capacity, reliability, and spectral efficiency. Massive MIMO utilizes large antenna arrays at base stations to serve multiple devices simultaneously through spatial multiplexing, which increases overall throughput while maintaining stable connectivity [5]. Beamforming complements this by directing concentrated signal energy toward targeted users or devices, rather than broadcasting uniformly, thus improving signal quality and reducing interference in multi-user environments [13].

In dense urban or industrial environments, where line-of-sight obstruction, signal fading, and device density pose substantial challenges, these technologies offer critical support. For instance, in a smart manufacturing facility, massive MIMO can handle the simultaneous uplink and downlink demands of numerous robotic sensors, while beamforming ensures deterministic delivery of control signals to actuators operating on sub-second decision cycles [13].

Despite their benefits, these technologies introduce implementation complexities. Massive MIMO systems rely heavily on accurate and timely channel state information, which becomes difficult to maintain under high mobility or with limited feedback capacity. Beamforming algorithms require real-time processing and adaptive calibration to cope with rapidly changing propagation conditions. These technical demands, along with deployment constraints such as antenna size and site limitations, must be checked to fully integrate these technologies into large-scale real-time IoT infrastructures [18].

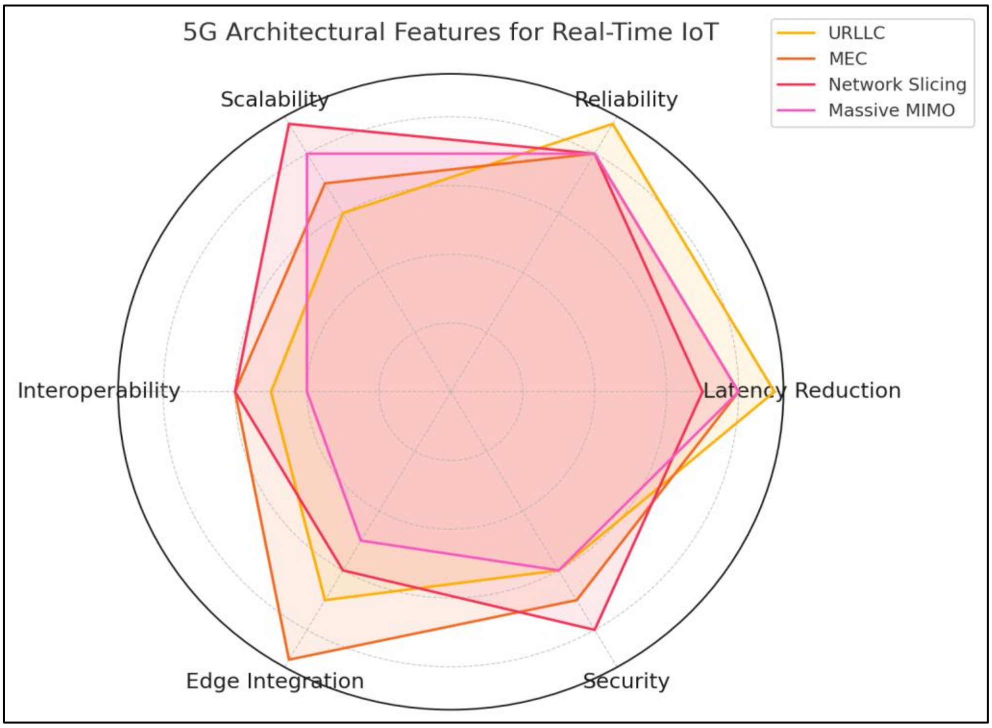


Figure 2 5G Architectural Features for Real-Time IoT

3. Real-time iot applications enabled by 5g

3.1. Autonomous Vehicles

Autonomous vehicles require high speed, very little latency and lots of bandwidth to remain safe in the real-time IoT. To operate effectively, vehicles, roads and surrounding elements must continuously share data with each other through what is known as V2X communication. Examples include V2V, V2I and V2N technologies, each one made to support traffic coordination, vehicle movement in intersections and safety alerts [19].

Low latency, strong data rates and stable connections in 5G networks are exactly what V2X needs. Because of these elements, cars can handle urgent tasks such as moving through merging lanes, joining other vehicles on roads, collecting sensor information together and taking prompt safety decisions if needed. To make sure safety is maintained, vehicles must send and receive control and telemetry data in less than a millisecond [20].

To support this, 5G employs ultra-reliable low-latency communication (URLLC), dynamic beamforming, and mobile edge computing to maintain deterministic links even in high-mobility environments. These techniques enable vehicles to process information at the edge of the network, reducing reliance on centralized cloud infrastructure and minimizing latency [20]. Despite these improvements, deployment in heterogeneous traffic environments remains challenged by factors such as signal degradation during handovers, variable link quality, and the need for precise synchronization between mobile nodes and roadside infrastructure [21].

3.2. Remote Healthcare and Telesurgery

The integration of 5G technology into healthcare infrastructure has opened new frontiers in the delivery of medical services, particularly in scenarios where time-sensitive diagnostics and interventions must occur across geographical distances. Among the most transformative applications is the use of wearable IoT devices for continuous monitoring of patient vitals. These devices collect and transmit data such as heart rate, blood oxygen levels, and electrocardiographic signals in real time, enabling early detection of anomalies and facilitating immediate clinical response [19].

Telesurgery represents a more advanced use case, in which surgical procedures are performed remotely using robotic systems controlled by specialists at distant locations. The feasibility and safety of such operations depend on the network's ability to deliver high-throughput, low-latency, and error-resilient communication. Control commands, video feeds, and haptic feedback must be exchanged between the surgeon and surgical robot with absolute precision and minimal delay to prevent procedural errors or mechanical misalignment [22].

To meet these demands, 5G offers architectural advantages such as ultra-reliable low-latency communication (URLLC), edge computing for localized decision-making, and quality-of-service guarantees through network slicing. These features allow remote medical systems to function with near-real-time responsiveness, even under varying network conditions. However, challenges persist, particularly in ensuring uninterrupted connectivity during network congestion, maintaining data privacy in distributed systems, and integrating edge intelligence with hospital infrastructure. Addressing these issues is essential to enabling the safe and scalable adoption of remote healthcare and telesurgery across both urban and underserved regions [22].

3.3. Industrial IoT (IIoT)

Industrial IoT environments rely on continuous, low-latency communication between machines, sensors, and control systems to execute time-sensitive tasks such as robotic motion coordination, process automation, and precision quality inspection. In these highly dynamic manufacturing settings, 5G provides the wireless infrastructure necessary to meet stringent demands for deterministic performance and ultra-reliable communication [23]. Unlike traditional wired architectures, 5G supports flexible deployment and reconfiguration of industrial assets without compromising responsiveness, an essential requirement for adaptive production lines and just-in-time operations.

One of the most impactful applications of 5G in IIoT is predictive maintenance. By leveraging real-time telemetry from interconnected machines, analytics systems can identify deviations from expected behavior and forecast mechanical failures before they occur [24]. This predictive capability minimizes unscheduled downtime, optimizes maintenance schedules, and reduces operational costs. Additionally, 5G's high connection density enables plant-wide instrumentation, allowing for granular performance monitoring across thousands of endpoints in large-scale facilities.

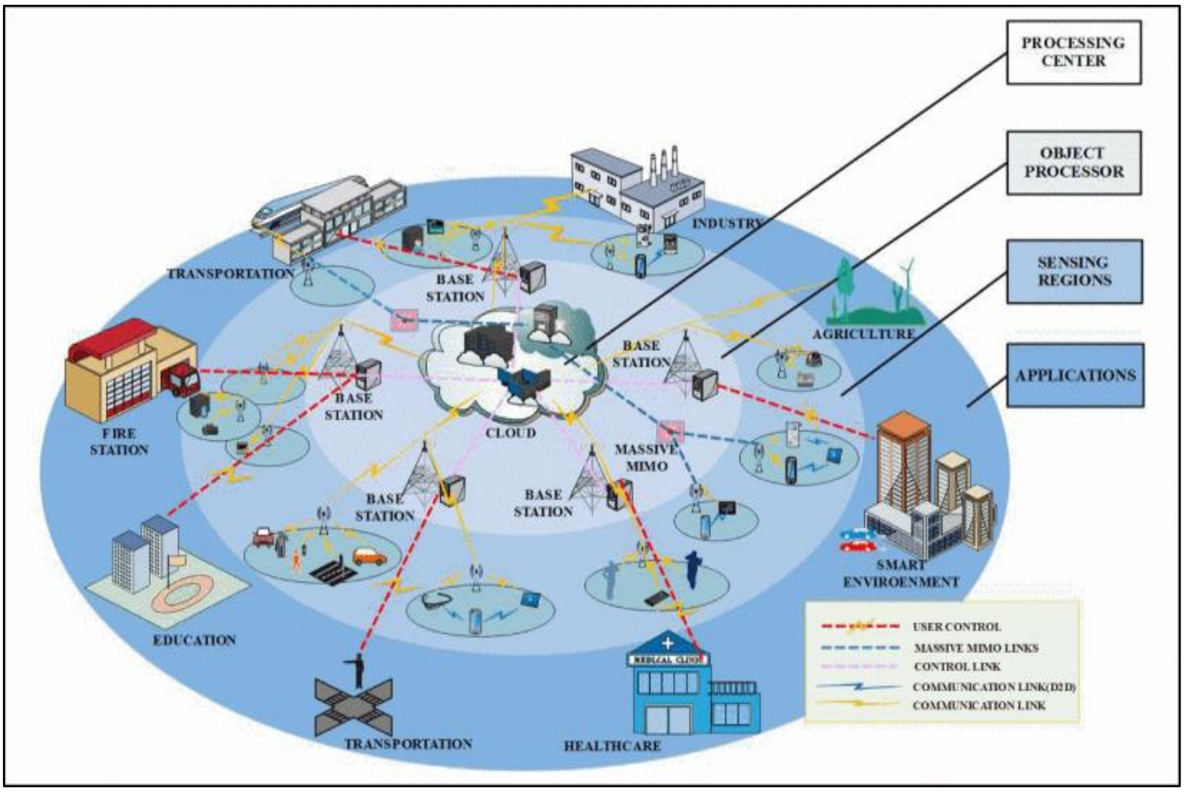


Figure 3 Illustrates how 5G interconnects diverse application verticals under a unified smart infrastructure paradigm [35]

However, deploying these systems at scale demands more than raw connectivity. Seamless integration with mobile edge computing is required to localize analytics and reduce cloud dependency, while network orchestration mechanisms must prioritize mission-critical traffic to maintain deterministic behavior under varying load conditions. Meeting these challenges is fundamental to realizing the full promise of Industry 4.0, where intelligent, self-regulating industrial systems operate with minimal human intervention [25].

3.4. Smart Cities and Energy Grids

The implementation of 5G-enabled IoT infrastructure is central to the advancement of smart cities, where interconnected systems must operate with precision, adaptability, and low-latency responsiveness. Core urban functions, such as intelligent traffic signal control, environmental condition monitoring, and dynamic emergency service routing, depend on seamless communication among distributed sensors, edge nodes, and centralized control platforms. In these time-sensitive environments, the deterministic communication capabilities of 5G ensure that critical signals are not delayed or lost during peak network usage [26].

The energy sector presents a parallel application of real-time IoT intelligence, particularly in the context of decentralized power generation and demand-side management. As smart grids incorporate diverse renewable sources, real-time load balancing, fault localization, and self-healing mechanisms become essential. 5G enables these capabilities by supporting high connection densities and ultra-low-latency data exchange between substations, grid-edge controllers, and consumption endpoints [27]. Edge computing further enhances this framework by enabling local decision-making, allowing systems to detect anomalies, reroute energy flows, or initiate recovery protocols autonomously without awaiting cloud-based instructions [28].

Together, 5G and edge-enabled IoT technologies provide the communication foundation for scalable, adaptive, and resilient infrastructure systems. Their role in smart cities and energy grids is not only to enhance operational efficiency but also to support long-term sustainability goals by reducing response time, minimizing resource waste, and improving service continuity in the face of environmental or systemic disruptions [28].

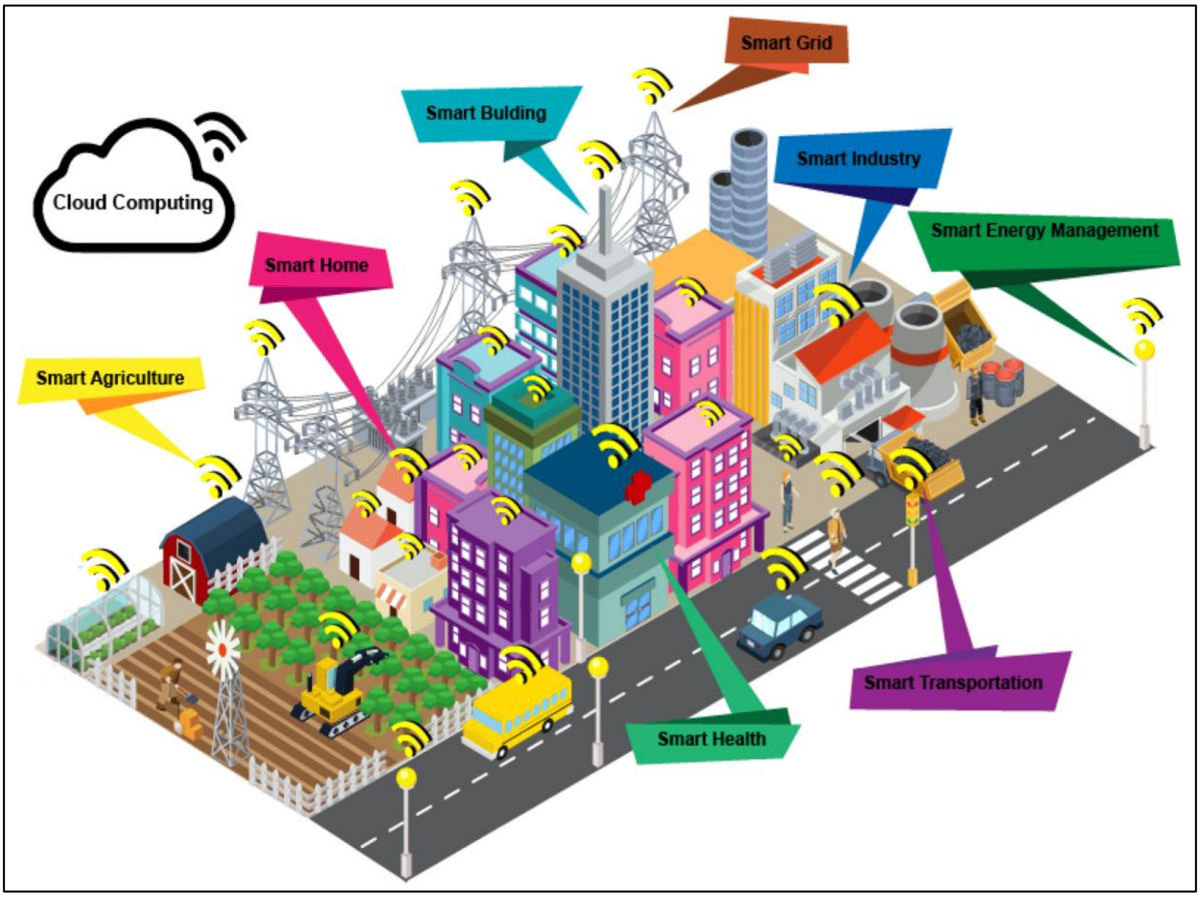


Figure 4 5G-enabled smart city architecture showing the integration of cloud computing, smart buildings, transportation, healthcare, agriculture, and energy systems [35]

4. Challenges and Limitations

4.1. Interoperability

One of the primary technical barriers to widespread 5G-enabled IoT adoption lies in ensuring interoperability across heterogeneous systems. Many current deployments must coexist with legacy infrastructures, including 4G LTE, Wi-Fi, and non-cellular IoT standards such as Zigbee or LoRaWAN. Backward compatibility introduces limitations in latency, throughput, and deterministic behaviour, especially problematic for time-sensitive IoT applications [28].

Hybrid network environments, where legacy and 5G-enabled devices operate concurrently, often require protocol translation, middleware orchestration, or hardware gateways. These intermediary layers can introduce additional delays, reduce reliability, and increase maintenance complexity [27]. Moreover, interoperability challenges extend beyond physical infrastructure to include data formats, security frameworks, and cloud-edge coordination mechanisms, making seamless integration across vendors and domains an ongoing concern [27].

Middleware solutions are employed to standardize data formats across different protocols. IoT gateways implement protocol translation layers, converting data into a unified format before transmitting it to the cloud [28]. Also, integrating legacy systems with IoT often involves middleware or gateways to facilitate communication between disparate systems [27].

Furthermore, ensuring seamless connectivity, data exchange, and service discovery across heterogeneous IoT devices and network components is critical. Interoperability challenges between IoT devices and 5G/6G network components can arise due to factors such as varying device capabilities, diverse communication protocols, and proprietary implementations [26].

Achieving interoperability in 5G-enabled IoT systems requires addressing both technical and organizational challenges. Employing standardized protocols, middleware solutions, and strategic integration techniques are essential step toward seamless integration across diverse systems and devices [28].

4.2. Energy Efficiency

While 5G technology is engineered to be more energy-efficient per bit transmitted, the exponential increase in connected devices within dense IoT deployments intensifies power constraints, particularly for edge devices operating on limited battery resources. Real-time IoT applications, such as continuous monitoring and high-frequency data transmission, impose significant demands on device energy budgets [29].

To address these challenges, several energy-saving mechanisms are being explored. Techniques like wake-up radios, power-aware protocol stacks, and optimized sleep cycles aim to reduce unnecessary energy consumption. For instance, passive wake-up radios can keep devices in a low-power sleep mode, activating them only upon receiving specific external signals, thereby mitigating idle listening and conserving energy [29].

However, implementing these energy-saving strategies often involves trade-offs. The necessity to maintain low latency and high reliability can conflict with aggressive energy conservation measures. Balancing persistent connectivity with energy efficiency remains a core optimization problem in large-scale 5G IoT systems. Moreover, integrating edge computing with 5G networks offers a pathway to enhance energy efficiency by processing data closer to the source, reducing the need for long-distance data transmission and thereby conserving energy [30].

4.3. Security and Privacy

The expansion of real-time IoT systems over 5G introduces a substantially larger and more complex attack surface. Unlike traditional networks, 5G architectures decentralize processing through mobile edge computing and virtualized functions, creating distributed trust boundaries that are harder to secure. This shift enables ultra-low latency and localized intelligence but also exposes new vulnerabilities in software-defined infrastructure, where threats can propagate rapidly across slices or orchestrated services if not properly contained [10], [31].

Mobile edge computing (MEC), for instance, brings compute resources closer to IoT endpoints, reducing latency but also bypassing centralized security controls traditionally applied at core data centers. Virtualized network functions (VNFs) and network slicing, essential for isolating critical services, may share physical infrastructure. Without strong isolation policies and tenant-aware security enforcement, a compromise in one slice could cascade into others, jeopardizing confidentiality and service integrity [10].

Traditional security mechanisms such as end-to-end encryption, firewalls, or access control lists remain essential but are not sufficient in real-time systems where computational overhead must be minimized. For example, implementing full encryption on lightweight IoT devices may introduce unacceptable processing delays or drain battery resources rapidly. This creates a trade-off between protection strength and real-time performance, a constraint that must be addressed through lightweight, hardware-assisted cryptographic methods or context-aware security policies [32].

Privacy concerns also intensify under this model. In smart cities and remote healthcare environments, real-time streams of highly sensitive data, location, health metrics, and biometric identifiers are transmitted continuously over public and private 5G channels. Ensuring that such data is anonymized, encrypted, and processed in compliance with local data protection regulations becomes a critical challenge, particularly when edge nodes process personal data autonomously [31], [13].

Furthermore, the security posture of 5G-enabled IoT systems depends not just on device-level protection but on the secure coordination of cloud-edge-device interactions, lifecycle management of credentials, and the trustworthiness of software updates delivered over-the-air. As attacks grow more sophisticated, adversaries are increasingly targeting firmware, orchestration layers, or exploiting supply chain vulnerabilities within the IoT ecosystem [31], [32].

To maintain trust, system designers must adopt a layered defense approach, combining identity management, continuous monitoring, behavioral anomaly detection, and secure boot processes. Given the real-time constraints, these measures must be engineered for speed, scalability, and minimal disruption to deterministic communication patterns [32].

4.4. Spectrum and Resource Management

Efficient spectrum utilization remains one of the most pressing challenges in sustaining the performance and scalability of 5G-enabled real-time IoT systems. Unlike consumer applications that can tolerate variable latency or bandwidth fluctuations, mission-critical IoT workloads, such as autonomous mobility or industrial automation, require guaranteed low-latency, high-reliability connections with minimal jitter and loss. In dense urban or industrial settings, where thousands of devices compete for limited radio resources, achieving these guarantees is technically complex and operationally fragile [6], [33].

Dynamic spectrum allocation has emerged as a potential mitigation strategy, allowing operators to reassign frequency bands in response to real-time network conditions. However, this approach relies on highly responsive and predictive traffic models to avoid performance degradation. Moreover, spectrum fragmentation across licensed, unlicensed, and shared bands introduces regulatory and interoperability challenges, particularly in cross-border or multi-operator deployments. These complications are further magnified by the introduction of private 5G networks, which may have limited access to spectrum and compete with public deployments for interference-free operation [6], [34].

The limitations in licensed spectrum availability also hinder the scalability of ultra-reliable low-latency communication (URLLC). While 5G is architected to support dedicated slices for latency-sensitive services, the underlying radio resource management mechanisms must still arbitrate access under physical constraints, particularly during network congestion or mobility handovers. In scenarios where multiple URLLC and enhanced mobile broadband (eMBB) flows coexist, interference coordination, scheduling granularity, and beamforming optimization become critical [4], [33].

Beyond spectrum, resource management must account for compute allocation at the edge, queuing delays in multi-access gateways, and backhaul constraints in cloud coordination. Even with network slicing, maintaining isolation and quality-of-service across virtualized networks requires end-to-end orchestration that spans the radio, transport, and application layers. The failure to align these layers results in performance bottlenecks that defeat the promise of real-time responsiveness [11], [34].

Addressing these limitations demands the adoption of intelligent orchestration frameworks that integrate machine learning for traffic prediction, cross-layer coordination for latency enforcement, and spectrum-sharing protocols that can dynamically mediate between competing service classes. Without such advances, the benefits of 5G for real-time IoT applications may remain constrained to narrowly controlled environments rather than scalable, city-wide or enterprise-wide deployments [34].

5. Future research directions

5.1. AI-Enhanced Network Management

As 5G networks evolve to support increasingly heterogeneous and dynamic IoT workloads, static rule-based management approaches become insufficient. Machine learning (ML) offers a pathway to adaptively optimize resource allocation, congestion control, and anomaly detection in real time [6]. Intelligent agents embedded within the control plane can learn traffic patterns, user mobility behaviors, and device profiles to predict demand spikes or failure points before they occur. This predictive capability enables proactive orchestration, reducing service interruptions and enhancing QoS assurance under volatile network conditions.

Additionally, reinforcement learning frameworks can be trained to manage radio access parameters, balance edge-compute workloads, and fine-tune slicing policies based on continuous feedback [34].

5.2. Blockchain Integration

As real-time IoT systems scale across decentralized infrastructures, ensuring data authenticity, synchronization, and coordination among untrusted entities becomes increasingly critical. Blockchain technologies offer a tamper-resistant mechanism to validate and log transactions across distributed nodes, making them particularly relevant for time-sensitive IoT applications where data integrity and non-repudiation are essential [6].

Smart contracts can automate access control policies and enforce security agreements in multi-stakeholder environments such as smart grids or logistics chains. When combined with edge computing, lightweight consensus protocols, such as Practical Byzantine Fault Tolerance (PBFT) or DAG-based architectures, may enable near-real-time validation without incurring the latency typically associated with traditional blockchain frameworks [27].

However, open challenges remain regarding scalability, energy efficiency, and regulatory alignment, especially in environments with constrained devices and strict timing guarantees. Future research must address how to adapt blockchain architectures to meet the latency and energy constraints of mission-critical IoT workloads without compromising trust or auditability [6], [27].

5.3. Towards 6G and Beyond

While 5G provides the foundation for real-time IoT systems, its architectural limits become evident in scenarios demanding ultra-reliable communication, extreme mobility, and large-scale network densification [6]. As a result, sixth-generation (6G) research is advancing toward novel physical-layer technologies that promise to overcome these limitations.

Emerging innovations include reconfigurable intelligent surfaces (RIS), terahertz (THz) communication bands, and integrated sensing-and-communication architectures [28]. Terahertz frequencies unlock ultra-wide bandwidths suitable for data-intensive IoT tasks but require breakthroughs in antenna miniaturization and line-of-sight propagation. RIS, on the other hand, enables programmable radio environments where signal reflections can be adaptively controlled, enhancing coverage, energy efficiency, and link reliability in dynamic environments [28].

These advancements aim to push end-to-end latency toward sub-millisecond targets while embedding ambient intelligence directly into the radio infrastructure. Yet, realizing 6G's promise will demand a holistic rethinking of protocol design, hardware interfaces, and orchestration logic across compute, transport, and application layers. Future work must address how to co-design these physical-layer innovations with intelligent control systems that maintain deterministic performance in real-time, mission-critical IoT environments [6].

5.4. Federated and Collaborative IoT Models

In conventional cloud-centric architectures, real-time IoT applications suffer from prohibitive latency, bandwidth saturation, and growing compliance burdens related to data residency and privacy. Federated learning presents a compelling alternative by enabling model training directly on distributed IoT endpoints. In this paradigm, data remains local while only model updates are exchanged, improving both privacy preservation and system responsiveness [25].

Beyond federated learning, collaborative IoT systems emphasize decentralized inference, where edge devices share local insights, such as sensor readings or environment maps, to arrive at joint decisions without centralized oversight.

This approach reduces uplink usage and minimizes inference delay in time-sensitive contexts like smart transportation or emergency response [21].

However, multiple open challenges remain. Model synchronization must be robust to constrained and asymmetric bandwidth, and systems must remain resilient to adversarial interference and device dropout. Heterogeneity in hardware capabilities and intermittent connectivity further complicate accuracy retention across training rounds.

6. Conclusion

The integration of real-time Internet of Things (IoT) systems with fifth-generation (5G) wireless networks marks a pivotal shift in how time-sensitive, data-driven applications are designed and deployed across critical sectors. From autonomous vehicles to remote healthcare and industrial automation, 5G's unique combination of ultra-reliable low-latency communication, massive machine-type connectivity, and mobile edge computing provides the architectural backbone required to meet the stringent demands of modern IoT ecosystems.

This paper has examined the core architectural enablers of 5G, such as network slicing, URLLC, MEC, and beamforming, that facilitate deterministic communication in latency-critical environments. It has also reviewed a range of high-impact use cases where these technologies are being applied, alongside an analysis of the structural limitations that currently hinder full-scale, dependable adoption. Key challenges include interoperability with legacy systems, energy efficiency at the device level, spectrum management, and the expanding security surface of distributed architectures.

Looking ahead, future research must address these limitations through cross-domain innovations. This includes the integration of AI for adaptive network management, blockchain for decentralized trust, and the exploration of 6G technologies that redefine physical-layer capabilities. Equally important are federated and collaborative models that preserve privacy and performance without relying on centralized infrastructure. Only through such holistic, interdisciplinary advancements can the full potential of real-time IoT over next-generation wireless systems be realized at scale.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed..

References

[1] H. Z., A. H. and M. M., "Internet of Things (IoT): Definitions, Challenges and Recent Research Directions," Int. J. Comput. Appl., vol. 128, no. 1, pp. 37–47, 2015, doi: 10.5120/ijca2015906430.

[2] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues," IEEE Commun. Surv. Tutor., vol. 22, no. 2, pp. 1–1, 2020, doi: 10.1109/comst.2019.2962586.

[3] A. A. Barakabitze, A. Ahmad, A. Hines, and R. Mijumbi, "5G Network Slicing Using SDN and NFV: A Survey of Taxonomy, Architectures and Future Challenges," Comput. Netw., vol. 167, p. 106984, 2019, doi: 10.1016/j.comnet.2019.106984.

[4] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View," IEEE Access, vol. 6, pp. 55765–55779, 2018, doi: 10.1109/access.2018.2872781.

[5] Q.-V. Pham et al., "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art," IEEE Access, vol. 8, pp. 116974–117017, 2020, doi: 10.1109/access.2020.3001277.

[6] A. K. M. B. Haque, M. O. M. Zihad, and M. R. Hasan, "5G and Internet of Things—Integration Trends, Opportunities, and Future Research Avenues," in 5G and Beyond, Singapore: Springer, 2023, pp. 1–20, doi: 10.1007/978-981-99-3668-7_11.

[7] IEEE 5G/6G Innovation Testbed, "Internet of Things (IoT) Integration: Identifying Blockages and Optimizing Resource Allocation in 5G/6G Networks," IEEE, 2024. [Online]. Available: https://testbed.ieee.org

[8] A. Y. Ding and M. Janssen, "Opportunities for Applications Using 5G Networks," Proc. 7th Int. Conf. Telecommun. Remote Sens., 2018, doi: 10.1145/3278161.3278166.

[9] J. Ordonez-Lucena et al., "Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges," IEEE Commun. Mag., vol. 55, no. 5, pp. 80–87, 2017, doi: 10.1109/mcom.2017.1600935.

[10] S. Gao et al., "Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey," Electronics, vol. 13, no. 10, p. 1860, 2024, doi: 10.3390/electronics13101860.

[11] A. N. Toosi et al., "Management and Orchestration of Network Slices in 5G, Fog, Edge, and Clouds," in Fog and Edge Computing: Principles and Paradigms, Wiley, 2019, pp. 79–96, doi: 10.1002/9781119525080.ch4.

[12] A. Jalalian, S. Yousefi, and T. Kunz, "Network Slicing in Virtualized 5G Core with VNF Sharing," J. Netw. Comput. Appl., p. 103631, 2023, doi: 10.1016/j.jnca.2023.103631.

[13] Ericsson, "5G URLLC - Achieving Industrial Automation," 2020. [Online]. Available: https://www.ericsson.com/en/cases/2020/accelerate-factory-automation-with-5g-urllc

[14] A. Maghsoudnia et al., "Ultra-Reliable Low-Latency in 5G: A Close Reality or a Distant Goal?," Proc. ACM HotNets'23, pp. 111–120, 2024, doi: 10.1145/3696348.3696862.

[15] M. A. Siddiqi, H. Yu, and J. Joung, "5G Ultra-Reliable Low-Latency Communication Implementation Challenges and Operational Issues with IoT Devices," Electronics, vol. 8, no. 9, p. 981, 2019, doi: 10.3390/electronics8090981.

[16] R. Zhu, L. Liu, H. Song, and M. Ma, "Multi-access Edge Computing Enabled Internet of Things: Advances and Novel Applications," Neural Comput. Appl., 2020, doi: 10.1007/s00521-020-05267-x.

[17] F. Giust et al., "Multi-Access Edge Computing: The Driver Behind the Wheel of 5G-Connected Cars," IEEE Commun. Stand. Mag., vol. 2, no. 3, pp. 66–73, 2018, doi: 10.1109/mcomstd.2018.1800013.

[18] C. Masterson, "Massive MIMO and Beamforming: The Signal Processing Behind the 5G Buzzwords," Analog Dialogue, vol. 51, 2017. [Online]. Available: https://www.analog.com/en/analog-dialogue/articles/massive-mimo-and-beamforming-the-signal-processing-behind-the-5g-buzzwords.html

[19] D. H. Devi et al., "5G Technology in Healthcare and Wearable Devices: A Review," Sensors, vol. 23, no. 5, p. 2519, 2023, doi: 10.3390/s23052519.

[20] B. Di, L. Song, Y. Li, and G. Y. Li, "Non-Orthogonal Multiple Access for High-Reliable and Low-Latency V2X Communications in 5G Systems," IEEE J. Sel. Areas Commun., vol. 35, no. 10, pp. 2383–2397, 2017, doi: 10.1109/jsac.2017.2726018.

[21] K. Zhang, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Mobile Edge Computing and Networking for Green and Low-Latency Internet of Things," IEEE Commun. Mag., vol. 56, no. 5, pp. 39–45, 2018, doi: 10.1109/mcom.2018.1700882.

[22] M. Dohler and V. Patel, "Cutting the Cord: Lifesaving Telesurgery in the Age of 5G," Ericsson Blog, Mar. 2024. [Online]. Available: https://www.ericsson.com/en/blog/2024/3/cutting-the-cord-lifesaving-telesurgery-in-the-age-of-5g

[23] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Smart Manufacturing and Tactile Internet Based on 5G in Industry 4.0: Challenges, Applications and New Trends," Electronics, vol. 10, no. 24, p. 3175, 2021, doi: 10.3390/electronics10243175.

[24] P. Jayaraman, A. Yavari, D. Georgakopoulos, A. Morshed, and A. Zaslavsky, "Internet of Things Platform for Smart Farming: Experiences and Lessons Learnt," Sensors, vol. 16, no. 11, p. 1884, 2016, doi: 10.3390/s16111884.

[25] F. Foukalas and A. Tziouvaras, "Edge AI for Industrial IoT Applications," IEEE Ind. Electron. Mag., 2021, doi: 10.1109/mie.2020.3026837.

[26] A. Saxena and V. Singh, "5G-Enabled Smart Cities," Turk. J. Comput. Math. Educ., vol. 11, no. 2, pp. 755–761, 2020, doi: 10.61841/turcomat.v11i2.14420.

[27] E. Esenogho, K. Djouani, and A. Kurien, "Integrating Artificial Intelligence, Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends, Challenges and Prospect," IEEE Access, pp. 1–1, 2022, doi: 10.1109/access.2022.3140595.

[28] M. R. Palattella et al., "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 510–527, 2016, doi: 10.1109/jsac.2016.2525418.

[29] H. Bello, Z. Xiaoping, R. Nordin, and J. Xin, "Advances and Opportunities in Passive Wake-Up Radios with Wireless Energy Harvesting for the Internet of Things Applications," Sensors, vol. 19, no. 14, p. 3078, 2019, doi: 10.3390/s19143078.

[30] Z. Cochran, "5G Energy Efficiency: A Sustainable Connectivity Solution," AT&T Business Insights Blog, 2024. [Online]. Available: https://www.business.att.com/learn/articles/5g-energy-efficiency-a-sustainable-connectivity-solution.html

[31] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things," arXiv preprint, arXiv:2008.03252, 2020. [Online]. Available: https://arxiv.org/abs/2008.03252

[32] J. Cook, S. ur Rehman, and K. M. Arif, "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions," arXiv preprint, arXiv:2304.00713, 2023. [Online]. Available: https://arxiv.org/abs/2304.00713

[33] A. K. Bairagi et al., "Coexistence Mechanism between eMBB and uRLLC in 5G Wireless Networks," IEEE Trans. Commun., vol. 69, no. 3, pp. 1736–1749, 2021, doi: 10.1109/tcomm.2020.3040307.

[34] V. Anand, "A View on 5G NR-IoT Devices: Reference Design Architecture," Capgemini Engineering, Aug. 1, 2022. [Online]. Available: https://www.capgemini.com/insights/expert-perspectives/a-view-on-5g-nr-iot-devices-reference-design-architecture

[35] IEEE Innovation at Work. "Unlocking IoT Data with 5G and AI," IEEE Innovation Spotlight, 2019. [Online]. Available: https://innovate.ieee.org/innovation-spotlight/5g-iot-ai/

[36] Guevara, L. and Auat Cheein, F. (2020). The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems. Sustainability, 12(16), p.6469. doi:https://doi.org/10.3390/su12166469.