Energy, Scalability, Data and Security in Massive IoT: Current Landscape and Future Directions

Imane Cheikh *Member, IEEE* , Sébastien Roy *Senior Member, IEEE*, Essaid Sabir *Senior Member, IEEE* , Rachid Aouami *Member, IEEE*

Abstract—The Massive Internet of Things (MIoT) envisions an interconnected ecosystem of billions of devices, fundamentally transforming diverse sectors such as healthcare, smart cities, transportation, agriculture, and energy management. However, the vast scale of MIoT introduces significant challenges, including network scalability, efficient data management, energy conservation, and robust security mechanisms. This paper presents a thorough review of existing and emerging MIoT technologies designed to address these challenges, including Low-Power Wide-Area Networks (LPWAN), 5G/6G capabilities, edge and fog computing architectures, and hybrid access methodologies. We further investigate advanced strategies such as AI-driven resource allocation, federated learning for privacy-preserving analytics, and decentralized security frameworks using blockchain. Additionally, we analyze sustainable practices, emphasizing energy harvesting and integrating green technologies to reduce environmental impact. Through extensive comparative analysis, this study identifies critical innovations and architectural adaptations required to support efficient, resilient, and scalable MIoT deployments. Key insights include the role of network slicing and intelligent resource management for scalability, adaptive protocols for real-time data handling, and lightweight AI models suited to the constraints of MIoT devices. This research ultimately contributes to a deeper understanding of how MIoT systems can evolve to meet the growing demand for seamless, reliable connectivity while prioritizing sustainability, security, and performance across diverse applications. Our findings serve as a roadmap for future advancements, underscoring the potential of MIoT to support a globally interconnected, intelligent infrastructure.

Index Terms—Massive Internet of Things (MIoT), scalability, Low-Power Wide-Area Networks (LPWAN), 5G, 6G, edge computing, fog computing, AI-driven resource allocation, federated learning, blockchain, energy harvesting, sustainability, data management, security, Industry 4.0, smart cities, healthcare IoT, transportation, energy management, network slicing, autonomous vehicles.

I. INTRODUCTION

The concept of the Internet of Things (IoT) has rapidly evolved over the last decade, with the number of connected devices expected to surpass 30 billion by 2025 [1]. The emergence of the *Massive Internet of Things* (MIoT) refers to a subset of IoT systems characterized by a vast number of devices generating large amounts of data and requiring highly scalable infrastructures. To support this density of devices

I. Cheikh, S. Roy and R. Aouami are with the Department of Electrical and Computer Engineering, University of Sherbrooke, Québec, Canada. (emails: imane.cheikh@usherbrooke.ca, sebastien.roy13@usherbrooke.ca, rachid.aouami@usherbrooke.ca).

E. Sabir is with the Department of Science and Technology, TELUQ, University of Quebec, Montreal, Canada.(email: essaid.sabir@teluq.ca).

Manuscript received August 17th, 2025; revised September, 2025.

and ensure reliable communication, Ultra-Dense IoT Networks (UDNs) have become essential. These networks enable efficient device connectivity and management in environments with extremely high device densities. MIoT deployments, often facilitated by UDNs, are predominantly found in areas such as smart cities, industrial automation, and large-scale environmental monitoring [2], [3].

Scalability in MIoT systems is critical due to the unique demands they impose on communication networks, data processing, energy efficiency, and security. Traditional IoT frameworks are not designed to handle the sheer scale of MIoT in terms of device count, data transmission, and processing requirements [4]. Addressing these scalability challenges is crucial for supporting widespread MIoT applications while maintaining performance, reliability, and security.

One of the key enablers for MIoT scalability is the development of advanced networking protocols such as Low Power Wide Area Networks (LPWANs), including NB-IoT and LoRaWAN, which allow for low-power, long-range communication over large geographical areas [5], [6]. Additionally, emerging computing paradigms such as edge and fog computing are pivotal in offloading computational tasks from centralized cloud platforms to network edges, reducing latency and improving scalability [7].

Another significant challenge in MIoT systems is managing the massive amounts of data generated by connected devices. Efficient data management techniques such as data compression, aggregation, and distributed data processing frameworks (e.g., Hadoop, Spark) are crucial for handling these large datasets [8]. Moreover, energy efficiency remains a key concern, as many MIoT devices are battery-operated and operate in environments with limited access to energy resources. Technologies such as energy harvesting and ultra-low-power communication protocols have emerged as essential solutions for ensuring the sustainability of MIoT deployments [9].

Finally, ensuring the security and privacy of MIoT systems becomes more challenging as the number of devices increases. Traditional centralized security models struggle to scale with the massive device count, prompting the exploration of decentralized solutions like blockchain to secure data transmission and device interactions in MIoT networks [10], [11].

In this paper, we present a comprehensive survey of scalable solutions for MIoT systems, focusing on four critical areas:

- **Network scalability**, where many devices must communicate without overwhelming network infrastructure.

- **Data management**, where vast amounts of data must be processed, stored, and analyzed in real-time.
- **Energy efficiency**, where devices, particularly those in remote or hard-to-reach locations, must operate with limited power resources.
- **Security and privacy**, where ensuring the integrity and safety of vast, distributed networks becomes increasingly complex as the number of devices grows.

We analyze existing approaches and highlight emerging trends that are poised to shape the future of MIoT. Figure 1 presents the main challenges of the massive IoT.
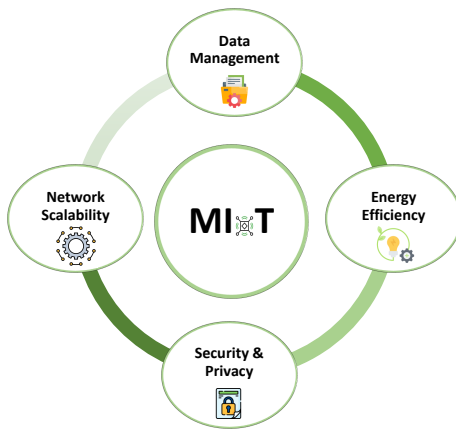

Fig. 1. Massive IoT main challenges.

Furthermore, this paper will also explore *emerging technologies* such as *Artificial Intelligence (AI)* and *Machine Learning (ML)*, which can enhance scalability by optimizing device management, predicting network congestion, and automating decision-making processes. AI-driven solutions can dynamically allocate resources, manage device health, and predict potential system failures before they occur, making large-scale IoT systems more resilient and efficient [12].

As the number of connected devices continues to grow, it is essential to look ahead at the future trends and technological innovations that will drive the next generation of scalable MIoT solutions. From 6G networks [13], which promise even greater capacity and faster speeds, to quantum computing, which could revolutionize data processing, the landscape of MIoT is poised for significant advancements. By understanding the current solutions and the challenges that remain, this paper will contribute to the ongoing conversation about how to scale IoT technologies for a connected future.

In conclusion, this paper aims to provide a detailed exploration of the *technologies, challenges, and solutions* surrounding the scalability of MIoT, highlighting both the current state of the field and the future directions that could define the next wave of innovation. By examining various networking protocols, data management strategies, and emerging technologies, it will offer insights into how MIoT systems can scale effectively while maintaining efficiency, security, and reliability.

A. Motivation

The unprecedented growth of connected devices in the MIoT domain presents significant challenges to existing network infrastructures. Forecasts suggest the number of IoT devices will surpass 75 billion by 2025, necessitating highly scalable, efficient, and secure frameworks. These challenges include network scalability, efficient data management, energy conservation, and robust security measures, forming the foundation of this study.

Network Scalability has become a critical concern as conventional networking architectures are unable to accommodate the enormous device density expected in IoT ecosystems. Current research highlights advanced strategies to address these issues. For example, Ramachandran et al. (2019) propose hybrid communication architectures that combine LPWAN with 5G technologies to enhance scalability and meet the growing demand for connectivity in dense IoT networks [14]. Furthermore, Khan et al. (2020) investigate network slicing techniques to allocate resources dynamically, ensuring optimal performance in diverse IoT applications [15].

Data Management is another pressing issue, given the vast amounts of data generated by IoT devices. Existing storage and processing solutions often fall short of the requirements for real-time analytics and decision-making. Modupe et al. (2024) emphasize the potential of edge computing frameworks in decentralizing data processing, reducing latency, and enabling rapid responses in time-sensitive IoT applications [16]. In addition, advancements in AI-driven analytics, as discussed by Zong et al. (2024), have further enhanced the ability to derive insights from large datasets without overburdening centralized servers [17].

Energy Efficiency remains a crucial aspect, particularly as many IoT devices operate with limited power supplies. Research by Tupe et al. (2022) focuses on energy-aware communication protocols that optimize power consumption without compromising data integrity, thereby prolonging device lifespans [18]. Similarly, studies on energy harvesting technologies show promise in making MIoT networks more sustainable by utilizing ambient energy sources [19].

Lastly, **Security and Privacy** challenges have become increasingly pronounced with the rise in connected devices. The growing attack surface demands multi-layered security frameworks. Cui et al. (2019) propose novel blockchain-based architectures to secure IoT environments while ensuring transparency and data immutability [20]. Meanwhile, AI-enabled intrusion detection systems are gaining traction for their ability to detect and mitigate sophisticated threats in real time [21].

In conclusion, this research aims to address these challenges by proposing innovative solutions that integrate scalability, efficient data handling, energy optimization, and robust security into a unified MIoT framework. By leveraging cutting-edge technologies and recent advancements, this study seeks to contribute to the development of sustainable and reliable IoT systems.

B. Scientific Contributions and Novelty

This paper presents a novel and integrative survey framework that addresses the scalability, energy efficiency, data

Sec. II: SCALABLE MIOT USE CASES
- Smart Cities
- Healthcare
- Agriculture
- Transportation
- Energy Management
- Industry 4.0 and Manufacturing
- Critical IoT Applications
- Metaverse & MIoT

Sec. IV: COMMUNICATION AND ACCESS TECHNIQUES FOR SCALABLE MIOT

Advanced MIoT Technologies
- Grant-Free Access
- Non-Orthogonal Multiple Access
- Cooperative Communication and Relaying
- Compressive Sensing
- Cloud Radio Access Network
- Sparse Code Multiple Access
- Multi-RATs & Hybrid Access Techniques

Sec. VI: EMERGING TRENDS AND FUTURE SOLUTIONS IN MIOT
- Artificial Intelligence and Machine Learning
- Edge and Fog Computing
- Network Slicing and 5G/6G Technologies
- Decentralized Protocols and Blockchain
- Sustainable Practices and Energy Harvesting
- Convergence of Metaverse and Massive IoT

Sec. I: INTRODUCTION

Sec. VIII: CONCLUSION

Sec. III: SCALABILITY CHALLENGES IN MIOT
- Network Scalability
- Data Management
- Energy Efficiency
- Security & Privacy

Sec. V: ANALITICAL TOOLS FOR MIOT OPTIMIZATION

Advanced MIoT Tools
- Game Theory
- MFG theory
- Artificial Intelligence and Machine Learning
- Queueing & Graph Theory
- Optimal Transport Theory
- Optimization & Control Theory
- Blockchain and Distributed Ledger Technology

Sec. VII: LESSONS LEARNED AND DESIGN GUIDELINES
- Key Lessons Learned
- Cross-Cutting Design Trade-offs
- Rules of Thumb (Quantitative Heuristics)
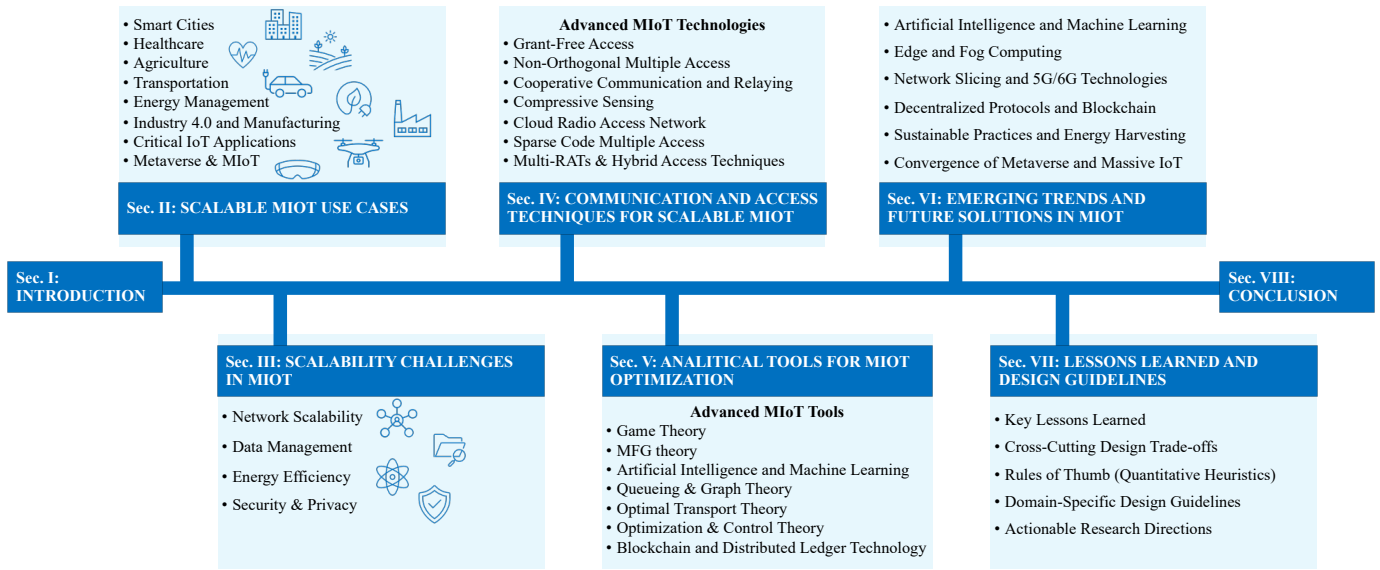- Domain-Specific Design Guidelines
- Actionable Research Directions

Fig. 2. Structure of the article.

management, and security challenges in the context of MIoT — not in isolation, but in a cohesive and interconnected manner. While existing surveys typically focus on one or two of these dimensions, our work offers a comprehensive and unified perspective that also emphasizes interdependencies and trade-offs among these domains, which are often overlooked. Our key scientific contributions and novel elements are:

- **Holistic Review of Scalable IoT Solutions**: We offer a broad review of existing scalable solutions in networking protocols, data management techniques, energy-efficient designs, and security frameworks. This review consolidates knowledge across multiple domains, providing a unified perspective on scalability in MIoT.
- **Comparative Analysis of Solutions**: A detailed comparative analysis is presented, highlighting the trade-offs between different approaches. This analysis is structured around key metrics such as scalability, efficiency, security, and cost-effectiveness. Our findings serve as a reference for choosing appropriate solutions based on specific MIoT application requirements.
- **Identification of Gaps and Emerging Trends**: We identify significant gaps in current solutions, such as limitations in security frameworks and energy inefficiency in large-scale deployments. In addition, we highlight emerging trends like edge and fog computing, 5G, and AI-powered IoT management, offering insights into how these technologies can address existing limitations.
- **Framework for Future Research**: Based on our review and analysis, we propose a framework for future research on scalable IoT systems, focusing on the integration of advanced technologies such as blockchain for secure IoT transactions, and hybrid cloud-edge architectures for efficient data processing. This framework provides guidelines for the development of next-generation IoT solutions.

Overall, this paper provides a roadmap for overcoming scalability challenges in MIoT, offering both theoretical insights

and practical guidelines for researchers and practitioners.

C. Research Approach

In this research, a comprehensive methodology was adopted to explore the scalability challenges and solutions for massive IoT systems. The approach can be divided into the following key phases:

1) Literature Review and Problem Definition: An in-depth review of academic publications, industrial reports, and standards from leading organizations such as IEEE, ITU, and ETSI was conducted. The objective was to define the scalability challenges in MIoT and identify existing frameworks and solutions addressing these challenges. The review focused on key areas such as network scalability, data management, energy efficiency, and security/privacy.

2) Selection Criteria for Scalable Solutions: The solutions considered were evaluated based on their ability to handle high volumes of IoT devices, flexibility for various use cases, and effectiveness in large-scale deployments. Key evaluation metrics included:

- **Scalability**: The ability to accommodate massive numbers of connected devices.
- **Efficiency**: Optimization of resources such as energy, network bandwidth, and storage.
- **Security and Privacy**: Robustness in protecting data and preventing unauthorized access.

3) Comparative Analysis: A comparative analysis was performed by categorizing scalable solutions into networking protocols and architectures, edge and fog computing, and data management techniques. The analysis evaluated factors such as implementation complexity, adaptability, resource efficiency, and trade-offs associated with each solution.

4) Emerging Trends and Future Directions: Emerging trends in MIoT, such as 5G networks, blockchain for IoT, and artificial intelligence for adaptive IoT management, were reviewed. Gaps in current solutions were identified, and

forward-looking recommendations based on new technological advancements were made.

D. Related Surveys

Throughout the past few years, numerous studies have been made to address the available options for MIoT scalable solutions. Each of these contributions addresses the challenge of network scalability, data delivery, efficiency, security, and privacy, with solutions aimed at these issues.

1) Network Scalability: [22] explores the integration of UDNs with other 5G-enabling technologies, such as millimeter waves (mmWave) and massive MIMO. This paper underscores the synergies between these technologies and their potential for addressing scalability and capacity demands in future networks. Similarly, [23] focuses on massive machine-type communications (mMTC) in ultra-dense cellular IoT networks. It investigates the challenges of scalability and resource allocation and proposes machine-learning-assisted solutions to optimize network performance. The survey includes a comprehensive review of techniques like reinforcement learning for managing high device density.

Furthermore, [24] provides a detailed study on mobility management in UDNs. It explores existing solutions and proposes future directions to handle challenges such as handover management and interference mitigation in high-density scenarios. The work [25] categorizes resource allocation techniques for UDNs into different classes and provides a detailed analysis of their applications in 5G and beyond networks. It also identifies open challenges in integrating these techniques with advanced technologies, such as network slicing and AI-based management systems.

An overview of UDNs is presented in [26], discussing their state-of-the-art solutions and potential future directions. It delves into architectural aspects, interference management, and capacity enhancement techniques essential for MIoT scalability. Finally, [27] surveys the evolution of UDNs, emphasizing their role in enabling scalable, efficient, and low-latency communications. The paper provides a critical analysis of existing technologies and suggests novel directions for future research.

A detailed study of the LoRaWAN protocol scalability to cope with mass deployments is also provided in [28]. The survey also addresses the challenges posed by interference in dense environments. It identifies the use of adaptive data rates and interference mitigation techniques as potential solutions to enhance network scalability. Similarly, in [29], the authors reviewed energy-efficient computing for MIoT networks in detail, examining low-power protocols and optimization models that help decrease energy costs in scaled IoT ecosystems.

An additional aspect is offered by [30], which discusses techniques of resource allocation through machine learning guidance so as to achieve improved scalability in ultra-dense cellular IoT networks. This survey identifies key issues, such as resource allocation in high-density areas, which remain a major challenge for MIoT scaling. In this regard, [31] looks into the problems of scalability of data transfer protocols and proposes distribution systems for efficient data transfer within massive IoT systems. These distributed systems are meant to meet the growing demand for scalable data management in MIoT applications.

2) Data Management: The survey [38] deals most specifically with IoT big data issues relating to its indexing and attempts to address this problem by proposing distributed databases and real-time data processing approaches for MIoT systems generating enormous quantities of data. This work complements other surveys addressing data management challenges by proposing innovative solutions to handle the ever-increasing data loads in MIoT ecosystems. Also, [32] offers fresh insights on age of information (AoI) within MIoT systems and provides optimization strategies for data freshness and latency problems in the majority of IoT time-critical applications. Another work [33] complements this research by analyzing the potential of deep reinforcement learning for improving federated learning efficiency in MIoT communications, with a focus on privacy-preserving data management.

Another relevant contribution [39] consists in an overview analysis of scalable networking architecture solutions, identifying load balancing and network flexibility as critical issues in MIoT networks. A related effort is [40], which reviews various network methodologies tailored for real-time analytics in MIoT ecosystems. It delves into the challenges posed by massive data generation, transmission, and processing in IoT systems.

3) Energy Efficiency: In [29] the authors reviewed energy-efficient computing for MIoT networks in detail, examining low-power protocols and optimization models that help decrease energy costs in scaled IoT ecosystems. Furthermore, [25] provides a comprehensive classification of resource allocation techniques for ultra-dense networks in 5G and beyond, highlighting energy-efficient methodologies for improving network performance. Moreover, [37] presents an extensive study on the role of energy efficiency in the transition towards 6G networks. The work examines optimization strategies aimed at minimizing energy consumption while maintaining reliable and scalable MIoT communications.

4) Security and Privacy: In the MIoT, security and privacy remain key areas which have been well studied by a couple of works. [34] presents security mechanisms based on blockchain technologies and decentralized architectures for MIoT systems and emphasizes the need for lightweight encryption for IoT devices in the MIoT context. This line of research is extended by [36], which explores the literature on improving the security of MIoT in 6G networks and providing privacy-friendly architectures based on new technologies.

5) Gaps in Prior Surveys: **Critical observations on the state of the art.**

- *Fragmentation across pillars*: Most surveys address network scalability, data management, energy, or security in isolation, with limited cross-layer co-design and almost no analysis of joint trade-offs (latency–reliability–energy).
- *Heterogeneous metrics*: The lack of harmonized KPI sets prevents fair comparisons (e.g., device density/km^2, energy/bit, battery lifetime at fixed duty cycle, signaling load per device).

TABLE I
COMPARATIVE ANALYSIS OF SCALABLE SOLUTIONS FOR MIoT FROM RECENT SURVEYS.

Survey	Year of Publication	Main Topics	Challenges Addressed	Network Scalability	Data Management	Energy Efficiency	Security & Privacy
Our Survey	–	Integrated framework for scalability, energy efficiency, security	Comprehensive solutions for MIoT challenges	✓	✓	✓	✓
[29]	2024	Energy-efficient computing for MIoT	Low-power protocols, energy optimization			✓	
[28]	2023	LoRaWAN scalability, adaptive data rates	Interference mitigation, network scalability	✓			
[32]	2023	AoI optimization	Latency, data freshness in MIoT		✓		
[33]	2023	Federated learning, deep reinforcement learning	Privacy-preserving data management		✓		✓
[34]	2023	Blockchain security mechanisms	Lightweight encryption, privacy enhancement				✓
[35]	2022	Resource management in 802.11ah WLAN	Spectrum reuse, network scalability	✓			
[36]	2021	Security for MIoT in 6G networks	Privacy-friendly architectures				✓
[37]	2021	Network slicing, AI-driven resource management	Scalability, energy optimization in 6G	✓		✓	
[25]	2021	Resource allocation techniques in UDNs	Scalability, AI-based management systems	✓		✓	
[38]	2021	IoT big data indexing	Real-time processing, data management in MIoT		✓		
[23]	2020	mMTC in ultra-dense cellular IoT networks	Scalability, resource allocation with ML	✓			
[22]	2020	UDNs with 5G (e.g., mmWave, MIMO)	Scalability, capacity enhancement	✓			
[24]	2020	Mobility management in UDNs	Handover management, interference mitigation	✓			
[39]	2020	Scalable networking architectures	Load balancing, network flexibility	✓			
[30]	2019	Machine learning for resource allocation	Scalability in ultra-dense IoT networks	✓			
[31]	2019	Distributed systems, data transfer protocols	Efficient data transfer, scalability	✓	✓		
[40]	2017	Network methodologies for real-time analytics	Massive data generation, IoT scalability	✓	✓		
[41]	2018	Resource allocation in ultra-dense networks	Interference mitigation, network capacity	✓			
[26]	2016	UDN solutions overview	Scalability, interference management	✓			
[27]	2016	Evolution of UDNs	Scalable, low-latency communication	✓			

- *Under-modeling of massive access and coexistence*: Few works rigorously evaluate *grant-free* schemes (NOMA/SCMA/coded slotted ALOHA), RACH overload, LoRaWAN collisions, or mMTC/URLLC/eMBB coexistence under realistic interference.
- *Insufficient end-to-end orchestration*: Most studies fail to cover edge–fog–cloud control loops, multi-RAT slicing (NB-IoT/5G/802.11ah/LoRaWAN), and control-plane delays (SDN/NFV) that directly impact scalability.
- *Data management and AI*: Existing works rarely analyze communication and aggregation costs in non-IID federated learning, robustness to poisoning or inference attacks, or compression/aggregation schemes compatible with strict SLAs.
- *Security foresight gaps*: The literature tends to overemphasize blockchain or lightweight crypto in isolation, while providing scarce frameworks that integrate *zero trust*, edge AI-based intrusion detection, and post-quantum cryptography tailored to MIoT constraints.

- *Reproducibility issues*: Most contributions fail to provide reference scenarios, tools/simulators, and published parameters (traffic, mobility, channels), which makes results hard to compare or replicate.

Our survey builds upon this body of work by providing an integrated framework that addresses the key challenges across four major dimensions: network scalability, data management, energy efficiency, security and privacy. In doing so, it contributes to the ongoing research efforts aimed at enabling scalable, secure, and energy-efficient MIoT deployments. Table I presents a comparative analysis of scalable solutions for MIoT from recent surveys.

E. Organization

The remainder of this paper is organized as follows:

In **Section II**, we present various *Scalable MIoT Use Cases*, highlighting the practical applications of massive IoT across industries such as smart cities, healthcare and agriculture. This

section outlines the benefits of scalability in these areas and their specific challenges.

Section III addresses the *Scalability Challenges in MIoT*, focusing on the key challenges of network scalability, data management, energy efficiency, and security & privacy. Additionally, a *Comparative Analysis of MIoT* is included to provide an in-depth evaluation of existing solutions against these challenges.

Section IV presents *Advanced Techniques for Scalable MIoT Networks*, where various advanced techniques are examined, including grant-free access, cooperative communication, and NOMA (Non-Orthogonal Multiple Access). This section delves into how these techniques contribute to enhancing network scalability, energy efficiency, and secure communication in large-scale MIoT deployments.

Section V explores Advanced Tools for Scalable MIoT Networks, where cutting-edge methodologies and technologies are analyzed for optimizing MIoT deployments. This section covers the role of artificial intelligence (AI) and machine learning (ML) in optimizing resource allocation and network adaptability.

Section VI explores the *Emerging Trends and Future Solutions* in MIoT. This section discusses the latest advancements and trends, such as artificial intelligence, edge computing, blockchain technology, and the anticipated impact of 6G networks on MIoT scalability.

Finally, **Section VII** presents the *Conclusions* of this work, summarizing the key findings and discussing the future direction of scalable MIoT solutions. Gaps in current solutions are highlighted and relevant avenues for further research and innovation are identified. Figure 2 provides a general overview of the paper structure, while acronym definitions are presented in Table II.

II. SCALABLE MIoT USE-CASES

The concept of Massive IoT encompasses diverse applications across various sectors, each presenting unique scalability requirements and challenges. The following sections outline specific use cases, illustrating how scalable solutions in MIoT can drive efficiency and innovation in these industries.

A. Smart cities

Smart cities use MIoT solutions to enhance urban infrastructure, sustainability, and quality of life. MIoT applications in these cities range from adaptive traffic management, smart lighting, waste management, air quality monitoring, and emergency response systems, all relying on real-time data from interconnected IoT devices to deliver timely insights and optimize operations [42]–[44].

A prominent example is adaptive traffic control, where sensors at intersections monitor vehicle flow and congestion patterns, and traffic signals adjust in real-time to reduce bottlenecks and improve traffic flow efficiency. This approach can cut down commute times by up to 30% in densely populated areas by processing data at the network edge, thus minimizing latency and ensuring faster response times [45], [46]. Edge computing frameworks integrated with such systems play

TABLE II
MAIN ABBREVIATIONS USED IN THIS ARTICLE.

Abbreviation	Definition
5G	Fifth Generation
6G	Sixth Generation
AF	Amplify-and-Forward Scheme
AI	Artificial Intelligence
AIS	Artificial Immune Systems
AoI	Age of Information
AR	Augmented Reality
BBU	Baseband Unit
BFT	Byzantine Fault Tolerance
CRAN	Cloud-Radio Access Network
CRN	Cognitive Radio Network
CS	Compressive Sensing
D2D	Device-to-Device Communication
DAG	Directed Acyclic Graph
DERs	Distributed Energy Resources
DF	Decode-and-Forward Scheme
DL	Deep Learning
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
DSA	Dynamic Spectrum Access
eMBB	Enhanced Mobile Broadband
FL	Federated Learning
IDS	Intrusion Detection Systems
IIoT	Industrial Internet of Things
IoT	Internet of Things
LPWAN	Low-Power Wide Area Network
MAC	Medium Access Control
MC-NOMA	Multi-Carrier Non-Orthogonal Multiple Access
MEC	Multi-access Edge Computing
MFG	Mean Field Game
MFGT	Mean Field Game Theory
MIoT	Massive Internet of Things
ML	Machine Learning
MLP	Machine Learning Processing
mMTC	Massive Machine Type Communication
mmWave	Millimeter-Wave
Multi-RAT	Multi-Radio Access Technology
NFV	Network Function Virtualization
NOMA	Non-Orthogonal Multiple Access
OFDMA	Orthogonal Frequency Division Multiple Access
OT	Optimal Transport
P2P	Peer-to-Peer Communication
PoS	Proof of Stake
PoW	Proof of Work
QoS	Quality of Service
RAN	Radio Access Network
RL	Reinforcement Learning
RRH	Remote Radio Head
SCMA	Sparse Code Multiple Access
SDN	Software-Defined Networking
SIC	Successive Interference Cancellation
THz	Terahertz
TTI	Transmission Time Interval
UAV	Unmanned Aerial Vehicle
URLLC	Ultra-Reliable Low-Latency Communication
VR	Virtual Reality
WLAN	Wireless Local Area Network
XR	Extended Reality

a critical role in ensuring low-latency data processing and reducing reliance on centralized servers, which is essential for handling the vast amounts of data generated by urban IoT networks [47], [48].

Smart lighting systems also contribute significantly to energy savings in urban areas by adjusting light levels based on occupancy and environmental data. Studies indicate that

implementing such systems can reduce energy consumption by nearly 50%, enhancing sustainability and reducing operational costs [49], [50]. Some advanced systems leverage AI-powered sensors and adaptive lighting algorithms to maintain optimal illumination only when necessary, creating a more sustainable urban infrastructure. Furthermore, waste management systems in smart cities now use IoT-enabled sensors on waste bins to track fill levels and optimize collection routes, which reduces fuel consumption and operational costs for waste management services [51], [52]. Such MIoT systems also allow cities to monitor air quality, noise pollution, and water quality, integrating data streams to form a comprehensive environmental monitoring network. This data not only improves municipal services but also empowers citizens to make informed decisions about health and well-being [53], [54].

Overall, smart cities benefit from MIoT solutions by achieving greater scalability, enhanced energy efficiency, and improved data management. However, challenges remain, particularly in managing the vast data generated and ensuring security and privacy across all interconnected devices.

B. Healthcare

The integration of MIoT applications in healthcare is revolutionizing patient monitoring, telemedicine, and health data management, providing solutions that are both scalable and patient-centered [55], [56]. Wearable devices, such as heart rate monitors and glucose sensors, continuously monitor patient vitals, transmitting data to healthcare providers for timely assessment and intervention. These devices allow early detection of health issues and minimize the need for in-person consultations, which is particularly beneficial for patients with chronic illnesses [57].

Managing the large volumes of health data generated by these devices poses challenges in data scalability, privacy, and network load. To address these, federated learning has been widely adopted to process data locally on devices, thus preserving patient privacy and reducing network dependency [58], [59]. This approach also enables continuous updates to AI models, improving healthcare delivery through adaptive learning without compromising sensitive patient information [60]. AI further enhances MIoT healthcare applications by analyzing massive datasets to identify patterns that may assist in proactive health management and predictive diagnosis [61], [62]. For example, AI algorithms can help identify early signs of diseases such as diabetes or cardiovascular conditions based on historical data, providing actionable insights for healthcare providers [63]. Additionally, advances in edge computing have facilitated faster data processing on wearable devices, which is essential for real-time health applications requiring low latency and reliability [64]. These technologies collectively foster a healthcare environment where MIoT systems can manage high device densities, ensure data security, and provide scalable solutions suitable for personalized and preventive healthcare.

C. Precision Agriculture

Precision agriculture leverages MIoT solutions to enhance productivity by using data from IoT sensors and remote sensing devices. These sensors, deployed across large agricultural fields, collect critical data on soil moisture, temperature, humidity, and nutrient levels, enabling farmers to make precise, data-driven decisions regarding irrigation, fertilization, and pest control [65]–[67]. Additionally, data from these sensors combined with weather forecasts and crop growth models provide valuable insights for optimizing resource allocation and minimizing waste, thereby supporting sustainable farming practices. As sensor networks expand in scale, maintaining connectivity becomes increasingly challenging, especially in remote areas. LPWANs like LoRaWAN and NB-IoT, alongside energy-efficient sensors, are crucial for scalability in these networks, enabling data transmission over vast distances with minimal energy consumption [68], [69]. In areas with limited connectivity, edge computing frameworks allow data to be processed locally, reducing the need for continuous data transmission and ensuring timely decisions even in remote settings [70].

Emerging AI-driven analytics are also proving beneficial in precision agriculture. By analyzing large-scale data from sensors, AI models can predict crop yields, optimize water usage, and detect pest infestations early. These insights lead to improved productivity and environmental sustainability [71], [72]. For example, integrating machine learning models with MIoT systems helps optimize fertilizer application rates based on real-time soil data, reducing over-fertilization and its environmental impact [73]. This combination of scalable MIoT infrastructure, energy-efficient networks, and AI analytics represents a transformative shift in agricultural practices, enabling farmers to enhance yields while conserving resources and promoting ecological sustainability.

D. Intelligent Transportation

MIoT applications in transportation are essential to the advancement of autonomous vehicles, real-time logistics, and fleet management. Autonomous vehicles (AVs) utilize MIoT infrastructure to communicate with nearby vehicles, road infrastructure, and environmental sensors, which is crucial for navigating complex urban environments and improving safety [74]–[76]. These applications generate substantial volumes of data, which need to be processed with high speed and minimal latency to ensure timely and reliable operation. As the number of connected vehicles grows, the scalability of MIoT solutions becomes critical to maintaining efficient and safe transport systems. To meet these high data and communication demands, MIoT in transportation relies on 5G technology and multi-access edge computing (MEC), which together support low-latency, high-throughput data processing at the network edge. MEC enables data to be processed closer to the AVs, reducing the need for continuous back-and-forth communication with centralized servers [77], [78]. Research shows that integrating 5G with MEC can significantly improve the responsiveness of AVs in high-density traffic, enhancing safety and scalability in urban settings [79], [80].

Furthermore, MIoT facilitates real-time logistics and fleet management. Logistics companies are using sensor-equipped vehicles and AI-driven analytics to track location, monitor vehicle health, and optimize delivery routes, leading to cost

savings and improved delivery times [81], [82]. Predictive maintenance, enabled by MIoT sensors, allows fleet operators to monitor vehicle conditions in real-time, reducing downtime and improving operational efficiency [83]. As the number of connected vehicles continues to increase, scalable MIoT frameworks are essential for ensuring these systems function seamlessly across various urban and rural environments.

E. Energy Management within Smart Grids

MIoT applications in energy management, particularly within smart grids, are revolutionizing how energy distribution and reliability are maintained by integrating real-time data from IoT-enabled devices, such as smart meters, substations, and energy management systems [84], [85]. These systems collect and analyze data to enable utilities to forecast energy demand, balance loads, reduce outages, and optimize the integration of renewable energy sources, thereby advancing sustainability goals. By leveraging MIoT, energy providers can enhance grid flexibility and efficiency, which is essential for meeting growing energy demands in urban and rural areas.

Scalability in MIoT-driven energy management is further enhanced by predictive algorithms that process historical consumption data, enabling accurate forecasting and effective demand-response actions [86], [87]. ML techniques contribute to the robustness of smart grids by supporting predictive maintenance, which can preempt equipment failures and reduce downtime [88]. Moreover, integrating renewable sources, such as solar and wind, into these grids requires adaptive MIoT architectures that can manage intermittent supply and fluctuating demand. Distributed energy resources (DERs) are increasingly used alongside MIoT-enabled devices for efficient energy storage and real-time distribution adjustments [89].

Research indicates that edge computing frameworks in MIoT can further improve the scalability and resilience of smart grids by reducing latency in data processing, thereby enabling faster and more localized decision-making [90]. Additionally, blockchain technology is being explored to enhance data security within energy management systems, providing tamper-resistant records of energy transactions and ensuring trust among distributed energy producers and consumers [91].

F. Industry 4.0 and Manufacturing

The adoption of MIoT in manufacturing is foundational to Industry 4.0, enabling the creation of smart factories that leverage interconnected devices for monitoring production lines, managing inventories, and optimizing processes [92], [93]. MIoT devices continuously gather and analyze data on machine performance, facilitating predictive maintenance that reduces unexpected downtime, minimizes repair costs, and enhances productivity [94]. Predictive maintenance is critical in manufacturing environments, where minor interruptions in the production process can lead to significant costs and delays.

Scalability in Industry 4.0 is paramount, as these environments often require supporting thousands of sensors, actuators, and controllers within a single factory [95]. High data volume and the need for low latency make it essential to deploy scalable solutions such as LPWANs, which provide long-range

communication for connected devices, and hybrid cloud-edge architectures that reduce latency by processing data closer to the source [96], [97]. These architectures not only allow for efficient data handling, but also improve data security and resilience by distributing processing across multiple layers.

MIoT's role in manufacturing extends to real-time quality control and inventory management. Sensors monitor environmental factors like temperature and humidity, ensuring products meet quality standards throughout production [98]. Additionally, automated inventory systems integrated with MIoT provide up-to-the-minute stock information, enhancing the ability to manage supply chains and reduce waste [99].

Future advancements in MIoT for manufacturing must focus on enhancing scalability and adaptability to support evolving Industry 4.0 requirements. These innovations include integrating artificial intelligence for adaptive process management and implementing advanced cyber-security measures to protect sensitive industrial data [100], [101]. As MIoT continues to develop, its role in transforming manufacturing will rely on adaptable architectures that can meet the dynamic demands of data-driven, interconnected industrial environments.

G. Critical IoT Applications

The advent of 5G technology has introduced a new communication paradigm known as Ultra-Reliable Low-Latency Communication (URLLC), which is specifically designed to meet the stringent requirements of critical IoT applications. Critical IoT use cases, such as industrial automation, autonomous vehicles, remote surgery, and smart grid management, demand ultra-high reliability, extremely low latency, and consistent throughput. These requirements are essential to ensure the safe and efficient operation of systems where even minor delays or failures can have catastrophic consequences [102].

The MIoT, consisting of tens of billions of connected devices, objects, and machines, relies on ubiquitous connectivity. Among them, certain IoT devices require URLLC [103].

URLLC achieves reliability levels of up to 99.999% through techniques like diversity, redundancy, and advanced error correction [104], while ensuring end-to-end latency as low as 1 millisecond via edge computing, short transmission time intervals (TTIs), and preemptive scheduling [105]. Additionally, constant throughput is maintained through dynamic resource allocation, QoS guarantees, and technologies like beamforming and massive MIMO. Despite its potential, challenges such as network synchronization, energy efficiency, and scalability must be addressed to fully realize URLLC's capabilities in supporting the next generation of critical IoT systems [106].

H. Metaverse and Massive IoT

The convergence of the Metaverse and MIoT is poised to revolutionize various industries by creating immersive, interactive, and data-rich environments. MIoT, characterized by the extensive deployment of interconnected devices, serves as a foundational layer for the Metaverse, enabling real-time data integration from the physical world into virtual spaces.

In healthcare, this integration facilitates advanced telemedicine and remote monitoring. IoT devices collect patient data, which can be visualized in the Metaverse, allowing healthcare professionals to assess and interact with patient information in a 3D virtual environment. This approach enhances diagnostic accuracy and patient engagement [107].

The retail sector also benefits from the fusion of MIoT and the Metaverse. IoT sensors track inventory and consumer behavior, while virtual platforms offer immersive shopping experiences. Customers can virtually try on products or explore digital showrooms, bridging the gap between online and physical retail [108].

In industrial applications, the concept of the industrial metaverse emerges, where IoT devices monitor machinery and processes, and digital twins replicate these systems in virtual environments. This setup allows for real-time monitoring, predictive maintenance, and optimization of operations, leading to increased efficiency and reduced downtime [109].

Moreover, the integration of IoT with the metaverse enhances smart city initiatives. IoT devices collect data on urban infrastructure, which can be visualized in the metaverse to simulate and manage city operations, improving resource allocation and urban planning [107].

In summary, the synergy between the metaverse and MIoT offers transformative potential across various sectors, enabling more interactive, efficient, and data-driven applications.

III. Scalability Challenges in MIoT

MIoT introduces unique scalability challenges across several dimensions—ranging from network architecture, data management, and energy efficiency to security and privacy concerns. The high density amplifies these challenges, in heterogeneous environments in which MIoT systems operate. Addressing these issues requires innovative approaches that balance performance, energy consumption, and data security while supporting massive connectivity and real-time processing.

In the following sections, we explore the key scalability challenges and potential solutions in MIoT environments.

A. Ultra-Dense IoT Networks

Network scalability is a fundamental aspect of MIoT systems, as it determines the ability of the network to support an increasing number of devices while maintaining performance, reliability, and efficiency. The rapid growth in IoT devices necessitates the development of scalable network architectures that can handle high device density, ensure low latency, manage resources efficiently, and handle interference effectively.

1) Challenges of Network Scalability: Scaling IoT networks presents several challenges, especially in high-density environments:

- **Device Density and Network Congestion**: As the number of connected devices increases, network congestion becomes a critical issue. Without proper management, congestion can lead to packet loss, increased latency, and reduced overall network performance. Research suggests that novel congestion control techniques are required to ensure smooth network operations in dense IoT environments [122], [123].
- **Latency Requirements**: Many IoT applications, particularly those requiring real-time processing such as autonomous vehicles and industrial automation, are highly sensitive to latency. High device densities can lead to increased traffic, resulting in longer delays. Effective techniques for managing latency, including optimized routing protocols and edge computing, are essential for meeting the stringent requirements of these applications [124], [125].
- **Resource Allocation**: Dynamic and efficient resource allocation is crucial for ensuring scalability in IoT networks. With the growing number of devices, allocating resources such as bandwidth, processing power, and memory becomes increasingly complex. Recent research highlights the importance of AI-driven solutions for dynamically managing resources to avoid network bottlenecks and enhance scalability [126], [127].
- **Interference Management**: In dense MIoT deployments, interference from overlapping wireless signals can degrade communication quality. Effective interference management strategies, such as adaptive power control and interference-aware protocols, are necessary to maintain reliable communication as the network scales [128], [129].
- **Protocol Scalability**: Traditional networking protocols, such as those used in legacy systems, were not designed to support the scale of MIoT. New or adapted protocols that can handle a large number of devices while minimizing signaling overhead and energy consumption are being researched and developed [130], [131].

2) Contemporary solutions: To address these challenges, several technological solutions have been proposed:

- **Cognitive Radio Networks (CRN)**: CRN enables dynamic spectrum access, allowing IoT devices to utilize unused frequency bands opportunistically. This approach significantly reduces congestion and improves the network's support of large-scale deployments. Cognitive techniques have shown promising results in optimizing network performance in dense environments [132], [133].
- **Millimeter-Wave (mmWave) Communications**: mmWave technology offers large bandwidths, enabling high data rates and accommodating many simultaneous connections. Although the propagation characteristics of mmWave signals lead to limited range and require advanced beamforming techniques, they offer a significant potential for scaling IoT networks in urban areas [134], [135].
- **Low-Power Wide-Area Networks (LPWANs)**: LPWAN technologies such as LoRaWAN and NB-IoT are designed to provide long-range, low-power communication, making them ideal for IoT networks with many devices. While these technologies excel in energy efficiency, addressing scalability in terms of data throughput remains a challenge [136], [137].
- **Software-Defined Networking (SDN)**: SDN allows for

TABLE III
COMPARISON OF NETWORK SCALABILITY APPROACHES IN MIOT NETWORKS

Technology	Key Features	Energy Consumption	Range / Density	Latency / Battery Life	Limitations	Metrics	References	Key Technical Insights
Cognitive Radio Networks (CRN)	Dynamic spectrum allocation w/ real-time sensing	—	—	—	Requires sophisticated spectrum sensing and decision-making	Spectrum sensing cost: 5–50 mW; Detection accuracy: 85–95%; Channel availability: 20–60%	[110]	CRNs enable opportunistic spectrum use in dense MIoT but require accurate sensing to avoid interference.
Millimeter-Wave (mmWave)	High-frequency bandwidth (30–300 GHz)	—	50–200 m	—	High path loss, limited range	Throughput: 1–10 Gbps; Blockage loss: 20–35 dB	[111]	Ultra-high data rates for short-range dense deployments.
NB-IoT & LTE-M	Cellular LPWAN in licensed band	1.7 mAh per 44-byte uplink	Millions of devices/km²	837 ms; up to 10 years	Limited bandwidth	MCL: 164 dB; Data rate: 20–250 kbps; Density: >100k/km²	[112], [113], [114]	Suitable for massive-scale, low-power MIoT.
LoRaWAN	Long-range, low-power star network	0.05–0.44 mJ/msg	1–10 km	1–13 years	Collision risk at scale	Data rate: 0.3–50 kbps; Duty cycle: 1%	[115], [116], [117]	Good for sparse deployments, less for dense MIoT.
Software-Defined Networking (SDN)	Centralized management	—	Flexible	—	Security concerns	Control latency: 1–10 ms; 10k–100k flows/s	[118]	Adaptive control but centralization risk.
Routing Protocols (RPL)	Energy-efficient routing	—	Thousands of nodes	—	Mobility issues	Control overhead: 10–20%; Hop count: 5–15	[119]	Effective for static networks.
ML-Assisted Scalability	Traffic prediction	—	—	Depends on model	Requires training data	Inference: 10–200 µJ; Training: 10 mJ–1 J	[120]	Improves resource allocation.
Edge / Fog Computing	Compute offload near data source	—	Scales with infrastructure	Reduces latency	Complex management	Latency reduction: 30–80%; Bandwidth savings: 40–90%	[121]	Good for time-sensitive MIoT.

the decoupling of the control plane from the data plane, providing more flexibility and scalability in managing network resources. SDN-based approaches enable centralized control, allowing the network to dynamically adapt to varying traffic conditions and device densities [138], [139].

- **Edge and Fog Computing**: Edge and fog computing architectures push data processing closer to IoT devices, reducing latency and bandwidth consumption. By enabling real-time data processing at the edge of the network, these computing paradigms are essential for scaling MIoT systems [140], [141].

Table III presents a comparative analysis of network scalability approaches in MIoT networks.

3) Future Research Directions: Future research on network scalability should focus on integrating these technologies to develop hybrid solutions. For example, combining cognitive radio techniques with SDN may improve both spectrum management and resource allocation. Additionally, incorporating machine learning techniques for predictive traffic and resource management could further enhance scalability in MIoT networks [142], [143]. Addressing these open challenges will pave the way for more resilient and efficient MIoT systems.

Network scalability is a fundamental challenge for the future of MIoT, as the number of connected devices continues to grow exponentially. Addressing issues related to device density, bandwidth limitations, and varying device requirements is critical for the continued expansion of IoT. While current solutions such as LPWAN, 5G, and mesh networks provide the backbone for scaling MIoT deployments, ongoing innovations, including 6G and satellite IoT networks, will be vital in ensuring the long-term scalability and success of the massive IoT landscape.

B. Data Management

MIoT systems involve billions of connected devices that generate vast amounts of data. Managing this data, in terms of storage, processing, analysis, and security, presents several challenges. Effective data management is essential for ensuring the scalability, reliability, and security of MIoT environments. This section highlights the primary challenges and proposed solutions for efficient data management in MIoT systems.

1) Challenges in Data Management: The large-scale nature of MIoT systems introduces various challenges:

1. Data Volume: MIoT environments generate an immense amount of data. For example, smart cities, with connected devices monitoring everything from traffic to air quality, produce terabytes of data per day. Storing and processing this data in traditional centralized cloud infrastructures leads to inefficiencies due to bandwidth constraints and latency [153]. Centralized systems become bottlenecks as the data load increases, demanding distributed data storage techniques [154].

2. Data Variety: The variety of data generated in MIoT systems is another key challenge. Devices produce structured,

TABLE IV
COMPARISON OF PROPOSED SOLUTIONS FOR DATA MANAGEMENT IN MASSIVE IoT.

Proposed Solution	Scalability	Efficiency	Security	Advantages	Challenges	Example of Technique	References	Key Technical Insights
Edge computing architectures	***	***	**	Reduces latency and bandwidth usage	Latency and bandwidth constraints	Local processing for real-time analytics	[121], [144]	Ideal for latency-sensitive MIoT tasks, but dependent on distributed infrastructure and consistent connectivity.
Data aggregation techniques	**	***	**	Lowers data transfer volume, reduces processing load	Data loss during aggregation	Hierarchical clustering for data compression	[145], [146]	Improves bandwidth efficiency and processing, but risk of accuracy loss when compressing critical data.
Fog computing approaches	***	**	***	Distributes computing resources, reduces cloud dependency	Complexity in deployment	Multi-tier processing to offload tasks from cloud	[147], [148]	Balances processing between cloud and edge, reducing latency, but requires complex orchestration.
Cloud-based data management	****	***	*	Provides high storage and processing capabilities	Data privacy concerns	Centralized data storage for extensive analytics	[149], [150]	Supports large-scale analytics and long-term storage but may introduce privacy and latency issues.
Machine learning for data analytics	**	***	***	Enhances predictive accuracy and pattern recognition	Model training, potential biases	Anomaly detection for device performance	[151], [152]	Enables advanced decision-making in MIoT, though training overhead and bias risks remain concerns.

Legend: * = Low, ** = Medium, *** = High, **** = Very High

semi-structured, and unstructured data, including sensor readings, video streams, audio signals, and logs. Integrating and managing such heterogeneous data within a single framework is difficult. Furthermore, different types of data require different methods of processing and storage, increasing system complexity. Big data technologies, such as Hadoop and Spark, are widely adopted to handle this diversity, providing flexible and scalable platforms [155].

3. Data Velocity: In addition to high volume, MIoT applications often require real-time or near real-time data processing. For instance, healthcare applications relying on IoT data for remote patient monitoring must process and analyze data continuously to enable immediate responses. This need for low-latency processing in the face of high data velocity is another core challenge in MIoT [156]. Traditional batch processing systems are unsuitable for these use cases, leading to the rise of stream processing systems and edge computing solutions [157].

4. Data Integrity and Security: The vast number of devices connected to MIoT systems increases the potential attack surface for cyber threats. Ensuring the security of data throughout its lifecycle—from collection to transmission and storage—is a major concern. In addition, ensuring the integrity of data, particularly when transmitted over unreliable networks, is essential for maintaining trust in IoT applications. Technologies like blockchain and encryption algorithms are crucial in addressing these security concerns [158], [159].

5. Energy Efficiency: Many IoT devices operate with limited computational power and energy resources. Efficiently managing data without draining device batteries is essential. Protocols that minimize the energy consumed during data transmission and processing are required to ensure the long-term viability of MIoT networks [160].

2) Contemporary solutions: Given these challenges, researchers have proposed several solutions:

1. Edge and Fog Computing: Edge computing involves processing data closer to the source (i.e., at the edge of the network), reducing latency and bandwidth requirements. This approach allows for data to be processed in real-time, alleviating the load on centralized cloud systems and reducing the distance that data must travel [161]. Fog computing extends the edge concept by enabling intermediate nodes between the cloud and edge devices, allowing for more distributed and scalable processing [162].

2. Federated Learning: In traditional centralized machine learning, data from IoT devices must be transferred to a central server for model training, which poses privacy and bandwidth issues. Federated learning mitigates this problem by training machine learning models locally on devices and sharing only the model updates, not the raw data. This approach enhances data privacy, reduces bandwidth consumption, and improves scalability [163]. Federated learning is particularly well-suited for MIoT environments, where privacy and energy efficiency are top concerns.

3. Blockchain for Data Security: Blockchain technology has emerged as a promising solution for enhancing security in distributed MIoT systems. Its decentralized and immutable ledger ensures that data is securely stored and can be audited without the risk of tampering [164]. Blockchain also supports secure data exchange between IoT devices, enhancing trust in peer-to-peer networks and reducing reliance on central authorities [165].

4. Data Compression and Aggregation: Data compression techniques can reduce the size of the data transmitted by IoT devices, addressing bandwidth limitations. Lossless compression methods maintain data integrity, while lossy techniques

can be employed for applications where some data loss is acceptable. In addition, data aggregation at the edge reduces redundancy and ensures that only relevant data is transmitted, optimizing both energy consumption and network usage [166].

5. Real-Time Data Processing Frameworks: To handle high-velocity data, real-time processing frameworks, such as Apache Kafka and Spark Streaming, have been adopted in MIoT. These systems provide scalable solutions for processing continuous data streams and generating actionable insights on-the-fly, which is crucial for applications like smart cities, healthcare, and industrial automation [167].

3) Future Directions: Future research in MIoT data management is expected to focus on further optimizing scalability, security, and energy efficiency. Integrating AI and machine learning techniques into data management frameworks will play a pivotal role in handling complex data streams, optimizing resource allocation, and predicting system behavior. Privacy-preserving techniques, such as homomorphic encryption and differential privacy, will be crucial in ensuring secure data processing in federated learning environments [168], [169]. Additionally, the emergence of 6G networks will provide the ultra-low latency and high bandwidth needed to support the next generation of MIoT systems [170].

Table IV summarizes several proposed solutions for data management in MIoT, focusing on their scalability, efficiency, security features, and the challenges they address.

C. Energy Efficiency

Energy efficiency is a critical aspect of the MIoT, as it directly influences the longevity, reliability, and scalability of IoT deployments. The large number of low-power devices operating in MIoT networks necessitates the development of energy-efficient communication protocols, data processing techniques, and resource management solutions. This section provides an in-depth review of the energy challenges faced by MIoT systems and the corresponding solutions and future research directions.

1) Challenges in Energy Efficiency: The scale and complexity of MIoT present several challenges to achieving energy efficiency:

- **Limited Power Resources:** Most IoT devices rely on batteries with limited lifespans, and the deployment of these devices in remote or inaccessible areas makes battery replacement costly and impractical [171].
- **Massive Data Generation:** The high volume of data generated by MIoT devices increases energy consumption during data transmission and processing, especially when cloud-based storage and processing are involved [172].
- **Network Scalability:** As the number of connected devices grows, managing the energy consumption of each device and ensuring efficient operation becomes a major challenge, particularly in heterogeneous networks with varying device capabilities [173], [174].
- **Interference and Congestion:** IoT devices operating in dense environments often experience interference and network congestion, leading to increased energy consumption due to repeated transmission attempts [175].

- **Sustainability:** Achieving energy efficiency at scale is crucial for the long-term sustainability of MIoT ecosystems, as large-scale deployments are expected to grow exponentially with the advent of 5G and 6G technologies [176], [177].

2) Contemporary solutions: Various solutions have been proposed to address these challenges, focusing on minimizing energy consumption while maintaining performance and scalability:

- **Energy Harvesting:** IoT devices can leverage energy harvesting techniques (e.g., solar, wind, and ambient radio frequency energy) to extend their operational lifespan, reducing dependency on battery replacements [190].
- **Low-Power Wide-Area Networks (LPWANs):** LPWAN technologies such as LoRaWAN, Sigfox, and NB-IoT are widely adopted for their energy-efficient communication capabilities over long distances, making them suitable for large-scale IoT deployments [182], [183].
- **Edge and Fog Computing:** By processing data closer to the source, edge and fog computing architectures significantly reduce the energy required for data transmission to the cloud, optimizing overall network energy consumption [186].
- **Energy-Efficient Routing Protocols:** Protocols such as energy-aware multi-hop routing reduce the energy consumption required for data transmission in large IoT networks by optimizing the paths taken by data packets based on energy availability and network conditions [191].
- **Machine Learning for Energy Management:** Advanced machine learning models are increasingly being used to predict energy consumption patterns and optimize resource allocation in real-time, improving energy efficiency in dynamic IoT environments [178], [179].

Table V summarizes several proposed solutions for energy efficiency in MIoT.

3) Future Directions: Future research is expected to further improve energy efficiency in MIoT through several emerging trends:

- **6G Integration:** The deployment of 6G networks will introduce ultra-low-latency and energy-efficient communication protocols designed specifically for MIoT systems, potentially reducing energy consumption at both the device and network levels [127], [192].
- **Federated Learning and Edge AI:** Federated learning allows IoT devices to collaboratively train models without sharing raw data, reducing communication energy costs. The integration of AI at the edge can also help in local decision-making, minimizing energy usage by reducing unnecessary data transmissions [193], [194].
- **Cooperative Energy Harvesting:** Techniques such as cooperative energy harvesting, where IoT devices share harvested energy with nearby devices, could provide a sustainable energy solution for long-term MIoT networks [195].
- **AI-Assisted Energy Management:** The application of AI for optimizing energy management in real-time,

TABLE V
COMPARISON OF ENERGY EFFICIENCY APPROACHES IN MIoT NETWORKS.

Approach	Proposed Solutions	Challenges Addressed	Advantages	References	Key Technical Insights	Typical Metrics
Machine learning-based optimization	Adaptive learning models to optimize energy consumption	High computation cost and large-scale data management	High efficiency and dynamic adaptation	[178], [179]	Adaptive optimization can significantly reduce power draw, but requires computational resources that may exceed device capabilities.	On-device inference energy: ~10–200 μJ per inference (depending on model/hardware). Training cost higher (mJ–J).
Sleep/Wake scheduling	Periodic wake-up and sleep cycles to save energy in IoT devices	Latency and synchronization	Low energy consumption during idle times	[180], [181]	Very effective for static, delay-tolerant applications; performance may degrade with high mobility or bursty traffic.	Duty-cycle example: 1% duty-cycle can extend battery life by ×50–100; sleep currents 10 μA achievable on many MCUs.
Low-power communication protocols	Implementation of low-power communication like LoRa and NB-IoT	Limited data rate and range	Ultra-low power consumption	[182], [183]	Best suited for sparse, low-data-rate deployments; limited suitability for real-time or high-throughput MIoT applications.	LoRaWAN: ~0.05–0.44 mJ per uplink message; NB-IoT: ~1.7 mAh per 44-byte uplink.
Energy harvesting techniques	Use of environmental energy sources for IoT devices	Environmental dependency and inconsistent energy supply	Extended device lifetime and self-sustainability	[184], [185]	Enables near-perpetual operation in ideal conditions; performance depends heavily on environmental factors.	Typical harvested power: ~1–1000 μW (solar, RF, thermal); usable duty-cycle highly variable by environment.
Edge computing	Computation offloading to edge devices to reduce energy consumption in central servers	Network scalability and latency	Energy savings by localizing processing	[186], [187]	Reduces transmission energy by processing locally; requires reliable edge infrastructure and orchestration.	Transmission vs local compute: local inference can reduce network-transmission energy by up to ~50–90% depending on payload and model.
Wake-up radios	Ultra-low-power receivers that activate devices only when needed	Integration complexity and limited communication range	Significant energy savings by reducing idle listening	[188], [189]	Highly effective in event-driven MIoT scenarios; range limitations may require hybrid connectivity solutions.	Wake-up receiver consumption: ~1–10 μW; reduces idle listening energy by orders of magnitude for sparse traffic patterns.

through adaptive algorithms that adjust network settings based on environmental factors and user demands, will play a key role in future energy-efficient MIoT systems [196].

- **Energy-Efficient Modulation Schemes:** Advanced modulation techniques designed to optimize energy usage in IoT networks, such as adaptive modulation and coding, are expected to be a future area of focus in both academia and industry [197].

In conclusion, addressing energy efficiency in MIoT requires a combination of innovative hardware solutions, adaptive protocols, and intelligent energy management systems. Continuous advancements in technologies such as 6G, edge computing, and AI are essential to overcoming the challenges faced by MIoT systems in achieving sustainable, scalable, and energy-efficient networks.

D. Security and Privacy

The rapid expansion of massive IoT networks has introduced numerous security and privacy risks due to the extensive number of connected devices, heterogeneous architectures, and diverse use cases. Ensuring the secure operation of MIoT ecosystems is challenging because of the inherent limitations of many IoT devices, which include constrained computing power, limited energy resources, and lack of standardized security protocols. This section provides an in-depth discussion of the challenges, proposed solutions, and future directions for improving security and privacy in MIoT systems.

1) Challenges in Security and Privacy: Several specific challenges hinder the effective implementation of security and privacy in MIoT environments:

- **Device Authentication and Authorization**: Managing authentication for billions of IoT devices is an immense task. Many IoT devices have limited processing capabilities, making traditional cryptographic algorithms unsuitable for large-scale deployment. Solutions must be lightweight, scalable, and capable of dealing with resource-constrained devices [198], [199].
- **Data Integrity and Confidentiality**: Data collected and transmitted by IoT devices is often sensitive, such as healthcare or industrial data. Ensuring that data is both

confidential and unaltered while traveling through insecure networks is a key challenge [200]. Encryption schemes must account for the computational limits of devices while maintaining strong security.

- **Privacy of Users and Devices**: MIoT networks often collect vast amounts of personal and contextual data from users. Protecting user privacy during data processing and sharing is essential, especially when IoT devices are deployed in sensitive environments such as smart homes or healthcare [201].

- **Scalability of Security Mechanisms**: The sheer scale of MIoT networks, which can encompass millions or billions of devices, creates challenges in scaling security mechanisms. Solutions need to maintain performance while protecting the vast number of devices in the network.

- **Secure Firmware and Software Updates**: Vulnerabilities in MIoT devices often emerge due to outdated firmware or software. Secure and scalable update mechanisms are required to ensure devices are patched without compromising security or overwhelming network resources [202].

- **Physical Security**: Many IoT devices are deployed in remote or unsupervised environments, making them susceptible to physical tampering and attacks. Ensuring physical protection and tamper-proofing of devices remains a significant challenge [203].

2) Contemporary solutions: Several research efforts have proposed novel solutions to address security and privacy concerns in MIoT:

- **Lightweight Cryptographic Algorithms**: Lightweight cryptographic algorithms have been developed to secure communications in resource-constrained IoT devices. These algorithms focus on reducing the computational complexity and energy consumption while maintaining robust security. For example, symmetric encryption techniques and lightweight hashing functions have been proposed to meet the needs of MIoT devices [198].

- **Blockchain-Based Solutions**: Blockchain technology has been explored for its potential to enhance security in MIoT networks. By creating decentralized and tamper-proof records, blockchain can be used for secure device authentication, data integrity, and transaction security [199]. Blockchain solutions eliminate the need for centralized trust, making the network more resilient to attacks.

- **AI-Driven Intrusion Detection Systems**: Machine learning and AI techniques have been employed to detect and mitigate security threats in MIoT networks. These AI-driven intrusion detection systems (IDS) continuously monitor network traffic and detect anomalies, allowing for real-time threat detection and response [204], [205], [209].

- **Edge Computing for Enhanced Security**: Edge computing offers a distributed model where security operations, such as data encryption, authentication, and anomaly detection, can be handled closer to the data source. This reduces latency and enables real-time processing of

security tasks, alleviating the load on centralized cloud servers [210].

Table VI summarizes several proposed solutions for security and privacy in MIoT.

3) Future Directions: As MIoT networks continue to evolve, security and privacy research must focus on future challenges and directions:

- **Post-Quantum Cryptography**: With the potential advent of quantum computers, traditional encryption methods may become vulnerable to attacks. Research into post-quantum cryptography is crucial to develop encryption techniques that can resist quantum-based threats [207].

- **Zero Trust Architecture**: Implementing a zero trust security model, where no device or user is inherently trusted, is becoming more relevant in large-scale MIoT networks. This approach minimizes the attack surface and ensures that security controls are applied consistently across all devices [208].

- **Federated Learning for Distributed Security**: Federated learning offers a novel approach to enhancing security in MIoT networks. By allowing devices to collaboratively learn security models without sharing raw data, federated learning can improve security and privacy while maintaining data locality [211].

- **Self-Healing Systems**: Future MIoT networks could benefit from self-healing systems that automatically detect and respond to security breaches. These systems would autonomously restore functionality, mitigate attacks, and enhance network resilience [212].

The future of MIoT security and privacy requires not only new cryptographic techniques and AI-driven security frameworks but also a comprehensive, multi-layered approach that integrates these techniques across the network infrastructure.

E. Interdependencies and Trade-offs among MIoT Dimensions

Although network scalability, data management, energy efficiency, and security/privacy are often analyzed separately in the literature, these four pillars are **deeply interdependent** in real MIoT deployments. Optimizing one dimension frequently introduces constraints on another. Understanding these interactions is central to designing viable and sustainable MIoT systems at scale.

1) Security vs. Energy Efficiency and Latency: Stronger cryptographic mechanisms (e.g., AES-128/256, ECC-256) increase computational demand on constrained microcontrollers, inflating both energy consumption and end-to-end latency. The energy cost of cryptographic processing can be approximated as:

$$E_{\text{crypto}} = C_{\text{cycles}} \times E_{\text{cycle}}, \tag{1}$$

where C_{cycles} represents the number of CPU cycles required for an encryption or decryption operation. Transitioning from lightweight ciphers such as SPECK or PRESENT ($\sim$ 10–30k cycles) to AES-256 or ECC-256 ($\sim$ 150–350k cycles) increases energy consumption by **5–10$\times$** on Cortex-M0/M3 devices [213].

In healthcare IoT, AES-256 may consume **25–40% more energy per packet** than lightweight ciphers and add **30–70**

TABLE VI
COMPARISON OF PROPOSED SOLUTIONS FOR SECURITY AND PRIVACY IN MASSIVE IoT.

Proposed Solution	Technique Used	Advantages	Challenges	References	Key Technical Insights
Lightweight cryptographic algorithms	Symmetric encryption, lightweight hashing	Energy-efficient, computationally feasible for resource-constrained IoT devices	Limited scalability, potentially weaker than traditional encryption methods	[198]	Ideal for low-power nodes; however, may require hybrid security layers to handle evolving threats.
Blockchain-based authentication	Decentralized, tamper-proof record-keeping	Enhanced device authentication, data integrity, decentralized trust	High computational overhead, latency in large-scale deployments	[199]	Improves trust in MIoT, but scalability remains an issue without lightweight consensus mechanisms.
AI-driven intrusion detection systems (IDS)	Machine learning-based anomaly detection	Real-time threat detection, adaptable to new threats, scalable	High computational requirements, data privacy concerns	[204], [205]	Effective against novel attacks; may require edge-based inference to reduce latency and energy costs.
Edge computing for security	Distributed security processing at the edge	Low latency, efficient resource utilization, real-time processing	Limited processing capabilities of edge nodes, synchronization between edge and cloud	[140], [206]	Suitable for latency-sensitive applications; demands careful orchestration to avoid data inconsistency.
Post-quantum cryptography	Quantum-resistant cryptographic algorithms	Resistant to quantum computing threats, secure for future IoT networks	High computational complexity, energy consumption	[207]	Future-proof security but impractical for current low-power MIoT nodes without hardware acceleration.
Zero trust architecture	Continuous verification, micro-segmentation	Reduces attack surface, ensures consistent security across devices	Implementation complexity, high resource consumption	[208]	Highly robust for heterogeneous IoT environments; best deployed incrementally to manage complexity.

ms latency on MCUs operating below 100 MHz [214]. Such overheads directly challenge URLLC requirements.

2) Scalability vs. Latency and Reliability: As device density increases (e.g., up to 10^5–10^6 devices/km^2), contention-based access such as grant-free or random access suffers from elevated collision probability. The probability of collision in a slot can be approximated by:

$$P_{\text{coll}} \approx 1 - e^{-\lambda T}, \qquad (2)$$

where λ is the device activation rate and T the slot duration. Higher P_{coll} leads to retransmissions, queueing delay, and increased energy expenditure, showing that *scalability, latency, and energy efficiency are tightly coupled through interference dynamics*.

3) Data Aggregation vs. Freshness and Granularity: Data aggregation reduces transmission load and energy consumption but increases the *Age of Information (AoI)* and reduces data granularity. Aggressive aggregation can increase AoI by **20–60%**, degrading the performance of AI-based MIoT analytics and real-time monitoring applications [214].

4) Post-Quantum Security vs. Energy Constraints: Lattice-based post-quantum cryptography (PQC) provides resistance against quantum attacks but incurs substantial computation overhead. Benchmarks on Cortex-M0/M4 and ESP32 platforms show **10–100 μJ per PQC operation**, exceeding the typical energy budget (5–20 μJ per operation) of battery-powered MIoT nodes [215]. PQC is therefore unsuitable for massive low-power deployments in its current form.

5) Edge Computing as a Mitigation Mechanism: Edge computing mitigates several of the above trade-offs by offloading computation closer to data sources:

- reduces raw-data transmission overhead,
- offloads heavy cryptographic operations to edge nodes,
- decreases end-to-end latency,
- alleviates cloud congestion and core-network load.

Such hybrid edge–cloud designs are particularly beneficial for latency-sensitive and security-critical MIoT systems [216].

6) Cross-Dimensional Mitigation Strategies:

- **Adaptive Security:** Adjust encryption strength dynamically based on battery level and data sensitivity [214].
- **Hardware-Accelerated Cryptography:** Dedicated AES/ECC accelerators reduce energy consumption by **3–7$\times$** compared to software implementations [217].
- **Hybrid Edge–Cloud Architectures:** Use local processing for delay-sensitive tasks while delegating heavy analytics to the cloud.

In summary, the four core MIoT dimensions are tightly interconnected. A **holistic joint-optimization approach** is necessary to maintain performance, security, energy sustainability, and scalability under real-world operational constraints. Figure 3 shows the key interdependencies and trade-offs among MIoT dimensions.
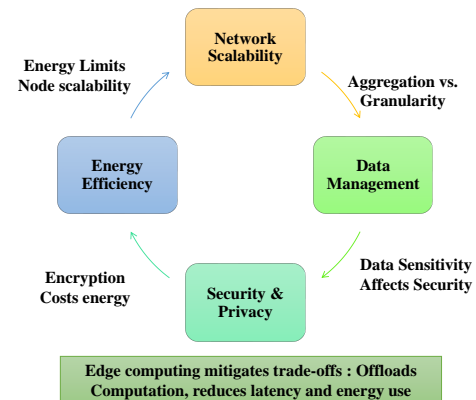

Fig. 3. Interdependencies and trade-offs among core MIoT dimensions.

IV. ADVANCED COMMUNICATION TECHNIQUES (PHY/MAC LAYER)

This section presents advanced communication and access techniques essential for supporting the massive scale and stringent performance requirements of MIoT systems. By focusing on physical and MAC-layer solutions such as non-orthogonal multiple access (NOMA), grant-free access, and sparse code multiple access (SCMA), we explore methods that enable efficient spectrum utilization, minimize latency, and improve connectivity density. These foundational technologies directly address the challenges of massive device access, interference mitigation, and ultra-reliable low-latency communications.

A. Grant-Free Access

Grant-free access allows devices to transmit data without requiring a scheduling request, which is particularly advantageous for MIoT environments with a high density of low-power devices. By eliminating the need for channel reservations, grant-free access minimizes latency and reduces energy consumption, making it suitable for time-sensitive and energy-constrained applications [218]. This approach has shown significant improvements in uplink performance, supporting thousands of devices per base station with minimal delay [219]. Recent studies also highlight its potential integration with machine learning to optimize access protocols dynamically [220].

Grant-free access mechanisms contribute to enhanced network scalability by alleviating congestion, particularly in networks with extensive device connections. In scenarios where a large number of IoT devices require frequent, low-data-rate communication, traditional grant-based methods can lead to significant signaling overhead, limiting network capacity [221]. Grant-free access bypasses this by permitting devices to send data directly, thereby increasing the total number of supported devices and optimizing the allocation of spectral resources [222]. This improvement is especially relevant in applications such as smart cities and industrial automation, where a high density of IoT devices operates within constrained frequency bands.

For IoT applications where devices are often battery-powered and operate in remote locations, energy efficiency is paramount. Grant-free protocols reduce energy expenditure by minimizing signaling and allowing for rapid data transmission. By avoiding the need for repeated handshakes and allocation processes, grant-free access conserves device energy and extends operational lifetimes, a critical factor for large-scale IoT deployments in sectors like agriculture and environmental monitoring [223]. Additionally, combining grant-free methods with energy-harvesting techniques holds promise for sustaining device functionality in energy-constrained MIoT scenarios [224].

B. Non-Orthogonal Multiple Access (NOMA)

NOMA enables simultaneous transmission of multiple users over the same time–frequency resource by assigning different power levels to different devices. This power-domain multiplexing increases spectral efficiency and enhances connectivity, making NOMA attractive for MIoT scenarios where thousands of devices must share limited radio resources [225].

The key principle of NOMA relies on superposition coding at the transmitter and successive interference cancellation (SIC) at the receiver [226]. Users with strong channel gains are allocated lower power, while weaker users receive higher power. At the receiver, SIC iteratively decodes signals according to their power ordering. In MIoT settings, this allows flexible user prioritization: critical or emergency IoT devices can be assigned higher power for reliable decoding [227].

Recent works explore hybrid NOMA combinations to further enhance performance. For example, Cooperative-NOMA allows nearby devices to relay messages, improving coverage and reliability in remote IoT deployments [228]. Machine learning techniques have also been integrated for real-time power control and interference management, enabling dynamic adaptation to network conditions [229]. In addition, the combination of NOMA with Cognitive Radio helps alleviate spectrum scarcity by enabling opportunistic spectrum access in industrial IoT scenarios [230], [231]. Multi-carrier NOMA (MC-NOMA) further reduces computational load by grouping users across subcarriers, improving spectral efficiency and supporting high device density [232].

Overall, NOMA provides flexible user prioritization, high connectivity, and strong integration potential with emerging 5G/6G technologies, highlighting its relevance in ultra-dense MIoT deployments.

1) Practical Implementation Challenges and Mitigation Strategies: Although NOMA offers theoretical performance gains, several practical issues arise in MIoT deployments:

- **SIC computational complexity:** SIC decoding grows approximately linearly with the number of superposed users, i.e.,

$$\mathcal{O}(K),$$

  where K is the number of user layers [233]. In MIoT networks with many devices per resource block, this leads to significant processing delay and energy consumption. Measurements report SIC energy costs on the order of several millijoules per decoding cycle for IoT-grade radios.
- **Latency and error propagation:** SIC relies on accurate channel estimation. In low-SNR environments typical of battery-powered sensors, decoding errors in early stages propagate through subsequent layers, degrading reliability. This is especially problematic for URLLC-style IoT applications.
- **Power allocation instability:** At high device density, dynamic channel variations make it difficult to maintain optimal power ratios, causing decoding failures and reducing spectral gains.

To address these issues, recent works propose low-complexity SIC variants such as PIC or MF-SIC [234], hybrid NOMA–OMA clustering to limit SIC depth, and ML-assisted power control for adaptive parameter tuning [235]. These strategies aim to balance spectral efficiency, latency, and

energy usage—three constraints that are critical in practical MIoT deployments.

C. Cooperative Communication and Relaying

Cooperative communication in MIoT networks utilizes relay nodes to enhance network coverage, improve signal reliability, and reduce power consumption, especially in areas with limited infrastructure or difficult environmental conditions. In MIoT, devices communicate through nearby relays rather than establishing direct links, which boosts both energy efficiency and connectivity. This approach is essential in applications such as remote agriculture, environmental monitoring, and industrial IoT, where direct connections to base stations are not always feasible [236].

- **Relay-Based Architectures:** Relay-based communications in MIoT include amplify-and-forward (AF) and decode-and-forward (DF) schemes.
  - *Amplify-and-Forward (AF):* Relays amplify the received signal and forward it, which is beneficial in scenarios with low processing power requirements.
  - *Decode-and-Forward (DF):* DF relays decode and re-encode signals before transmission, providing higher reliability, but requiring more processing power [237].

  Relay-based architectures improve network robustness by enabling devices to rely on intermittent transmissions, reducing the need for direct, continuous connections to the base station [238]. Studies show that cooperative relay networks can improve energy efficiency by up to 30%, particularly when combined with compressive sensing techniques that help reduce data redundancy [239].
- **Multi-Hop Relaying and its Benefits:** Multi-hop relaying, where signals pass through multiple relay nodes, offers significant advantages for MIoT.
  - This approach reduces the energy load on individual devices, enabling extended connectivity over large distances—beneficial in widely dispersed environments such as rural agriculture [240].
  - Multi-hop cooperative networks can also mitigate interference and improve quality QoS in dense MIoT environments [241].

  Research has shown that multi-hop networks improve scalability by dynamically adjusting relay paths according to network conditions and energy availability [240].
- **Compressive Sensing (CS) and Cooperative Communication:** Integrating compressive sensing with cooperative communication is a growing trend in MIoT, reducing the amount of transmitted data and conserving energy and bandwidth.
  - CS enables data reduction by exploiting the sparse nature of signals, which is particularly advantageous in applications with high data redundancy [239].
  - Combined with cooperative relaying, CS can reduce transmission frequency, extending the operational life of energy-constrained devices [242].
- **ML and Dynamic Relay Selection:** Recent advancements have applied machine learning to dynamically optimize relay selection, improving energy efficiency and service quality.
  - ML-based relay selection techniques, such as reinforcement learning, adaptively manage relay resources based on network status, energy levels, and traffic demand [243].
  - ML-driven relay selection improves network adaptability, making MIoT systems more resilient to changes in topology and demand, particularly beneficial in industrial IoT [244].

In summary, cooperative communication and relaying provide significant advantages for scalable and energy-efficient MIoT networks. By incorporating compressive sensing and machine learning, these techniques continue to evolve as robust solutions for the connectivity challenges in diverse IoT applications. Future research should focus on enhancing relay selection algorithms and developing new cooperative strategies to maximize efficiency and reliability in ultra-dense MIoT environments.

D. Compressive Sensing (CS)

CS has gained prominence in MIoT due to its ability to significantly reduce the volume of transmitted data by capturing only the most critical information, making it ideal for applications with strict energy and bandwidth limitations, such as environmental monitoring and smart metering [245]. Leveraging the sparsity in data—where most data points carry redundant or non-essential information—CS allows MIoT devices to transmit compressed signals, which can be reconstructed with high accuracy at the receiver, thus conserving both energy and bandwidth resources [246].

- **Data Sparsity and Energy Conservation:** Compressive sensing takes advantage of the sparse nature of data in many MIoT applications. For example, environmental monitoring data (such as soil moisture or temperature readings) often changes gradually over time, leading to highly compressible signals. By transmitting only key data points, CS minimizes energy expenditure on data transmission, enabling prolonged device lifespans in remote or energy-constrained settings [247].
- **Integration with Edge Computing:** A recent trend in CS-based MIoT is its integration with edge computing. By moving part of the CS processing to edge nodes close to data sources, MIoT systems reduce reliance on centralized cloud infrastructure, which, in turn, decreases latency and enhances real-time performance in large-scale applications [248]. This combination is especially beneficial in use cases like real-time traffic monitoring, where delays could impact the effectiveness of data-driven insights [249].
- **Adaptive Sensing and Machine Learning Enhancements:** Recent research has introduced adaptive CS methods, where devices adjust their sensing parameters based on the data's sparsity level and network conditions. By incorporating machine learning algorithms to predict optimal compression ratios, adaptive CS can further reduce

data transmissions while maintaining high data fidelity [250].

- **Compressed Data Aggregation Techniques:** Another development is compressed data aggregation, where multiple devices jointly compress and aggregate their data before transmission. In multi-device MIoT scenarios, this approach reduces network congestion and prevents data duplication, which is particularly useful in applications like industrial IoT and remote sensing [251].

Despite its benefits, CS in MIoT still faces challenges, particularly in handling high-dimensional data and in achieving reconstruction accuracy in noisy environments. Researchers are exploring hybrid CS methods that combine CS with denoising algorithms to improve signal fidelity, as well as distributed CS frameworks that distribute computation across edge nodes, offering enhanced scalability for ultra-dense IoT deployments [246].

In summary, compressive sensing provides a highly effective solution for conserving bandwidth and energy in MIoT applications, especially when combined with edge computing and machine learning. Future advancements are likely to focus on adaptive sensing techniques and robust data aggregation to further enhance scalability and efficiency in diverse MIoT environments.

E. Cloud Radio Access Network (C-RAN)

C-RAN is a centralized architecture that consolidates Baseband Units (BBUs) in a central location, allowing for more dynamic and efficient resource management. In traditional networks, BBUs are distributed across cell sites, but in C-RAN, these units are pooled in a central data center, enabling flexible resource allocation based on real-time network demand. This centralization not only enhances network scalability in urban and high-density settings but also optimizes hardware utilization and reduces operational costs [252].

- **Enhanced Scalability and Flexibility:** The pooling of BBUs in C-RAN architecture provides a flexible allocation of resources, supporting the massive connectivity required in MIoT applications, such as smart cities and large-scale industrial automation. C-RAN's centralized structure enables operators to quickly adapt to fluctuating network demands, significantly enhancing scalability in MIoT ecosystems [253].
- **Latency Reduction with Edge Integration:** Recent studies suggest that integrating C-RAN with edge computing frameworks can minimize latency and boost real-time data processing capabilities. For instance, edge computing can be employed to perform preliminary data processing close to the IoT devices, reducing the need for data to travel back to centralized BBUs, which is especially critical for latency-sensitive applications like autonomous transportation and healthcare monitoring [254], [255].
- **Energy Efficiency and Power Management:** C-RAN can also contribute to energy efficiency, a crucial consideration in MIoT, by enabling more granular control over power allocation. By deactivating idle BBUs or adjusting power based on traffic load [256]. Techniques like dynamic spectrum allocation within C-RAN also further reduce unnecessary energy expenditure, benefiting both operators and the environment [25].
- **Network Slicing Compatibility for MIoT Services:** An added advantage of C-RAN is its compatibility with network slicing, where specific resources can be dedicated to different MIoT services within the same physical infrastructure. For instance, one slice could prioritize low-latency requirements for real-time applications, while another could focus on high-bandwidth services. This adaptability is invaluable for complex IoT ecosystems such as smart cities, where diverse applications must coexist seamlessly [257].

Despite its benefits, C-RAN faces challenges related to data center infrastructure requirements and fronthaul limitations. High-capacity fronthaul connections are essential to link distributed Remote Radio Heads (RRHs) to centralized BBUs, which can be costly and complex to implement in areas with limited fiber infrastructure. Researchers are currently investigating solutions such as wireless fronthaul alternatives and hybrid C-RAN/Distributed RAN models to address these challenges and make C-RAN more accessible for large-scale MIoT deployment [258]. C-RAN presents a scalable, efficient solution for managing massive connectivity and dynamic traffic in MIoT applications. Its combination with edge computing, energy-efficient practices, and compatibility with network slicing highlights its potential to meet the diverse and demanding requirements of future MIoT networks.

F. Sparse Code Multiple Access (SCMA)

SCMA extends the principles of NOMA by mapping user data directly to multi-dimensional sparse codewords, enabling a large number of IoT devices to share limited frequency resources with low collision probability [259]. The sparsity of SCMA codebooks reduces mutual interference and supports massive connectivity—an essential property for MIoT systems where devices transmit small and sporadic packets [262].

- **Interference Mitigation and Spectrum Efficiency:** Sparse coding significantly reduces interference by ensuring that only a subset of codeword elements overlaps among users. This enables high-density deployments such as smart healthcare and environmental sensing [263].
- **ML-Enhanced Decoding:** Deep learning–based SCMA decoders can learn complex channel behaviors and reduce detection iterations compared to classical message passing, improving performance in noisy and time-varying MIoT environments [264], [265].
- **Applications in Healthcare and Environmental Monitoring:** SCMA is increasingly adopted for continuous monitoring applications, where reliable low-power transmissions from many sensors are required [266].

Ongoing research explores optimized codebook design and the integration of SCMA with 6G edge computing frameworks to enhance support for URLLC applications [267].

TABLE VII
COMPARATIVE ANALYSIS OF SCALABLE TECHNIQUES IN MIoT.

Technique	Reference	Network Scalability	Data Management	Energy Efficiency	Security/ Privacy	Advantages	Drawbacks	Key Technical Insights
Grant-Free Access	[219]	✓	✓			Efficient in high device density; reduces latency	Potential collisions in dense networks; limited QoS	Best for ultra-dense MIoT with sporadic traffic; requires collision mitigation strategies like advanced scheduling.
Non-Orthogonal Multiple Access (NOMA)	[225]	✓	✓	✓		Improved spectral efficiency; energy-saving	Complexity in power allocation; interference risks	Maximizes spectral efficiency; power-domain and code-domain variants can be tuned for energy-constrained devices.
Cooperative Communication	[236]	✓		✓		Extends network coverage; saves power	Increased relay node costs; potential delays	Useful for coverage extension in rural MIoT; optimal relay selection reduces delays and energy usage.
Compressed Sensing (CS)	[245]	✓	✓	✓		Reduces data load; saves bandwidth	Quality degradation under high compression	Effective for sparse MIoT data streams; requires careful tuning of compression ratios to preserve data integrity.
Cloud-Radio Access Network (C-RAN)	[252]	✓	✓		✓	Efficient resource utilization; centralized management	Latency concerns; data privacy risks	Centralizes MIoT resource control; edge integration can mitigate latency and privacy issues.
Sparse Code Multiple Access (SCMA)	[259]	✓		✓		Increases user capacity; lowers transmission power	High decoding complexity; power allocation required	Suited for dense uplink MIoT; requires low-complexity decoders for constrained devices.
Multi-RAT Systems	[260]	✓	✓	✓		Balances load across networks; supports device heterogeneity	Complexity in protocol compatibility; potential interference	Enables seamless MIoT connectivity; dynamic RAT selection improves QoS in mixed environments.
Hybrid Access Techniques	[261]	✓	✓	✓	✓	Flexible combination of techniques; adaptive to needs	Complexity in protocol design; interoperability issues	Combines benefits of multiple access schemes; AI-based adaptation improves performance in diverse MIoT deployments.

1) Practical Implementation Challenges and Mitigation Strategies: Despite its advantages, SCMA faces several practical challenges:

- **Codebook Design Complexity:** Optimal sparse codebook design is combinatorial and grows rapidly with the number of users and modulation order. Codebook optimization often requires high-dimensional search and can exceed the capabilities of constrained IoT nodes [268].
- **Storage and Management Overhead:** Large codebooks must be stored, distributed, and updated across millions of devices. This creates signaling overhead and memory demands that challenge small IoT microcontrollers [269].
- **Detection Complexity:** SCMA decoding typically relies on Message Passing Algorithms whose complexity is approximately

$$\mathcal{O}(d_f M^{d_f}),$$

where d_f is the factor-node degree and M is the codebook size [270]. This exponential relationship imposes high energy and latency costs for sub-100 MHz IoT devices.

Recent mitigation approaches include stepwise or hierarchical codebook construction [269], hybrid allocation to reduce memory footprint, and ML-based detection that reduces the number of message-passing iterations [271]. These innovations improve scalability and reduce energy consumption, making SCMA more suitable for real-world MIoT deployments.

G. Multi-RAT Systems

In the pursuit of scalable and resilient MIoT architectures, Multi-Radio Access Technology (Multi-RAT) systems offer significant promise by enabling devices to seamlessly connect to multiple network technologies concurrently. Multi-RAT systems integrate various radio access technologies—such as Wi-Fi, LTE, and 5G, with potential extensions to future 6G networks—to adaptively meet the demands of diverse MIoT applications [260], [272]. This integration addresses a key challenge in MIoT scalability by enabling efficient use of available network resources while supporting heterogeneous device connectivity in real-time. For instance, IoT devices in smart cities can leverage LTE for wide-area coverage and

Wi-Fi for high-throughput data transmission when available, thereby optimizing bandwidth and reducing congestion [273].

An important feature of Multi-RAT systems is their ability to support dynamic resource allocation. With adaptive multi-channel access, these systems can balance the load across different frequencies and reduce interference, enhancing network reliability and reducing latency [274]. Multi-RAT systems also facilitate advanced QoS provisioning, which is crucial for handling latency-sensitive applications such as autonomous driving and telemedicine. Furthermore, they enhance energy efficiency by allowing devices to switch to lower-power communication modes depending on network conditions [275].

However, multi-RATs systems also face substantial challenges. The management of handovers and interference between various RATs demands sophisticated algorithms capable of real-time decision-making. High hardware complexity is another challenge, as IoT devices must be equipped with multiple communication modules, potentially impacting device costs and energy usage [276]. Future research will likely focus on optimizing Multi-RAT architectures through advanced AI-based algorithms for predictive resource management and interference mitigation, as well as exploring hybrid frameworks that combine Multi-RAT with other scalable solutions like SDN and CRN [22], [277]. These developments are expected to position Multi-RAT as a foundational technique in scalable MIoT deployments.

H. Hybrid Access Techniques

Hybrid access techniques, such as Non-Orthogonal Multiple Access with Orthogonal Frequency Division Multiple Access (NOMA-OFDMA), combine multiple access methods to optimize network performance across diverse scenarios. These hybrid approaches are designed to adapt flexibly to varying data traffic patterns and network conditions, balancing spectral efficiency, latency, and energy consumption. Hybrid techniques are particularly well-suited for MIoT applications that require both high data rates and low latency, such as real-time industrial monitoring and smart city infrastructure [261].

- **Enhanced Resource Allocation and Flexibility:** Hybrid methods like NOMA-OFDMA allow dynamic resource allocation by combining the spectral efficiency of NOMA with the robustness of OFDMA in handling high device densities. For instance, hybrid methods can allocate more resources to high-priority tasks, such as critical data from medical monitoring devices, while reserving fewer resources for less time-sensitive tasks [278].
- **Energy Efficiency and Reduced Consumption:** Hybrid access techniques have been shown to reduce energy consumption significantly—by approximately 20-30%—when compared to traditional access methods. This energy efficiency is achieved by adaptively switching between NOMA and OFDMA based on current network load and requirements, making these methods suitable for energy-intensive MIoT applications, such as remote environmental monitoring and industrial automation [278].
- **Application in Diverse MIoT Environments:** Hybrid methods support a wide range of MIoT use cases. In

smart city applications, for example, hybrid access systems can adjust connectivity resources based on real-time demands from sensors and actuators, ensuring efficient energy usage and network performance. In industrial automation, hybrid access helps maintain stable connectivity even under heavy network loads, supporting continuous data exchange in processes like predictive maintenance [279].

Ongoing research in hybrid access focuses on integrating these techniques with machine learning algorithms to optimize resource allocation further. Machine learning can predict traffic patterns and device requirements, allowing for a more effective allocation of hybrid access resources. Additionally, hybrid methods are being explored for compatibility with emerging 6G networks, which promise ultra-low latency and high device density capabilities [280].

Hybrid access techniques offer a versatile solution for managing the diverse requirements of MIoT systems, providing flexibility, scalability, and energy efficiency across various application domains. Their adaptability positions them as a key component in the evolution of next-generation IoT networks. Each of these techniques offers unique solutions to MIoT challenges, and their combination holds promise for creating adaptable, efficient, and robust MIoT systems. Continued innovation in these areas is essential to meet the growing demands of MIoT applications in diverse fields. Table VII provides a comparative analysis of some existing scalable techniques for massive IoT.

V. ANALYTICAL AND INTELLIGENCE TOOLS (SYSTEM AND APPLICATION LAYERS)

In contrast, this section addresses computation and intelligence tools designed to optimize MIoT networks at the system and application layers. We delve into artificial intelligence and machine learning methods, game-theoretic frameworks, and optimization algorithms that facilitate adaptive resource allocation, distributed control, and decision-making under uncertainty. These tools play a critical role in enabling scalable, autonomous, and robust operation of MIoT deployments by transforming data into actionable insights and orchestrating complex network behaviors.

A. Game Theory for Resource Allocation

Game theory has emerged as a promising approach to manage resource allocation and optimize MIoT network performance under competitive or cooperative scenarios. In high-density MIoT networks, devices often compete for limited resources such as bandwidth and power. Game theory provides strategic frameworks that allow devices to make autonomous decisions that balance individual utility with overall network efficiency [281].

Specifically, in cooperative game-theoretic approaches, MIoT devices collaborate to maximize shared benefits, such as improving energy efficiency through cooperative relaying and dynamic spectrum access [282]. Non-cooperative game theory, on the other hand, is useful for scenarios where devices compete for resources, such as in power allocation

TABLE VIII
PRACTICAL CHALLENGES AND MITIGATION STRATEGIES FOR GAME-THEORETIC RESOURCE ALLOCATION IN MIoT

Challenge	Description	Mitigation Strategy
Utility Function Modeling	Difficulty in reflecting heterogeneous QoS and energy needs in dynamic settings	Use hybrid, multi-objective utility functions combining throughput, latency, and energy metrics
Convergence Time	Prolonged iterations in large-scale or mobile environments	Apply fast-converging learning algorithms such as regret-minimization and RL-accelerated strategies
Implementation Overhead	High signaling cost for decentralized decision-making	Use edge-assisted computation and clustering to reduce signaling

and interference mitigation tasks. Emerging research has also explored reinforcement learning integrated with game theory for adaptive and decentralized resource management, significantly enhancing network scalability and adaptability in real-time conditions [283].

1- Cooperative Game Theory: In cooperative game-theoretic approaches, MIoT devices collaborate to maximize shared benefits. For example, cooperative relaying allows devices with limited range or power to communicate through intermediary nodes, extending coverage and saving energy. DSA can be improved with cooperative games by allowing devices to share spectrum opportunities more efficiently, reducing interference in crowded networks [284]. Cooperative games also aid in power control for energy savings, which is crucial in battery-operated IoT devices [281].

These cooperative strategies enable various enhancements in MIoT networks, including the following key techniques :

- *Dynamic Spectrum Sharing*: Efficiently allocates unused spectrum to devices with low latency needs [285].
- *Relay Selection and Data Offloading*: Reduces device workload and conserves energy by offloading data through cooperative relays [286].
- *Interference Management*: Devices collaborate to minimize interference, increasing data transmission reliability and network throughput [282].

2- Non-Cooperative Game Theory: Non-cooperative game theory is essential when MIoT devices operate independently and may compete for shared resources. In a typical non-cooperative setup, each device acts in its own interest, often without regard to the impact on other devices. This approach is especially useful in dense MIoT scenarios where many devices transmit simultaneously. Game-theoretic techniques like Nash Equilibrium allow devices to reach stable states where no device can improve its performance unilaterally. This is beneficial for applications like power allocation, spectrum access, and interference mitigation [283].

Several key techniques leverage non-cooperative game theory to optimize resource allocation and maintain network efficiency in competitive MIoT environments:

- *Power Allocation*: Optimal power levels are assigned to each device to ensure efficient spectrum utilization, minimizing the risk of interference.
- *Bandwidth Sharing*: Allocates bandwidth in high-density networks to prevent congestion and enhance throughput.
- *Interference Mitigation*: Devices autonomously adjust their parameters to minimize interference with others, maintaining efficient communication [299].

3- Reinforcement Learning and Game Theory Integration: Reinforcement learning (RL) integrated with game theory has shown significant promise in MIoT due to its adaptability and scalability. RL-based game-theoretic approaches allow devices to learn optimal strategies in real-time by interacting with their environment. This hybrid approach is beneficial for applications that require flexible adaptation to dynamic network conditions, such as real-time spectrum allocation and device power management [179], [281].

- *Real-Time Adaptability*: RL allows devices to adjust strategies based on evolving network conditions.
- *Scalability*: Scalable decision-making is essential for MIoT networks with thousands of devices.
- *Enhanced Efficiency*: Reduces energy use and increases throughput by enabling efficient, real-time resource management [300].

4- Practical Challenges and Mitigation Strategies: Despite its potential, applying game theory in MIoT faces several technical challenges:

- **Utility Function Modeling:** Accurately defining utility functions is difficult in dynamic MIoT environments where QoS requirements, channel conditions, and energy constraints vary over time [301]. Hybrid utility functions combining throughput, latency, and energy efficiency metrics have been proposed to improve realism [302].
- **Convergence Time:** Non-cooperative and repeated games may require many iterations to converge, especially in mobile or ultra-dense IoT networks. Fast-converging algorithms, such as regret-minimization and learning-augmented games, have been shown to reduce convergence time significantly [303].
- **Implementation Overhead:** Decentralized game solutions can impose heavy signaling overhead for strategy exchange. Edge-assisted coordination has been suggested to offload computation and reduce control message exchange [304].

Table VIII summarizes these challenges and potential mitigation strategies.

Game theory offers flexible, powerful tools for managing MIoT resources. Cooperative approaches enhance collaborative tasks like relaying and spectrum sharing, while non-cooperative methods optimize competitive tasks such as power allocation. The integration of RL with game theory enables adaptive, efficient resource allocation, further boosting the performance and scalability of MIoT networks.

TABLE IX
MFG vs. Traditional Game Theory in MIoT.

Aspect	MFG Theory	Traditional Game Theory	References
Scalability	Handles large-scale IoT networks efficiently by approximating population dynamics using mean-field equations.	Struggles with computational complexity as the number of players increases, requiring pairwise interactions.	[287], [288]
Real-Time Adaptability	Enables devices to adapt strategies dynamically based on real-time mean-field trends.	Static solutions or slower adaptability due to reliance on predefined game-theoretic strategies.	[289], [290]
Communication Overhead	Reduces device-to-device communication by aggregating information in the mean field.	Requires frequent exchanges of information for strategy updates between all players.	[291], [292]
Energy Efficiency	Encourages energy-efficient behavior by aligning individual strategies with global network dynamics.	Focuses on local optimization, which may not align with global energy-saving goals.	[293], [294]
Interference Mitigation	Devices adjust autonomously to minimize aggregate interference based on mean-field feedback.	Mitigation relies on direct strategy negotiations or centralized optimization.	[295], [296]
Resource Allocation Flexibility	Offers dynamic spectrum and power allocation based on population dynamics.	Often restricted to predefined, static allocation rules.	[297], [298]

B. Mean Field Game (MFG) Theory

MFG Theory is a powerful tool for managing resource allocation and optimizing system performance in networks with a large number of devices. MFG theory is particularly advantageous in scenarios where the interactions between individual devices and the aggregate behavior of the system must be analyzed. It offers scalability by simplifying the modeling of complex networks and addressing challenges like interference, energy consumption, and resource contention [292].

1- Key characteristics and applications of MFG in MIoT:

- **Scalability for high-density networks:** MFG theory models the collective behavior of a vast number of MIoT devices without requiring explicit pairwise interactions. This scalability is critical for dense MIoT environments, where traditional game-theoretic approaches become computationally infeasible [287], [305].
- **Dynamic resource allocation:** Devices dynamically adapt their strategies by responding to the mean field, which represents the average effect of the population. This approach ensures efficient power allocation, spectrum sharing, and interference mitigation in real-time, adapting to changing network conditions [306].
- **Energy efficiency and lifetime optimization:** MFG enables energy-constrained MIoT devices to optimize their actions, such as reducing transmit power or switching to sleep modes, based on global network trends. This approach extends the lifetime of battery-powered devices while maintaining network performance [282].
- **Interference and congestion management:** By modeling devices' strategies as influenced by mean-field dynamics, MFG allows IoT devices to adjust their parameters to minimize interference and avoid congestion autonomously. This improves data transmission reliability and supports efficient network operation under heavy traffic loads [295].
- **Integration with RL:** RL enhances MFG frameworks by enabling devices to learn optimal strategies in evolving network environments. For example, an MFG-based RL approach can dynamically allocate spectrum resources by learning the distribution of device demands, improving fairness and reducing latency [292].

- **Spectrum Sharing:** Devices dynamically access unused spectrum, balancing their transmission power to minimize interference and maximize spectrum utilization [287].
- **Load Balancing:** In edge-computing environments, MFG enables efficient task offloading by balancing the load among servers, improving processing speed and reducing latency [307].
- **Mobility Management:** In mobile IoT networks, MFG supports the coordination of device handovers to maintain connectivity and reduce power usage during transitions [308].

Table IX provides a point-by-point comparative analysis between MFG theory and traditional game theory in the context of MIoT networks.

C. Artificial Intelligence and Machine Learning

AI and ML have emerged as transformative technologies in the optimization of MIoT networks. AI-driven techniques are crucial for managing the complexity of MIoT ecosystems, enabling efficient resource allocation, dynamic protocol adaptation, and anomaly detection.

a) Federated Learning (FL): FL facilitates distributed model training across IoT devices, preserving user privacy by keeping data localized. FL addresses the challenge of processing data from billions of devices without compromising confidentiality. Recent advancements in FL have enhanced its communication efficiency and model aggregation for resource-constrained devices [33], [309].

b) Deep Reinforcement Learning (DRL): DRL provides real-time, adaptive solutions for dynamic spectrum access, power allocation, and interference management. DRL has demonstrated significant potential in optimizing resource use in ultra-dense IoT deployments, offering a robust framework for decision-making in uncertain environments [33], [300]. Moreover, DRL-based models are increasingly integrated with edge computing to minimize latency and computation overhead [194].

c) Bio-Inspired Intelligence: Bio-inspired intelligence offers innovative solutions to enhance the scalability of MIoT networks by emulating strategies observed in natural systems. A notable example is the application of swarm intelligence, which draws inspiration from the collective behaviors of social insects like ants and bees. In MIoT networks, swarm intelligence facilitates decentralized decision-making and self-organization, enabling efficient management of extensive device arrays without centralized control. This approach enhances scalability by allowing devices to interact locally and adaptively, leading to emergent global behaviors that optimize network performance [310].

Additionally, bio-inspired algorithms such as artificial immune systems (AIS) have been employed to bolster network security within MIoT frameworks. By mimicking the adaptive and learning capabilities of biological immune systems, AIS can detect and respond to anomalies and threats in a distributed manner, thereby maintaining the integrity and resilience of large-scale IoT deployments [311].

The decentralized nature of bio-inspired approaches aligns well with the requirements of MIoT, where traditional centralized management can become a bottleneck. By leveraging principles from biological systems, MIoT networks can achieve greater scalability, adaptability, and robustness, effectively managing the complexities associated with massive device interconnectivity [312].

D. AI/ML Implementation Challenges in MIoT

While AI and ML offer powerful tools for resource management, anomaly detection, and predictive analytics in MIoT, their deployment on constrained devices faces multiple practical limitations. We summarize the principal challenges and mitigation strategies below.

1) Model memory footprint and storage constraints: State-of-the-art neural networks often contain millions of parameters; even modest CNNs or RNNs can exceed the RAM/flash budgets of typical microcontrollers (tens to a few hundred kilobytes). Model compression techniques — *pruning*, *quantization*, *knowledge distillation* and *low-rank factorization* — are therefore essential to fit models on-device while retaining acceptable accuracy. Recent comprehensive surveys outline these methods and their trade-offs for edge and TinyML deployments [313].

2) Energy cost of on-device inference: Energy per inference varies widely with model architecture, hardware, and clocking. Recent TinyML benchmarking reports show practical energy figures in the range of a few to a few dozen microjoules per inference for small keyword-spotting (KWS) or anomaly detection tasks on specialized MCUs/NPUs (e.g., MLPerf Tiny and recent TinyML studies report ~35 µJ – 100 µJ per inference for efficient accelerators; generic MCUs without accelerators are orders of magnitude less efficient). Accurate profiling must separate pre-inference, inference, and post-inference phases to avoid underestimation. These realistic energy profiles are critical to compare on-device inference vs. offloading to edge servers [314].

3) Computation latency and real-time constraints: Many MIoT applications (industrial control, health monitoring) require strict latency bounds. Even when a model fits memory, CPU/NPU throughput can bottleneck responsiveness. Techniques such as operator fusion, compiler-level optimization (e.g., TFLite Micro [315] optimizations), and use of hardware accelerators (NPUs, DSPs) help meet latency targets, but they change the energy/area trade-off [316].

4) Data acquisition, heterogeneity and quality: Training reliable models requires representative, high-quality data. MIoT deployments suffer from intermittent connectivity, label scarcity, sensor drift, and non-iid distributions across devices. In federated setups, client heterogeneity and biased local datasets produce aggregation bias and fairness issues unless addressed explicitly (client selection, personalized FL, bias mitigation). Recent FL surveys discuss communication costs, client selection, and robustness to non-iid data as core research challenges [317].

5) Security, privacy and trust: On-device ML must be resilient to data poisoning, model inversion, and backdoor attacks. Secure aggregation, differential privacy, and robust aggregation rules add computational and communication overhead, and may increase model size or inference cost — a practical trade-off that must be considered for constrained nodes [318].

6) Mitigation strategies and best practices:

- **Model compression pipeline:** combine pruning, quantization, knowledge distillation to produce compact models with low inference cost; use structured pruning for hardware-friendly sparsity [319].
- **Hardware-aware NAS and compiler optimizations:** perform search/optimization with target MCU/NPU constraints (memory, MACs, latency) and deploy via optimized runtimes (e.g., TensorFlow Lite Micro, vendor SDKs) [320].
- **Energy-aware benchmarking:** measure energy across pre/infer/post phases with high-resolution instrumentation (dual-trigger methods) to obtain credible µJ/inference numbers rather than relying on theoretical FLOP-based estimates [321].
- **Hybrid inference and offloading:** adopt dynamic approaches that run ultra-light models locally and offload heavier tasks to nearby edge servers when network and energy budgets permit [322].
- **Federated learning adaptations:** reduce communication via model-update compression, selective parameter updates, and client clustering; use robust aggregation and personalization to mitigate non-iid effects and data quality issues [323].

In summary, deploying AI/ML in MIoT requires not only algorithmic advances but a full-stack co-design (model, compiler/runtime, hardware, and data-collection pipeline). Quantitative benchmarking and reproducible energy/latency measurements are critical to demonstrate feasibility for target MIoT applications.

E. Queueing & Graph Theory

Utilising queueing theory and graph theory are vital to increase scalability of MIoT networks. Queueing theory provides a set of tools to model and analyze the performance of network systems under different types of traffic conditions, which is useful in devising effective policies for resource allocation. So, for example, researchers can forecast via queueing models how systems will behave when they are under the most load and furthermore what kind of behavior mitigating traffic congestion measures should be introduced to scale networks [122], [324]. On the other hand, graph theory provides a formal framework for efficient topological representation and manipulations of MIoT networks. Such graph representations capture the connections between network nodes and can be used to discover optimal routing paths, bottlenecks, and maintain node connectivity [325], [326].

The AoI in MIoT networks is a key performance indicator related to the freshness of the information from any devices. For applications that require very timely data updates, such as environmental monitoring, industrial automation, and smart healthcare, it is critical to maintain a low AoI. Several studies have been carried out to investigate the age of information in dense IoT networks based on queueing theory [327]–[329].

The study [330] combines stochastic geometry and queueing theory to quantify the scalability of uncoordinated multiple access in massive wireless networks. The authors develop a spatiotemporal model to characterize and design uncoordinated multiple access strategies, providing insights into the maximum spatiotemporal traffic density that can be accommodated, while satisfying operational constraints.

The research [331] explores the application of graph theory in optimizing IoT-based healthcare systems. The authors utilize graph-theoretic approaches to model the connectivity of healthcare devices, aiming to enhance system efficiency and reliability. The study demonstrates how graph theory can be applied to design and optimize the topology of connected healthcare systems within the IoT framework.

The paper [332] addresses the scalability challenges of uncoordinated multiple access in IoT networks. By integrating queueing models and graph-theoretic approaches, the authors analyze the performance and scalability of random access protocols in large-scale IoT deployments. The study provides valuable insights into the design of scalable access mechanisms for massive IoT networks.

F. Optimal transport theory

Transport theory plays a crucial role in optimizing scalability and efficiency in MIoT networks by providing mathematical frameworks for resource allocation, data distribution, and network optimization. Optimal transport (OT) theory, which models the most efficient ways to transfer resources or data, has been increasingly applied in MIoT for tasks such as data imputation, federated learning, and load balancing.

For instance, in industrial IoT (IIoT) environments, missing data is a major challenge that affects system reliability and decision-making. The study [333] applies OT theory to efficiently reconstruct missing IIoT data, ensuring accuracy and preserving structural information. Similarly, federated learning, a key approach for distributed intelligence in MIoT, benefits from OT-based frameworks, as seen in [334], which leverages OT to enhance model convergence and robustness in decentralized AIoT systems.

Beyond data handling, transport theory is also essential in optimizing participant allocation in mobile crowd sensing, where large numbers of IoT devices collect and process environmental data. [335] demonstrates how OT theory can effectively allocate sensing tasks while minimizing energy consumption and network congestion. Additionally, [336] integrates OT with game theory to balance computational loads in fog computing, enhancing MIoT network performance and scalability.

In cloud-edge collaborative environments, optimal transport principles assist in efficient task scheduling and resource allocation. [337] explores how OT can optimize data flows, reducing delays and improving real-time processing capabilities in industrial settings. Similarly, [338] demonstrates the benefits of OT for offloading computational tasks in large-scale MIoT networks, leading to improved latency and energy efficiency.

Finally, OT-based methodologies are being extended to advanced control mechanisms in large-scale IoT networks. [339] introduces structured OT for ensemble control, allowing efficient estimation and coordination of distributed IoT agents. Moreover, resource allocation in cloud-edge collaborative IoT is enhanced by federated reinforcement learning, as shown in [340], where OT optimally distributes computational resources among IoT nodes.

These studies highlight the growing importance of optimal transport theory in MIoT, offering solutions for data integrity, learning efficiency, resource allocation, and network optimization, all of which are critical for ensuring scalable and robust IoT deployments.

G. Optimization & Control Theory

Optimization and control theory play a crucial role in enhancing the scalability and efficiency of MIoT networks. These mathematical frameworks help manage the vast number of interconnected devices and complex data flows inherent in MIoT systems.

One significant application is in the optimization of resource allocation. In [271], the authors provide a comprehensive analysis of resource allocation strategies within IoT networks, emphasizing how optimization techniques enhance resource management. They discuss the integration of machine learning algorithms with optimization methods to improve resource distribution in both low-power and mobile IoT networks.

Control theory also contributes to managing the dynamic aspects of MIoT networks. In [341], the authors explore control algorithms tailored for large-scale networks, including IoT systems. The research emphasizes the importance of distributed and stochastic optimization techniques, such as gradient tracking methods, to enhance the performance and reliability of massive IoT networks. By employing these approaches, the study demonstrates improved convergence

rates and robustness in dynamic and time-varying network environments.

Furthermore, the integration of SDN with IoT has been studied to enhance network scalability and management. The survey in [342] discusses how SDN's centralized control and programmability facilitate the handling of large-scale IoT deployments. The authors examine various optimization strategies for controller placement, which is critical for the efficient operation of SDN-enabled IoT networks.

These studies underscore the essential role of optimization and control theory in addressing key challenges related to scalability, resource allocation, network stability, and system management in MIoT networks.

H. Blockchain and Distributed Ledger Technology (DLT)

Blockchain technology has revolutionized security and privacy frameworks in MIoT, ensuring data integrity, trust, and fault tolerance in decentralized systems.

a) Decentralized Trust Models: By removing the need for central authorities, blockchain enables trust among heterogeneous IoT devices. Smart contracts facilitate automated operations, reducing human intervention and associated vulnerabilities. Hybrid blockchain systems that combine public and private ledgers are being deployed for scalability and cost-effectiveness [343], [344].

b) Energy-Efficient Consensus Mechanisms: Traditional consensus protocols like Proof of Work (PoW) are computationally expensive and unsuitable for energy-constrained MIoT devices. Lightweight mechanisms such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance (BFT) are increasingly adopted for their low energy footprint and faster consensus achievement [345], [346].

c) Blockchain-Integrated Security Frameworks: The integration of blockchain with AI enhances MIoT security by enabling predictive threat detection and automated response mechanisms. Blockchain-based identity management systems ensure secure and authenticated device interactions, reducing the risk of impersonation attacks [347], [348].

These advanced tools collectively enable the MIoT ecosystem to meet the demanding requirements of next-generation networks, paving the way for enhanced scalability, energy efficiency, and security. Table X provides a comparative analysis of some existing scalable tools for massive IoT.

VI. EMERGING TRENDS AND FUTURE SOLUTIONS

The rapid expansion of massive IoT presents a myriad of scalability challenges that necessitate innovative approaches. Several emerging trends and future solutions are increasingly gaining traction in the literature, signaling a transformative shift towards more efficient, resilient, and adaptive MIoT systems.

A. Artificial Intelligence and Machine Learning

The integration of AI and ML techniques is expected to be pivotal in addressing scalability and operational efficiency in MIoT systems. AI and ML enable dynamic resource allocation, predictive maintenance, and efficient data management,

which are crucial in dense MIoT environments [123], [349]. For instance, AI-driven predictive analytics can optimize network resources by forecasting traffic patterns, allowing for pre-emptive resource distribution and reducing latency [350]. Such techniques also improve energy efficiency by identifying low-activity periods and adjusting device operation accordingly [351].

ML algorithms, particularly reinforcement learning and federated learning, have shown promise for real-time network adaptation. These algorithms can respond to fluctuating data demands, facilitating on-the-fly adjustments in MIoT network configurations and enhancing scalability [33], [352]. For instance, reinforcement learning can be utilized to manage network congestion by dynamically rerouting traffic to less congested paths [353]. Federated learning, on the other hand, supports privacy-preserving data analysis by processing data locally on devices, which reduces data transfer demands and enhances security [354].

Despite these benefits, challenges remain. AI implementations often require high computational power, which can be difficult to achieve in resource-constrained IoT devices. Additionally, the need for extensive, high-quality training data limits the applicability of some AI models in MIoT environments. Future research aims to address these limitations by developing lightweight AI models suitable for low-power devices, thereby expanding the practical deployment of AI and ML in MIoT [323]. Another promising approach is the hybrid use of cloud and edge AI to distribute computational loads and enhance real-time decision-making across the network [355].

B. Edge and Fog Computing

The paradigms of edge and fog computing have become critical in managing the scalability of massive IoT systems. These architectures reduce latency and bandwidth demands by processing data closer to the source, minimizing the strain on centralized cloud infrastructures and enabling real-time analytics [356], [357]. This local processing capability is essential for time-sensitive applications, such as autonomous vehicles, smart manufacturing, and remote healthcare monitoring, where delays can impact safety and performance [358].

Recent studies have emphasized the need for optimizing the placement of edge and fog resources to achieve effective load balancing and network resilience [359]. Strategies include using SDN and Network Function Virtualization (NFV) to dynamically allocate resources based on real-time network traffic, ensuring seamless operation under high data loads [360]. Additionally, energy-efficient fog nodes and AI-driven algorithms can predict traffic patterns, further enhancing scalability and energy management in large-scale MIoT environments [361]. Future advancements in edge and fog computing will likely focus on optimizing these deployment strategies and leveraging AI to adapt to network demands in real-time, which is essential for the sustainable growth of MIoT applications.

C. Network Slicing and 5G/6G Technologies

The deployment of 5G and the anticipated roll-out of 6G technologies present substantial opportunities for enhancing

TABLE X
COMPARATIVE ANALYSIS OF SCALABLE TOOLS IN MIoT.

Tools	Reference	Network Scalability	Data Management	Energy Efficiency	Security/ Privacy	Advantages	Drawbacks
Game Theory	[282], [283]	✓	✓	✓		Optimizes resource allocation; adaptive in competitive or cooperative scenarios	Complexity in real-time implementation; computation-intensive
Mean Field Game Theory	[287], [305]	✓	✓	✓	✓	Handles massive device interactions efficiently; decentralized decision-making	Complexity in mathematical modeling; convergence issues in some scenarios
Artificial Intelligence and Machine Learning	[33], [300], [309]	✓	✓	✓	✓	Enables intelligent resource allocation, adaptive protocols, and privacy-preserving federated learning	Requires high computational power; challenges in model scalability for constrained devices
Queueing & Graph Theory	[122], [324]	✓	✓	✓		Models large-scale network dynamics; improves throughput and congestion management	Complexity in real-world implementation; potential scalability issues in large-scale scenarios
Optimal Transport Theory	[333], [334]	✓	✓	✓		Efficient data flow optimization; enhances load balancing and federated learning	Computational cost in large-scale networks; requires precise modeling
Optimization & Control Theory	[271], [341]	✓	✓	✓	✓	Ensures stability in large-scale MIoT; supports adaptive control and optimization	Requires accurate system modeling; high computational complexity in real-time control
Blockchain and Distributed Ledger Technology	[344]– [346]	✓	✓		✓	Decentralized trust; robust against cyberattacks; supports secure data exchange	High latency; energy consumption in some consensus mechanisms

MIoT scalability. Network slicing, which allows multiple virtual networks to operate on a single physical infrastructure, enables tailored connectivity solutions for various MIoT applications [362]. This capability allows IoT devices with diverse requirements—from low-power sensors to high-bandwidth applications—to coexist without interference, effectively optimizing network performance [363].

In addition, 5G and future 6G technologies introduce URLLC and mMTC, addressing scalability by supporting dense device connectivity and high-speed data transfer [364]. These technologies aim to support real-time applications, such as autonomous vehicles, smart healthcare, and industrial automation, by delivering high-speed connectivity and minimizing latency [365].

Moreover, the integration of AI and ML into network infrastructures is expected to be a focus of future research, enabling dynamic network management that adapts to real-time conditions and user demands [366]. Through AI-driven network optimization, MIoT systems could allocate resources proactively, thus improving scalability and user experience across diverse applications. Future advancements in 6G, such as the use of THz frequencies, may further enhance network slicing capabilities, allowing for unprecedented data speeds and supporting MIoT ecosystems [367].

D. Decentralized Protocols and Blockchain

Decentralized protocols and blockchain technology offer promising solutions to enhance both the security and scalability of MIoT systems. By enabling secure, distributed data exchanges without the need for centralized authorities, blockchain helps eliminate single points of failure, reduce latency, and improve data integrity [368], [369]. This approach is particularly useful in large-scale IoT deployments where traditional centralized systems can become bottlenecks due to high data volumes and network traffic.

The integration of lightweight blockchain solutions is a focus of recent research, as these frameworks aim to accommodate the resource constraints of IoT devices. For instance, new consensus mechanisms, such as PoS and DAG-based blockchains, offer reduced computational requirements compared to PoW, making them more feasible for IoT applications [370], [371]. Furthermore, advancements in interoperable blockchain systems enable communication across different platforms, fostering broader adoption in MIoT ecosystems [372].

However, challenges persist, including the need for improved scalability in blockchain networks and interoperability across various decentralized systems. Future research is anticipated to focus on hybrid blockchain architectures that leverage multiple consensus mechanisms, such as combining PoS with DAG-based approaches, to optimize scalability while ensuring robust security [373], [374]. Such models can enhance the feasibility of large-scale MIoT systems by improving transaction throughput and energy efficiency, addressing key demands in high-density IoT networks.

E. Sustainable Practices and Energy Harvesting

Sustainability is a central focus in the development of MIoT, with a growing emphasis on energy-efficient designs and renewable energy sources. Energy harvesting technologies such as solar, wind, and kinetic energy are increasingly integrated into MIoT devices, enabling them to operate autonomously and reduce dependence on non-renewable power sources [375], [376]. These technologies allow devices in remote or off-grid locations to remain functional without frequent

battery replacements, supporting long-term, sustainable IoT deployment [142].

Recent advancements also include piezoelectric and thermoelectric energy harvesting, where devices generate power from environmental vibrations or temperature differences, making them particularly useful in industrial IoT applications [377], [378]. Future MIoT designs will likely focus on low-power architectures that incorporate these energy-harvesting techniques, ensuring scalability without sacrificing environmental sustainability [379].

Additionally, research suggests that by combining energy harvesting with efficient data transmission protocols and low-power communication standards, MIoT networks can maintain high performance while minimizing environmental impact. This approach will be essential as MIoT systems scale to support millions of devices across various applications, ensuring a balance between technological growth and ecological responsibility [19], [380].

In summary, the landscape of MIoT is rapidly evolving, with various emerging trends and solutions poised to address scalability challenges. The integration of AI, edge computing, network slicing, decentralized protocols, and sustainable practices will be key to enabling efficient, resilient, and scalable MIoT systems in the future.

F. Convergence of Metaverse and Massive IoT

The convergence of the Metaverse and MIoT is poised to redefine digital interactions by creating immersive, data-rich environments that seamlessly blend the physical and virtual worlds. This integration leverages the extensive connectivity of MIoT devices to enhance the Metaverse's functionality, offering real-time, context-aware experiences across various sectors.

- Enhanced Immersive Experiences: MIoT devices serve as a bridge between the physical and virtual realms, enabling the Metaverse to incorporate real-time data from the physical world. This fusion allows for more dynamic and interactive virtual environments, where users can experience augmented reality (AR) and virtual reality (VR) applications that respond to live physical inputs [107].
- Integration with Advanced Technologies: The synergy between MIoT and the Metaverse is further amplified by the adoption of technologies such as AI, 5G, and blockchain. AI facilitates intelligent data processing and decision-making within the Metaverse, 5G ensures the high-speed connectivity required for seamless interactions, and blockchain provides secure data transactions and asset ownership verification [381].
- Development of Digital Twins: By integrating MIoT data, the Metaverse can host digital twins—virtual replicas of physical entities—that mirror real-time changes and behaviors. This capability is invaluable for simulations, predictive maintenance, and optimizing operations in industries such as manufacturing and urban planning [109].
- Advancements in Edge Computing: To manage the vast amounts of data generated by MIoT devices, edge computing solutions are being developed. Processing data

closer to its source reduces latency and enhances the responsiveness of Metaverse applications, leading to more fluid and real-time user experiences [382].

As 6G networks emerge, they are expected to adopt a joint sensing and communication paradigm, further increasing IoT density. This advancement will enable ultra-reliable, low-latency interactions within metaverse environments, enhancing applications such as digital twins and extended reality (XR). However, challenges related to scalability, energy efficiency, and security must be addressed to ensure the successful integration of MIoT within the metaverse [383].

The fusion of the Metaverse and MIoT is an emerging trend that promises to transform how we interact with digital and physical spaces. By embracing this convergence, future solutions will offer more immersive, efficient, and secure applications across various domains, from smart cities to personalized healthcare.

VII. Lessons Learned and Design Guidelines

This section synthesizes cross-cutting lessons from the surveyed literature and distills actionable guidance for designing and operating MIoT systems across scalability, data, energy, and security dimensions.

A. Key Lessons Learned

L1 — Working across Edge, Fog, and Cloud is more efficient than Cloud-only solutions Research indicates that a combination of Edge, Fog, and Cloud is a must for MIoT, as it enhances workload performance while minimizing latency, backhaul load, and energy per bit in constrained nodes [216], [384], [385]. Increasingly, a striated compute fabric (device $\rightarrow$ edge $\rightarrow$ cloud) is the emerging baseline architecture.

L2 — LPWANs narrow throughput for improved range and efficiency LoRaWAN and NB-IoT LPWANs offer multi-year battery lifespans and kilometers of coverage at the expense of slimmer payloads and restricted duty cycles [115], [386]–[388]. These systems scale with advanced ADR/spreading-factor (LoRaWAN) and mobility/attachment (NB-IoT) optimization.

L3 — Grant-free and Non-orthogonal Access broaden connectivity for massive devices but complicate the collision management complexity of the receiver system. NOMA and grant-free access methods increase the connection density, but increase the complexity on the receiver side. Solutions to simultaneous SIC and other device-bound systems need to be addressed [225], [389].

L4 — The data quality determines the value of analytics. MIoT systems tend to work with Non-IID, sparse, and noisy data. Aggregation methods, online anomaly detection, and label-efficient learning are vital to maintain model utility [390], [391]. Federated learning decreases the data movement and privacy risk but needs algorithms tailored to the heterogeneity and the communication-efficient protocols [391], [392].

L5 — Energy as the primary limitation at the network edge. Techniques such as wake-up radios, aggressive sleep scheduling, and event-driven sensing consistently demonstrate

the most significant enhancements in device lifetime. Although energy harvesting can further prolong operational duration, its effectiveness remains highly dependent on specific workloads and environmental conditions [184], [393], [394]. Furthermore, for on-device machine learning to be practical, models must undergo quantization, pruning, and sparsification to reduce computational demands [391].

L6 — Necessity of lightweight and layered "Security by Design." Implementing lightweight cryptographic methods, hardware-based roots of trust, and local or edge-level attestation mechanisms can mitigate security risks without exceeding the limited resource budgets of edge devices. While blockchain technology offers potential benefits in terms of data integrity and auditability, its deployment must be constrained to lightweight consensus protocols or permissioned environments to manage latency and energy consumption effectively [395]–[397].

B. Cross-Cutting Design Trade-offs

T1 — Trade-offs between security, energy consumption, and latency. Enhancing security through stronger cryptographic algorithms and more frequent handshake protocols improves security guarantees but incurs increased computational overhead and airtime usage. Strategies such as edge-based session resumption, utilization of compact cipher suites, and batching of communications can mitigate these costs, balancing security requirements with energy and latency constraints [395], [397].

T2 — Connectivity density versus receiver complexity. An increase in device density facilitated by non-orthogonal multiple access (NOMA) or grant-free access mechanisms leads to elevated processing demands at the base station, such as SIC or message passing algorithm (MPA) decoding, as well as greater coordination overhead. To address these challenges, a hybrid access approach combining OFDMA with grant-free access, alongside density-aware scheduling strategies, has been proposed [225], [389].

T3 — Local processing versus battery life. While edge analytics can significantly reduce the volume of backhaul transmissions, they impose additional computational load on local processors, thereby increasing energy consumption. Optimal performance is achieved through event-driven sensing paradigms, the deployment of compact machine learning models, and intermittent inference techniques, all of which contribute to maintaining a low average current draw [216], [384], [391].

C. Rules of Thumb (Quantitative Heuristics)

- *LPWAN payload budgeting:* Typical uplink payload sizes should be maintained at 12–50 bytes, and duty cycles should not exceed 1
- *Battery life planning:* For coin-cell nodes (approximately 220,mAh), daily energy expenditure should remain below 5,mC to achieve operational lifetimes exceeding one year. Wake-up receivers and compressive or event-triggered reporting mechanisms contribute significantly to reducing average current draw [115], [393].

- *Federated learning rounds:* Federated learning frameworks should perform rounds at intervals of 10–100 seconds, using quantized or sparse updates to minimize radio energy consumption, while personalization or clustered FL strategies can help mitigate the effects of non-IID data [391], [392].

D. Domain-Specific Design Guidelines

Smart Cities. In smart city applications, multi-RAT hierarchies should be deployed, leveraging LoRaWAN and NB-IoT for low-data-rate telemetry tasks, while LTE-M and 5G networks can support high-bandwidth services such as video streaming and actuation. Analytics capabilities should be deployed at roadside or edge locations to address latency-sensitive tasks such as traffic management, while cloud resources should be reserved for city-wide model training. Grant-free uplink mechanisms can efficiently handle event-driven bursts and anomaly detection, thereby improving noise filtering and responsiveness [216], [384], [388]–[390].

Healthcare and Wearables. Healthcare and wearable applications should prioritize energy efficiency and data privacy by integrating ultra-low-power radios, wake-up receivers, intermittent sensing strategies, and on-device inference for simple classification tasks. Encrypted data summaries should be offloaded to edge gateways, and federated or split learning approaches should be employed to maintain raw data locally and protect user privacy [391]–[393].

Industrial IoT. For industrial IoT scenarios requiring URLLC control loops, inference should be performed at on-premises edge nodes, and licensed cellular bands (LTE-M/5G) with network slicing should be utilized. In deployments with large numbers of sensors, grant-free access combined with compressive sensing techniques can mitigate congestion. Furthermore, hardware-based roots of trust and permissioned blockchain technologies can ensure secure and auditable transaction records when necessary [389], [396], [398].

E. Actionable Research Directions

- **Lightweight, convergence-aware access for MIoT:** Research should focus on hybrid grant-free and NOMA access schemes that incorporate SIC, taking into account the computational constraints of both devices and base stations, while maintaining system stability under bursty traffic conditions [225], [389].
- **Energy-efficient tiny machine learning:** Development efforts should target quantization-aware training, model sparsity exploitation, and event-triggered inference mechanisms designed specifically for models smaller than 10 kB, suitable for deployment on MCU-class devices [391].
- **Trust mechanisms with bounded overhead:** Permissioned or DAG-based distributed ledgers, combined with edge-assisted verification processes, should be investigated to ensure security while keeping latency and energy consumption within stringent MIoT constraints [396], [397].
- **Data quality management pipelines:** Federated learning frameworks should integrate robust aggregation methods,

anomaly detection, and concept drift monitoring to handle non-IID and intermittent data streams typical of MIoT systems [390], [391].

VIII. CONCLUDING REMARKS

The MIoT presents an unprecedented opportunity to connect billions of devices across industries, from smart cities to agriculture, offering solutions that enhance productivity, efficiency, and quality of life. However, achieving a scalable MIoT network requires addressing key challenges in network capacity, data management, energy efficiency, and security. This paper has explored a range of current and emerging solutions to tackle these challenges, including LPWAN, 5G, edge computing, and virtualized network infrastructures, alongside emerging approaches like artificial intelligence, blockchain, and machine learning.

As MIoT ecosystems grow, advanced techniques such as grant-free access, NOMA, cooperative communication, and compressive sensing will play a central role in achieving scalability. Integrating these solutions with AI-driven optimization and federated learning offers the potential for a more efficient and adaptive MIoT network. However, future research must focus on refining these technologies for real-world deployment, with particular attention to maintaining energy efficiency, minimizing latency, and strengthening security and privacy.

Ultimately, the path forward for scalable MIoT involves a combination of technical innovation, regulatory support, and cross-industry collaboration. As networks evolve towards 6G and beyond, an emphasis on sustainable practices and adaptable architectures will be essential. The insights provided in this paper can serve as a foundation for future efforts to create robust, secure, and scalable MIoT solutions that meet the demands of an increasingly interconnected world.

REFERENCES

[1] Cisco, "Cisco annual internet report (2018–2023) white paper," 2018.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] W. Sun, Q. Wang, N. Zhao, H. Zhang, C. Shen, and L. W.-C. Wong, *Ultra-Dense Heterogeneous Networks*. CRC Press, 2022.

[4] A. Zanella *et al.*, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[5] I. Cheikh, R. Aouami, E. Sabir, M. Sadik, and S. Roy, "Multi-layered energy efficiency in lora-wan networks: A tutorial," *IEEE Access*, vol. 10, pp. 9198–9231, 2022.

[6] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[7] M. Laroui, B. Nour, H. Moungla, M. A. Cherif, H. Afifi, and M. Guizani, "Edge and fog computing for iot: A survey on current research activities & future directions," *Computer Communications*, vol. 180, pp. 210–231, 2021.

[8] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, and I. Yaqoob, "Big iot data analytics: architecture, opportunities, and open research challenges," *ieee access*, vol. 5, pp. 5247–5261, 2017.

[9] S. Popli, R. K. Jha, and S. Jain, "A survey on energy efficient narrowband internet of things (nbiot): architecture, application and challenges," *IEEE access*, vol. 7, pp. 16739–16776, 2018.

[10] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[11] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE internet of things journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[12] R. Priyadarshi, "Exploring machine learning solutions for overcoming challenges in iot-based wireless sensor network routing: a comprehensive review," *Wireless Networks*, pp. 1–27, 2024.

[13] R. Chataut, M. Nankya, and R. Akl, "6g networks and the ai revolution—exploring technologies, applications, and emerging challenges," *Sensors*, vol. 24, no. 6, p. 1888, 2024.

[14] G. S. Ramachandran and B. Krishnamachari, "Towards a large scale iot through partnership, incentive, and services: A vision, architecture, and future directions," *Open Journal of Internet Of Things (OJIOT)*, vol. 5, no. 1, pp. 80–92, 2019.

[15] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, "Network slicing: Recent advances, taxonomy, requirements, and open research challenges," *IEEE Access*, vol. 8, pp. 36009–36028, 2020.

[16] O. T. Modupe, A. A. Otitoola, O. J. Oladapo, O. O. Abiona, O. C. Oyeniran, A. O. Adewusi, A. M. Komolafe, and A. Obijuru, "Reviewing the transformational impact of edge computing on real-time data processing and analytics," *Computer Science & IT Research Journal*, vol. 5, no. 3, pp. 693–702, 2024.

[17] Z. Zong and Y. Guan, "Ai-driven intelligent data analytics and predictive analysis in industry 4.0: Transforming knowledge, innovation, and efficiency," *Journal of the Knowledge Economy*, pp. 1–40, 2024.

[18] U. L. Tupe, S. D. Babar, S. P. Kadam, and P. N. Mahalle, "Research perspective on energy-efficient protocols in iot: emerging development of green iot," *International Journal of Pervasive Computing and Communications*, vol. 18, no. 2, pp. 145–170, 2022.

[19] D. Ma, G. Lan, M. Hassan, W. Hu, and S. K. Das, "Sensing, computing, and communications for energy harvesting iots: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1222–1250, 2019.

[20] P. Cui, U. Guin, A. Skjellum, and D. Umphress, "Blockchain in iot: current trends, challenges, and future roadmap," *Journal of Hardware and Systems Security*, vol. 3, pp. 338–364, 2019.

[21] B.-X. Wang, J.-L. Chen, and C.-L. Yu, "An ai-powered network threat detection system," *IEEE Access*, vol. 10, pp. 54029–54037, 2022.

[22] M. A. Adedoyin and O. E. Falowo, "Combination of ultra-dense networks and other 5g enabling technologies: A survey," *IEEE Access*, vol. 8, pp. 22893–22932, 2020.

[23] P.-V. Mekikis *et al.*, "Toward massive machine type communications in ultra-dense cellular iot networks: Current issues and machine learning-assisted solutions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 300–318, 2020.

[24] S. M. A. Zaidi, M. Manalastas, H. Farooq, and A. Imran, "Mobility management in emerging ultra-dense cellular networks: A survey, outlook, and future research directions," *IEEE Access*, vol. 8, pp. 183505–183533, 2020.

[25] N. Sharma and K. Kumar, "Resource allocation trends for ultra dense networks in 5g and beyond networks: A classification and comprehensive survey," *Physical Communication*, vol. 48, p. 101415, 2021.

[26] M. Kamel, W. Hamouda, and A. Youssef, "Ultra-dense networks: A survey," *IEEE Communications surveys & tutorials*, vol. 18, no. 4, pp. 2522–2545, 2016.

[27] W. Yu, H. Xu, H. Zhang, D. Griffith, and N. Golmie, "Ultra-dense networks: Survey of state of the art and future directions," in *2016 25th international conference on computer communication and networks (ICCCN)*, pp. 1–10, IEEE, 2016.

[28] M. Jouhari, N. Saeed, M.-S. Alouini, and E. M. Amhoud, "A survey on scalable lorawan for massive iot: Recent advances, potentials, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1841–1876, 2023.

[29] M. H. Alsharif, A. H. Kelechi, A. Jahid, R. Kannadasan, M. K. Singla, J. Gupta, and Z. W. Geem, "A comprehensive survey of energy-efficient computing to enable sustainable massive iot networks," *Alexandria Engineering Journal*, vol. 91, pp. 12–29, 2024.

[30] S. K. Sharma and X. Wang, "Toward massive machine type communications in ultra-dense cellular iot networks: Current issues and machine learning-assisted solutions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 426–471, 2019.

[31] O. Mämmelä, P. Karhula, and J. Mäkelä, "Scalability analysis of data transfer in massive internet of things applications," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–7, IEEE, 2019.

[32] Q. Abbas, S. A. Hassan, H. K. Qureshi, K. Dev, and H. Jung, "A comprehensive survey on age of information in massive iot networks," *Computer Communications*, vol. 197, pp. 199–213, 2023.

[33] P. Tam, R. Corrado, C. Eang, and S. Kim, "Applicability of deep reinforcement learning for efficient federated learning in massive iot communications," *Applied Sciences*, vol. 13, no. 5, p. 3083, 2023.

[34] A. Alotaibi and A. Barnawi, "Securing massive iot in 6g: Recent solutions, architectures, future directions," *Internet of Things*, vol. 22, p. 100715, 2023.

[35] A. Farhad and J.-Y. Pyun, "Resource management for massive internet of things in ieee 802.11 ah wlan: Potentials, current solutions, and open challenges," *Sensors*, vol. 22, no. 23, p. 9509, 2022.

[36] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[37] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji, and V. C. Leung, "Enabling massive iot toward 6g: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 11891–11915, 2021.

[38] Z. Kouahla, A.-E. Benrazek, M. A. Ferrag, B. Farou, H. Seridi, M. Kurulay, A. Anjum, and A. Asheralieva, "A survey on big iot data indexing: Potential solutions, recent advancements, and open issues," *Future Internet*, vol. 14, no. 1, p. 19, 2021.

[39] M. Rao *et al.*, "Scalable networking architectures for massive iot: A comprehensive review," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 867–896, 2020.

[40] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, "A survey on network methodologies for real-time analytics of massive iot data and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1457–1477, 2017.

[41] Y. Teng, M. Liu, F. R. Yu, V. C. Leung, M. Song, and Y. Zhang, "Resource allocation for ultra-dense networks: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2134–2168, 2018.

[42] R. Ravish and S. R. Swamy, "Intelligent traffic management: A review of challenges, solutions, and future perspectives," *Transport and Telecommunication Journal*, vol. 22, no. 2, pp. 163–182, 2021.

[43] P. R. Negi, A. Gautam, and S. Verma, "Smartcitynet: Adaptive resource management for urban iot networks," in *2024 IEEE International Conference on Smart Power Control and Renewable Energy (ICSPCRE)*, pp. 1–7, IEEE, 2024.

[44] M. A. Fadhel, A. M. Duhaim, A. Saihood, A. Sewify, M. N. Al-Hamadani, A. Albahri, L. Alzubaidi, A. Gupta, S. Mirjalili, and Y. Gu, "Comprehensive systematic review of information fusion methods in smart cities and urban environments," *Information Fusion*, p. 102317, 2024.

[45] L. U. Khan, I. Yaqoob, N. H. Tran, S. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-computing-enabled smart cities: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10200–10232, 2020.

[46] V. Katariya, A. D. Pazho, G. A. Noghre, H. Tabkhi, *et al.*, "Vegaedge: Edge ai confluence for real-time iot-applications in highway safety," *Internet of Things*, vol. 27, p. 101268, 2024.

[47] Q. Liu, J. Gu, J. Yang, Y. Li, D. Sha, M. Xu, I. Shams, M. Yu, and C. Yang, "Cloud, edge, and mobile computing for smart cities," *Urban Informatics*, pp. 757–795, 2021.

[48] M. Chinnici and S. De Vito, "Iot meets opportunities and challenges: edge computing in deep urban environment," *Dependable IoT for Human and Industry*, pp. 241–272, 2022.

[49] G. Gagliardi, M. Lupia, G. Cario, F. Tedesco, F. Cicchello Gaccio, F. Lo Scudo, and A. Casavola, "Advanced adaptive street lighting systems for smart cities," *Smart Cities*, vol. 3, no. 4, pp. 1495–1512, 2020.

[50] E. Zanaj, G. Caso, L. De Nardis, A. Mohammadpour, Ö. Alay, and M.-G. Di Benedetto, "Energy efficiency in short and wide-area iot technologies—a survey," *Technologies*, vol. 9, no. 1, p. 22, 2021.

[51] B. Fang, J. Yu, Z. Chen, A. I. Osman, M. Farghali, I. Ihara, E. H. Hamza, D. W. Rooney, and P.-S. Yap, "Artificial intelligence for waste management in smart cities: a review," *Environmental Chemistry Letters*, vol. 21, no. 4, pp. 1959–1989, 2023.

[52] I. Hussain, A. Elomri, L. Kerbache, and A. El Omri, "Smart city solutions: Comparative analysis of waste management models in iot-enabled environments using multiagent simulation," *Sustainable Cities and Society*, vol. 103, p. 105247, 2024.

[53] A. Kaginalkar, S. Kumar, P. Gargava, and D. Niyogi, "Review of urban computing in air quality management as smart city service: An integrated iot, ai, and cloud technology perspective," *Urban Climate*, vol. 39, p. 100972, 2021.

[54] S. L. Ullo and G. R. Sinha, "Advances in smart environment monitoring systems using iot and sensors," *Sensors*, vol. 20, no. 11, p. 3113, 2020.

[55] K. Boikanyo, A. M. Zungeru, B. Sigweni, A. Yahya, and C. Lebekwe, "Remote patient monitoring systems: Applications, architecture, and challenges," *Scientific African*, vol. 20, p. e01638, 2023.

[56] S. Krishnamoorthy, A. Dua, and S. Gupta, "Role of emerging technologies in future iot-driven healthcare 4.0 technologies: A survey, current challenges and future directions," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 1, pp. 361–407, 2023.

[57] S. O. Ajakwe, C. I. Nwakanma, D.-S. Kim, and J.-M. Lee, "Key wearable device technologies parameters for innovative healthcare delivery in b5g network: A review," *IEEE Access*, vol. 10, pp. 49956–49974, 2022.

[58] X. Gu, F. Sabrina, Z. Fan, and S. Sohail, "A review of privacy enhancement methods for federated learning in healthcare systems," *International Journal of Environmental Research and Public Health*, vol. 20, no. 15, p. 6539, 2023.

[59] X. Yin, Y. Zhu, and J. Hu, "A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions," *ACM Computing Surveys (CSUR)*, vol. 54, no. 6, pp. 1–36, 2021.

[60] R. R. Irshad, S. S. Sohail, S. Hussain, D. Ø. Madsen, A. S. Zamani, A. A. A. Ahmed, A. A. Alattab, M. M. Badr, and I. M. Alwayle, "Towards enhancing security of iot-enabled healthcare system," *Heliyon*, vol. 9, no. 11, 2023.

[61] M. W. P. Maduranga, V. Tilwari, R. Rathnayake, and C. Sandamini, "Ai-enabled 6g internet of things: Opportunities, key technologies, challenges, and future directions," in *Telecom*, vol. 5, pp. 804–822, MDPI, 2024.

[62] M. Dadkhah, M. Mehraeen, F. Rahimnia, and K. Kimiafar, "Use of internet of things for chronic disease management: an overview," *Journal of Medical Signals & Sensors*, vol. 11, no. 2, pp. 138–157, 2021.

[63] E. Khodadadi and S. Towfek, "Internet of things enabled disease outbreak detection: A predictive modeling system.," *Journal of Intelligent Systems & Internet of Things*, vol. 10, no. 1, 2023.

[64] A. A. Abdellatif, A. Mohamed, C. F. Chiasserini, M. Tlili, and A. Erbad, "Edge computing for smart health: Context-aware approaches, opportunities, and challenges," *IEEE Network*, vol. 33, no. 3, pp. 196–203, 2019.

[65] M. S. Farooq and S. Akram, "Iot in agriculture: challenges and opportunities.," *Journal of Agricultural Research (03681157)*, vol. 59, no. 1, 2021.

[66] H. M. Jawad, R. Nordin, S. K. Gharghan, A. M. Jawad, and M. Ismail, "Energy-efficient wireless sensor networks for precision agriculture: A review," *Sensors*, vol. 17, no. 8, p. 1781, 2017.

[67] C. D. Ha, P. T. Minh, P. Van Tien, P. P. Thu, P. M. Trien, *et al.*, "Iot solutions for smart farming: A comprehensive review on the current trends, challenges and future prospects for sustainable agriculture," *Journal of Forestry Science and Technology*, vol. 8, no. 2, pp. 028–035, 2023.

[68] O. Ali, M. K. Ishak, M. K. L. Bhatti, I. Khan, and K.-I. Kim, "A comprehensive review of internet of things: Technology stack, middlewares, and fog/edge computing interface," *Sensors*, vol. 22, no. 3, p. 995, 2022.

[69] S. Getahun, H. Kefale, and Y. Gelaye, "Application of precision agriculture technologies for sustainable crop production and environmental sustainability: A systematic review," *The Scientific World Journal*, vol. 2024, no. 1, p. 2126734, 2024.

[70] X. Zhang, Z. Cao, and W. Dong, "Overview of edge computing in the agricultural internet of things: Key technologies, applications, challenges," *Ieee Access*, vol. 8, pp. 141748–141761, 2020.

[71] P. Nama, S. Pattanayak, and H. S. Meka, "Ai-driven innovations in cloud computing: Transforming scalability, resource management, and predictive analytics in distributed systems," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, no. 12, p. 4165, 2023.

[72] P. Kuppusamy, J. K. Suresh, and S. Shanmugananthan, "Machine learning-enabled internet of things solution for smart agriculture operations," in *Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries*, pp. 84–115, IGI Global, 2023.

[73] A. Sharma, A. Jain, P. Gupta, and V. Chowdary, "Machine learning applications for precision agriculture: A comprehensive review," *IEEE Access*, vol. 9, pp. 4843–4873, 2020.

[74] S. Shivkumar and M. Supriya, "A framework for fleet management using iot and predictive analytics," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–6, IEEE, 2024.

[75] F. A. Butt, J. N. Chattha, J. Ahmad, M. U. Zia, M. Rizwan, and I. H. Naqvi, "On the integration of enabling wireless technologies and sensor fusion for next-generation connected and autonomous vehicles," *IEEE Access*, vol. 10, pp. 14643–14668, 2022.

[76] Z. E. Ahmed, A. A. Hashim, R. A. Saeed, and M. M. Saeed, "Mobility management enhancement in smart cities using software defined networks," *Scientific African*, vol. 22, p. e01932, 2023.

[77] G. Suciu, I. Hussain, I. A. Esanu, C. Beceanu, R.-I. Vatasoiu, and M.-C. Vochin, "Role of 5g in vehicular network for smart vehicles in smart cities," in *2021 IEEE 27th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, pp. 382–387, IEEE, 2021.

[78] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi, "Edge computing for autonomous driving: Opportunities and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1697–1716, 2019.

[79] A. E. Braten, F. A. Kraemer, and D. Palma, "Autonomous iot device management systems: Structured review and generalized cognitive model," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4275–4290, 2020.

[80] A. R. Javed, F. Shahzad, S. ur Rehman, Y. B. Zikria, I. Razzak, Z. Jalil, and G. Xu, "Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects," *Cities*, vol. 129, p. 103794, 2022.

[81] M. Farahpoor, O. Esparza, and M. Soriano, "Comprehensive iot-driven fleet management system for industrial vehicles," *IEEE access*, 2023.

[82] I. Zrelli and A. Rejeb, "A bibliometric analysis of iot applications in logistics and supply chain management," *Heliyon*, vol. 10, no. 16, 2024.

[83] A. C. del Castillo and A. K. Parlikad, "Dynamic fleet management: integrating predictive and preventive maintenance with operation workload balance to minimise cost," *Reliability Engineering & System Safety*, p. 110243, 2024.

[84] R. Pal, S. Chavhan, D. Gupta, A. Khanna, S. Padmanaban, B. Khan, and J. J. Rodrigues, "A comprehensive review on iot-based infrastructure for smart grid applications," *IET renewable power generation*, vol. 15, no. 16, pp. 3761–3776, 2021.

[85] S. A. A. Abir, A. Anwar, J. Choi, and A. Kayes, "Iot-enabled smart energy grid: Applications and challenges," *IEEE access*, vol. 9, pp. 50961–50981, 2021.

[86] F. A. Alaba, U. Sani, E. G. Dada, and B. H. Mohammed, "Aiot-enabled smart grids: Advancing energy efficiency and renewable energy integration," in *Artificial Intelligence of Things for Achieving Sustainable Development Goals*, pp. 59–79, Springer, 2024.

[87] S. B. Meena, P. R. Patil, S. Kandharkar, N. Hemalatha, A. Khade, K. K. Dixit, and N. Chinthamu, "The evolution of smart grid technologies: Integrating renewable energy sources, energy storage, and demand response systems for efficient energy distribution," *Nanotechnology Perceptions*, pp. 1098–1109, 2024.

[88] M. Arafat, M. Hossain, and M. M. Alam, "Machine learning scopes on microgrid predictive maintenance: Potential frameworks, challenges, and prospects," *Renewable and Sustainable Energy Reviews*, vol. 190, p. 114088, 2024.

[89] M. H. Raza, Y. M. Rind, I. Javed, M. Zubair, M. Q. Mehmood, and Y. Massoud, "Smart meters for smart energy: a review of business intelligence applications," *IEEE Access*, 2023.

[90] R. Salama and F. Al-Turjman, "Smart grid with internet of things applications," *NEU Journal for Artificial Intelligence and Internet of Things*, vol. 4, no. 2, 2024.

[91] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in iot-enabled smart-grid system," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5744–5761, 2020.

[92] C. Thuemmler and C. Bai, "Health 4.0: Application of industry 4.0 design principles in future asthma management," *Health 4.0: How virtualization and big data are revolutionizing healthcare*, pp. 23–37, 2017.

[93] S. Kolasani, "Revolutionizing manufacturing, making it more efficient, flexible, and intelligent with industry 4.0 innovations," *International Journal of Sustainable Development Through AI, ML and IoT*, vol. 3, no. 1, pp. 1–17, 2024.

[94] O. Kanoun, S. Khriji, S. Naifar, S. Bradai, G. Bouattour, A. Bouhamed, D. El Houssaini, and C. Viehweger, "Prospects of wireless energy-aware sensors for smart factories in the industry 4.0 era," *Electronics*, vol. 10, no. 23, p. 2929, 2021.

[95] A. A. Mirani, G. Velasco-Hernandez, A. Awasthi, and J. Walsh, "Key challenges and emerging technologies in industrial iot architectures: A review," *Sensors*, vol. 22, no. 15, p. 5836, 2022.

[96] Y. Wu, H.-N. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial iot: Integrated approaches for smart transportation, smart energy, and smart factory," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1175–1211, 2022.

[97] M. Islam, H. M. M. Jamil, S. A. Pranto, R. K. Das, A. Amin, and A. Khan, "Future industrial applications: Exploring lpwan-driven iot protocols," *Sensors*, vol. 24, no. 8, p. 2509, 2024.

[98] S. Sahoo and C.-Y. Lo, "Smart manufacturing powered by recent technological advancements: A review," *Journal of Manufacturing Systems*, vol. 64, pp. 236–250, 2022.

[99] M. Soori, B. Arezoo, and R. Dastres, "Internet of things for smart factories in industry 4.0, a review," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 192–204, 2023.

[100] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, "Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios," *Ieee Access*, vol. 8, pp. 23022–23040, 2020.

[101] M. Shahin, M. Maghanaki, A. Hosseinzadeh, and F. F. Chen, "Advancing network security in industrial iot: a deep dive into ai-enabled intrusion detection systems," *Advanced Engineering Informatics*, vol. 62, p. 102685, 2024.

[102] B. S. Khan, S. Jangsher, A. Ahmed, and A. Al-Dweik, "Urllc and embb in 5g industrial iot: A survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1134–1163, 2022.

[103] T. N. Weerasinghe, I. A. Balapuwaduge, and F. Y. Li, "Priority-based initial access for urllc traffic in massive iot networks: Schemes and performance analysis," *Computer Networks*, vol. 178, p. 107360, 2020.

[104] 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.

[105] B. Adhikari, M. Jaseemuddin, and A. Anpalagan, "Resource allocation for co-existence of embb and urllc services in 6g wireless networks: A survey," *IEEE Access*, 2023.

[106] S. K. Sharma, I. Woungang, A. Anpalagan, and S. Chatzinotas, "Toward tactile internet in beyond 5g era: Recent advances, current issues, and future directions," *Ieee Access*, vol. 8, pp. 56948–56991, 2020.

[107] R. Asif and S. R. Hassan, "Exploring the confluence of iot and metaverse: Future opportunities and challenges," *IoT*, vol. 4, no. 3, pp. 412–429, 2023.

[108] LeewayHertz, "Metaverse use cases and benefits," 2025.

[109] T. M. Fernández-Caramés and P. Fraga-Lamas, "Forging the industrial metaverse towards industry 5.0: Where augmented/mixed reality, iiot, opportunistic edge computing and digital twins meet," *IEEE Access*, 2024.

[110] H. Yu and Y. B. Zikria, "Cognitive radio networks for internet of things and wireless sensor networks," 2020.

[111] M. Elbayoumi, M. Ibrahim, S. Elhoushy, W. Hamouda, and A. Youssef, "Performance analysis of cellular ultradense iot networks with wireless backhauls," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15774–15787, 2023.

[112] D. Yang, X. Zhang, X. Huang, L. Shen, J. Huang, X. Chang, and G. Xing, "Understanding power consumption of nb-iot in the wild: tool and large-scale measurement," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, pp. 1–13, 2020.

[113] M. Lukic, S. Sobot, I. Mezei, D. Vukobratovic, and D. Danilovic, "In-depth real-world evaluation of nb-iot module energy consumption," in *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 261–265, IEEE, 2020.

[114] R. K. Singh, P. P. Puluckul, R. Berkvens, and M. Weyn, "Energy consumption analysis of lpwan technologies and lifetime estimation for iot application," *Sensors*, vol. 20, no. 17, p. 4794, 2020.

[115] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the energy performance of lorawan," *Sensors*, vol. 17, no. 10, p. 2364, 2017.

[116] B. Teymuri, R. Serati, N. A. Anagnostopoulos, and M. Rasti, "Lp-mab: Improving the energy efficiency of lorawan using a reinforcement-learning-based adaptive configuration algorithm," *Sensors*, vol. 23, no. 4, p. 2363, 2023.

[117] M. A. Almuhaya, W. A. Jabbar, N. Sulaiman, and S. Abdulmalek, "A survey on lorawan technology: Recent trends, opportunities, simulation tools and future directions," *Electronics*, vol. 11, no. 1, p. 164, 2022.

[118] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing iot services through software defined networking and edge computing: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1761–1804, 2020.

[119] M. Y. Arafat and S. Moh, "Routing protocols for unmanned aerial vehicle networks: A survey," *IEEE access*, vol. 7, pp. 99694–99720, 2019.

[120] M. Esmaeili, M. Rahimi, H. Pishdast, D. Farahmandazad, M. Khajavi, and H. J. Saray, "Machine learning-assisted intrusion detection for enhancing internet of things security," *arXiv preprint arXiv:2410.01016*, 2024.

[121] S. S. Bamber, N. Dogra, S. K. Alhawat, J. K. Jaswal, and A. K. Sekhon, "Navigating the fog: A comprehensive survey and comparative analysis of fog computing architectures," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1201–1206, IEEE, 2024.

[122] S. K. Sharma and X. Wang, "Distributed caching enabled peak traffic reduction in ultra-dense iot networks," *IEEE Communications Letters*, vol. 22, no. 6, pp. 1252–1255, 2018.

[123] A. Umar, Z. Khalid, M. Ali, M. Abazeed, A. Alqahtani, R. Ullah, and H. Safdar, "A review on congestion mitigation techniques in ultra-dense wireless sensor networks: State-of-the-art future emerging artificial intelligence-based solutions," *Applied Sciences*, vol. 13, no. 22, p. 12384, 2023.

[124] N. Jiang, Y. Deng, A. Nallanathan, X. Kang, and T. Q. Quek, "Analyzing random access collisions in massive iot networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 10, pp. 6853–6870, 2018.

[125] V. Chunduri, A. Kumar, A. Joshi, S. R. Jena, A. Jumaev, and S. More, "Optimizing energy and latency trade-offs in mobile ultra-dense iot networks within futuristic smart vertical networks," *International Journal of Data Science and Analytics*, pp. 1–13, 2023.

[126] N. Sharma and K. Kumar, "Energy efficient clustering and resource allocation strategy for ultra-dense networks: A machine learning framework," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1884–1897, 2022.

[127] X. Shen, W. Liao, and Q. Yin, "A novel wireless resource management for the 6g-enabled high-density internet of things," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 32–39, 2022.

[128] B. Shilpa, H. P. Gupta, R. K. Jha, and S. S. Hashmi, "Lora interference issues and solution approaches in dense iot networks: a review," *Telecommunication Systems*, pp. 1–23, 2024.

[129] H. Lin, K. S. Kim, and W.-Y. Shin, "Interference-aware opportunistic random access in dense iot networks," *IEEE Access*, vol. 8, pp. 93472–93486, 2020.

[130] H. Alahmadi, F. Bouabdallah, and A. Al-Dubai, "A novel time-slotted lora mac protocol for scalable iot networks," *Future Generation Computer Systems*, vol. 134, pp. 287–302, 2022.

[131] M. Slabicki, G. Premsankar, and M. Di Francesco, "Adaptive configuration of lora networks for dense iot deployments," in *NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–9, IEEE, 2018.

[132] A. Al-Dulaimi, S. Al-Rubaye, J. Cosmas, and A. Anpalagan, "Planning of ultra-dense wireless networks," *IEEE Network*, vol. 31, no. 2, pp. 90–96, 2017.

[133] G. Chopra and S. Ahmed, "Advancement in resource allocation for future generation of communications," *Current and Future Cellular Systems: Technologies, Applications, and Challenges*, 2025.

[134] W. Wang, H. Yang, S. Li, X. Liu, and Z. Wan, "Adaptive ue handover management with mar-aided multivariate dqn in ultra-dense networks," *Journal of Network and Systems Management*, vol. 33, no. 1, p. 17, 2025.

[135] J. Kim, J. Lee, and S. Bahk, "Energy-efficient and robust communication in multi-connectivity enabled mmwave ultra-dense networks," *IEEE Transactions on Green Communications and Networking*, 2024.

[136] M. Ouaissa, M. Ouaissa, Z. Boulouard, S. El Himer, and I. U. Khan, "Low-power wide area network for large-scale iot: Fundamentals, technologies, and challenges," in *Low-Power Wide Area Network for Large Scale Internet of Things*, pp. 1–14, CRC Press, 2024.

[137] S. M. Mousavi, A. Khademzadeh, and A. M. Rahmani, "The role of low-power wide-area network technologies in internet of things: A systematic and comprehensive review," *International Journal of Communication Systems*, vol. 35, no. 3, p. e5036, 2022.

[138] A. A. Ateya, A. D. Algarni, M. Hamdi, A. Koucheryavy, and N. F. Soliman, "Enabling heterogeneous iot networks over 5g networks with ultra-dense deployment—using mec/sdn," *Electronics*, vol. 10, no. 8, p. 910, 2021.

[139] P. Yang, Y. Zhang, and J. Lv, "Load optimization based on edge collaboration in software defined ultra-dense networks," *IEEE Access*, vol. 8, pp. 30664–30674, 2020.

[140] H. Guo, J. Liu, J. Zhang, W. Sun, and N. Kato, "Mobile-edge computation offloading for ultradense iot networks," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4977–4988, 2018.

[141] R. Patel and R. Arya, "Trust-based resource allocation and task splitting in ultra-dense mobile edge computing network," *Peer-to-Peer Networking and Applications*, vol. 18, no. 1, pp. 1–17, 2025.

[142] O. Alamu, A. Gbenga-Ilori, M. Adelabu, A. Imoize, and O. Ladipo, "Energy efficiency techniques in ultra-dense wireless heterogeneous networks: An overview and outlook," *Engineering Science and Technology, an International Journal*, vol. 23, no. 6, pp. 1308–1326, 2020.

[143] G. Yu, R. Liu, Q. Chen, and Z. Tang, "A hierarchical sdn architecture for ultra-dense millimeter-wave cellular networks," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 79–85, 2018.

[144] R. S. Yarrabothu and G. R. Murthy, "Ultra-dense deployments in next-generation networks and metaverse," in *Towards Wireless Heterogeneity in 6G Networks*, pp. 33–69, CRC Press, 2024.

[145] Y. Dong, H. Hu, Q. Liu, T. Lv, Q. Chen, and J. Zhang, "Modelling and performance analysis of over-the-air computing in cellular iot networks," *IEEE Wireless Communications Letters*, 2024.

[146] X. Zhou, W. Liang, J. She, Z. Yan, I. Kevin, and K. Wang, "Two-layer federated learning with heterogeneous model aggregation for 6g supported internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 5308–5317, 2021.

[147] B. Premalatha and P. Prakasam, "A review on fog computing in 5g wireless technologies: Research challenges, issues and solutions," *Wireless Personal Communications*, pp. 1–30, 2024.

[148] D. Wang, K. B. A. Bakar, B. Isyaku, and L. Lei, "An asynchronous data transmission policy for task offloading in edge-computing enabled ultra-dense iot.," *Computers, Materials & Continua*, vol. 81, no. 3, 2024.

[149] H. Zhang, Y. Dong, J. Cheng, M. J. Hossain, and V. C. Leung, "Fronthauling for 5g lte-u ultra dense cloud small cell networks," *IEEE Wireless Communications*, vol. 23, no. 6, pp. 48–53, 2016.

[150] S. M. Mohammed, A. Al-Barrak, and N. T. Mahmood, "Enabling technologies for ultra-low latency and high-reliability communication in 6g networks.," *Ingénierie des Systèmes d'Information*, vol. 29, no. 3, 2024.

[151] A. Shabbir, S. Rizvi, M. M. Alam, and M. M. Su'ud, "Optimized energy management and small cell activation in ultra-dense networks through a data-driven approach," *PeerJ Computer Science*, vol. 10, p. e2475, 2024.

[152] M. M. Y. Al-Quraan, *Federated learning empowered ultra-dense next-generation wireless networks*. PhD thesis, University of Glasgow, 2024.

[153] X. Ge, S. Tu, G. Mao, C.-X. Wang, and T. Han, "5g ultra-dense cellular networks," *IEEE wireless communications*, vol. 23, no. 1, pp. 72–79, 2016.

[154] S. Chen, F. Qin, B. Hu, X. Li, and Z. Chen, "User-centric ultra-dense networks for 5g: Challenges, methodologies, and directions," *IEEE Wireless Communications*, vol. 23, no. 2, pp. 78–85, 2016.

[155] S. Chen, R. Ma, H.-H. Chen, H. Zhang, W. Meng, and J. Liu, "Machine-to-machine communications in ultra-dense networks—a survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1478–1503, 2017.

[156] E. Demarchou, C. Psomas, and I. Krikidis, "Mobility management in ultra-dense networks: Handover skipping techniques," *IEEE Access*, vol. 6, pp. 11921–11930, 2018.

[157] R. Baldemair, T. Irnich, K. Balachandran, E. Dahlman, G. Mildh, Y. Selén, S. Parkvall, M. Meyer, and A. Osseiran, "Ultra-dense networks in millimeter-wave frequencies," *IEEE Communications Magazine*, vol. 53, no. 1, pp. 202–208, 2015.

[158] V. O. Nyangaresi, "Terminal independent security token derivation scheme for ultra-dense iot networks," *Array*, vol. 15, p. 100210, 2022.

[159] K. M. B. Hasan, M. Sajid, M. A. Lapina, M. Shahid, and K. Kotecha, "Blockchain technology meets 6 g wireless networks: A systematic survey," *Alexandria Engineering Journal*, vol. 92, pp. 199–220, 2024.

[160] J. Wang, X. Ma, Z. Chen, L. Zheng, W. Xie, and X. Wang, "Secrecy wireless information and power transfer in ultra-dense cloud radio access networks," *IEEE Transactions on Wireless Communications*, 2024.

[161] A. Mijuskovic, A. Chiumento, R. Bemthuis, A. Aldea, and P. Havinga, "Resource management techniques for cloud/fog and edge computing: An evaluation framework and classification," *Sensors*, vol. 21, no. 5, p. 1832, 2021.

[162] R. P. Singh, G. Mishra, M. K. Singh, and S. Jain, "An analysis of edge communication architectures for ultra-dense fog networks," in *2024 2nd International Conference on Disruptive Technologies (ICDT)*, pp. 681–686, IEEE, 2024.

[163] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021.

[164] Z. Chen, S. Chen, H. Xu, and B. Hu, "A security authentication scheme of 5g ultra-dense network based on block chain," *IEEE Access*, vol. 6, pp. 55372–55379, 2018.

[165] A. Kiran, P. Mathivanan, M. Mahdal, K. Sairam, D. Chauhan, and V. Talasila, "Enhancing data security in iot networks with blockchain-based management and adaptive clustering techniques," *Mathematics*, vol. 11, no. 9, p. 2073, 2023.

[166] G. Zhu, J. Xu, K. Huang, and S. Cui, "Over-the-air computing for wireless data aggregation in massive iot," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 57–65, 2021.

[167] N. Sharma, M. Magarini, D. N. K. Jayakody, V. Sharma, and J. Li, "On-demand ultra-dense cloud drone networks: Opportunities, challenges and benefits," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 85–91, 2018.

[168] J. Jagannath, N. Polosky, A. Jagannath, F. Restuccia, and T. Melodia, "Machine learning for wireless communications in the internet of things: A comprehensive survey," *Ad Hoc Networks*, vol. 93, p. 101913, 2019.

[169] N. Rajule, M. Venkatesan, R. Menon, and A. Kulkarni, "Adaptive reinforcement learning based joint approach for energy efficiency in ultra dense networks: Arjun model," *Cluster Computing*, vol. 28, no. 2, p. 85, 2025.

[170] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, "6g internet of things: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 359–383, 2021.

[171] P.-G. Ye, J. Zheng, X. Ren, J. Huang, Z. Zhang, Y. Pang, and G. Kou, "Optimizing resource allocation in uav-assisted ultra-dense networks for enhanced performance and security," *Information Sciences*, p. 120788, 2024.

[172] B. Mao, X. Zhou, J. Liu, and N. Kato, "On an intelligent hierarchical routing strategy for ultra-dense free space optical low earth orbit satellite networks," *IEEE Journal on Selected Areas in Communications*, 2024.

[173] O. Alruwaili, J. Logeshwaran, Y. Natarajan, M. A. Alrowaily, S. K. Patel, and A. Armghan, "Incremental rbf-based cross-tier interference mitigation for resource-constrained dense iot networks in 5g communication system," *Heliyon*, 2024.

[174] A. Lavric, A. I. Petrariu, and V. Popa, "Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions," *IEEE Access*, vol. 7, pp. 35816–35825, 2019.

[175] I.-G. Lee and M. Kim, "Interference-aware self-optimizing wi-fi for high efficiency internet of things in dense networks," *Computer Communications*, vol. 89, pp. 60–74, 2016.

[176] A. Salam, "Internet of things for sustainable community development: introduction and overview," in *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*, pp. 1–31, Springer, 2024.

[177] S. Sharanya, "Challenges in 5g building sustainable networks and its opportunities," *Resource Management in Advanced Wireless Networks*, pp. 267–289, 2025.

[178] S. Malta, P. Pinto, and M. Fernández-Veiga, "Using reinforcement learning to reduce energy consumption of ultra-dense networks with 5g use cases requirements," *IEEE Access*, vol. 11, pp. 5417–5428, 2023.

[179] Y. Li, X. Zhao, and H. Liang, "Throughput maximization by deep reinforcement learning with energy cooperation for renewable ultradense iot networks," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 9091–9102, 2020.

[180] F. Salahdine, J. Opadere, Q. Liu, T. Han, N. Zhang, and S. Wu, "A survey on sleep mode techniques for ultra-dense networks in 5g and beyond," *Computer Networks*, vol. 201, p. 108567, 2021.

[181] A. Ghosh and I. Saha Misra, "Enabling sustainable green communication in three-tier 5g ultra dense hetnet with sleep cycle modulated energy harvesting," *Wireless Networks*, pp. 1–24, 2024.

[182] M. Bembe, A. Abu-Mahfouz, M. Masonta, and T. Ngqondi, "A survey on low-power wide area networks for iot applications," *Telecommunication Systems*, vol. 71, pp. 249–274, 2019.

[183] G. Stanco, A. Navarro, F. Frattini, G. Ventre, and A. Botta, "A comprehensive survey on the security of low power wide area networks for the internet of things," *ICT Express*, 2024.

[184] S. Zeadally, F. K. Shaikh, A. Talpur, and Q. Z. Sheng, "Design architectures for energy harvesting in the internet of things," *Renewable and Sustainable Energy Reviews*, vol. 128, p. 109901, 2020.

[185] H. Zhang, S. Huang, C. Jiang, K. Long, V. C. Leung, and H. V. Poor, "Energy efficient user association and power allocation in millimeter-wave-based ultra dense networks with energy harvesting base stations," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 9, pp. 1936–1947, 2017.

[186] M. Ahmed, S. Raza, A. A. Soofi, F. Khan, W. U. Khan, F. Xu, S. Chatzinotas, O. A. Dobre, and Z. Han, "A survey on reconfigurable intelligent surfaces assisted multi-access edge computing networks: State of the art and future challenges," *Computer Science Review*, vol. 54, p. 100668, 2024.

[187] A. Asghari and M. K. Sohrabi, "Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet," *Computer Science Review*, vol. 51, p. 100616, 2024.

[188] M. Valta, P. Koskela, and J. Hiltunen, "Wake-up radio implementation for internet of things," *International Journal of Autonomous and Adaptive Communications Systems*, vol. 9, no. 1-2, pp. 85–102, 2016.

[189] A. Kozłowski and J. Sosnowski, "Energy efficiency trade-off between duty-cycling and wake-up radio techniques in iot networks," *Wireless Personal Communications*, vol. 107, no. 4, pp. 1951–1971, 2019.

[190] L. Wang, K.-K. Wong, S. Jin, G. Zheng, and R. W. Heath, "A new look at physical layer security, caching, and wireless energy harvesting for heterogeneous ultra-dense networks," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 49–55, 2018.

[191] A. Mughees, M. Tahir, M. A. Sheikh, and A. Ahad, "Energy-efficient ultra-dense 5g networks: recent advances, taxonomy and future research directions," *IEEE Access*, vol. 9, pp. 147692–147716, 2021.

[192] A. L. Imoize, H. I. Obakhena, F. I. Anyasi, and S. N. Sur, "A review of energy efficiency and power control schemes in ultra-dense cell-free massive mimo systems for sustainable 6g wireless communication," *Sustainability*, vol. 14, no. 17, p. 11100, 2022.

[193] A. Nazir, J. He, N. Zhu, M. S. Anwar, and M. S. Pathan, "Enhancing iot security: a collaborative framework integrating federated learning, dense neural networks, and blockchain," *Cluster Computing*, pp. 1–26, 2024.

[194] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, "When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5g ultradense network," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2238–2251, 2020.

[195] A. Taneja, N. Saluja, and S. Rani, "An energy efficient dynamic framework for resource control in massive iot network for smart cities," *Wireless Networks*, vol. 30, no. 5, pp. 4447–4458, 2024.

[196] M. A. Jamshed, F. Ayaz, A. Kaushik, C. Fischione, and M. Ur-Rehman, "Green uav-enabled internet-of-things network with ai-assisted noma for disaster management," in *2024 IEEE 35th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–6, IEEE, 2024.

[197] L. Yu, J. Wu, and P. Fan, "Energy efficient designs of ultra-dense iot networks with nonideal optical front-hauls," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7934–7945, 2019.

[198] L. Sleem and R. Couturier, "Speck-r: An ultra light-weight cryptographic scheme for internet of things," *Multimedia Tools and Applications*, vol. 80, no. 11, pp. 17067–17102, 2021.

[199] A. S. Khan, M. I. B. Yahya, K. B. Zen, J. B. Abdullah, R. B. A. Rashid, Y. Javed, N. A. Khan, and A. M. Mostafa, "Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6g-based (6-cmas) cellular network," *IEEE Access*, vol. 11, pp. 20524–20541, 2023.

[200] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5g in the internet of things era: An overview on security and privacy challenges," *Computer Networks*, vol. 179, p. 107345, 2020.

[201] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, S. B. Taher, M. Kabir, S. Muyeen, and A. H. Gandomi, "Towards a secure 5g-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities," *IEEE Access*, 2024.

[202] G. Chopra, R. K. Jha, and S. Jain, "A survey on ultra-dense network and emerging technologies: Security challenges and possible solutions," *Journal of Network and Computer Applications*, vol. 95, pp. 54–78, 2017.

[203] H. Xue, D. Chen, N. Zhang, H.-N. Dai, and K. Yu, "Integration of blockchain and edge computing in internet of things: A survey," *Future Generation Computer Systems*, vol. 144, pp. 307–326, 2023.

[204] O. Aouedi, T.-H. Vu, A. Sacco, D. C. Nguyen, K. Piamrat, G. Marchetto, and Q.-V. Pham, "A survey on intelligent internet of things: Applications, security, privacy, and future directions," *IEEE communications surveys & tutorials*, 2024.

[205] M. A. Ferrag, O. Friha, B. Kantarci, N. Tihanyi, L. Cordeiro, M. Debbah, D. Hamouda, M. Al-Hawawreh, and K.-K. R. Choo, "Edge learning for 6g-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses," *IEEE Communications Surveys & Tutorials*, 2023.

[206] 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," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4004–4022, 2020.

[207] R. Asif, "Post-quantum cryptosystems for internet-of-things: A survey on lattice-based algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, 2021.

[208] S. Li, M. Iqbal, and N. Saxena, "Future industry internet of things with zero-trust security," *Information Systems Frontiers*, pp. 1–14, 2022.

[209] F. Pelekoudas-Oikonomou, P. H. Mirzaee, W. Hathal, G. Mantas, J. Rodriguez, H. Cruickshank, and Z. Sun, "Federated learning-based intrusion detection systems for massive iot," *Security and Privacy for 6G Massive IoT*, pp. 101–128, 2025.

[210] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the internet of things," *IEEE access*, vol. 6, pp. 6900–6919, 2017.

[211] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[212] A. Asghar, H. Farooq, and A. Imran, "Self-healing in emerging cellular networks: Review, challenges, and research directions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1682–1709, 2018.

[213] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities," *IEEE access*, vol. 9, pp. 28177–28193, 2021.

[214] P. He, Y. Zhou, and X. Qin, "A survey on energy-aware security mechanisms for the internet of things," *Future Internet*, vol. 16, no. 4, p. 128, 2024.

[215] T. Liu, G. Ramachandran, and R. Jurdak, "Post-quantum cryptography for internet of things: a survey on performance and optimization," *arXiv preprint arXiv:2401.17538*, 2024.

[216] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE internet of things journal*, vol. 3, no. 5, pp. 637–646, 2016.

[217] A. Bhavya and K. Sudharshan, "Optimizing energy efficiency in battery-powered iot devices through hardware optimization and voltage scaling," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21769–21773, 2025.

[218] S. Nadif, E. Sabir, H. Elbiaze, and A. Haqiq, "Green grant-free power allocation for ultra-dense internet of things: A mean-field perspective," *Journal of Network and Computer Applications*, p. 103908, 2024.

[219] K. Lai, J. Lei, Y. Deng, L. Wen, G. Chen, and W. Liu, "Analyzing uplink grant-free sparse code multiple access system in massive iot networks," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5561–5577, 2021.

[220] J. H. I. de Souza and T. Abrão, "Deep learning-based activity detection for grant-free random access," *IEEE Systems Journal*, vol. 17, no. 1, pp. 940–951, 2022.

[221] T. Kim and B. C. Jung, "Performance analysis of grant-free multiple access for supporting sporadic traffic in massive iot networks," *IEEE Access*, vol. 7, pp. 166648–166656, 2019.

[222] H. S. Jang, B. C. Jung, T. Q. Quek, and D. K. Sung, "Resource-hopping-based grant-free multiple access for 6g-enabled massive iot networks," *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15349–15360, 2021.

[223] L. Liu, E. G. Larsson, W. Yu, P. Popovski, C. Stefanovic, and E. De Carvalho, "Sparse signal processing for grant-free massive connectivity: A future paradigm for random access protocols in the internet of things," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 88–99, 2018.

[224] S. Nadif, E. Sabir, H. Elbiaze, and A. Haqiq, "Grant-free power allocation for ultra-dense internet of things environments: A mean-field perspective," *arXiv preprint arXiv:2402.00008*, 2023.

[225] M. Shirvanimoghaddam, M. Dohler, and S. J. Johnson, "Massive non-orthogonal multiple access for cellular iot: Potentials and limitations," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 55–61, 2017.

[226] W. B. Ameur, *Study of non-orthogonal multiple access schemes for the massive deployment of IoT in future cellular networks*. PhD thesis, INSA de Rennes, 2021.

[227] S. Islam, M. Zeng, O. A. Dobre, and K.-S. Kwak, "Non-orthogonal multiple access (noma): How it meets 5g and beyond," *arXiv preprint arXiv:1907.10001*, 2019.

[228] A. Celik, A. Chaaban, B. Shihada, and M.-S. Alouini, "Topology optimization for 6g networks: A network information-theoretic approach," *IEEE vehicular technology magazine*, vol. 15, no. 4, pp. 83–92, 2020.

[229] C. A. Gomez, A. Shami, and X. Wang, "Machine learning aided scheme for load balancing in dense iot networks," *Sensors*, vol. 18, no. 11, p. 3779, 2018.

[230] H. B. Salameh, S. Abdel-Razeq, and H. Al-Obiedollah, "Integration of cognitive radio technology in noma-based b5g networks: State of the art, challenges, and enabling technologies," *IEEE Access*, vol. 11, pp. 12949–12962, 2023.

[231] X. Liu and X. Zhang, "Noma-based resource allocation for cluster-based cognitive industrial internet of things," *IEEE transactions on industrial informatics*, vol. 16, no. 8, pp. 5379–5388, 2019.

[232] J. Zeng, T. Lv, R. P. Liu, X. Su, M. Peng, C. Wang, and J. Mei, "Investigation on evolving single-carrier noma into multi-carrier noma in 5g," *IEEE Access*, vol. 6, pp. 48268–48288, 2018.

[233] Z. Ding, X. Lei, G. K. Karagiannidis, R. Schober, J. Yuan, and V. K. Bhargava, "A survey on non-orthogonal multiple access for 5g networks: Research challenges and future trends," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 10, pp. 2181–2195, 2017.

[234] S. Bisen, V. Bhatia, and P. Brida, "Successive interference cancellation with multiple feedback in noma-enabled massive iot network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2024, no. 1, p. 71, 2024.

[235] S. A. H. Mohsan, Y. Li, A. V. Shvetsov, J. Varela-Aldás, S. M. Mostafa, and A. Elfikky, "A survey of deep learning based noma: State of the art, key aspects, open challenges and future trends," *Sensors*, vol. 23, no. 6, p. 2946, 2023.

[236] B.-J. Chang and S.-H. Liou, "Adaptive cooperative communication for maximizing reliability and reward in ultra-dense small cells lte-a toward 5g cellular networking," *Computer Networks*, vol. 115, pp. 16–28, 2017.

[237] D. Yang, Y. Cai, Y. Li, X. Jin, and J. Bao, "Optimized decode-and-forward multirelay selection and power allocation in cooperative wireless networks," *Electronics*, vol. 13, no. 17, p. 3541, 2024.

[238] F. Ke, Y. Lin, Y. Liu, H. Zhou, M. Wen, and Q. Zhang, "Task offloading, caching and matching in ultra-dense relay networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 3, pp. 4010–4025, 2022.

[239] Z. Gao, L. Dai, S. Han, I. Chih-Lin, Z. Wang, and L. Hanzo, "Compressive sensing techniques for next-generation wireless communications," *IEEE Wireless Communications*, vol. 25, no. 3, pp. 144–153, 2018.

[240] S. Saadat, D. Chen, and T. Jiang, "Multipath multihop mmwave backhaul in ultra-dense small-cell network," *Digital Communications and Networks*, vol. 4, no. 2, pp. 111–117, 2018.

[241] D. D. Misra and K. K. Sarma, "Cooperative routing mechanism in the 5g ultra dense network," in *2018 5th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 721–725, IEEE, 2018.

[242] D. Lin, Q. Wang, W. Min, J. Xu, and Z. Zhang, "A survey on energy-efficient strategies in static wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 17, no. 1, pp. 1–48, 2020.

[243] I. A. Bartsiokas, P. K. Gkonis, D. I. Kaklamani, and I. S. Venieris, "A dl-enabled relay node placement and selection framework in multicellular networks," *IEEE Access*, 2023.

[244] S. P. Tera, R. Chinthaginjala, G. Pau, and T. H. Kim, "Towards 6g: An overview of the next generation of intelligent network connectivity," *IEEE Access*, 2024.

[245] Y. Mei, Z. Gao, Y. Wu, W. Chen, J. Zhang, D. W. K. Ng, and M. Di Renzo, "Compressive sensing-based joint activity and data detection for grant-free massive iot access," *IEEE Transactions on Wireless Communications*, vol. 21, no. 3, pp. 1851–1869, 2021.

[246] H. Djelouat, A. Amira, and F. Bensaali, "Compressive sensing-based iot applications: A review," *Journal of Sensor and Actuator Networks*, vol. 7, no. 4, p. 45, 2018.

[247] V. K. Singh, V. K. Singh, and M. Kumar, "In-network data processing based on compressed sensing in wsn: A survey," *Wireless Personal Communications*, vol. 96, pp. 2087–2124, 2017.

[248] A. L. Machidon and V. Pejović, "Deep learning for compressive sensing: a ubiquitous systems perspective," *Artificial Intelligence Review*, vol. 56, no. 4, pp. 3619–3658, 2023.

[249] S. Liu, P. Cheng, Z. Chen, W. Xiang, B. Vucetic, and Y. Li, "Contextual user-centric task offloading for mobile edge computing in ultra-dense network," *IEEE Transactions on Mobile Computing*, vol. 22, no. 9, pp. 5092–5108, 2022.

[250] A. L. Machidon and V. Pejovic, "Deep learning techniques for compressive sensing-based reconstruction and inference–a ubiquitous systems perspective," *arXiv preprint arXiv:2105.13191*, 2021.

[251] X. Xu, R. Ansari, A. Khokhar, and A. V. Vasilakos, "Hierarchical data aggregation using compressive sensing (hdacs) in wsns," *ACM Transactions on Sensor Networks (TOSN)*, vol. 11, no. 3, pp. 1–25, 2015.

[252] M. F. Hossain, A. U. Mahin, T. Debnath, F. B. Mosharrof, and K. Z. Islam, "Recent research in cloud radio access network (c-ran) for 5g cellular systems-a survey," *Journal of Network and Computer Applications*, vol. 139, pp. 31–48, 2019.

[253] I. Farhat, F. G. Awan, U. Rashid, H. Anwaar, I. Khezami, I. Boulka-ibet, B. Neji, and F. Nzanywayingoma, "Recent trends in cloud radio access networks," *IEEE Access*, 2024.

[254] S.-H. Park, S. Jeong, J. Na, O. Simeone, and S. Shamai, "Collaborative cloud and edge mobile computing in c-ran systems with minimal end-to-end latency," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 7, pp. 259–274, 2021.

[255] A. Bhandari, A. G. IEEE, S. T. IEEE, J. J. R. IEEE, R. Sharma, and A. Singh, "Latency optimized c-ran in optical backhaul and rf fronthaul architecture for beyond 5g network: A comprehensive survey," *Computer Networks*, p. 110459, 2024.

[256] I. A. Alimi, A. M. Abdalla, A. Olapade Mufutau, F. Pereira Guiomar, I. Otung, J. Rodriguez, P. Pereira Monteiro, and A. L. Teixeira, "Energy efficiency in the cloud radio access network (c-ran) for 5g mobile networks: Opportunities and challenges," *Optical and Wireless Convergence for 5G Networks*, pp. 225–248, 2019.

[257] K. Alam, M. A. Habibi, M. Tammen, D. Krummacker, W. Saad, M. Di Renzo, T. Melodia, X. Costa-Pérez, M. Debbah, A. Dutta, *et al.*, "A comprehensive overview and survey of o-ran: Exploring slicing-aware architecture, deployment options, and use cases," *arXiv preprint arXiv:2405.03555*, 2024.

[258] I. A. Alimi, A. L. Teixeira, and P. P. Monteiro, "Toward an efficient c-ran optical fronthaul for the future networks: A tutorial on technologies, requirements, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 708–769, 2017.

[259] M. Rebhi, K. Hassan, K. Raoof, and P. Chargé, "Sparse code multiple access: Potentials and challenges," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1205–1238, 2021.

[260] P.-H. Kuo and A. Mourad, "User-centric multi-rats coordination for 5g heterogeneous ultra-dense networks," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 6–8, 2018.

[261] A. Flizikowski, T. Marciniak, T. A. Wysocki, and O. Oyerinde, "Selected aspects of non orthogonal multiple access for future wireless communications," *Mathematics in Computer Science*, vol. 17, no. 2, p. 10, 2023.

[262] L. Yu, Z. Liu, M. Wen, D. Cai, S. Dang, Y. Wang, and P. Xiao, "Sparse code multiple access for 6g wireless communication networks: Recent advances and future directions," *IEEE Communications Standards Magazine*, vol. 5, no. 2, pp. 92–99, 2021.

[263] D. Keniya, "Performance analysis of codebooks for uplink scma systems," Master's thesis, California State University, Fullerton, 2020.

[264] P. Liu, K. An, J. Lei, Y. Sun, W. Liu, and S. Chatzinotas, "Computation rate maximization for scma-aided edge computing in iot networks: A multi-agent reinforcement learning approach," *IEEE Transactions on Wireless Communications*, 2024.

[265] S. Bhardwaj and D.-S. Kim, "Deep q-learning based sparse code multiple access for ultra reliable low latency communication in industrial wireless networks," *Telecommunication Systems*, vol. 83, no. 4, pp. 409–421, 2023.

[266] B. T. Mulatu, *Contention Based SCMA for NB-IoT Uplink Communication using Finite Memory Sequential Learning*. PhD thesis, Waseda University, 2018.

[267] Y. Lu, C. Han, C. Maple, M. Dianati, and A. Mouzakitis, "State-of-the-art of sparse code multiple access for connected autonomous vehicle application," *Enabling 5G Communication Systems to Support Vertical Industries*, 2019.

[268] Q. Luo, Z. Liu, G. Chen, P. Xiao, Y. Ma, and A. Maaref, "A design of low-projection scma codebooks for ultra-low decoding complexity in downlink iot networks," *IEEE Transactions on Wireless Communications*, vol. 22, no. 10, pp. 6608–6623, 2023.

[269] Y. Zhang and L. Zhang, "Resource allocation for scma-based iot systems with layered multicast," *IEEE Access*, vol. 9, pp. 144776–144785, 2021.

[270] Y. Ge, L. Liu, S. Huang, D. González, Y. L. Guan, and Z. Ding, "Low-complexity memory amp detector for high-mobility mimo-otfs scma systems," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 807–812, IEEE, 2023.

[271] Z. Li, "An overview of machine learning-driven resource allocation in iot networks," *arXiv preprint arXiv:2412.19478*, 2024.

[272] O. Galinina, A. Pyattaev, S. Andreev, M. Dohler, and Y. Koucheryavy, "5g multi-rat lte-wifi ultra-dense small cells: Performance dynamics, architecture, and trends," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1224–1240, 2015.

[273] M. Amine, A. Walid, A. Kobbane, and J. Ben-Othman, "New user association scheme based on multi-objective optimization for 5g ultra-dense multi-rat hetnets," in *2018 IEEE international conference on communications (ICC)*, pp. 1–6, IEEE, 2018.

[274] T. Nguyen and R. Martin, "Adaptive multi-rat solutions for enhanced iot scalability," *Sensors*, vol. 24, no. 4, pp. 1204–1215, 2024.

[275] L. Williams and P. Brown, "Quality of service in multi-rat iot: Challenges and opportunities," *Sensors*, vol. 24, no. 2, pp. 1124–1136, 2024.

[276] R. Mozny, P. Masek, D. Moltchanov, M. Stusek, P. Mlynek, Y. Koucheryavy, and J. Hosek, "Characterizing optimal lpwan access delay in massive multi-rat smart grid deployments," *Internet of Things*, vol. 25, p. 101001, 2024.

[277] K. Zia, A. Chiumento, and P. J. Havinga, "Ai-enabled reliable qos in multi-rat wireless iot networks: Prospects, challenges, and future directions," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1906–1929, 2022.

[278] H. V. Nguyen, H. M. Kim, G.-M. Kang, K.-H. Nguyen, V.-P. Bui, and O.-S. Shin, "A survey on non-orthogonal multiple access: From the perspective of spectral efficiency and energy efficiency," *Energies*, vol. 13, no. 16, p. 4106, 2020.

[279] S. Sidiq, J. A. Sheikh, F. Mustafa, and B. A. Malik, "A new method of hybrid optimization of small cell range development and density for energy efficient ultra-dense networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 7, p. e4476, 2022.

[280] A. Balcı and R. Sokullu, "Massive connectivity with machine learning for the internet of things," *Computer Networks*, vol. 184, p. 107646, 2021.

[281] B. T. Tinh, L. D. Nguyen, H. H. Kha, and T. Q. Duong, "Practical optimization and game theory for 6g ultra-dense networks: Overview and research challenges," *IEEE Access*, vol. 10, pp. 13311–13328, 2022.

[282] C. Yang, J. Li, M. Sheng, A. Anpalagan, and J. Xiao, "Mean field game-theoretic framework for interference and energy-aware control in 5g ultra-dense networks," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 114–121, 2017.

[283] A. Khodmi, S. B. Rejeb, N. Agoulmine, and Z. Choukair, "A joint power allocation and user association based on non-cooperative game theory in an heterogeneous ultra-dense network," *IEEE Access*, vol. 7, pp. 111790–111800, 2019.

[284] M. S. SHAH, S. Kittipiyakul, Y. Lim, *et al.*, *Cooperative and collaborative resource management in small cell networks using game theory*. PhD thesis, Thammasat University, 2019.

[285] C. Wu, J. Sheng, Y. Wang, and B. Ai, "Game-theory-based spectrum sharing of industrial iot networking in high-speed railway heterogeneous communication system," *IEEE Transactions on Cognitive Communications and Networking*, 2023.

[286] G. Li, Y. Zhao, and D. Li, "Game-theoretic user association in ultra-dense networks with device-to-device relays," *Wireless Personal Communications*, vol. 95, pp. 2691–2708, 2017.

[287] M. E. Mkiramweni, C. Yang, and Z. Han, "Mean field games for 5g ultra-dense networks: A resource management perspective," *Ultra-Dense Networks for 5G and Beyond: Modelling, Analysis, and Applications*, p. 65, 2019.

[288] D. Shi, H. Gao, L. Wang, M. Pan, Z. Han, and H. V. Poor, "Mean field game guided deep reinforcement learning for task placement in cooperative multiaccess edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9330–9340, 2020.

[289] T. Li, C. Li, C. Yang, J. Shao, Y. Zhang, L. Pang, L. Chang, L. Yang, and Z. Han, "A mean field game-theoretic cross-layer optimization for multi-hop swarm uav communications," *Journal of Communications and Networks*, vol. 24, no. 1, pp. 68–82, 2021.

[290] J. Moura and D. Hutchison, "Game theory for multi-access edge computing: Survey, use cases, and future trends," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 260–288, 2018.

[291] P. Semasinghe, S. Maghsudi, and E. Hossain, "Game theoretic mechanisms for resource management in massive wireless iot systems," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 121–127, 2017.

[292] R. A. Banez, L. Li, C. Yang, and Z. Han, *Mean field game and its applications in wireless networks*. Springer, 2021.

[293] T. AlSkaif, M. G. Zapata, and B. Bellalta, "Game theory for energy efficiency in wireless sensor networks: Latest trends," *Journal of Network and Computer Applications*, vol. 54, pp. 33–61, 2015.

[294] D. Wang, W. Wang, Z. Han, and Z. Zhang, "Delay optimal random access with heterogeneous device capabilities in energy harvesting networks using mean field game," *IEEE Transactions on Wireless Communications*, vol. 20, no. 9, pp. 5543–5557, 2021.

[295] Y. Zhang, C. Yang, J. Li, and Z. Han, "Distributed interference-aware traffic offloading and power control in ultra-dense networks: Mean field game with dominating player," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 8814–8826, 2019.

[296] L. Li, Y. Xu, Z. Zhang, J. Yin, W. Chen, and Z. Han, "A prediction-based charging policy and interference mitigation approach in the wireless powered internet of things," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 439–451, 2018.

[297] F. Rahmani, J. H. Joloudari, S. Shamshirband, and S. Mostafavi, "Game theory and evolutionary-optimization methods applied to resource allocation problems in emerging computing environments: a survey," *arXiv preprint arXiv:2012.11355*, 2020.

[298] N. Sawyer and D. B. Smith, "Flexible resource allocation in device-to-device communications using stackelberg game theory," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 653–667, 2018.

[299] X. Wang, B. Liu, and X. Su, "A power allocation scheme using non-cooperative game theory in ultra-dense networks," in *2018 27th Wireless and Optical Communication Conference (WOCC)*, pp. 1–5, IEEE, 2018.

[300] W. Chen, X. Qiu, T. Cai, H.-N. Dai, Z. Zheng, and Y. Zhang, "Deep reinforcement learning for internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1659–1692, 2021.

[301] A. Jaddoa, G. Sakellari, E. Panaousis, G. Loukas, and P. G. Sarigiannidis, "Dynamic decision support for resource offloading in heterogeneous internet of things environments," *Simulation Modelling Practice and Theory*, vol. 101, p. 102019, 2020.

[302] M. A. R. Ibrahim, N. I. Jaini, and K. M. N. K. Khalif, "A comprehensive review of hybrid game theory techniques and multi-criteria decision-making methods," in *Journal of Physics: Conference Series*, vol. 1988, p. 012056, IOP Publishing, 2021.

[303] Z. Liwen, F. Qamar, M. Liaqat, M. N. Hindia, and K. A. Z. Ariffin, "Toward efficient 6g iot networks: A perspective on resource optimization strategies, challenges, and future directions," *IEEE Access*, vol. 12, pp. 76606–76633, 2024.

[304] Q. Jiang, X. Xu, Q. He, X. Zhang, F. Dai, L. Qi, and W. Dou, "Game theory-based task offloading and resource allocation for vehicular networks in edge-cloud computing," in *2021 IEEE International Conference on Web Services (ICWS)*, pp. 341–346, IEEE, 2021.

[305] R. Zheng, H. Wang, M. De Mari, M. Cui, X. Chu, and T. Q. Quek, "Dynamic computation offloading in ultra-dense networks based on mean field games," *IEEE Transactions on Wireless Communications*, vol. 20, no. 10, pp. 6551–6565, 2021.

[306] M. Huang, P. E. Caines, R. P. Malhame, and G. Yin, "Large population stochastic dynamic games: Closed-loop mckean–vlasov systems and the nash certainty equivalence principle," *IEEE Transactions on Automatic Control*, vol. 52, no. 4, pp. 683–696, 2006.

[307] Y. Wang, C. Yang, T. Li, X. Mi, L. Li, and Z. Han, "A survey on mean-field game for dynamic management and control in space-air-ground network," *IEEE Communications Surveys & Tutorials*, 2024.

[308] L. Li, Q. Cheng, X. Tang, T. Bai, W. Chen, Z. Ding, and Z. Han, "Resource allocation for noma-mec systems in ultra-dense networks: A learning aided mean-field game approach," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1487–1500, 2020.

[309] M. Aggarwal, V. Khullar, and N. Goyal, "A comprehensive review of federated learning: Methods, applications, and challenges in privacy-preserving collaborative model training," *Applied Data Science and Smart Systems*, pp. 570–575, 2024.

[310] A. Alabdulatif and N. N. Thilakarathne, "Bio-inspired internet of things: current status, benefits, challenges, and future directions," *Biomimetics*, vol. 8, no. 4, p. 373, 2023.

[311] A. Rehman and O. Alharbi, "Bioinspired blockchain framework for secure and scalable wireless sensor network integration in fog–cloud ecosystems," *Computers*, vol. 14, no. 1, p. 3, 2024.

[312] Z. Jakšić, S. Devi, O. Jakšić, and K. Guha, "A comprehensive review of bio-inspired optimization algorithms including applications in microelectronics and nanophotonics," *Biomimetics*, vol. 8, no. 3, p. 278, 2023.

[313] P. V. Dantas, W. Sabino da Silva Jr, L. C. Cordeiro, and C. B. Carvalho, "A comprehensive review of model compression techniques in machine learning," *Applied Intelligence*, vol. 54, no. 22, pp. 11804–11844, 2024.

[314] S. Heydari and Q. H. Mahmoud, "Tiny machine learning and on-device inference: A survey of applications, challenges, and future directions," *Sensors*, vol. 25, no. 10, p. 3191, 2025.

[315] R. David, J. Duke, A. Jain, V. Janapa Reddi, N. Jeffries, J. Li, N. Kreeger, I. Nappier, M. Natraj, T. Wang, *et al.*, "Tensorflow lite micro: Embedded machine learning for tinyml systems," *Proceedings of machine learning and systems*, vol. 3, pp. 800–811, 2021.

[316] S. Somvanshi, M. M. Islam, G. Chhetri, R. Chakraborty, M. S. Mimi, S. A. Shuvo, K. S. Islam, S. A. Javed, S. A. Rafat, A. Dutta, *et al.*, "From tiny machine learning to tiny deep learning: A survey," *arXiv preprint arXiv:2506.18927*, 2025.

[317] E. Dritsas and M. Trigka, "Federated learning for iot: A survey of techniques, challenges, and applications," *Journal of Sensor and Actuator Networks*, vol. 14, no. 1, p. 9, 2025.

[318] D. Chai, L. Wang, L. Yang, J. Zhang, K. Chen, and Q. Yang, "A survey for federated learning evaluations: Goals and measures," *IEEE transactions on knowledge and data engineering*, vol. 36, no. 10, pp. 5007–5024, 2024.

[319] N. Benarba and S. Bouchenak, "Bias in federated learning: A comprehensive survey," *ACM Computing Surveys*, 2025.

[320] Z. Li, H. Li, and L. Meng, "Model compression for deep neural networks: A survey," *Computers*, vol. 12, no. 3, p. 60, 2023.

[321] P. Bartoli, C. Veronesi, A. Giudici, D. Siorpaes, D. Trojaniello, and F. Zappa, "Benchmarking energy and latency in tinyml: A novel method for resource-constrained ai," *arXiv preprint arXiv:2505.15622*, 2025.

[322] M. Adam and U. Baroud, "Federated learning for iot: Applications, trends, taxonomy, challenges, current solutions, and future directions," *IEEE Open Journal of the Communications Society*, 2024.

[323] N. Schizas, A. Karras, C. Karras, and S. Sioutas, "Tinyml for ultra-low power ai and large scale iot deployments: A systematic review," *Future Internet*, vol. 14, no. 12, p. 363, 2022.

[324] Y. M. Abdelradi, A. A. El-Sherif, and L. H. Afify, "A queueing theory approach to small-cell assisted iot traffic offloading," in *2019 IEEE Global Conference on Internet of Things (GCIoT)*, pp. 1–7, IEEE, 2019.

[325] J. Cao, T. Peng, X. Liu, W. Dong, R. Duan, Y. Yuan, W. Wang, and S. Cui, "Resource allocation for ultradense networks with machine-learning-based interference graph construction," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2137–2151, 2019.

[326] M. J. Daas, M. Jubran, and M. Hussein, "Energy management framework for 5g ultra-dense networks using graph theory," *IEEE Access*, vol. 7, pp. 175313–175323, 2019.

[327] B. Zhou and W. Saad, "Performance analysis of age of information in ultra-dense internet of things (iot) systems with noisy channels," *IEEE transactions on wireless communications*, vol. 21, no. 5, pp. 3493–3507, 2021.

[328] B. Zhou and W. Saad, "Age of information in ultra-dense iot systems: Performance and mean-field game analysis," *IEEE Transactions on Mobile Computing*, 2023.

[329] B. Zhou and W. Saad, "Age of information in ultra-dense computation-intensive internet of things (iot) systems," in *2021 19th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt)*, pp. 1–8, IEEE, 2021.

[330] G. Chisci, H. ElSawy, A. Conti, M.-S. Alouini, and M. Z. Win, "Uncoordinated massive wireless networks: Spatiotemporal models and multiaccess strategies," *IEEE/ACM Transactions on Networking*, vol. 27, no. 3, pp. 918–931, 2019.

[331] F. Zaman, M. Aloqaily, F. Sallabi, K. Shuaib, and J. B. Othman, "Application of graph theory in iot for optimization of connected healthcare system," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2020.

[332] G. Chisci, H. ElSawy, A. Conti, M.-S. Alouini, and M. Z. Win, "On the scalability of uncoordinated multiple access for the internet of things," in *2017 International Symposium on Wireless Communication Systems (ISWCS)*, pp. 402–407, IEEE, 2017.

[333] H. Wang, Z. Chen, Z. Liu, L. Pan, H. Xu, Y. Liao, H. Li, and X. Liu, "Spot-i: Similarity preserved optimal transport for industrial iot data imputation," *IEEE Transactions on Industrial Informatics*, 2024.

[334] Y.-H. Chiang, K. Terai, T.-W. Chiang, H. Lin, Y. Ji, and J. C. Lui, "Optimal transport based one-shot federated learning for artificial intelligence of things," *IEEE Internet of Things Journal*, 2023.

[335] S. B. Azmy, N. Zorba, and H. S. Hassanein, "Optimal transport for mobile crowd sensing participants," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2019.

[336] S. F. Abedin, A. K. Bairagi, M. S. Munir, N. H. Tran, and C. S. Hong, "Fog load balancing for massive machine type communications: A game and transport theoretic approach," *IEEE Access*, vol. 7, pp. 4204–4218, 2018.

[337] Q. Zhang, Y. Jiang, X. Ge, Y. Huang, and Y. Liu, "Distributed data flow scheduling optimization in industrial internet of things based on optimal transport theory," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12961–12974, 2023.

[338] Z. Li, X. Zhou, Y. Liu, C. Fan, and W. Wang, "A computation offloading model over collaborative cloud-edge networks with optimal transport theory," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1006–1011, IEEE, 2020.

[339] I. Haasler, J. Karlsson, and A. Ringh, "Control and estimation of ensembles via structured optimal transport," *IEEE Control Systems Magazine*, vol. 41, no. 4, pp. 50–69, 2021.

[340] D. Gan, X. Ge, and Q. Li, "An optimal transport-based federated reinforcement learning approach for resource allocation in cloud-edge collaborative iot," *IEEE Internet of Things Journal*, 2023.

[341] D. T. A. Nguyen, D. T. Nguyen, and A. Nedic, "Distributed stochastic optimization with gradient tracking over time-varying directed networks," in *2023 57th Asilomar Conference on Signals, Systems, and Computers*, pp. 1605–1609, IEEE, 2023.

[342] A. Abderrahmane, H. Drid, and A. Behaz, "A survey of controller placement problem in sdn-iot network," *International Journal of Networked and Distributed Computing*, pp. 1–15, 2024.

[343] O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous iot systems," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 2, pp. 726–739, 2023.

[344] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, "Hybrid blockchain platforms for the internet of things (iot): A systematic literature review," *Sensors*, vol. 22, no. 4, p. 1304, 2022.

[345] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1007–1016, IEEE, 2018.

[346] S. M. S. Saad, R. Z. R. M. Radzi, and S. H. Othman, "Comparative analysis of the blockchain consensus algorithm between proof of stake and delegated proof of stake," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, pp. 175–180, IEEE, 2021.

[347] F. H. Alghamedy, N. El-Haggar, A. Alsumayt, Z. Alfawaer, M. Al-shammari, L. Amouri, S. S. Aljameel, and S. Albassam, "Unlocking a promising future: integrating blockchain technology and fl-iot in the journey to 6g," *IEEE Access*, 2024.

[348] Y. Zuo, "Exploring the synergy: Ai enhancing blockchain, blockchain empowering ai, and their convergence across iot applications and beyond," *IEEE Internet of Things Journal*, 2024.

[349] M. R. Mahmood, M. A. Matin, P. Sarigiannidis, and S. K. Goudos, "A comprehensive review on artificial intelligence/machine learning algorithms for empowering the future iot toward 6g era," *IEEE Access*, vol. 10, pp. 87535–87562, 2022.

[350] F. Firouzi, B. Farahani, and A. Marinšek, "The convergence and interplay of edge, fog, and cloud in the ai-driven internet of things (iot)," *Information Systems*, vol. 107, p. 101840, 2022.

[351] T. Malleeshwaran, T. Prasanna, J. A. Daniel, *et al.*, "Ai-driven iot framework for optimal energy management in consumer devices," in *2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL)*, pp. 746–751, IEEE, 2024.

[352] S. Savazzi, M. Nicoli, and V. Rampa, "Federated learning with cooperating devices: A consensus approach for massive iot networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4641–4654, 2020.

[353] J. Ma, S. Hasegawa, S.-J. Kim, and M. Hasegawa, "A reinforcement-learning-based distributed resource selection algorithm for massive iot," *Applied Sciences*, vol. 9, no. 18, p. 3730, 2019.

[354] K. A. Awan, I. U. Din, A. Almogren, and J. J. Rodrigues, "Privacy-preserving big data security for iot with federated learning and cryptography," *IEEE Access*, vol. 11, pp. 120918–120934, 2023.

[355] Y. Wu, "Cloud-edge orchestration for the internet of things: Architecture and ai-powered data processing," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12792–12805, 2020.

[356] U. M. Malik, M. A. Javed, S. Zeadally, and S. ul Islam, "Energy-efficient fog computing for 6g-enabled massive iot: Recent trends and future opportunities," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14572–14594, 2021.

[357] S. P. Singh, A. Nayyar, R. Kumar, and A. Sharma, "Fog computing: from architecture to edge computing and big data processing," *The Journal of Supercomputing*, vol. 75, pp. 2070–2105, 2019.

[358] B. Ali, M. A. Pasha, S. ul Islam, H. Song, and R. Buyya, "A volunteer-supported fog computing environment for delay-sensitive iot applications," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3822–3830, 2020.

[359] T. Goethals, F. De Turck, and B. Volckaert, "Near real-time optimization of fog service placement for responsive edge computing," *Journal of Cloud Computing*, vol. 9, no. 1, p. 34, 2020.

[360] P. P. Ray and N. Kumar, "Sdn/nfv architectures for edge-cloud oriented iot: A systematic review," *Computer Communications*, vol. 169, pp. 129–153, 2021.

[361] G. K. Walia, M. Kumar, and S. S. Gill, "Ai-empowered fog/edge resource management for iot applications: A comprehensive review, research challenges and future perspectives," *IEEE Communications Surveys & Tutorials*, 2023.

[362] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, 2021.

[363] R. Gomes, D. Vieira, Y. Ghamri-Doudane, and M. F. de Castro, "Network slicing for massive machine type communication in iot-5g scenario," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, pp. 1–7, IEEE, 2021.

[364] S. R. Pokhrel, J. Ding, J. Park, O.-S. Park, and J. Choi, "Towards enabling critical mmtc: A review of urllc within mmtc," *IEEE access*, vol. 8, pp. 131796–131813, 2020.

[365] O. Elgarhy, L. Reggiani, M. M. Alam, A. Zoha, R. Ahmad, and A. Kuusik, "Energy efficiency and latency optimization for iot urllc and mmtc use cases," *IEEE Access*, 2024.

[366] J. S. Martins, T. C. Carvalho, R. Moreira, C. B. Both, A. Donatti, J. H. Corrêa, J. A. Suruagy, S. L. Corrêa, A. J. Abelem, M. R. Ribeiro, *et al.*, "Enhancing network slicing architectures with machine learning, security, sustainability and experimental networks integration," *IEEE Access*, vol. 11, pp. 69144–69163, 2023.

[367] A. M. Alwakeel and A. K. Alnaim, "Network slicing in 6g: A strategic framework for iot in smart cities," *Sensors*, vol. 24, no. 13, p. 4254, 2024.

[368] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong, and L. Chen, "A survey of decentralizing applications via blockchain: The 5g and beyond perspective," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2191–2217, 2021.

[369] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, 2019.

[370] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, "A survey on long-range attacks for proof of stake protocols," *IEEE access*, vol. 7, pp. 28712–28725, 2019.

[371] I. H. Abdulqadder, D. Zou, and I. T. Aziz, "The dag blockchain: A secure edge assisted honeypot for attack detection and multi-controller based load balancing in sdn 5g," *Future Generation Computer Systems*, vol. 141, pp. 339–354, 2023.

[372] Y. Pang, "A new consensus protocol for blockchain interoperability architecture," *IEEE Access*, vol. 8, pp. 153719–153730, 2020.

[373] W. Villegas-Ch, J. Govea, R. Gurierrez, and A. Mera-Navarrete, "Optimizing security in iot ecosystems using hybrid artificial intelligence and blockchain models: A scalable and efficient approach for threat detection," *IEEE Access*, 2025.

[374] X. Lu, C. Jiang, and P. Wang, "A survey on consensus algorithms of blockchain based on dag," in *Proceedings of the 2024 6th Blockchain and Internet of Things Conference*, pp. 50–58, 2024.

[375] P. D. Diamantoulakis, V. K. Papanikolaou, and G. K. Karagiannidis, "Optimization of ultra-dense wireless powered networks," *Sensors*, vol. 21, no. 7, p. 2390, 2021.

[376] D. Pradhan and K. Priyanka, "Rf-energy harvesting (rf-eh) for sustainable ultra dense green network (sudgn) in 5g green communication," *Saudi Journal of Engineering and Technology*, vol. 5, no. 6, pp. 258–264, 2020.

[377] T. Kucova, M. Prauzek, J. Konecny, D. Andriukaitis, M. Zilys, and R. Martinek, "Thermoelectric energy harvesting for internet of things

devices using machine learning: A review," *CAAI Transactions on Intelligence Technology*, vol. 8, no. 3, pp. 680–700, 2023.

[378] M. Shirvanimoghaddam, K. Shirvanimoghaddam, M. M. Abolhasani, M. Farhangi, V. Z. Barsari, H. Liu, M. Dohler, and M. Naebe, "Towards a green and self-powered internet of things using piezoelectric energy harvesting," *Ieee Access*, vol. 7, pp. 94533–94556, 2019.

[379] F. Mazunga and A. Nechibvute, "Ultra-low power techniques in energy harvesting wireless sensor networks: Recent advances and issues," *Scientific African*, vol. 11, p. e00720, 2021.

[380] G. Famitafreshi, M. S. Afaqui, and J. Melià-Seguí, "A comprehensive review on energy harvesting integration in iot systems from mac layer perspective: Challenges and opportunities," *Sensors*, vol. 21, no. 9, p. 3097, 2021.

[381] I. F. All, "Preparing for the next wave of innovation: The ongoing evolution of ai and metaverse," 2025.

[382] Y. Wang and J. Zhao, "Mobile edge computing, metaverse, 6g wireless communications, artificial intelligence, and blockchain: Survey and their convergence," in *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, pp. 1–8, IEEE, 2022.

[383] H. Wymeersch, S. Saleh, A. Nimr, R. Halili, R. Berkvens, M. H. Moghaddam, J. M. Mateos-Ramos, A. Stavridis, S. Wänstedt, S. Barmpounakis, *et al.*, "Joint communication and sensing for 6g-a cross-layer perspective," in *2024 IEEE 4th International Symposium on Joint Communications & Sensing (JC&S)*, pp. 01–06, IEEE, 2024.

[384] M. Satyanarayanan, "The emergence of edge computing," *Computer*, 2017.

[385] M. Chiang and T. Zhang, "Fog and iot: An overview of research opportunities," *IEEE Internet of things journal*, vol. 3, no. 6, pp. 854–864, 2016.

[386] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *ieee communications surveys & tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[387] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of lorawan," *IEEE Communications magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[388] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of lpwan technologies for large-scale iot deployment," *ICT express*, vol. 5, no. 1, pp. 1–7, 2019.

[389] P. Popovski, J. J. Nielsen, C. Stefanovic, E. De Carvalho, E. Strom, K. F. Trillingsgaard, A.-S. Bana, D. M. Kim, R. Kotaba, J. Park, *et al.*, "Wireless access for ultra-reliable low-latency communication: Principles and building blocks," *Ieee Network*, vol. 32, no. 2, pp. 16–23, 2018.

[390] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," *arXiv preprint arXiv:1901.03407*, 2019.

[391] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, *et al.*, "Advances and open problems in federated learning," *Foundations and trends® in machine learning*, vol. 14, no. 1–2, pp. 1–210, 2021.

[392] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. Kiddon, J. Konečnỳ, S. Mazzocchi, B. McMahan, *et al.*, "Towards federated learning at scale: System design," *Proceedings of machine learning and systems*, vol. 1, pp. 374–388, 2019.

[393] R. Piyare, A. L. Murphy, C. Kiraly, P. Tosato, and D. Brunelli, "Ultra low power wake-up radios: A hardware and networking survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2117–2157, 2017.

[394] B. Clerckx, R. Zhang, R. Schober, D. W. K. Ng, D. I. Kim, and H. V. Poor, "Fundamentals of wireless information and power transfer: From rf energy harvester models to signal and system designs," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 4–33, 2018.

[395] M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in *2014 international conference on privacy and security in mobile systems (PRISMS)*, pp. 1–8, IEEE, 2014.

[396] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE access*, vol. 4, pp. 2292–2303, 2016.

[397] U. V. Menon, V. B. Kumaravelu, C. V. Kumar, A. Rammohan, S. Chinnadurai, R. Venkatesan, H. Hai, and P. Selvaprabhu, "Ai-powered iot: A survey on integrating artificial intelligence with iot for enhanced security, efficiency, and smart applications," *IEEE Access*, 2025.

[398] C. Pan, M. Elkashlan, J. Wang, J. Yuan, and L. Hanzo, "User-centric c-ran architecture for ultra-dense 5g networks: Challenges and methodologies," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 14–20, 2018.