IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 November 2023, accepted 23 December 2023, date of publication 10 January 2024, date of current version 29 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3352508

TOPICAL REVIEW

Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities

SHAMS FORRUQUE AHMED[1], MD. SAKIB BIN ALAM[2], SHAILA AFRIN[3], SABIHA JANNAT RAFA[3], SAMANTA BINTE TAHER[4], MALIHA KABIR[3], S. M. MUYEEN[5], (Fellow, IEEE), AND AMIR H. GANDOMI[6,7], (Senior Member, IEEE)

[1]Department of Mathematics and Physics, North South University, Dhaka 1229, Bangladesh
[2]Department of Data Science and Artificial Intelligence, Asian Institute of Technology, Khlong Nueng, Chang Wat Pathum Thani 12120, Thailand
[3]Science and Math Program, Asian University for Women, Chattogram 4000, Bangladesh
[4]Department of Computer Science and Engineering, BRAC University, Dhaka 1212, Bangladesh
[5]Department of Electrical Engineering, Qatar University, Doha, Qatar
[6]Faculty of Engineering and Information Technology, University of Technology Sydney, Sydney, NSW 2007, Australia
[7]University Research and Innovation Center (EKIK), Óbuda University, 1034 Budapest, Hungary

Corresponding author: S. M. Muyeen (sm.muyeen@qu.edu.qa)

Open Access funding provided by the Qatar National Library.

ABSTRACT 5G and the Internet of Things (IoT) are a potent combination that offers a vast IoT infrastructure that can support billions of connected devices while maintaining reliability, affordability, and high-speed connectivity. Nevertheless, the integration of 5G-enabled IoT has received insufficient attention from security analysts, engineers, and researchers, resulting in a lack of information and viable solutions. This study investigates the benefits and issues associated with 5G-enabled IoT, including its privacy and security concerns as well as the technology drivers that enable its various layers. By incorporating 5G technology into IoT, several enhancements have been achieved, including enhanced reliability, simplicity, practicability, analysis, efficiency, agility, flexibility, and accessibility. To achieve the full potential of 5G for IoT, however, researchers must also address many research obstacles, such as designing the 5G-IoT architecture, managing committed machine interactions, and addressing security concerns. A promising strategy for overcoming these obstacles involves ensuring compatibility of operating systems with all devices, which will lead to the development of modern open-source standardization for smooth communication across diverse devices. This innovation will improve the security and privacy of 5G-enabled IoT devices by equipping their hardware with the intelligence to recognize, verify, and authorize processes with predetermined characteristics. This will provide authorized users with full autonomy and persistent connectivity, enhancing the overall user experience. However, 5G requires a thorough examination of its implications and difficulties. A safer and more efficient ecosystem for 5G-enabled IoT may be established by addressing these concerns and encouraging industry-wide collaboration.

INDEX TERMS IoT, Internet of Things, 5G-enabled IoT, 5G, 5G-IoT technology, IoT architecture.

I. INTRODUCTION

The IoT is a worldwide system based on common communication protocols that employ a variety of data collection and transmission methods. IoT components were expected to connect more than 34 billion devices worldwide as of 2021 [1]. Since the devices increase each year, huge data are generated, which is problematic as these data are large [2], [3], have more modes [4], [5], move at a faster rate [6], [7], [8], have better data quality [9], [10], [11], and are heterogeneous [12], [13]. In the meantime, 5G networks are emerging as a major driver of IoT innovation and are setting the basis

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

for billions of internet-connected sensors. The co-existence of a 5G network with IoT allows high data transfer rates, low energy usage for devices with limited resources [14], [15], [16], minimal latency (less than 2 milliseconds) [17], [18], [19], and the unification of disparate technologies or platforms. Moreover, there are several methods and technologies that researchers have anticipated over the years for adapting the IoT to the 5G network. Some of these methods are full-duplex (FD) [20], [21], [22], massive multiple-input multiple-output (mMIMO) [23], [24], [25], [26], millimeter-wave (mmWave) [27], [28], and machine-to-machine (M2M) communications [29], [30], [31]. These methods can contribute significantly to the provision of sophisticated services and connect billions of heterogeneous and homogeneous sensor-equipped devices.

The foundation of 5G has been built upon the 4G LTE network, which has already provided users with data, internet, and phone services [8]. The 5G network will considerably enhance speed and reliability, enabling future IoT devices to connect effectively and quickly. 5G networks offer more than 20 times the speed of 4G and a stable internet connection for a significant number of devices at once [32]. 5G networks have a wide gigabit broadcasting capability and can support about 65,000 simultaneous connections. They allow bi-directional shaping of bandwidths and are more secure than a 4G network [3], [33], [34]. The five main architectures of 5G in an IoT network are the network layer, the IoT sensor layer, the communication layer, the architecture layer, and the application layer [22], [35], [36], [37]. These architectures are involved in the data collection process, computation, analysis, and information exchange between the device and communication networks. The development of IoT services has enabled numerous industries, including intelligent home interconnection [38], [39], [40], surgery through remote equipment [41], [42], [43], [44], linked autos, and essential operations. 5G-enabled IoT encompasses a wide range of improvements, including sensitivity, speed, high bandwidth, and multi-device communication. 5G-IoT can be implemented in households, healthcare, cities, smart industries and transportation, thereby enhancing quality of life.

5G has ushered in a massive transformation in the wireless technology sector. With the expansion of 5G-enabled IoT devices and networks, both challenges and security concerns are increasing. These issues include bandwidth efficiency, minimal latency, relatively inexpensive, the need for an extended battery life and reduced energy consumption [45]. Even though the 5G network is faster than normal networks, assuring connectivity in a broad area with a large number of devices and enabling high mobility for these devices is extremely difficult. 5G-enabled IoT devices require a longer battery life because of the increasing power consumption, power deficiency, and battery backup requirements of smart devices [46]. Moreover, a huge number of sensors must be placed in an area to connect a wide variety of devices. When many sensor nodes are installed, the number of connected devices increases, which poses coverage issues [47]. These are the issues with IoT scalability, and software-defined networking may provide a solution [48], [49], [50], [51]. The review studies emphasize the importance of addressing these issues and highlight the need for standardization to protect personal data in the expanding attack surface of 5G-enabled IoT.

While some studies have reviewed 5G-IoT technology and its challenges, few have focused on standards and technical difficulties [8], [52], [53], [54]. Yet, standards and technical difficulties have been the focus of very few review articles. For instance, Shafique et al. [52] discussed the issues associated with 5G-enabled IoT in extensible depth and provided solutions for these challenges. They highlighted how implementing quality of service (QoS) criteria in modern 5G-IoT applications will be difficult because of the changing traffic patterns as well as privacy and connection concerns. However, they did not consider the security issues that may arise when the attack surface expands as the usage of 5G-enabled IoT increases. Sicari also [54] addressed the issues related to the security and privacy of 5G-enabled IoT. The main challenges that have been discussed include data security, disclosure of resources, detecting rogue nodes and trust, as well as recording and reporting. However, how standardization may be incorporated into the protocol to control the security issues or if the existing tools and approaches can be used to resolve these issues was not addressed. In another study [53], the effects of network slicing on 5G-enabled IoT were described. In addition to outlining the benefits of 5G-IoT and its potential uses, the study also discussed the limitations, such as scalability, dynamic security, and variety of applications. However, the issues were addressed in great depth, and the future directions were more generalized than specific. Most of the previous reviews [35], [44], [52], [54], [55], [56], [57], [58], [59], [60], [61] emphasised either privacy and security concerns, enabling technology drivers in 5G-IoT layers, 5G-enabled IoT requirements, or/and challenges, prospects and opportunities of 5G-IoT as shown in Table 1. In contrast, this review concentrates on privacy and security concerns, enabling technology drivers in 5G-IoT layers, and 5G-enabled IoT requirements, providing consumers with valuable insights and enhancing the dependability of their connected devices in light of the potential growth of 5G networks. This comprehensive survey provides valuable insights for researchers, engineers, and policymakers seeking to develop and implement secure and efficient 5G-enabled IoT solutions in an ever-changing technological landscape.

II. OVERVIEW OF THE 5G-IOT ARCHITECTURE

The IoT has been using 4G networks for a long time, but it is becoming increasingly inadequate in meeting the needs of a growing population and more sophisticated IoT applications. The 5G networks are being utilized to largely expand current IoT to improve telecommunication services. Integrating a 5G-enabled IoT framework (Figure 1), supported by

TABLE 1. A comparison between the recent previous reviews and the current one.

Review studies	Main objective (s)	Background and key visions of 5G-IoT	Enabling technology drivers in 5G-IoT layers	Requirements in 5G-enabled IoT	Privacy and security of 5G technology	Challenges, prospects and opportunities of 5G-IoT
Current review	Investigate the benefits and issues associated with 5G-enabled IoT, including its security and privacy issues as well as the technology drivers that enable its various layers.	✓	✓	✓	✓	✓
[35]	Analyze IoT in 5G wireless systems and discuss its potential impact and challenges.	×	✓	×	✓	✓
[44]	Provide an overview of the security protocols used in 5G-enabled IoT communications.	×	×	×	✓	
[52]	Overview of IoT technology, its use cases, challenges, and prospects, with a particular emphasis on the 5G-IoT scenario and its key enabling technologies	✓	×	×	×	✓
[54]	Examine prospective avenues of research concerning 5G systems that are secure and aware of privacy, while evaluating the current security and privacy measures customized for 5G networks.	×	×	×	✓	×
[55]	Investigate the present state of the art, crucial enabling technologies, research patterns, and obstacles associated with 5G IoT.	×	✓	✓	×	×
[56]	Discuss the relationship between IoT and 5G wireless, and how they can work together to create a connected living.	×	×	✓	×	×
[57]	Analyze security risks and provide hierarchical solutions for building secure 5G applications.	×	✓	×	✓	×
[58]	Identify privacy issues in 5G and present solutions to meet privacy protection goals through both regulatory and technological approaches.	×	×	×	✓	×
[59]	Discuss the impact and importance of 5G technology on IoT applications.	×	×	×	×	✓
[60]	Provide an overview of IoT communication solutions and strategies, including the potential of 5G networks.	✓	×	×	×	✓
[61]	Investigate the potential of 5G networks for IoT applications in industrial automation, and explore the available technologies and solutions.	×	✓	×	×	×

✓: discussion available; ×: discussion not available

edge computing and smart sensing devices, represents a new era in the way data is transmitted and processed. Here, 5G networks facilitate rapid data transfer with nearly nonexistent latency [62], allowing for faultless interaction between various intelligent devices. Complementing this infrastructure, edge computing enables the processing and analysis of data at the edge of the network, decreasing reliance on centralized cloud computing and enhancing the potential for timely decisions. Smart sensing devices, on the other hand, can accurately capture and interpret data from the real world because they are equipped with technologically advanced sensors and AI algorithms. Bringing together 5G wireless connectivity, edge computing, and smart sensing devices has the potential to drive innovation across a wide range of sectors, from autonomous vehicles and smart cities to healthcare and industrial automation, radically reshaping the way we connect to and engage with our environments and paving the way for previously unattainable levels of productivity and connectivity.

The security and network advantages of IoT are propelling the evolution of the Internet [55]. However, they pose several issues such as huge numbers of nodes, security, and new protocols. 5G technology enables the incorporation of new technologies into IoT to provide innovative and effective solutions to these issues. For instance, in the agriculture sector, 5G-powered IoT can be utilized for optimization and

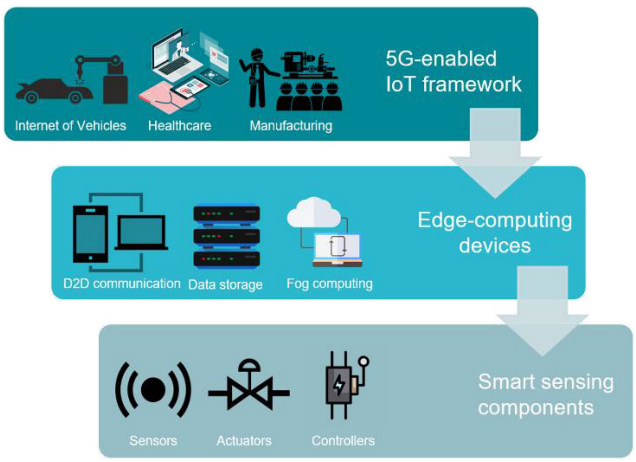


FIGURE 1. 5G-enabled IoT framework.

monitoring crop conditions in real time, ensuring efficient resource usage and higher yields [63].

A substantial quantity of devices will be connected in the near future via the 5G-IoT architecture, which will pave the path for cutting-edge applications including smart cities, the Internet of Vehicles (IoV), manufacturing, agriculture, and healthcare [35]. Wireless sensors, controllers, and actuators are standard components of the 5G-IoT architecture. The communication layer is made up of a device-to-device

(D2D) and connection sub-layer, data storage, fog computing, application, management service, process, collaboration, and security layers [64]. Within the framework of IoV, 5G-enabled IoT can provide real-time traffic data, enabling smart vehicles to navigate efficiently and avoid congested routes, enhancing road safety, and reducing traffic congestion [65].

A study conducted by Rahimi et al. [66] explored the unreliability of IoT 4.0 architecture with growing customer demands. They discussed a next-generation IoT framework based on 5G's new technologies with particular benefits such as D2D architecture and communication. The proposed combined architecture was found to be efficient, agile, scalable, non-complex, and able to satisfy demands. 5G-enabled IoT can be implemented in the healthcare industry to facilitate remote patient monitoring. This would enable medical practitioners to track health metrics and administer timely interventions, thereby improving patient care and decreasing the frequency of hospital visits [67].

Another service-oriented network management framework proposed by Huang et al. [9] offered an architecture that can support effectively managing 5G-enabled IoT systems. This framework lowers network traffic and simplifies the management of the network by introducing a SAaC (service aggregation and caching) scheme. To travel across the data-centric system architecture, SAaC first converts the information into services. The study showed that the SAaC approach decreased reaction time by 20.52-56.09%, traffic by 10.85-37.67%, and energy usage by less than 50% when compared to standard methods. Combining the services lowers the congestion and energy requirements. In smart cities, 5G-enabled IoT can optimize energy usage by intelligently managing street lighting and environmental monitoring, reducing energy consumption and carbon emissions [68].

III. BACKGROUND AND KEY VISIONS OF 5G-IOT

A. BACKGROUND OF 5G-IOT

IoT systems, which connect billions of devices via wireless communications, employ a variety of wireless technologies, including 2G, 3G, 4G, Bluetooth, and Wi-Fi, among others [11]. 1G was limited to voice. Voice and texting were handled by 2G, whereas voice, messaging, and data were handled by 3G, and 4G networks were developed for broadband internet experiences. IoT is vastly used, yet 3G and 4G are not entirely suited for IoT systems [11]. The basis for 5G development will be laid by 4G LTE, which provides users with phones, data, and the internet. 5G will considerably enhance capacity and speed, allowing future IoT devices to connect reliably and quickly. The present 4G LTE technology can deliver 1 Gbps transfer speeds, although factors such as Wi-Fi signals, microwaves, buildings, and other objects can disrupt the 4G signal [69]. Users might get speeds of up to 10 Gbps on 5G networks, and they can connect a huge number of devices at once [55].

To meet the demands of Industry 4.0, smart environments, and other applications, 5G networks and standards are projected to address 4G network issues, e.g. better intricate communications, computing capacities of devices, smart intelligence, and so on [70]. Because systems with IoT devices demand quicker data, 5G is the best option for them. Many IoT applications are now limited by cellular network latency. They are already employing cellular networks such as 4G LTE that are connected to the cloud; however, gadgets in these IoT solutions create so much data that processing and analyzing it rapidly is problematic. When data volume rises, latency increases, which increases delay, and necessitates the use of a faster network, such as 5G. Due to increasing latency, 4G LTE's efficacy is reduced [71].

Machine-type communication (MTC) systems in healthcare projects, smart city projects, and other IoT applications require massive connection networks, resulting in IoT heterogeneity and several implementation issues. Short-ranged MTC, e.g., BLE v4.0 [72], ZigBee [73], Wi-Fi, and long-range communications, for instance, Low power wide area (LPWA) [74], RPMA [75], Sigfox [76], LoRa [76], and so on, have all been deployed in the last two decades. As a mobile-based LPWA solution for IoT, the 3G partnership project (3GPP) has provided Enhanced-MTC (eMTC)—an extensible global system for mobile communication for IoT and narrowband IoT (NBIoT) [69]. Existing cellular networks cannot support MTC communications, which are critical in the IoT. In this situation, the forthcoming 5G networks might be a viable answer. In comparison to the current 4G (LTE), 5G may deliver the fastest data rates for cellular networks with very low latency and better coverage of MTC communications, allowing for the most demanding IoT applications. M2M connectivity facilitates enormous devices and allows the goal of a linked society [77], [78].

Significant work on 5G-IoT has been done in the last few years [79]. Some leading tech companies have collaborated on a 5G wireless study to disclose a revolutionary set of ''neuroscience-based algorithms'' that accommodate video qualities to the needs of the human eye, implying that wireless networks will have built-in human intelligence [55]. 5G will make a significant contribution to the IoT by adding a huge quantity of devices to build a truly huge IoT network that employs devices to communicate and exchange data without human assistance. Given the diverse range of applications, it is challenging for the IoT to determine if a device can meet application requirements [29]. Existing IoT systems mostly leverage specialized application domains, for instance, Bluetooth Low Energy (BLE), ZigBee, and others. Other technologies include Wi-Fi, LP-WA network, and mobile communication (e.g., MTC with 3GPP, and 4G (LTE)), among others. The IoT is continually growing, with new technologies being suggested and established ones expanding into new application domains.

By making IoT and 5G technologies more approachable and flexible, open-source standardization plays a crucial role

in developing their widespread adoption and further development. The open-source standardization model embodies a collaborative and inclusive approach to promote interoperability, innovation, and cost-effectiveness. By utilizing open-source technologies and principles, this initiative promotes the collaborative involvement of developers, researchers, and industry stakeholders in establishing the required standards and protocols for the smooth integration of 5G and IoT technologies. Several noteworthy initiatives and components exist within this domain. These include the open-source 5G core network [80], and open-source IoT platforms [81] such as Eclipse IoT [82], ThingsBoard [83], and IoTMiddleware [84]. Additionally, there are IoT protocols like message queuing telemetry transport (MQTT) [85] and constrained application protocol (CoAP), as well as edge computing frameworks [86], software-defined networking (SDN) [87], network function virtualization (NFV), device management and security, and test and validation tools. The implementation of such a democratized approach not only expedites the rollout of IoT solutions enabled by 5G technology, but also guarantees a framework that is more versatile and adaptable. This framework facilitates the advancement of interconnected devices and services, contributing to the development of a more intelligent and interconnected global community.

B. KEY VISIONS OF 5G-IOT

By 2030, approximately 80 billion devices will be associated with the network and 20.5 billion devices are expected to be connected [35]. In numerous technological domains, IoT and 5G technologies are transforming and paving the way in the fourth industrial revolution. D2D, M2M, vehicle-to-anything (V2A), and vehicle-to-vehicle (V2V) are examples of IoT ideas in which sensors, communication networks, and networked devices provide every convenience [35]. Smart industries, smart transportation, smart healthcare systems, smart agriculture, smart homes, and other life-changing applications may all benefit from IoT. 5G augments IoT by providing better data speeds, shorter latency, less power requirement, and greater flexibility.

The rapid advancement of IoT and 5G technologies promises to provide significant benefits to end-users, notably consumers and businesses [88]. Client information may be used by businesses to improve their services and products. They can also check their resources by using area trackers and remote locking on selected devices [89]. Government and open experts can save medical service costs by arranging improved wellness assistance through remote wellness monitoring, especially for older citizens. Furthermore, lowering the overall upkeep cost of the structures, street maintenance, and smart road lighting may make people's lives easier.

Logistics, retail management, and various ISPs may all benefit from it [90]. The transfer of information between vehicles, streetlights, and sensors via IoT in-vehicle communication may be employed in collision-prone and accident-prone scenarios. Smart houses employ smart lighting, smart energy monitoring, and connections between various electrical gadgets. Public safety and agriculture may both benefit from IoT. In the industrial IoT, robotics internet may be accomplished for smart factories [91]. Some of the top cellular, semiconductor, and service companies are performing research experiments to access 5G wireless technology by 2030 [35]. 5G research and testing are currently taking place at multiple research institutes with world-class laboratory facilities. Recent developments in cellular technologies promise to achieve higher internet speeds and longer battery life, and also improve spectral efficiency, long-range communications, and the ability to communicate with millions of devices. 5G-IoT might be the biggest transformative technology in the information technology domain.

For ubiquitous edge intelligence, image augmented reality, virtual reality, tactile web, and tactile-controlled systems, future data-intensive Industrial Internet of Things (IIoT) services will include real-time broadband (uplink) [92]. Integrated communications and localization services will also be required. To enable these systems, the wireless industrial internet needs to maintain broad and fine-grained coverages as well as context-aware connectivity and ML-enabled flexible network architecture [93]. 5G will be implemented in big urban areas initially, therefore IoT applications for streetlights and traffic lights are likely to be employed first [71]. When 5G is completely operational and covers the entire region, the smart city as a larger idea will be realized using a quicker 5G network where objects interact and make the best decisions and gadgets. At various levels, these applications range from smart homes and smart agriculture to autonomous automobiles and robots. The IoT will change how businesses, governments, and customers connect with the outside world. The analysis revolution, which encompasses machine learning (ML) and artificial intelligence (AI), is the next key item in IoT. This revolution makes smart decisions, autocorrects mistakes, and calibrates devices for improved performance.

IV. ENABLING TECHNOLOGY DRIVERS IN 5G-IOT LAYERS

Drivers of enabling technology in the 5G-IoT layers are crucial to the realization of a connected future. These innovations extend all areas from ultra-low-latency communication technologies that enable real-time applications like autonomous vehicles and industrial automation to energy-efficient designs that lengthen the battery life of IoT devices, guaranteeing their longevity and reducing operational costs. To secure data protection and accommodate the massive number of IoT devices predicted to be linked to 5G networks, robust security mechanisms and scalable network architectures are essential drivers [94]. Furthermore, the introduction of edge computing, ML, and AI within the 5G-IoT framework introduces a revolutionary potential for processing data nearer to its source, improving data analysis, and driving automation across many different industries. The full potential of 5G-IoT, which will revolutionize industries and enrich our daily lives, can only be accomplished by leveraging these enabling technology drivers, which require standardization

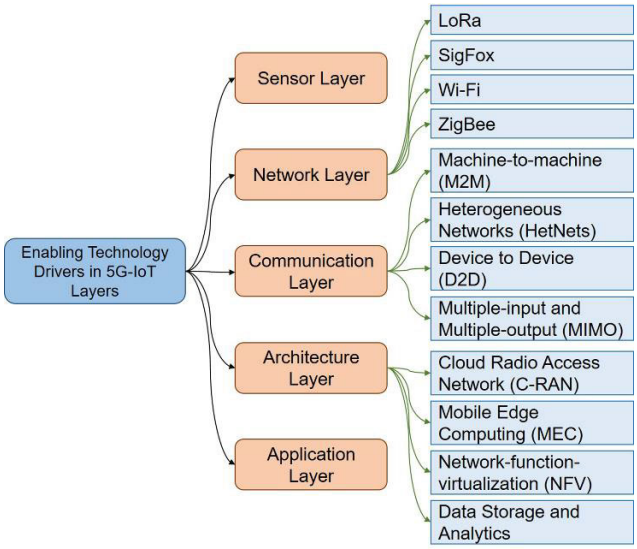


FIGURE 2. Enabling technology drivers in 5G-IoT layers.

efforts, regulatory frameworks, and the collaborative engagement of industry and academia.

The ultra-connectivity required for the future cannot be achieved with the network technologies of the present. When executing extensive IoT initiatives, it is often necessary to integrate wireless and wired network technologies. The stability, response time, mobility, scalability, and security needed for the mission-critical facilities in the ecosystem of IoT could be taken by 5G [95]. The global consumer IoT technology adoption will reach a peak of 100% by 2030 [96]. For end users, 5G offers fundamental conditions and ubiquitous connectivity. These conditions include low latency, maximum throughput, high versatility, efficient power utilization systems, and quick information transmission to enable a large number of devices. The forthcoming 5G technology will support tens of billions of connections, offer a bandwidth efficiency of 10 Gbps, and have a very low latency of 1 ms [55]. The quantity of IoT applications will increase because of the fifth-generation (5G) mobile network, including smart thermostats, kitchen appliances, security cameras, and others [95]. Several crucial enabling technologies, ranging from physical connectivity to IoT applications, are included in the 5G-enabled IoT. The key enabling technology drivers in 5G-IoT are outlined in Figure 2. The recent studies conducted on the communication, architecture, and application layers have been compiled together with their benefits, drawbacks, and potential solutions in Table 2.

V. REQUIREMENTS IN 5G-ENABLED IOT

IoT technology is changing our lives by offering a large number of applications that rely on the communications of extremely diverse devices. Several studies were conducted on the challenging domains of IoT, and the significant aspects of IoT are: low cost of deployment, a large number of linked

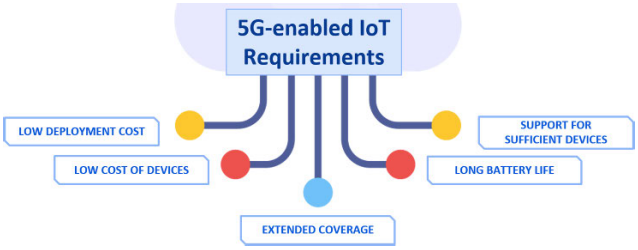


FIGURE 3. Enabling technology drivers in 5G-IoT layers.

devices, and long battery life for billions of low-power, low-cost devices (Figure 3).

A. LOW DEPLOYMENT COST

The expense of infrastructure and deployment is a sensitive issue in addition to the cost of IoT devices. The low-cost roll-out of 5G-IoT services can be attributable to several factors, including the introduction of new technologies with enhanced spectral efficiency, adaptable architecture, and additional spectrum allocation [22], [113]. To ensure low deployment costs, the performance outcomes of the proposed system's design must be exact, repeatable, and re-implementable in the dynamic testing environment. To achieve accurate measurements, the suggested design is evaluated frequently over a given length of the period with specific trial and testbed configurations that allow for precise performance results in the 5G-IoT.

The use of SDN and NFV in 5G implementation will be cost-effective [113]. The remote network function virtualization (WNFV) virtualizes the whole network function to facilitate the implementation of 5G-IoT, with NFV decoupling adaptable and scalable hardware with core network operations to allow 5G-IoT to be focused on a generic cloud server as a complement to 5G networks [114]. 5G NFV will revolutionize the method by which 5G-IoT networks are built, allowing for scalable and adaptable network services. The radio access network's viability will likewise be greatly improved by the NFV. Oughton and Frias [115] analyzed deployment costs in the United Kingdom by grouping places with comparable cost characteristics into distinct 'geotypes.' It discovered that, using current capital intensity, 90% of the population will be served at 50Mbps and the rest 10% will face exponential price rises by 2027. The study reported that spectrum can help reduce the cost of deploying a network that can offer 10 Mbps for each client in rural regions. The findings show that big headline speeds in rural areas should be avoided by policymakers.

Nguyen et al. [116] examined an SDN and DMM-based method. The avoidance of infrastructure-deployment expenses of mobility-related modules at the point of access is a fundamental benefit of this strategy. The control and data planes are also orthogonal in this design. The scalability of SDN with DMM was investigated in this study; however, it did not account for bandwidth consumption penalties or

TABLE 2. Summary of recent studies on the communication, architecture and application layers associated with their advantages and disadvantages.

5G-IoT Layer	Technology drivers	Ref.	Main Task	Outcome	Advantages	Disadvantages	Potential solutions
Communication layer	M2M	Bulashenko et al. [30]	Developed a model of M2M traffic and analyzing its characteristics	Developed a novel framework for M2M communication in wireless sensor systems	Provided greater range, reduced latency, increased throughput, and used less energy	Security and large-scale data collection were important concerns; in these networks, cloud-to-IoT compatibility was commonly hindered	Possible solutions consist of fine-tuning network slicing to accommodate various IoT needs, enhancing quality of service management, and deploying cutting-edge routing protocols to expedite data transmission. The use of distributed data processing and edge computing work together to improve data efficiency while decreasing latency. When combined with strong security measures, efficient resource orchestration guarantees maximum resource utilization. Effective communication in the 5G-IoT landscape is enabled by scalable communication protocols, comprehensive device management, and cooperation with regulatory bodies. Collectively, these approaches address issues and guarantee safe, efficient communication across a wide range of IoT use cases.
	HetNets	Waheidi et al. [98]	Installed extremely dense tiny cellular systems as a part of the architecture of heterogeneous networks	Based on the multi-armed bandit sport, developed a decentralized multiclass CA-MAB	The CA-throughput MABs and efficiency of energy were at 10% of the centralized approach; mobility caused to rise by less than 5%.	The parameters decreased as the network's compaction increased	
		Wu et al. [99]	Robustly predicted traffic for 5G HetNet IoT applications	Compressed sensing-based constructed linear predictors could capture traffic patterns while also lowering computational issues and sampling latency	The suggested system could effectively increase performance while saving time and money; had a low sampling overhead and was highly accurate in predicting the traffic load.	With the growing amount of data traffic flowing between the WLAN system and the supplying GPRS supporting node in the HetNet architecture, a standstill situation could develop	
	MIMO	Bana et al. [100]	Applied massive MIMO to IoT connectivity	Large MIMO could be advantageous in IoT connectivity settings, but it requires close coordination between physical-layer approaches and protocol design	Offered a wireless communication route with fast speed to accommodate a variety of applications without expanding bandwidth or carrier signal	The requirement for many antennae; the expense of the equipment compared to available equipment; the restricted availability of accessible driver support	
	D2D	Hayat et al. [101]	Provided thorough analysis regarding device identification in D2D communication	Evaluation based on rapid system throughput, low latency rates, and effective detection in cellular networks	As the cell interface was often not permitted at out-of-band frequencies, any CU could employ IBD communications	Comparing overlay communication to underlay communication, the intervention between CU and D2D seemed challenging	
		Gaba et al. [102]	Applied D2D security configuration protocol to safeguard important smart city applications	Facilitated the use of adaptive screening to allow Wi-Fi devices to recognize the appearance of DoS assaults; protecting the devices' irreplaceable resources	Formal detection accuracy using BAN logic was used to confirm the protocol; earlier network attacks detection and increased security from MITM attacks compared to the traditional method	Although D2D offers more protection, it is still susceptible to online threats, including computer viruses and IP spoofing	
Architecture layer	MCC	Pallavi et al. [103]	Prominent system for 5G heterogeneous networks enabled energy-efficient mobility management	The suggested system used the elective repetition multi-objective optimization method	ERMO2 system reduced energy loss rate in a heterogeneous network	Data security; difficulties with connections and functionality	Network slicing optimization enables IoT applications to use specialized virtual networks. Data transfer and latency are improved by efficient resource management, dynamic resource allocation, and robust QoS mechanisms. Real-time data processing near IoT devices is possible with advanced edge computing. Prior to network transmission, distributed data processing and analytics at the network edge filter and aggregate data. Establishing secure, efficient communication frameworks requires regulatory collaboration. These solutions address architecture layer issues to improve 5G IoT application scalability, security, and adaptability.
	C-RAN	Tong et al. [104]	Suggested PBFT consensus algorithm for the C-RAN enabled by blockchain	Mitigation of harmful fraud risk and expansion of the blockchain network	Results of the trial demonstrated that trust-fault PBFT's tolerance performance outperformed that of the conventional one; the blockchain network increased in scale	Requirement for significant fronthaul capacity; BBU collaboration and clustering	
	MEC	Zhang et al. [105]	Implemented an automated disease diagnosis and remote health monitoring telemedicine structure based on MEC and AI	Demonstrated the ability to speed up data analysis and cut down on transmission time	The suggested model revealed high accuracy through prediction in the ECG dataset; demonstrated a more effective capacity for medical data processing	Due to the enormous data, security issues in edge computing are considered to be severe; edge computing costs seemed to be very high; advanced infrastructure was needed	
	SDN	Tadros et al. [106]	Evaluated models that utilized LC-PD control system management	The mechanism of LC-PD control plane design boosted communication effectiveness and QoS	The simulation utilized the Mininet-WIFI emulator; comparatively, the LC-PD control plane design improved the QoS of Internet services	To install the Software-defined-network (SDN) controller, the complete system architecture had to be changed	
	NFV	Liyanage et al. [87]	Integrated NFV and MEC to demonstrate how to fulfill the growing networking requirements	MEC could leverage the NFVI as the virtual server to execute mobile edge services with other VNFs	Less capacity was required for the network hardware; put a limit on network power usage; decreased costs for system maintenance; streamlined network upgrades	Need to cohabit with hardware objects in a hybrid cloud environment; NFV settings demanded abstract IT management, in contrast to traditional IT systems	
	Data analytics	Chettri et al. [35]	Optimized effective physical layer processing and communication in the IoT environment	Classification of big data analytics to serve the purpose of data storage and analytics	Transformation of complex information and sensor visualization techniques; automated processes through machine learning; foresaw abnormalities in the product, and process to reduce the chance of failures	Breached the privacy regulations; could be utilized to manipulate client records; might deepen data polarization	
Application layer	eMBB, mmWave, LTE-M and NB-IoT	Minoli et al. [107]	Utilization and implementations of eMBB and mmWave frequencies for 5G-IoT smart city	NB-IoT, and LTE-M both 3GPP technologies, were anticipated to continue to be fully supported in 5G networks	Consensus-based and non-linear decision-making are employed by the 3GPP in terms of technical contribution; the 3GPP databases are not intended for in-depth analysis	Contrary to proprietary technologies, 3GPP-standardized systems often have a large ecosystem and offer a minimum level of efficiency irrespective of the operator	Developing flexible software platforms that can support several IoT applications is an important strategy. The massive amount of data generated by IoT devices necessitates improved data analytics and ML algorithms to derive actionable insights. Trust in IoT applications can only be built through measures like robust encryption and user consent mechanisms. The establishment of
	RNN	Will et al. [108]	Blockchain RNN for IoT cybersecurity	Blockchain applications could be successfully integrated into the infrastructure of smart cities utilizing neural networks	Durability and storage capacities; manufacturing time and energy; security issue	Validation outcomes showed that online attackers might be located and recognized	
	Radio Frequency Identification (RFID)	Thayananthan [109]	Accessibility of treatment facilities and an effective method of handling medical records	CRM principles and IoT and RFID applications improved healthcare facilities through ICT	Compared to scanners, RFID technologies are frequently more expensive; RFID technology seemed more difficult to	ICT utilizing RFID enhanced the quality of e-health applications and healthcare services, exceeding CRM values	

TABLE 2. *(Continued.)* **Summary of recent studies on the communication, architecture and application layers associated with their advantages and disadvantages.**

				comprehend; can be less trustworthy		transparent data usage policies and compliance standards requires cooperation between industry stakeholders and regulatory bodies. These solutions allow the 5G-IoT application layer to overcome issues with data management, security, and scalability, unlocking the full potential of IoT technology.
CNN	Anand et al. [110]	CNN-DMA model to identify malware attacks	The model outperformed Deep-Q, BPNN, RNN-LSTM and other algorithms in terms of accuracy (99%)	Few operations cause CCN to operate much slower; CNN with numerous layers and lack of GPU led to time consuming process	Highly effective; hybrid models could be utilized to combat data security issues	
mMTC, WLAN network (LWIP)	Dzocovic et al. [111]	A femtocell home connection and the 5G network slice notion were coupled to create a 5G home automation solution	Provided extended coverage	Flawed Wi-Fi access based on security	Implementation of a femtocell home router proved to be efficient	
DMM	Shin et al. [112]	Using DMM, a secure path optimization system for smart home systems	Protocol outperformed existing techniques in testing	Security issue; expensive and high setup cost; data loss and overloading issue	The recommended protocol could also be extended to 5G architectures that are standalone and not isolated	
Network Slicing	Walia et al. [113]	Network slice management system enabling the deployment of functions across business models	The methods had an impact on virtualization and enabling use cases for smart factories	Several simultaneous slices may be hampered by an attack on the central infrastructure; data isolation could be another security challenge	Feasible for a smart factory to handle the setup, running, and administration	

the consequences of inter-slice heterogeneity. 5G fixed wireless access (FWA) makes broadband services speedy and cost-effective in regions in which fixed-lined broadband is unavailable. 5G FWA users are expected to have a substantial influence in rising and established economies by providing broadband to places in which fixed-lined carriers no longer operate. Users will benefit most since FWA will give speeds comparable to fiber-based services. Moreover, connecting a home to broadband using FWA can save 74% on per-bit costs than a wired connection [117].

B. LOW COST OF DEVICES

Multi-access edge computing (MEC) places AI, data analytics, and optimization capabilities at the edge and keeps the IoT solution simple and affordable [118]. IoT devices may create massive data. Allowing low-latency execution of this data, rather than in the cloud or on the devices, can help IoT systems maintain their adaptability and allow devices to function with minimal maintenance. Measuring computational complexity can help to ensure the low cost of devices. It assists in increasing the system's efficiency by determining its computational feasibility. It allows for the assessment of additional complexity calculations generated by supplemental apps that are introduced as the system evolves [119].

3GPP has updated its Release 13 specifications to cover narrowband IoT (NB-IoT). In contrast to short-range techniques such as Bluetooth, ZigBee, and others, NB-IoT techniques enable low-powered broad-area communication in the licensed spectrum [55]. With NB-IoT, a tiny bandwidth of roughly 200 kHz may be deployed. It also offers increased coverage, enhanced energy-efficient battery performance, and fewer complications for low-cost gadgets [120]. Reducing cost and high array gain have been the focus of research in both narrowband and broadband mmWave communication, including analog beamforming, hybrid beamforming, and electromagnetism. Zeng and Zhang [121] demonstrated how a lens antenna array-empowered mmWave MIMO communication architecture with fixed radio frequency (RF) connectivity may achieve cost efficiency and substantial antenna gains.

Researchers are developing and implementing low-cost devices in different fields. A low-cost smart power meter model was developed by [122]. The smart power meter's wM-Bus radio module enabled them to be involved in IoT scenarios as a progressed infrastructure, which is already in use for smart water and gas metering. Popa et al. [123] presented a food-observing system that contains low-cost sensors. The humidity level, gas level, and temperature of vacuum-packed meals were all continually monitored by the system. Six air quality IoT devices were constructed in this study [124], each containing four distinct low-cost particulate matter (PM) sensors, and those were distributed at two separate locations in the experiment's region. These tools were outfitted with low power wide area network (LoRaWAN) transceivers to evaluate LPWAN coverage at a city size. The study indicated that a few low-cost PM sensors are capable of observing air quality and identifying PM characteristics and LoRaWAN is appropriate for city-scaled sensor coverage when the connection is a problem. It is widely acknowledged that LoRa is among the most promising technologies for long-range, low-power data transmissions [125]. LoRa has also the capability to function as a self-contained network without any associated subscription fees [126].

C. EXTENDED COVERAGE

Physical device connectivity needs sufficient network bandwidth, long battery life, and enhanced coverage for the devices to reach difficult places [56]. This search for wide-sensing applicability is projected as a key roadblock for legacy wireless communications. With dozens to hundreds of antenna components, Massive MIMO is a rising 5G technology. Larger numbers of antennas enhance signal dimension, which provides higher aggregate data rates, better radiant energy efficiency, and greater interference robustness [127]. Massive MIMO is essential for increasing spectrum efficiency. Multi-user MIMO (MU-MIMO), Very-large MIMO (VLM), and other advanced MIMO algorithms have

recently been developed. The 3GPP LTE-A standard featured MU-MIMO that boosts network capacity by using a larger number of antennas at the base station (BS) [128].

Spatial multiplexing, when combined with high bandwidth, would increase network capacity and decrease signaling, congestion, and network overloads [56]. HetNets are rapidly developing into nested tiny cells, including picocells, microcells, and femtocells [129]. Tiny-cell HetNets are the key components of the upcoming 5G network [98]. These low-powered tiny BSs fill in coverage gaps in the network. In the crowded IoT world, boosted coverage support is a crucial design aspect, and this can be achieved by HetNets. The MTC architecture, for example, was suggested by the European Telecommunication Standard Institute and the 3GPP, in which machine-type devices can connect to the networks via old BSs or tiny cells [130].

To offer long-range communication, LoRa uses a spread-spectrum approach with frequency shifting key modulation that allows data to be demodulated even below the noise floor [131]. The technique notably develops the link budget of the LoRa application. Because of its long-range, LoRa is appropriate for metering systems in mMTC services that require prolonged coverage because of deployment circumstances such as being in a high-rise building's basement. To reduce energy usage and increase coverage capacity, Chafii et al. [132] developed an ML algorithm that is based on a dynamic spectrum. The random selection approach has been replaced with a more effectual method that selects the channels with the highest possibility of being available, the finest coverage, and the fewest repeats.

Kocak et al. [133] demonstrated how, under prolonged coverage, user equipment with inadequate battery life can minimize power usage by reducing payload transmission. Using narrowband resource allocations, preamble acknowledgments, and low-power objectives, in particular, Lujan et al. [134] developed an approach for improving NB-IoT large connections in severe coverage circumstances. This method is centered on optimizing link adaption to reduce radio resource utilization of shared channels. It employed a look-up table, in particular, to speed up the convergence of the key connection parameters, including coding and modulation scheme, along with the number of repeats.

D. LONG BATTERY LIFE

The majority of IoT devices are projected to be battery-powered to allow wireless communication. Substituting or charging batteries would not be simple and cost-effective. Small batteries are also utilized to power IoT-enabled embedded devices [2]. As a result, the need for longer battery life is an impending challenge in IoT implementation that must not be overlooked. The energy consumption for sending messages is generally low, according to typical M2M traffic patterns () [135]. Even though the addition of an add-on power-saving mode for machine-type communications in 3GPP Release 12 [2], assuring extended battery life in IoT devices in orthogonal frequency division-based LTE networks remains a distant prospect [56].

Services with both delay tolerance and delay sensitivity have fixed battery life and bandwidth constraints that facilitate discontinuous communication [136]. The delay-tolerant network is appropriate for a few applications to some extent. It should be carefully examined since some crucial applications such as healthcare, self-driving cars, etc. are high-priority and time-sensitive applications i.e., delay-intolerant. D2D (the short-ranged connection between two devices) is a novel method of data transfer that will improve the 5G-IoT by reducing power consumption, balancing load, and improving the quality of services for users [137].

Frøytlog et al. [138] demonstrated a wake-up radio (WUR) driven IoT testbed prototype with a two-tier end device to IoT server connectivity via Bluetooth-low-energy and long-term-evaluation system. The approach is aimed toward a 5G-IoT situation in which battery-driven huge IoT gadgets are unable to connect directly to the 3GPP network. The two-tier system has been constructed and tested and consists of an Android phone with a specific application, a wake-up transmitter, and numerous nano-watt WUR-enhanced IoT systems. It proves that the system can meet the criteria for longevity (more than 10 years) and data transfer latency requirements (having an application-layer delay level of one second) using real-world tests. In terms of power usage, Alobaidy et al. [139] compared NBIoT, Sigfox, and LoRaWAN. The study revealed that while important power management measures might result in significant power reductions, getting a larger battery lifespan for NBIoT was not easy. Compared to NB-IoT, LoRaWAN and Sigfox techniques demonstrated more battery efficiency.

E. SUPPORT FOR SUFFICIENT DEVICES

The ability of a system to manage a growing number of devices is referred to as scalability. Service overhead, such as bandwidth, latency, energy efficiency, security, etc. may be affected by the number of related gadgets in the network. Because 5G-driven IoT may handle more devices than conventional IoT, scalability should be addressed while designing security and data analytics solutions. Given the significance of data analytics and security in 5G-driven IoT, the suggested design should be relatively dependable and performance-oriented. Low reliability and performance might cause overall 5G-enabled IoT processes to fail, resulting in financial losses and allowing attackers to profit [119].

Heterogeneous networks (HetNet) aim to meet the on-demand needs of service-driven 5G-IoT. HetNets makes it possible for 5G-IoT to deliver on-demand data transfer speeds. Recently, several 5G HetNet solutions were created [66], [140]. The 5G-IoT will install billions of devices with limited resources. A variety of HetNet technologies have been proposed to maintain the service quality for devices in 5G-IoT [140]. MTC devices are becoming a more important part of our daily lives. MTC applications include several distinct characteristics, for instance, a massive quantity of devices.

Nowadays blockchain and AI technologies are being used in 5G-IoT services. Any consensus required to add a new block to a blockchain involves contact between the nodes, hence the network's communication bandwidth is critical [141]. A peer-to-peer network is made up of numerous devices that run at different speeds. There are both fast and sluggish nodes in a network. The network's data propagation speed is slowed by these sluggish nodes. Klarman et al. [142] suggested 'bloXroute,' a blockchain distribution network, to improve blockchain scalability. BloXroute can only send all blocks to all of its Gateways in a fair manner. BloXroute enables encrypted blocks, which prevents the block from being stopped because of its content or any other characteristic.

Escolar et al. [50] developed a novel 5G software firewall architecture for a 5G-IoT network with enhanced capabilities. The architecture has been proven using challenging use cases of huge MTCs involving 1 million devices, totaling 4 Gbps, and 1 million firewall regulations. The approach had a significant performance of roughly 8% packet loss, according to the results of the experiments. However, excessive scalability might be studied within the framework of network slicing and its management, where multiple sorts of measures must be conducted on similar types of traffic to ensure the model's stability.

VI. PRIVACY AND SECURITY OF 5G TECHNOLOGY

Privacy is a right of every individual protected and enhanced by a complex and ever-changing regulatory system. Security in the virtual environment, on the other hand, creates rules and initiatives for safeguarding data and the system's integrity through the delivery of safe access to data availability and the prevention of exchanged information or modification [143]. 5G, the next mobile generation, is projected to provide a slew of innovative features and a better user experience. However, sufficient data and user privacy protection methods are essential because they contribute to society by merging vertical industries like e-health, smart grids, banking, manufacturing, and transportation.

A. KEY ASPECTS OF 5G SECURITY

The strength and dependability of future wireless networks depend critically on certain aspects of 5G security. Authentication, integrity, availability, and confidentiality are the four key security aspects of existing mobile networks. Security controls in 5G have been developed to address many of the risks in today's 2G/3G/4G networks. Because 5G will introduce new and vital applications, it is critical to think of privacy from the architect's perspective, such as observability, unlinkability, anonymity, and pseudonymity [113], [114]. These controls contain new verification features, enhanced subscriber identity safety, and supplementary security procedures. Compared to existing cellular networks' security mechanisms predicated on securing basic connectivity and end-user privacy, the 5G cellular system intends to provide a heightened security strategy. It is implemented across the entire network to tackle authentication, authorization, and accounting challenges for heterogeneous computer networks.

Several dimensions of security and privacy are key design concerns for IoT applications. In real-world contexts, 'Secure by Design' is a modern government practice aimed at ensuring a stable and extensive IoT ecosystem for clients that results in the use of mutual verification, a presumed open network, and an acknowledgment that all links could be tapped. 5G also offers a multi-layered network architecture, requiring security services to be implemented at the network, transport, and application layers [146]. The device identification and the deployment procedure are two of the most essential components in protecting any IoT network. Because MTC devices have restricted processing capacity due to their resource scarcity, they may not be able to trigger current security mechanisms already in use on the internet.

Sturdy encryption and authentication strategies such as advanced encryption suite (AES), Diffie-Hellman (DH), and RivestShamir-Adleman (RSA) are used for confidential data transport, and data exchange, management, and transport, as well as digital signatures. They require a high-performing VOLUME XX, 2017 9 platform as they are centered on cryptographic suites with robust protocols, which is not appropriate for future IoT resource-constrained gadgets [147]. Furthermore, to suit the notions of forthcoming IoT networks, authentication and authorization will necessitate re-engineering. The use of blockchain in the IoT aids in eliminating centralization and making transactions safer, autonomous, and transparent. The general ledger in this architecture is blockchain, which keeps all messages among devices legitimate [148], [149].

5G's unprecedented connectivity and rapid speeds, however, introduce new risks and difficulties. Data security, user privacy, network infrastructure security, and cyberattack resilience are all included in this category of considerations. When it comes to protecting sensitive information and valuable resources on a network, the most important measures are robust encryption mechanisms, secure authentication protocols, and efficient intrusion detection systems. Moreover, with the rise of IoT devices in 5G networks, it becomes more challenging to guarantee the safety of such a vast and varied collection of interconnected devices. Establishing best practices and frameworks that can adapt to the evolving threat landscape and guarantee that 5G networks are secure by design requires close cooperation between industry stakeholders, standardization bodies, and regulatory authorities. Taking care of these key issues is crucial to creating a reliable and resilient 5G ecosystem that can fulfill the promises of the next generation of connectivity without compromising users' privacy and security.

B. PRIVACY OF 5G NETWORK

Privacy in 5G networks involves user data, individual rights, and communication confidentiality in a connected world. Because 5G networks will foment massive evolution in terms

of everyday life activities and access modalities to digital services, privacy will be critical. In addition, 5G presents new service-oriented and structural needs, unlike earlier mobile networks, and calls for strict regulations and privacy standards [58]. For entire ecosystems, including users and other stakeholders, 5G privacy will be crucial. Consequently, to achieve widespread adoption and acceptance, 5G privacy concerns must be tackled thoroughly. Data, location, and identity privacy are the three primary aspects of user privacy in a 5G network [144].

By analyzing the features of specific services, 5G technology would be able to provide users with personalized network services. As a result, privacy standards in the 5G network may differ depending on the service. However, service-oriented privacy requirements will be possible with 5G technology. Users' health information, for example, will necessitate a higher level of privacy in specific healthcare applications. ''location-based services'' (LBS) are frequently used when it comes to the growth of future wireless technologies. In such instances, users' locations are actively monitored with the launch of 5G, which would allow seamless and constant availability of services [150]. Besides, this type of tracking service aids businesses in improving existing services and developing new user-friendly ones. However, it creates severe privacy concerns for users.

The seamless and efficient implementation of a 5G private network depends on several factors such as the flexibility to explore and iterate fast at less expense, the availability of complementary assets and knowledge, and data competence. With the flexibility of the 5G network, even customers with robust security requirements can run their secondary authentication algorithms, protocols, and sector-specific features [151]. Any organization operating in the 5G environment should develop a processor and urge its legal teams to do a transfer impact analysis among the policy choices for preventing privacy risks and obstacles. A hybrid solution, where private or confidential data is stored regionally, near, and within an individual's national borders (edge cloud), and less-sensitive data is saved in the cloud, could be a viable alternative [152]. Industry, regulatory bodies, and technology developers need to pay close attention to ensure that 5G networks can evolve in a way that respects and protects personal privacy to strike a balance between 5G's transformative potential and the preservation of individual privacy rights in the digital age.

VII. CHALLENGES, PROSPECTS AND OPPORTUNITIES OF 5G-IOT

The IoT vision's challenges were offered for future reference as there is no one-size-fits-all approach for establishing IoT use cases. Virtualization of network parts and novel deployment paradigms such as intent-based networking and SDN are essential facilitators of 5G and IoT scenarios [153]. Furthermore, there is a vast new scenario for network security concerns to be examined, and it is especially conducive to the implementation of AI and ML approaches to improve and generate new network-based services. IoT has already found uses in many business sectors, providing automation, information, and other services that previously were not possible. Even so, several entities overlook the hurdles IoT devices pose to 5G networks when it comes to technical management, standardization, securing network architecture, and privacy.

A. STANDARDIZATION CHALLENGES

The standardization of 5G security is yet in the development process, and numerous relevant organizations are making significant contributions to its fast evolution. By integrating billions of smart devices to generate truly enormous IoT, where they mutually interact and share data without external assistance, 5G can substantially improve the forthcoming IoT. Currently, the recognition of a device's capability to fulfill application requirements is an obstacle for the IoT due to the heterogeneous nature of application domains [154]. Privacy and security concerns, unstructured data, and data analysis techniques are some issues in standards within 5GIoT. A study by Li et al. [55], specifically designed solely for the correlation between IoT and 5G, disclosed that one of the critical barriers of a 5G-IoT architecture is associated with VOLUME XX, 2017 9 standardization. It includes regulatory standards, technology standards (e.g., network protocols, wireless communication, and data accumulation standards), and data privacy and security (e.g., protection of general data, cryptographic primitives, algorithms for data analysis, and unstructured data).

Multiple macrocell base stations, small-cell base stations, and several UEs can cause interference in 5G networks. As a result, a procedure for power regulation, channel allocation, cell affiliation, and load balancing that is efficient and dependable in terms of flawless interference management is required [155]. The 5G-IoT is a sophisticated ecosystem capable of bridging the gap between humans and their surroundings. The concept of ''IoT as a service'' could emerge because of destined standardization [156]. 5G networks must be capable of supporting scalable user demand throughout the coverage region because multiple users may seek a set of services simultaneously [157]. Several studies have suggested NFV- and SDN-based architectures to solve this issue as their fusion offers benefits to succeed in high network efficacy and performance [158], [159], [160]. The importance of supporting QoS also heightened the relevance of describing and classifying various classes. To improve coverage and satisfy other resource needs, it is vital to retrieve data from the network in both static and dynamic ways. Consequently, end-to-end (E2E) SDN technologies were recommended and deployed to fulfill the requirements of 5G and beyond [158].

B. CACHING AND DATA PROCESSING

Implementing caching and data processing at network nodes in 5G IoT networks presents several complex issues that require careful consideration. Because of the heterogeneous nature of 5G IoT networks, encompassing a diverse array of

devices with varying competencies and connectivity alternatives, ensuring seamless compatibility between edge devices and caching solutions can be complicated [155]. Intelligent algorithms are essential for effective cache management, entailing decisions on relevant data to cache at network nodes and determining optimal timing for data updates or eviction. This process involves striking a delicate balance between data freshness and cache hit rates. The absence of standardization may impede widespread adoption and contribute to fragmentation within the IoT ecosystem [161], [162], [163].

Recently, several initiatives have been introduced to reward caching participants and improve the caching procedure. For example, in a 5G-enabled IoT network, Mirzaee et al. [164] proposed a caching strategy designed to tackle a competitive scenario in which multiple 5G mobile network operators and content providers are involved. They also suggested a novel iterative algorithm to examine the Stackelberg equilibrium hinged on the convex optimization method. The experimental results from various simulations revealed that the game-based incentive strategy offers significant improvements by alleviating the burden on backhaul links while enhancing the quality of user experience.

Another study by Ekawu [165] investigated how to optimize the use of radio resources in 5G-enabled massive IoT networks through cooperative edge caching. They proposed the DRL-CCC and IBBM-RRA algorithms to optimize caching decisions and radio resource allocation respectively. The DRL-CCC algorithm reduced DQN overestimations, accelerating convergence speed. However, the DRL-CCC algorithm's applicability may be limited in scenarios with massive base stations. Meanwhile, the IBBMRRA algorithm efficiently handled large-scale CIP problems with numerous integer variables. The algorithms effectively improved the content caching hit ratio and reduced content retrieving delays. Overcoming these issues necessitates associative research in computer science, hardware design, security, networking, and data management. In addition, expansion in machine learning, edge computing, and distributed systems is crucial in unlocking the complete potential of caching and data processing in 5G IoT networks.

C. TECHNICAL ISSUES

There is still a significant distance between the commitments and the initial deployment of 5G networks. As a result, specific technologies should be utilized in the installation of 5G. For example, reception and transmission at mmWave have significant path-loss and a high absorption rate from atmospheric conditions such as rain and flora. It paves the way for a novel concept: a tiny, low-power cellular base station. Consequently, a mini cellular design in the form of a micro-, pico-, or femtocell is necessary to reduce path loss and refine coverage at mmWaves [52]. High throughput and low latency are other requirements of 5G technology that are met by incorporating full-duplex tech, which emphasizes antennas' transceiving process [166]. However, these techniques are still in the early stages, and work to address their shortcomings and develop a comprehensive 5G enabling system is ongoing. Many issues remain in the architecture design, including scalability, network management [167], [168], interoperability, heterogeneity [55], [169], and privacy risks.

While scalability is important, there are still technical holes in SDN that must be rectified [69]. The scalable SDCN is a concern for network scalability since it empowers the core network with a high level of flexibility. IoT application implementation is complex due to its vast scale, heterogeneous environment, and resource-constrained gadgets. Likewise, collecting and disseminating data in the physical world is a challenge in efficiency and capabilities. Interference is a significant aspect that can potentially control the entire network performance and reduce the QoS capacity in the femtocells installation. Therefore, to achieve adequate standards of QoS, research into interference management algorithms and approaches linked to interference cancellation and/or avoidance is essential [170]. Handoff administration in 5G technology VOLUME XX, 2017 9 encounters the same issues as contemporary cellular networks, such as improved routing, low latency, security, and a lower threat of losing services, making it harder to manage [155].

D. TRANSITION FROM 5G TO 6G

The transition stage from 5G to 6G technology poses several significant challenges and complexities that demand careful consideration and research efforts. First and foremost, one of the most pressing problems in this transition is the need for a comprehensive understanding of the fundamental differences between these two generations of wireless technology [171]. As 6G is still in its infancy, it lacks welldefined standards and specifications, making the transition inherently uncertain. Secondly, the increased frequency bands and technological advancements in 6G introduce concerns related to electromagnetic spectrum management [172], interference mitigation [173], and radio wave propagation characteristics [174]. These obstacles necessitate substantial research and development to ensure the smooth integration and deployment of 6G networks. Furthermore, building on existing studies from 5G can be problematic, as 6G may require a paradigm shift in network architecture and design [175]. This necessitates thorough revision and adaptation of existing research findings and methodologies to suit the unique demands of 6G technology.

One of the major concerns is the integration of 6G with available infrastructure and systems [176]. The transformation to 6G will require significant hardware and software upgrades, and compatibility issues with older networks and devices must be addressed. This involves not only technological considerations but also complex regulatory and standardization challenges. Another key problem is the sustainability and energy efficiency of 6G networks. As 6G is expected to push the boundaries of technology with higher

rates of data, lower latency, and an explosion of connected devices, it will likely demand even more power [177].

Finding eco-friendly and sustainable solutions, such as green energy sources and advanced power management, is essential to prevent a substantial increase in the carbon footprint of the telecommunication industry. To navigate the challenges successfully, an increased focus on interdisciplinary research, collaboration, and investment in foundational studies is imperative. Only by addressing these issues and building upon the lessons of 5G can the transition to 6G technology be smooth, efficient, and fruitful.

E. SECURITY GUARANTEE AND PRIVACY ISSUES

This expeditious 5G prowess will not only supplement the network and serve as a 4G upgrade but will also pave the way for a new tactic in which technical capabilities such as latency, data speed, connectivity, etc. will have a more significant influence than in earlier generations (i.e., 3G, 4G). When the 5G network comes online, the security threat breaches will be relatively higher. D2D communication will be challenging because of its undeviating connectivity across adjacent devices and the massive number of devices linked to 5G [161]. Security is a crucial challenge owing to the heterogeneity of machines, Flash NetFlow traffic, physical connectivity to actuators, radio interfaces safety, sensors, and entities, roaming security, and most pertinently, the accessibility of the systems that are fixed to the internet across a wireless communication medium [162].

Current findings have shown possible security issues that must be confronted to safeguard the security of emerging 5G services, equipment, and clients. For instance, multi-tenant shared cloud systems necessitate robust isolation at different stages to prevent unauthorized resource usage and protect the integrity of consumers' data [163]. To prevent the exploitation of network components accessible to apps, programmable network frameworks like SDN (software defined networking) need credentials and approval for applications. Malicious code assaults, the inability to get security patches, smart meter hacking, sniffing attacks, eavesdropping, and denial of service cyberattacks are all security concerns [164], [165].

The rapid development of wireless sensor networks (WSNs) in IoT has led to the adoption of intelligent features to address security issues. For instance, Xu et al. [178] focused on securing the routing process against attacks such as data tampering, path loss, sniffing, and network takeover. They introduced a trust routing algorithm (BiTRS) that effectively detects and prevents attacks without disrupting data routing among network devices. The algorithm combines ant colony optimizations (ACO) and physarum autonomic optimization (PAO) to adapt to dynamic changes in the network nodes that define the route to the target node. Nevertheless, the algorithm does not contemplate energy conservation, a crucial element in 5G IoT.

Identity, data, and location could pose privacy concerns from the users' viewpoint. User location privacy is primarily targeted by semantic information intrusions, boundary attacks, and timing attacks. Building up a false base station that no longer has ingress to temporary mobile subscribers' identities leads to similar assaults [179]. Communication service providers, virtual mobile network operators, and network infrastructure operators are some actors in 5G networks. Security and privacy are distinct concerns for each of these entities. This synchronization of mismatched privacy standards may be an obstacle in the 5G because mobile operators may lose system control and depend on new actors. Furthermore, the 5G network has no physical borders because of the storage of cloud-based data, and NFV (network function virtualization) technology implications. Since different countries have varying levels of data protection based on their chosen context, users' data privacy stored in another country's cloud is threatened [180], [181].

The most sought-after technologies to meet current requirements in networking are Software Defined Networking (SDN) and Network Functions Virtualization VOLUME XX, 2017 9 (NFV), which leverage the advancements in cloud computing, including mobile edge computing. However, new concerns have emerged regarding the secure implementation of these technologies and the protection of user privacy in future wireless networks. Ongoing research seeks to address security concerns demonstrated by Zhou et al. [182], who have put forth a secure system for D2D communication. This system relies on elliptic curve cryptography and lightweight authenticated encryption with associated data (ciphers, specifically designed for IoT devices with limited resources. This framework ensures data confidentiality, integrity, and UE authentication in each data transmission step, offering improved performance, energy efficacy, and protection against security issues such as privacy sniffing, impersonation, eavesdropping, location spoofing, and free-riding.

An issue affecting IoT security communication is the inability to blend a shared architecture and specific security methods. A combination of blockchain technology and IoT systems can mitigate some security issues [55]. Identity verification systems must be investigated and designed to resolve these issues and verify secure end-to-end connections for IoT networks for resource-constrained gadgets. The true identity of mobile IoT users should be hidden from everyone but should be accessible by an administrator if necessary, and location privacy is critical because it can expose the precise position of the device. For efficient adoption of IoT use cases, both forward and backward safety should be offered [183]. Meanwhile, an anonymization system can be one of the viable techniques to ensure the subscriber's unlinkability and device identity [184]. However, energy consumption, slower data transactions, scalability, lack of standards, low storage space, and low processing power are only a few of the major issues. According to various figures, the number of IoT devices is growing, which necessitates more battery strength and speed for processing. Block mining is computationally expensive and energy-intensive in blockchain technology [185].

F. OPPORTUNITIES AND PROSPECTS OF 5G-IOT

In each domain, experts are working to advance their research. Because of the soaring expectations and needs of 5G-equipped IoT networks navigated by unimagined use cases, substantial research studies have been undertaken. The expected revolutionary transformation to 5G is that it will bring new radio (NR)-based deployment, which may further ameliorate 4G/LTE-based small cell networks with ultra-low latency and ultra-reliable transmissions [170]. The 5G-IoT combines multiple technologies that have a profound effect on IoT applications. It's worth noting that allowing modern IoT connection in license-permitted spectrum bands will be a significant promoter for evaluating IoT use cases, as it allows for a variety of applications and service opportunities to be combined into a single network [55].

Given the limitations of data transfer networks, transferring vast information to the cloud for deep learning will waste a lot of energy, cause a lot of delay, and lower the efficacy of deep learning activities [178]. To address the difficulty of a cloud-centric system, Song et al. [186] recommended an incremental and autonomous computational architecture and framework for deep learningdependent IoT implementations. Successful intelligent techniques will require IoT nodes to work in a variety of operational environments, as well as with the cloud and network to maximize system intelligence while reducing energy consumption [187].

Because of the excessive data rates in 5G-IoT and computation-intensive artificial intelligence techniques can be used for several user applications. With the network's high data transmission capacity, effective deep learning techniques, including virtual speech identification and video categorization, can be used through wireless 5G-IoT nodes [178]. The convergence of AI, 5G, and IoT has a greater chance of transforming the business environment by allowing intelligent real-time decisions. The key motivation for incorporating artificial intelligence into 5G-IoT frameworks is to accredit networks to automatically modify their settings as the environment's demands or parameters change [188]. The novel 5G network ought to be capable of providing productive solutions for management and orchestration, mobility management, service provisioning management, and radio resource management, making devoted purpose networks redundant instead of warranting dynamic network reconfigurations [182]. The 5G facilitates the tactile internet at the wireless networks' edge. The content, however, will need to be localized to the edge of networks to reduce bandwidth needs and latency.

As evidenced in the literature, there is a lot of potential and a lot of complexity in 5G-enabled IoT, which presents a lot of open research areas that need to be examined carefully. The reliability of low-latency communications is essential for use cases like autonomous vehicles and industrial automation. For instance, Chen et al. [189] reported that for effective control, inter-vehicle communication must be highly reliable and have a low latency [190]. Low latency and high

TABLE 3. Future research opportunities in 5G-enabled Iot.

Specific area	Research opportunities
AI and machine learning	In order to analyze, detect anomalies, and make decisions based on huge amounts of data produced by IoT devices, machine learning and AI techniques can be used effectively. Developing this area of study can improve IoT performance.
Ultra-reliable low-latency communication	Researching novel approaches and protocols to attain high reliability and ultra-low latency is essential for IoT applications like telemedicine, autonomous vehicles, and industrial automation.
Edge and fog computing	Research the viability of edge and fog computing to relocate cloud-based data processing and analytics closer to end-user IoT devices, thereby lowering latency and bandwidth demands.
Interoperability and standards	Establish and improve interoperability standards that guarantee IoT devices from different manufacturers can interact together.
Energy-efficient IoT devices	Determine how to design low-power communication systems and energy harvesting strategies into IoT devices and networks to increase device lifetimes.
Device management and lifecycle	Examine effective approaches to managing devices, such as onboarding, provision, and later life, to guarantee a consistent and long-lasting IoT ecosystem.
Network slicing and resource allocation	Explore more efficient and adaptive 5G network slicing methods to dynamically allocate resources to IoT devices based on their needs and applications.
Security and privacy	In 5G networks, secure IoT data and devices with advanced security mechanisms, encryption protocols, and authentication methods that account for IoT deployment scale and diversity.
Human-machine interaction	The accessibility and practicality of 5G-IoT systems can be enhanced by studying the development of user-friendly interfaces and human-machine interaction strategies.
5G-IoT testbeds	Construct and analyze real-world 5G-IoT testbeds to evaluate the efficacy, scalability, and safety of 5G-enabled IoT applications.
Blockchain and distributed	Investigate how blockchain and distributed ledger technologies can be

TABLE 3. *(Continued.)* **Future research opportunities in 5G-enabled Iot.**

ledger technologies	incorporated into 5G-IoT applications to improve reliability, safety, and data integrity.
Data processing and analytics	Establish new ways of processing and analyzing IoT data streams, such as stream processing, data compression, and data fusion, to gather useful information.
QoS and network management	Explore methods for achieving efficient network management in 5G networks and guaranteeing QoS for a wide variety of IoT devices.
Regulatory and ethical aspects	Study more about the ethical and legal considerations that must be made when deploying 5G-IoT, such as ensuring compliance with data protection and privacy laws.
Sustainable IoT	Explore energy-efficient protocols for communication, eco-friendly materials, and other sustainable options for IoT.
Environmental monitoring	Monitor the air and weather quality with the help of 5G IoT. There may be far-reaching implications for ecological preservation if this area of study is pursued.

reliability are also needed for precise operation in manufacturing processes and power system automation services, as demonstrated by several studies [189], [191], [192]. However, the reliability of low-latency communications can be difficult to achieve in practice due to factors like network congestion and device limitations. Remote and inaccessible deployments rely heavily on the battery life of energy-efficient IoT devices, making it critical to strike a balance between power optimization and functional capabilities. Developing lightweight yet effective solutions is a significant challenge when trying to ensure strong security and privacy measures across a landscape of resource-constrained devices. Connecting billions of IoT devices of varying types and capabilities necessitates novel VOLUME XX, 2017 9 network architectures that can effectively manage this diversity.

Complex deployment, management, and security issues arise with edge computing, a solution for lowering latency, and network slicing, which provides customization for specific IoT applications. Intelligent spectrum-sharing mechanisms are needed for spectrum management in congested radio environments, and data privacy and resource constraints must be addressed before machine learning and AI can be integrated into IoT devices. The ever-present requirement for standardization highlights the dynamic character of technology. When it comes to environmental monitoring, scalability and accuracy in sensing are paramount, while the integration of disparate systems is a challenge for smart city and healthcare applications. These unexplored topics highlight both the promise and the complexities of 5G-enabled IoT, calling for an interdisciplinary strategy that brings together technological advancement, data protection, government oversight, and the fluid combination of many different kinds of applications.

There is a substantial abundance of research opportunities in the 5G-enabled IoT field, which is continuously evolving due to the rapid advancements in technology. Table 3 summarizes several open research opportunities within this particular field:

VIII. CONCLUSION

5G-enabled IoT encompasses a variety of critical enabling technologies, including IoT applications and tangible connections. It was reviewed in this paper with a focus on the technical aspects. The paper highlighted enabling technology drivers in 5G-IoT layers, 5G-enabled IoT needs, as well as their security, prospects and challenges. It was demonstrated that all future services and applications must incorporate the IoT, which necessitates a large infrastructure, a substantial amount of device nodes, and a flexible and broad spectrum of bandwidth. Because of these requirements, 5G is a crucial enabler for the IoT. It was also found that 5G-enabled IoT can meet the demands of future IoT applications; nevertheless, this new prototype presents significant challenges, including scalability, secure communications, standardization issues, and other associated issues. By encouraging the growth of cutting-edge open-source protocols for simple communication across all devices, a universally compatible operating system could minimize these issues. A collective effort to resolve these challenges will lay a solid foundation for a 5G-enabled era in which everyone will be connected through IoT.

REFERENCES

[1] Y. Perwej, K. Haq, F. Parwej, M. Mumdouh, and M. Hassan, "The Internet of Things (IoT) and its application domains," *Int. J. Comput. Appl.*, vol. 975, no. 8887, p. 182, 2019.

[2] P. Annamalai, J. Bapat, and D. Das, "Emerging access technologies and open challenges in 5G IoT: From physical layer perspective," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2018, pp. 1–6, doi: 10.1109/ANTS.2018.8710133.

[3] T. Tran, D. Navrátil, P. Sanders, J. Hart, R. Odarchenko, C. Barjau, B. Altman, C. Burdinat, and D. Gomez-Barquero, "Enabling multicast and broadcast in the 5G core for converged fixed and mobile networks," *IEEE Trans. Broadcast.*, vol. 66, no. 2, pp. 428–439, Jun. 2020, doi: 10.1109/TBC.2020.2991548.

[4] H. Fattah, *5G LTE narrowband Internet of Things (NB-IoT)*. Boca Raton, FL, USA: CRC Press, Sep. 2018, doi: 10.1201/9780429455056.

[5] N. Kumar and R. Khanna, "A compact multi-band multi-input multi-output antenna for 4G/5G and IoT devices using theory of characteristic modes," *Int. J. RF Microw. Comput.-Aided Eng.*, vol. 30, no. 1, Jan. 2020, Art. no. e22012, doi: 10.1002/MMCE.22012.

[6] J. Dadkhah Chimeh, "Compelling services for 5G creation," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2020, pp. 1–6, doi: 10.1109/WCNCW48565.2020.9124735.

[7] V. Dhasarathan, M. Singh, and J. Malhotra, "Development of high-speed FSO transmission link for the implementation of 5G and Internet of Things," *Wireless Netw.*, vol. 26, no. 4, pp. 2403–2412, May 2020, doi: 10.1007/S11276-019-02166-5.

[8] S. Painuly, P. Kohli, P. Matta, and S. Sharma, "Advance applications and future challenges of 5G IoT," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2020, pp. 1381–1384, doi: 10.1109/ICISS49785.2020.9316004.

[9] M. Huang, A. Liu, N. N. Xiong, T. Wang, and A. V. Vasilakos, "An effective service-oriented networking management architecture for 5G-enabled Internet of Things," *Comput. Netw.*, vol. 173, May 2020, Art. no. 107208, doi: 10.1016/j.comnet.2020.107208.

[10] S. Huang, Z. Zeng, K. Ota, M. Dong, T. Wang, and N. N. Xiong, "An intelligent collaboration trust interconnections system for mobile information control in ubiquitous 5G networks," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 347–365, Jan. 2021, doi: 10.1109/TNSE.2020.3038454.

[11] M. Vaezi, A. Azari, S. R. Khosravirad, M. Shirvanimoghaddam, M. M. Azari, D. Chasaki, and P. Popovski, "Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road toward 6G," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1117–1174, 2nd Quart., 2022, doi: 10.1109/COMST.2022.3151028.

[12] M. Asad, A. Basit, S. Qaisar, and M. Ali, "Beyond 5G: Hybrid end-to-end quality of service provisioning in heterogeneous IoT networks," *IEEE Access*, vol. 8, pp. 192320–192338, 2020, doi: 10.1109/ACCESS.2020.3032704.

[13] N. Javaid, A. Sher, H. Nasir, and N. Guizani, "Intelligence in IoT-based 5G networks: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 94–100, Oct. 2018, doi: 10.1109/MCOM.2018.1800036.

[14] K. Ali, H. X. Nguyen, Q.-T. Vien, P. Shah, M. Raza, V. Paranthaman, B. Er-Rahmadi, M. Awais, S. U. Islam, and J. P. C. Rodrigues, "Review and implementation of resilient public safety networks: 5G, IoT, and emerging technologies," *IEEE Netw.*, vol. 35, no. 2, pp. 18–25, Mar. 2021, doi: 10.1109/MNET.011.2000418.

[15] B. S. Awoyemi, A. S. Alfa, and B. T. J. Maharaj, "Resource optimisation in 5G and Internet-of-Things networking," *Wireless Pers. Commun.*, vol. 111, no. 4, pp. 2671–2702, Apr. 2020, doi: 10.1007/S11277-019-07010-9.

[16] M. A. Siddiqi, H. Yu, and J. Joung, "5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices," *Electronics*, vol. 8, no. 9, p. 981, Sep. 2019, doi: 10.3390/ELECTRONICS8090981.

[17] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *J. Ind. Inf. Integr.*, vol. 10, pp. 10–19, Jun. 2018, doi: 10.1016/J.JII.2018.04.001.

[18] S. Henry, A. Alsohaily, and E. S. Sousa, "5G is real: Evaluating the compliance of the 3GPP 5G new radio system with the ITU IMT-2020 requirements," *IEEE Access*, vol. 8, pp. 42828–42840, 2020, doi: 10.1109/ACCESS.2020.2977406.

[19] 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, doi: 10.1109/ACCESS.2020.2980369.

[20] S. Li, Q. Ni, Y. Sun, G. Min, and S. Al-Rubaye, "Energy-efficient resource allocation for industrial cyber-physical IoT systems in 5G era," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2618–2628, Jun. 2018, doi: 10.1109/TII.2018.2799177.

[21] B. Q. Vuong, R. Gautier, H. Q. Ta, L. L. Nguyen, A. Fiche, and M. Marazin, "Joint semi-blind self-interference cancellation and equalisation processes in 5G QC-LDPC-encoded short-packet full-duplex transmissions," *Sensors*, vol. 22, no. 6, p. 2204, Mar. 2022, doi: 10.3390/S22062204.

[22] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019, doi: 10.1109/JIOT.2019.2927379.

[23] U. Gustavsson, P. Frenger, C. Fager, T. Eriksson, H. Zirath, F. Dielacher, C. Studer, A. Pärssinen, R. Correia, J. N. Matos, D. Belo, and N. B. Carvalho, "Implementation challenges and opportunities in beyond-5G and 6G communication," *IEEE J. Microw.*, vol. 1, no. 1, pp. 86–100, Jan. 2021, doi: 10.1109/JMW.2020.3034648.

[24] I. Ishteyaq and K. Muzaffar, "Multiple input multiple output (MIMO) and fifth generation (5G): An indispensable technology for sub-6 GHz and millimeter wave future generation mobile terminal applications," *Int. J. Microw. Wireless Technol.*, vol. 14, no. 7, pp. 932–948, Sep. 2022, doi: 10.1017/S1759078721001100.

[25] A. Kumar, M. A. Albreem, M. Gupta, M. H. Alsharif, and S. Kim, "Future 5G network based smart hospitals: Hybrid detection technique for latency improvement," *IEEE Access*, vol. 8, pp. 153240–153249, 2020, doi: 10.1109/ACCESS.2020.3017625.

[26] A. Ly and Y.-D. Yao, "A review of deep learning in 5G research: Channel coding, massive MIMO, multiple access, resource allocation, and network security," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 396–408, 2021, doi: 10.1109/OJCOMS.2021.3058353.

[27] M. A. Abed, S. Kurnaz, and A. H. Mohammed, "Synopsis on study of extended mobility management of 5G network using millimetre wave communication," in *Proc. 4th Int. Symp. Multidisciplinary Stud. Innov. Technol. (ISMSIT)*, Oct. 2020, pp. 1–8, doi: 10.1109/ISMSIT50672.2020.9254500.

[28] S. F. Jilani, Q. H. Abbasi, and A. Alomainy, "Inkjet-printed millimetre-wave PET-based flexible antenna for 5G wireless applications," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Aug. 2018, pp. 1–3, doi: 10.1109/IMWS-5G.2018.8484603.

[29] R. Ali, Y. B. Zikria, A. K. Bashir, S. Garg, and H. S. Kim, "URLLC for 5G and beyond: Requirements, enabling incumbent technologies and network intelligence," *IEEE Access*, vol. 9, pp. 67064–67095, 2021, doi: 10.1109/ACCESS.2021.3073806.

[30] A. Bulashenko, S. Piltyay, A. Polishchuk, and O. Bulashenko, "New traffic model of M2M technology in 5G wireless sensor networks," in *Proc. IEEE 2nd Int. Conf. Adv. Trends Inf. Theory (ATIT)*, Nov. 2020, pp. 125–131, doi: 10.1109/ATIT50783.2020.9349305.

[31] E. Esenogho, K. Djouani, and A. M. Kurien, "Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect," *IEEE Access*, vol. 10, pp. 4794–4831, 2022, doi: 10.1109/ACCESS.2022.3140595.

[32] S. Sharma, K. K. Ghanshala, and S. Mohan, "Blockchain-based Internet of Vehicles (IoV): An efficient secure ad hoc vehicular networking architecture," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 452–457, doi: 10.1109/5GWF.2019.8911664.

[33] D. Jiménez-Soria, F. J. Martín-Vega, and M. C. Aguayo-Torres, "Coordinated multicast/unicast transmission on 5G: A novel approach for linear broadcasting," *Wireless Pers. Commun.*, vol. 121, no. 2, pp. 1273–1287, Nov. 2021, doi: 10.1007/S11277-021-09057-Z.

[34] M. Simon, E. Kofi, L. Libin, and M. Aitken, "ATSC 3.0 broadcast 5G unicast heterogeneous network converged services starting release 16," *IEEE Trans. Broadcast.*, vol. 66, no. 2, pp. 449–458, Jun. 2020, doi: 10.1109/TBC.2020.2985575.

[35] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

[36] H. Rahimi, A. Zibaeenejad, P. Rajabzadeh, and A. A. Safavi, "On the security of the 5G-IoT architecture," in *Proc. Int. Conf. Smart Cities Internet Things*, Sep. 2018, pp. 1–8, doi: 10.1145/3269961.3269968.

[37] K. Saleem, G. M. Alabduljabbar, N. Alrowais, J. Al-Muhtadi, M. Imran, and J. J. P. C. Rodrigues, "Bio-inspired network security for 5G-enabled IoT applications," *IEEE Access*, vol. 8, pp. 229152–229160, 2020, doi: 10.1109/ACCESS.2020.3046325.

[38] B. Dzogovic, B. Santos, J. Noll, V. T. Do, B. Feng, and T. V. Do, "Enabling smart home with 5G network slicing," in *Proc. IEEE 4th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Feb. 2019, pp. 543–548, doi: 10.1109/CCOMS.2019.8821727.

[39] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: A survey on application potential," *Appl. Energy*, vol. 257, Jan. 2020, Art. no. 113972, doi: 10.1016/J.APENERGY.2019.113972.

[40] F. Liu, Y. Lv, P. Yang, Y. Liu, Z. Xu, and J. Luo, "Innovation of business model for electrical household appliance enterprises to deploy IoT+AI and IoT+5G," in *Proc. Int. Conf. e-Commerce Internet Technol. (ECIT)*, Apr. 2020, pp. 245–247, doi: 10.1109/ECIT50008.2020.00063.

[41] R. S. Abujassar, H. Yaseen, and A. S. Al-Adwan, "A highly effective route for real-time traffic using an IoT smart algorithm for tele-surgery using 5G networks," *J. Sensor Actuator Netw.*, vol. 10, no. 2, p. 30, Apr. 2021, doi: 10.3390/JSAN10020030.

[42] N. Gupta, S. Sharma, P. K. Juneja, and U. Garg, "SDNFV 5G-IoT: A framework for the next generation 5G enabled IoT," in *Proc. Int. Conf. Adv. Comput., Commun. Mater. (ICACCM)*, Aug. 2020, pp. 289–294, doi: 10.1109/ICACCM50413.2020.9213047.

[43] D. Haider, X. Yang, and Q. H. Abbasi, "Post-surgical fall detection by exploiting the 5G C-band technology for eHealth paradigm," *Appl. Soft Comput.*, vol. 81, Aug. 2019, Art. no. 105537, doi: 10.1016/J.ASOC.2019.105537.

[44] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. P. C. Rodrigues, "Security in 5G-enabled Internet of Things communication: Issues, challenges, and future research roadmap," *IEEE Access*, vol. 9, pp. 4466–4489, 2021, doi: 10.1109/ACCESS.2020.3047895.

[45] M. M. Alsulami and N. Akkari, "The role of 5G wireless networks in the Internet-of-Things (IoT)," in *Proc. 1st Int. Conf. Comput. Appl. Inf. Secur.*, Sep. 2018, pp. 1–8, doi: 10.1109/CAIS.2018.8471687.

[46] H. Shariatmadari, R. Ratasuk, S. Iraji, A. Laya, T. Taleb, R. Jäntti, and A. Ghosh, "Machine-type communications: Current status and future perspectives toward 5G systems," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 10–17, Sep. 2015, doi: 10.1109/MCOM.2015.7263367.

[47] L. Tello-Oquendo, S.-C. Lin, I. F. Akyildiz, and V. Pla, "Software-defined architecture for QoS-aware IoT deployments in 5G systems," *Ad Hoc Netw.*, vol. 93, Oct. 2019, Art. no. 101911, doi: 10.1016/j.adhoc.2019.101911.

[48] S. Behrad, E. Bertin, S. Tuffin, and N. Crespi, "A new scalable authentication and access control mechanism for 5G-based IoT," *Future Gener. Comput. Syst.*, vol. 108, pp. 46–61, Jul. 2020, doi: 10.1016/J.FUTURE.2020.02.014.

[49] A. Eid, J. Hester, and M. M. Tentzeris, "A scalable high-gain and large-beamwidth mm-wave harvesting approach for 5G-powered IoT," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Jun. 2019, pp. 1309–1312, doi: 10.1109/MWSYM.2019.8700758.

[50] A. M. Escolar, J. M. A. Calero, and Q. Wang, "Highly-scalable software firewall supporting one million rules for 5G NB-IoT networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6, doi: 10.1109/ICC40277.2020.9149152.

[51] G. Su and M. Moh, "Improving energy efficiency and scalability for IoT communications in 5G networks," in *Proc. 12th Int. Conf. Ubiquitous Inf. Manage. Commun.*, Jan. 2018, pp. 1–8, doi: 10.1145/3164541.3164547.

[52] 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, doi: 10.1109/ACCESS.2020.2970118.

[53] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021, doi: 10.1109/COMST.2021.3067807.

[54] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the Internet of Things era: An overview on security and privacy challenges," *Comput. Netw.*, vol. 179, Oct. 2020, Art. no. 107345, doi: 10.1016/J.COMNET.2020.107345.

[55] S. Li, L. D. Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018, doi: 10.1016/j.jii.2018.01.005.

[56] M. Agiwal, N. Saxena, and A. Roy, "Towards connected living: 5G enabled Internet of Things (IoT)," *IETE Tech. Rev.*, vol. 36, no. 2, pp. 190–202, Mar. 2019, doi: 10.1080/02564602.2018.1444516.

[57] Q. Qiu, S. Liu, S. Xu, and S. Yu, "Study on security and privacy in 5G-enabled applications," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–15, Dec. 2020, doi: 10.1155/2020/8856683.

[58] M. Liyanage, J. Salo, A. Braeken, T. Kumar, S. Seneviratne, and M. Ylianttila, "5G privacy: Scenarios and solutions," in *Proc. IEEE 5G World Forum (5GWF)*, Jul. 2018, pp. 197–203, doi: 10.1109/5GWF.2018.8516981.

[59] M. Khuntia, D. Singh, and S. Sahoo, "Impact of Internet of Things (IoT) on 5G," in *Intelligent and Cloud Computing: Proceedings of ICICC 2019*, vol. 2. Singapore: Springer, 2021, pp. 125–136.

[60] G. A. Sampedro, S. L. Huyo, R. G. Kim, Y. J. Aruan, and M. Abisado, "Application of 5G infrastructure for IoT: Challenges and opportunities," in *Proc. 2nd Int. Conf. Electron. Electr. Eng. Intell. Syst. (ICEIS)*, Nov. 2022, pp. 153–157.

[61] K. Khujamatov, D. Khasanov, E. Reypnazarov, and N. Akhmedov, "Existing technologies and solutions in 5G-enabled IoT for industrial automation," in *Blockchain for 5G-Enabled IoT: The New Wave for Industrial Automation*. Springer, 2021, pp. 181–221, doi: 10.1007/978-3-030-67490-8_8.

[62] E. O'Connell, D. Moore, and T. Newe, "Challenges associated with implementing 5G in manufacturing," *Telecom*, vol. 1, no. 1, pp. 48–67, Jun. 2020.

[63] Y. Tang, S. Dananjayan, C. Hou, Q. Guo, S. Luo, and Y. He, "A survey on the 5G network and its impact on agriculture: Challenges and opportunities," *Comput. Electron. Agricult.*, vol. 180, Jan. 2021, Art. no. 105895, doi: 10.1016/j.compag.2020.105895.

[64] H. Moudoud, L. Khoukhi, and S. Cherkaoui, "Prediction and detection of FDIA and DDoS attacks in 5G enabled IoT," *IEEE Netw.*, vol. 35, no. 2, pp. 194–201, Mar. 2021, doi: 10.1109/MNET.011.2000449.

[65] B. Pawłowicz, M. Salach, and B. Trybus, "Smart city traffic monitoring system based on 5G cellular network, RFID and machine learning," in *Proc. KKIO Softw. Eng. Conf.* Pułtusk, Poland: Springer, Sep. 2018, pp. 151–165.

[66] H. Rahimi, A. Zibaeenejad, and A. A. Safavi, "A novel IoT architecture based on 5G-IoT and next generation technologies," in *Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2018, pp. 81–88, doi: 10.1109/IEMCON.2018.8614777.

[67] N. Gupta, P. K. Juneja, S. Sharma, and U. Garg, "Future aspect of 5G-IoT architecture in smart healthcare system," in *Proc. 5th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2021, pp. 406–411.

[68] C. Yang, P. Liang, L. Fu, G. Cui, F. Huang, F. Teng, and Y. A. Bangash, "Using 5G in smart cities: A systematic mapping study," *Intell. Syst. Appl.*, vol. 14, May 2022, Art. no. 200065, doi: 10.1016/j.iswa.2022.200065.

[69] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018, doi: 10.1109/ACCESS.2017.2779844.

[70] T. Lei, Z. Cai, and L. Hua, "RETRACTED: 5G-oriented IoT coverage enhancement and physical education resource management," *Microprocess. Microsyst.*, vol. 80, Feb. 2021, Art. no. 103346, doi: 10.1016/j.micpro.2020.103346.

[71] Y. Hao, "Investigation and technological comparison of 4G and 5G networks," *J. Comput. Commun.*, vol. 9, no. 1, pp. 36–43, 2021, doi: 10.4236/jcc.2021.91004.

[72] J. Rosenthal, A. Pike, and M. S. Reynolds, "A 1 Mbps 158 pJ/bit Bluetooth low energy (BLE) compatible backscatter communication uplink for wireless neural recording in an animal cage environment," in *Proc. IEEE Int. Conf.*, Apr. 2019, pp. 1–6, doi: 10.1109/RFID.2019.8719266.

[73] H. A. H. Alobaidy, J. S. Mandeep, R. Nordin, and N. F. Abdullah, "A review on ZigBee based WSNs: Concepts, infrastructure, applications, and challenges," *Int. J. Electr. Electron. Eng. Telecommun.*, vol. 9, no. 3, pp. 189–198, 2020, doi: 10.18178/ijeetc.9.3.189-198.

[74] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Exp.*, vol. 3, no. 1, pp. 14–21, Mar. 2017, doi: 10.1016/j.icte.2017.03.004.

[75] M. Kamel, W. Hamouda, and A. Youssef, "Uplink performance of NOMA-based combined HTC and MTC in ultradense networks," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7319–7333, Aug. 2020, doi: 10.1109/JIOT.2020.2984805.

[76] H. Mroue, A. Nasser, S. Hamrioui, B. Parrein, E. Motta-Cruz, and G. Rouyer, "MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT," in *Proc. IEEE Middle East North Africa Commun. Conf.*, Apr. 2018, pp. 1–5, doi: 10.1109/MENACOMM.2018.8371016.

[77] L. Chettri, R. Bera, and J. K. Barauh, "Performance analysis of 3GPP NB-IoT downlink system towards 5G machine type communication (5G-MTC)," *J. Commun.*, vol. 16, no. 8, pp. 355–362, 2021, doi: 10.12720/jcm.16.8.355-362.

[78] L. Liao and C. Ji, "Wireless resource management and resilience optimization of the M2M-oriented mobile communication system," *J. Sensors*, vol. 2021, pp. 1–11, Dec. 2021, doi: 10.1155/2021/9596606.

[79] S. Painuly, S. Sharma, and P. Matta, "Future trends and challenges in next generation smart application of 5G-IoT," in *Proc. 5th Int. Conf. Comput. Methodologies Commun.*, 2021, pp. 354–357, doi: 10.1109/ICCMC51019.2021.9418471.

[80] G. Lando, L. A. F. Schierholt, M. P. Milesi, and J. A. Wickboldt, "Evaluating the performance of open source software implementations of the 5G network core," in *Proc. IEEE/IFIP Netw. Operations Manag. Symp.*, May 2023, pp. 1–7.

[81] A. A. Ismail, H. S. Hamza, and A. M. Kotb, "Performance evaluation of open source IoT platforms," in *Proc. IEEE Global Conf. Internet Things (GCIoT)*, Dec. 2018, pp. 1–5.

[82] E. Anthi, S. Ahmad, O. Rana, G. Theodorakopoulos, and P. Burnap, "EclipseIoT: A secure and adaptive hub for the Internet of Things," *Comput. Secur.*, vol. 78, pp. 477–490, Sep. 2018.

[83] M. Henschke, X. Wei, and X. Zhang, "Data visualization for wireless sensor networks using ThingsBoard," in *Proc. 29th Wireless Opt. Commun. Conf. (WOCC)*, May 2020, pp. 1–6.

[84] O. Toutsop, K. Kornegay, and E. Smith, "A comparative analyses of current IoT middleware platforms," in *Proc. 8th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2021, pp. 413–420.

[85] D. Borsatti, W. Cerroni, F. Tonini, and C. Raffaelli, "From IoT to cloud: Applications and performance of the MQTT protocol," in *Proc. 22nd Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2020, pp. 1–4.

[86] M. Liyanage, P. Porambage, A. Y. Ding, and A. Kalla, "Driving forces for multi-access edge computing (MEC) IoT integration in 5G," *ICT Exp.*, vol. 7, no. 2, pp. 127–137, Jun. 2021, doi: 10.1016/j.icte.2021.05.007.

[87] S. Kumar, M. C. Trivedi, P. Ranjan, and A. Punhani, *Evolution of Software-Defined Networking Foundations for IoT and 5G Mobile Networks*. Hershey, PA, USA: IGI Global, 2020.

[88] S. Mishra and A. R. Tripathi, "IoT platform business model for innovative management systems," *Int. J. Financial Eng.*, vol. 7, no. 3, Sep. 2020, Art. no. 2050030, doi: 10.1142/s2424786320500309.

[89] S. K. Rao and R. Prasad, "Impact of 5G technologies on Industry 4.0," *Wireless Pers. Commun.*, vol. 100, no. 1, pp. 145–159, May 2018, doi: 10.1007/s11277-018-5615-7.

[90] I. Taboada and H. Shee, "Understanding 5G technology for future supply chain management," *Int. J. Logistics Res. Appl.*, vol. 24, no. 4, pp. 392–406, Jul. 2021, doi: 10.1080/13675567.2020.1762850.

[91] M. Condoluci, T. Mahmoodi, M. A. Lema, and M. Dohler, "5G IoT industry verticals and network requirements," in *Powering the Internet of Things With 5G Networks*. Hershey, PA, USA: IGI Global, 2017.

[92] A. Mahmood, L. Beltramelli, S. Fakhrul Abedin, S. Zeb, N. I. Mowla, S. A. Hassan, E. Sisinni, and M. Gidlund, "Industrial IoT in 5G-and-beyond networks: Vision, architecture, and design trends," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 4122–4137, Jun. 2022, doi: 10.1109/TII.2021.3115697.

[93] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020, doi: 10.1109/MWC.001.1900488.

[94] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[95] M. Attaran, "The impact of 5G on the evolution of intelligent automation and industry digitization," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 5, pp. 5977–5993, 2021, doi: 10.1007/S12652-020-02521-X.

[96] J. R. Bhat, S. A. AlQahtani, and M. Nekovee, "FinTech enablers, use cases, and role of future Internet of Things," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 35, no. 1, pp. 87–101, Jan. 2023.

[97] Y. M. Waheidi, M. Jubran, and M. Hussein, "User driven multiclass cell association in 5G HetNets for mobile & IoT devices," *IEEE Access*, vol. 7, pp. 82991–83000, 2019, doi: 10.1109/ACCESS.2019.2924521.

[98] S. Wu, W. Mao, C. Liu, and T. Tang, "Dynamic traffic prediction with adaptive sampling for 5G HetNet IoT applications," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–11, Jun. 2019, doi: 10.1155/2019/4687272.

[99] A.-S. Bana, E. de Carvalho, B. Soret, T. Abrão, J. C. Marinello, E. G. Larsson, and P. Popovski, "Massive MIMO for Internet of Things (IoT) connectivity," *Phys. Commun.*, vol. 37, Dec. 2019, Art. no. 100859, doi: 10.1016/j.phycom.2019.100859.

[100] O. Hayat, R. Ngah, and Y. Zahedi, "In-band device to device (D2D) communication and device discovery: A survey," *Wireless Pers. Commun.*, vol. 106, no. 2, pp. 451–472, May 2019, doi: 10.1007/s11277-019-06173-9.

[101] G. S. Gaba, G. Kumar, T.-H. Kim, H. Monga, and P. Kumar, "Secure device-to-device communications for 5G enabled Internet of Things applications," *Comput. Commun.*, vol. 169, pp. 114–128, Mar. 2021, doi: 10.1016/j.comcom.2021.01.010.

[102] L. Pallavi, A. Jagan, and B. T. Rao, "ERMO2 algorithm: An energy efficient mobility management in mobile cloud computing system for 5G heterogeneous networks," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 9, no. 3, p. 1957, Jun. 2019, doi: 10.11591/ijece.v9i3.pp1957-1967.

[103] W. Tong, X. Dong, Y. Shen, and J. Zheng, "BC-RAN: Cloud radio access network enabled by blockchain for 5G," *Comput. Commun.*, vol. 162, pp. 179–186, Oct. 2020, doi: 10.1016/j.comcom.2020.08.020.

[104] Y. Zhang, G. Chen, H. Du, X. Yuan, M. Kadoch, and M. Cheriet, "Real-time remote health monitoring system driven by 5G MEC-IoT," *Electronics*, vol. 9, no. 11, p. 1753, Oct. 2020, doi: 10.3390/electronics9111753.

[105] C. N. Tadros, M. R. M. Rizk, and B. M. Mokhtar, "Software defined network-based management for enhanced 5G network services," *IEEE Access*, vol. 8, pp. 53997–54008, 2020, doi: 10.1109/ACCESS.2020.2980392.

[106] D. Minoli and B. Occhiogrosso, "Practical aspects for the integration of 5G networks and IoT applications in smart cities environments," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–30, Aug. 2019, doi: 10.1155/2019/5710834.

[107] W. Serrano, "The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities," *J. Netw. Comput. Appl.*, vol. 175, Feb. 2021, Art. no. 102909, doi: 10.1016/j.jnca.2020.102909.

[108] V. Thayananthan, "Healthcare management using ICT and IoT based 5G," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 4, pp. 305–312, 2019, doi: 10.14569/ijacsa.2019.0100437.

[109] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, and D. Kerr, "An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications," *Sensors*, vol. 21, no. 19, p. 6346, Sep. 2021, doi: 10.3390/s21196346.

[110] B. Dzogovic, B. Santos, T. Van Do, B. Feng, T. Van Do, and N. Jacot, "Bringing 5G into user's smart home," in *Proc. IEEE Int. Conf Dependable, Autonomic Secure Comput., Int. Conf Pervasive Intell. Comput., Int. Conf Cloud Big Data Comput., Int. Conf Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 782–787, doi: 10.1109/DASC/PiCom/CBDCom/CYBERSCITECH.2019.00145.

[111] D. Shin, K. Yun, J. Kim, P. V. Astillo, J.-N. Kim, and I. You, "A security protocol for route optimization in DMM-based smart home IoT networks," *IEEE Access*, vol. 7, pp. 142531–142550, 2019, doi: 10.1109/ACCESS.2019.2943929.

[112] J. S. Walia, H. Hämmäinen, K. Kilkki, and S. Yrjölä, "5G network slicing strategies for a smart factory," *Comput. Ind.*, vol. 111, pp. 108–120, Oct. 2019, doi: 10.1016/j.compind.2019.07.006.

[113] N. A. Anagnostopoulos, S. Ahmad, T. Arul, D. Steinmetzer, M. Hollick, and S. Katzenbeisser, "Low-cost security for next-generation IoT networks," *ACM Trans. Internet Technol.*, vol. 20, no. 3, pp. 1–31, Aug. 2020, doi: 10.1145/3406280.

[114] X. Ge, R. Zhou, and Q. Li, "5G NFV-based tactile internet for mission-critical IoT services," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6150–6163, Jul. 2020, doi: 10.1109/JIOT.2019.2958063.

[115] E. J. Oughton and Z. Frias, "The cost, coverage and rollout implications of 5G infrastructure in Britain," *Telecommun. Policy*, vol. 42, no. 8, pp. 636–652, Sep. 2018, doi: 10.1016/j.telpol.2017.07.009.

[116] T.-T. Nguyen, C. Bonnet, and J. Harri, "SDN-based distributed mobility management for 5G networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–7, doi: 10.1109/WCNC.2016.7565106.

[117] W. Xie, N. T. Mao, and K. Rundberget, "Cost comparisons of backhaul transport technologies for 5G fixed wireless access," in *Proc. IEEE 5G World Forum (5GWF)*, Jul. 2018, pp. 159–163, doi: 10.1109/5GWF.2018.8516977.

[118] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018.

[119] S. Rathore, J. H. Park, and H. Chang, "Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT," *IEEE Access*, vol. 9, pp. 90075–90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[120] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3GPP narrowband Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 117–123, Mar. 2017, doi: 10.1109/MCOM.2017.1600510CM.

[121] Y. Zeng and R. Zhang, "Millimeter wave MIMO with lens antenna array: A new path division multiplexing paradigm," *IEEE Trans. Commun.*, vol. 64, no. 4, pp. 1557–1571, Apr. 2016, doi: 10.1109/TCOMM.2016.2533490.

[122] F. Abate, M. Carratú, C. Liguori, and V. Paciello, "A low cost smart power meter for IoT," *Measurement*, vol. 136, pp. 59–66, Mar. 2019, doi: 10.1016/j.measurement.2018.12.069.

[123] A. Popa, M. Hnatiuc, M. Paun, O. Geman, D. J. Hemanth, D. Dorcea, L. H. Son, and S. Ghita, "An intelligent IoT-based food quality monitoring approach using low-cost sensors," *Symmetry*, vol. 11, no. 3, p. 374, 2019, doi: 10.3390/sym11030374.

[124] S. J. Johnston, P. J. Basford, F. M. J. Bulot, M. Apetroaie-Cristea, N. H. C. Easton, C. Davenport, G. L. Foster, M. Loxham, A. K. R. Morris, and S. J. Cox, "City scale particulate matter monitoring using LoRaWAN based air quality IoT devices," *Sensors*, vol. 19, no. 1, p. 209, Jan. 2019, doi: 10.3390/s19010209.

[125] B. S. Chaudhari, M. Zennaro, and S. Borkar, "LPWAN technologies: Emerging application characteristics, requirements, and design considerations," *Future Internet*, vol. 12, no. 3, p. 46, Mar. 2020.

[126] B. Chaudhari and S. Borkar, "Design considerations and network architectures for low-power wide-area networks," in *LPWAN Technologies for IoT and M2M Applications*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 15–35.

[127] R. Chataut and R. Akl, "Massive MIMO systems for 5G and beyond networks—Overview, recent trends, challenges, and future research direction," *Sensors*, vol. 20, no. 10, p. 2753, May 2020, doi: 10.3390/s20102753.

[128] B. Yang, Z. Yu, J. Lan, R. Zhang, J. Zhou, and W. Hong, "Digital beamforming-based massive MIMO transceiver for 5G millimeter-wave communications," *IEEE Trans. Microw. Theory Techn.*, vol. 66, no. 7, pp. 3403–3418, Jul. 2018, doi: 10.1109/TMTT.2018.2829702.

[129] W. Dghais, M. Souilem, H. R. Chi, A. Radwan, and A. M. Taha, "Dynamic clustering for power effective small cell deployment in HetNet 5G networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–5, doi: 10.1109/ICC40277.2020.9149059.

[130] D. Vukobratovic, D. Jakovetic, V. Skachek, D. Bajovic, D. Sejdinovic, G. Karabulut Kurt, C. Hollanti, and I. Fischer, "CONDENSE: A reconfigurable knowledge acquisition architecture for future 5G IoT," *IEEE Access*, vol. 4, pp. 3360–3378, 2016, doi: 10.1109/ACCESS.2016.2585468.

[131] *LoRa Modulation Basics AN1200.22*, Semtech, Camarillo, CA, USA, May 2015.

[132] M. Chafii, F. Bader, and J. Palicot, "Enhancing coverage in narrow band-IoT using machine learning," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6, doi: 10.1109/WCNC.2018.8377263.

[133] M. A. Kocak, K. Balachandran, J. H. Kang, K. Karakayali, and K. M. Rege, "On the design of preamble for autonomous communications with extended coverage," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5, doi: 10.1109/VTCSPRING.2017.8108688.

[134] E. Luján, J. A. Zuloaga Mellino, A. D. Otero, L. R. Vega, C. G. Galarza, and E. E. Mocskos, "Extreme coverage in 5G narrowband IoT: A LUT-based strategy to optimize shared channels," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2129–2136, Mar. 2020, doi: 10.1109/JIOT.2019.2959552.

[135] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, "NB-IoT system for M2M communication," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–5, doi: 10.1109/WCNCW.2016.7552737.

[136] O. Madamori, E. Max-Onakpoya, C. Grant, and C. Baker, "Using delay tolerant networks as a backbone for low-cost smart cities," in *Proc. IEEE Int. Conf. Smart Comput.*, Jun. 2019, pp. 468–471, doi: 10.1109/SMARTCOMP.2019.00090.

[137] A. Orsino, A. Ometov, G. Fodor, D. Moltchanov, L. Militano, S. Andreev, O. N. C. Yilmaz, T. Tirronen, J. Torsner, G. Araniti, A. Iera, M. Dohler, and Y. Koucheryavy, "Effects of heterogeneous mobility on D2D- and drone-assisted mission-critical MTC in 5G," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 79–87, Feb. 2017, doi: 10.1109/MCOM.2017.1600443CM.

[138] A. Froytlog, T. Foss, O. Bakker, G. Jevne, M. A. Haglund, F. Y. Li, J. Oller, and G. Y. Li, "Ultra-low power wake-up radio for 5G IoT," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 111–117, Mar. 2019, doi: 10.1109/MCOM.2019.1701288.

[139] H. A. H. Alobaidy, M. J. Singh, R. Nordin, N. F. Abdullah, C. G. Wei, and M. L. Siang Soon, "Real-world evaluation of power consumption and performance of NB-IoT in Malaysia," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 11614–11632, Jul. 2022, doi: 10.1109/JIOT.2021.3131160.

[140] H. Malik, J. L. R. Sarmiento, M. M. Alam, and M. A. Imran, "Narrowband-Internet of Things (NB-IoT): Performance evaluation in 5G heterogeneous wireless networks," in *Proc. IEEE 24th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Sep. 2019, pp. 1–6, doi: 10.1109/CAMAD.2019.8858461.

[141] A. D. Dwivedi, R. Singh, K. Kaushik, R. R. Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Trans. Emerg. Telecommun. Technol.*, vol. 32, p. e4329, Jul. 2021, doi: 10.1002/ett.4329.

[142] U. Klarman, S. Basu, and A. Kuzmanovic, "bloXroute: A scalable trustless blockchain distribution network," Bloxroute.Com, White Paper, Mar. 2018, pp. 1–12. [Online]. Available: https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf

[143] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, Aug. 2014, doi: 10.1016/J.JCSS.2014.02.005.

[144] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User privacy, identity and trust in 5G," in *A Comprehensive Guide to 5G Security*. Hoboken, NJ, USA: Wiley, Feb. 2018, pp. 267–279, doi: 10.1002/9781119293071.CH12.

[145] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P. K. Nakarmi, M. Näslund, P. O'Hanlon, J. Papay, J. Suomalainen, M. Surridge, J.-P. Wary, and A. Zahariev, "A security architecture for 5G networks," *IEEE Access*, vol. 6, pp. 22466–22479, 2018, doi: 10.1109/ACCESS.2018.2827419.

[146] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J. J. Ramos-Munoz, J. Lorca, and J. Folgueira, "Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 80–87, May 2017.

[147] K. Jaswal, T. Choudhury, R. L. Chhokar, and S. R. Singh, "Securing the Internet of Things: A proposed framework," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, May 2017, pp. 1277–1281, doi: 10.1109/CCAA.2017.8230015.

[148] D.-R. Berte, "Defining the IoT," in *Proc. Int. Conf. Bus. Excell.*, May 2018, vol. 12, no. 1, pp. 118–128, doi: 10.2478/PICBE-2018-0013.

[149] R. M. Haris and S. Al-Maadeed, "Integrating blockchain technology in 5G enabled IoT: A review," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 367–371, doi: 10.1109/ICIOT48696.2020.9089600.

[150] *5G and Data Privacy: An Overview for Policymakers*, GSMA Association, London, U.K., 2020.

[151] T. W. Nowak, M. Sepczuk, Z. Kotulski, W. Niewolski, R. Artych, K. Bocianiak, T. Osko, and J.-P. Wary, "Verticals in 5G MEC-use cases and security challenges," *IEEE Access*, vol. 9, pp. 87251–87298, 2021.

[152] P. Camps-Aragó, S. Delaere, and P. Ballon, "5G business models: Evolving mobile network operator roles in new ecosystems," in *Proc. CTTE-FITCE Smart Cities Inf. Commun. Technol. CTTE-FITCE*, Sep. 2019, pp. 1–6, doi: 10.1109/CTTE-FITCE.2019.8894822.

[153] N. Zhang, P. Yang, S. Zhang, D. Chen, W. Zhuang, B. Liang, and X. S. Shen, "Software defined networking enabled wireless network virtualization: Challenges and solutions," *IEEE Netw.*, vol. 31, no. 5, pp. 42–49, May 2017, doi: 10.1109/MNET.2017.1600248.

[154] F. Ihirwe, A. Indamutsa, D. D. Ruscio, S. Mazzini, and A. Pierantonio, "Cloud-based modeling in IoT domain: A survey, open challenges and opportunities," in *Proc. ACM/IEEE Int. Conf. Model Driven Eng. Lang. Syst. Companion (MODELS-C)*, Oct. 2021, pp. 73–82, doi: 10.1109/MODELS-C53483.2021.00018.

[155] N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," *Phys. Commun.*, vol. 18, pp. 64–84, Mar. 2016, doi: 10.1016/J.PHYCOM.2015.10.006.

[156] A. Banafa. (2016). IoT Standardization and Implementation Challenges—IEEE Internet of Things. IEEE. Accessed: Jan. 20, 2024. [Online]. Available: https://iot.ieee.org/articles-publications/newsletter/july-2016/iot-standardization-and-implementation-challenges.html

[157] R. Ullah, S. H. Ahmed, and B.-S. Kim, "Information-centric networking with edge computing for IoT: Research challenges and future directions," *IEEE Access*, vol. 6, pp. 73465–73488, 2018, doi: 10.1109/ACCESS.2018.2884536.

[158] C. Bouras, A. Kollia, and A. Papazois, "SDN & NFV in 5G: Advancements and challenges," in *Proc. 20th Conf. Innov. Clouds, Internet Netw. (ICIN)*, Mar. 2017, pp. 107–111, doi: 10.1109/ICIN.2017.7899398.

[159] S. Khan Tayyaba and M. A. Shah, "5G cellular network integration with SDN: Challenges, issues and beyond," in *Proc. Int. Conf. Commun., Comput. Digit. Syst. (C-CODE)*, Mar. 2017, pp. 48–53, doi: 10.1109/C-CODE.2017.7918900.

[160] J. Liu, T. Zhao, S. Zhou, Y. Cheng, and Z. Niu, "CONCERT: A cloud-based architecture for next-generation cellular systems," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 14–22, Dec. 2014, doi: 10.1109/MWC.2014.7000967.

[161] X. Shen, "Device-to-device communication in 5G cellular networks," *IEEE Netw.*, vol. 29, no. 2, pp. 2–3, Mar. 2015, doi: 10.1109/MNET.2015.7064895.

[162] H. Lauer and N. Kuntze, "Hypervisor-based attestation of virtual environments," in *Proc. Int. IEEE Conf. Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People, Smart World Congr. (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, Jul. 2016, pp. 333–340, doi: 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0067.

[163] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Out-VM monitoring for malicious network packet detection in cloud," in *Proc. ISEA Asia Secur. Privacy (ISEASP)*, Jan. 2017, pp. 1–10, doi: 10.1109/ISEASP.2017.7976995.

[164] P. Haji Mirzaee, M. Shojafar, H. Cruickshank, and R. Tafazolli, "Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures)," *IEEE Access*, vol. 10, pp. 52922–52954, 2022, doi: 10.1109/ACCESS.2022.3174259.

[165] V. Ekawu, "Software defined networking a review: Security issues and solutions pre-maters project in computer networks," Tech. Rep., 2017.

[166] S. K. Sharma, T. E. Bogale, L. B. Le, S. Chatzinotas, X. Wang, and B. Ottersten, "Dynamic spectrum sharing in 5G wireless networks with full-duplex technology: Recent advances and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 674–707, 1st Quart., 2018, doi: 10.1109/COMST.2017.2773628.

[167] M. Ndiaye, G. Hancke, and A. Abu-Mahfouz, "Software defined networking for improved wireless sensor network management: A survey," *Sensors*, vol. 17, no. 5, p. 1031, May 2017, doi: 10.3390/S17051031.

[168] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," *Comput. Electr. Eng.*, vol. 66, pp. 274–287, Feb. 2018, doi: 10.1016/J.COMPELECENG.2017.02.026.

[169] M. Elkhodr, S. Shahrestani, and H. Cheung, "The Internet of Things : New interoperability, management and security challenges," *Int. J. Netw. Secur. Appl.*, vol. 8, no. 2, pp. 85–102, Mar. 2016, doi: 10.5121/ijnsa.2016.8206.

[170] F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 28–65, 1st Quart., 2019, doi: 10.1109/COMST.2018.2864779.

[171] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, "Towards 6G Internet of Things: Recent advances, use cases, and open challenges," *ICT Exp.*, vol. 9, no. 3, pp. 296–312, Jun. 2023, doi: 10.1016/j.icte.2022.06.006.

[172] M. Matinmikko-Blue, S. Yrjölä, and P. Ahokangas, "Spectrum management in the 6G era: The role of regulation and spectrum sharing," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.

[173] N. Rubab, S. Zeb, A. Mahmood, S. A. Hassan, M. I. Ashraf, and M. Gidlund, "Interference mitigation in RIS-assisted 6G systems for indoor industrial IoT networks," in *Proc. IEEE 12th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Jun. 2022, pp. 211–215.

[174] H. Tataria, M. Shafi, A. F. Molisch, M. Dohler, H. Sjöland, and F. Tufvesson, "6G wireless systems: Vision, requirements, challenges, insights, and opportunities," *Proc. IEEE*, vol. 109, no. 7, pp. 1166–1199, Jul. 2021.

[175] A. H. Sodhro, S. Pirbhulal, Z. Luo, K. Muhammad, and N. Z. Zahid, "Toward 6G architecture for energy-efficient communication in IoT-enabled smart automation systems," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5141–5148, Apr. 2021.

[176] 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 Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[177] K. K. Pramanik and K. Shekokar, "6G massive wireless energy transfer for sustainable IoT," in *Proc. Int. Conf. Artif. Intell. Smart Commun. (AISC)*, Jan. 2023, pp. 1268–1272.

[178] X. Xu, D. Li, Z. Dai, S. Li, and X. Chen, "A heuristic offloading method for deep learning edge services in 5G networks," *IEEE Access*, vol. 7, pp. 67734–67744, 2019, doi: 10.1109/ACCESS.2019.2918585.

[179] K. Norrman, M. Naslund, and E. Dubrova, "Protecting IMSI and user privacy in 5G networks," in *Proc. 9th EAI Int. Conf. Mobile Multimedia Commun.*, Dec. 2016, pp. 159–166, doi: 10.4108/EAI.18-6-2016.2264114.

[180] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018, doi: 10.1109/MCOMSTD.2018.1700063.

[181] S. Banik, I. S. Cardenas, and J. H. Kim, "IoT platforms for 5G network and practical considerations: A survey," in *Ubiquitous Networking: 5th International Symposium, UNet 2019, Limoges, France, November 20–22, 2019, Revised Selected Papers 5*. Springer, pp. 205–225.

[182] X. Zhou, R. Li, T. Chen, and H. Zhang, "Network slicing as a service: Enabling enterprises' own software-defined cellular networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 146–153, Jul. 2016, doi: 10.1109/MCOM.2016.7509393.

[183] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 26–33, Jan. 2017, doi: 10.1109/MCOM.2017.1600363CM.

[184] Z. Iftikhar et al., "Privacy preservation in resource-constrained IoT devices using blockchain—A survey," *Electronics*, vol. 10, no. 14, p. 1732, 2021.

[185] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized BlockChain for IoT," in *Proc. IEEE/ACM 2nd Int. Conf. Internet-Things Design Implement. (IoTDI)*, Apr. 2017, pp. 173–178, doi: 10.1145/3054977.3055003.

[186] M. Song, K. Zhong, J. Zhang, Y. Hu, D. Liu, W. Zhang, J. Wang, and T. Li, "In-situ AI: Towards autonomous and incremental deep learning for IoT systems," in *Proc. IEEE Int. Symp. High Perform. Comput. Architecture (HPCA)*, Feb. 2018, pp. 92–103, doi: 10.1109/HPCA.2018.00018.

[187] B. Chatterjee, N. Cao, A. Raychowdhury, and S. Sen, "Context-aware intelligence in resource-constrained IoT nodes: Opportunities and challenges," *IEEE Des. Test.*, vol. 36, no. 2, pp. 7–40, Apr. 2019, doi: 10.1109/MDAT.2019.2899334.

[188] P. Kiss, A. Reale, C. J. Ferrari, and Z. Istenes, "Deployment of IoT applications on 5G edge," in *Proc. IEEE Int. Conf. Future IoT Technol. (Future IoT)*, Jan. 2018, pp. 1–9, doi: 10.1109/FIOT.2018.8325595.

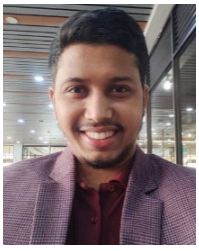
[189] H. Chen, R. Abbas, P. Cheng, M. Shirvanimoghaddam, W. Hardjawana, W. Bao, Y. Li, and B. Vucetic, "Ultra-reliable low latency cellular networks: Use cases, challenges and approaches," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 119–125, Dec. 2018.

[190] D. Rico and P. Merino, "A survey of end-to-end solutions for reliable low-latency communications in 5G networks," *IEEE Access*, vol. 8, pp. 192808–192834, 2020.

[191] G. Pocovi, H. Shariatmadari, G. Berardinelli, K. Pedersen, J. Steiner, and Z. Li, "Achieving ultra-reliable low-latency communications: Challenges and envisioned system enhancements," *IEEE Netw.*, vol. 32, no. 2, pp. 8–15, Mar. 2018.

[192] O. N. Yilmaz, "Ultra-reliable and low-latency 5G communication," in *Proc. Eur. Conf. Netw. Commun.(EuCNC)*, 2016, pp. 1–2.

SHAMS FORRUQUE AHMED received the Ph.D. degree from Central Queensland University, Australia, in 2016. He is currently an Associate Professor of mathematics with North South University (NSU), Dhaka, Bangladesh. Before joining NSU, he was a Postdoctoral Research Fellow with Deakin University, Australia. He joined NSU, as an Assistant Professor of mathematics, in 2016. He was an Associate Professor of mathematics and computational science with Asian University for Women (AUW), Chattogram. He has 127 publications, including book, book chapters, and journal articles. His research interests include energy and environment, computational fluid dynamics, and the Internet of Things. He was also awarded the International Postgraduate Research Award (IPRA) to pursue the Ph.D. degree. He received the Thesis Academic Excellence Award from Central Queensland University for his excellent Ph.D. research work, in 2016. He also received the Academic Merit Award for his excellent contribution to AUW, in 2022.



MD. SAKIB BIN ALAM received the Bachelor of Science degree in computer science and engineering from International Islamic University Chittagong, Bangladesh. He is currently pursuing the Master of Science degree in data science and artificial intelligence with the Asian Institute of Technology, Thailand. His research interests include artificial intelligence, the IoT, and deep learning.

SHAILA AFRIN is currently pursuing the bachelor's degree in bioinformatics and biotechnology with Asian University for Women, Chattogram, Bangladesh. Her research interests include computational biology, the IoT, data science, and in-silico analysis.

SABIHA JANNAT RAFA is currently pursuing the bachelor's degree in bioinformatics and biotechnology with Asian University for Women, Chattogram, Bangladesh. Her research interests include deep learning, the Internet of Things, and energy and environment.

SAMANTA BINTE TAHER is currently pursuing the degree in computer science and engineering with BRAC University, Dhaka, Bangladesh. Her research interests include deep learning, the Internet of Things, and machine learning.

MALIHA KABIR is currently pursuing the bachelor's degree in bioinformatics and biotechnology with Asian University for Women, Chattogram, Bangladesh. Her research interests include energy and environment, next-generation sequencing, and translational bioinformatics.

S. M. MUYEEN (Fellow, IEEE) received the B.Sc. (Eng.) degree in electrical and electronic engineering from the Rajshahi University of Engineering Technology (RUET), Bangladesh, formerly known as the Rajshahi Institute of Technology, in 2000, and the M.Eng. and Ph.D. degrees in electrical and electronic engineering from the Kitami Institute of Technology, Japan, in 2005 and 2008, respectively. He is currently a Full Professor with the Electrical Engineering Department, Qatar University. He has been a keynote speaker and an invited speaker at many international conferences, workshops, and universities. He has published more than 350 papers in different journals and international conferences. He has published seven books as the author or an editor. His research interests include power system stability and control, electrical machine, FACTS, energy storage systems (ESS), renewable energy, and HVDC systems. He is a fellow of Engineers Australia. He is serving as an Editor/an Associate Editor for many prestigious journals from IEEE, IET, and other publishers, including IEEE TRANSACTIONS ON ENERGY CONVERSION, IEEE POWER ENGINEERING LETTERS, *IET Renewable Power Generation*, and *IET Generation, Transmission & Distribution*. He is a Chartered Professional Engineers, Australia.

AMIR H. GANDOMI (Senior Member, IEEE) is currently a Professor of data science and an ARC DECRA Fellow with the Faculty of Engineering and Information Technology, University of Technology Sydney (UTS). He is also affiliated as a Distinguished Professor with Obuda University, Budapest. Prior to joining UTS, he was an Assistant Professor with the Stevens Institute of Technology, USA, and a Distinguished Research Fellow with the BEACON Center, Michigan State University, USA. He has published over 400 journal articles and 14 books which collectively have been cited more than 48,000 times (H-index = 99). His research interests include global optimization and (big) data analytics using machine learning and evolutionary computations in particular. He has been named as one of the most influential scientific minds and received the Highly Cited Researcher Award (top 1% publications and 0.1% researchers) from Web of Science for six consecutive years. He has received multiple prestigious awards for his research excellence and impact, such as the 2023 Achenbach Medal and the 2022 Walter L. Huber Prize, the highest-level mid-career research award in all areas of civil engineering. He has served as an associate editor, an editor, and the guest editor for several prestigious journals, such as an Associate Editor for *IEEE Networks* and IEEE INTERNET OF THINGS JOURNAL. He is active in delivering keynotes and invited talks. In the recent most impactful researcher list, done by Stanford University and released by Elsevier, he is ranked as the top 1,000 researchers (top 0.01%) and top 50 researchers in the AI and image processing subfield, in 2021. He also ranked 17th in GP bibliography among more than 15,000 researchers.

Open Access funding provided by 'Qatar National Library' within the CRUI CARE Agreement