A Comprehensive Review on the Internet of Things Network

Gazi Zahirul Islam [1,2,*] and S. M. A. Motakabber [1]

[1] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia
[2] Department of Computer Science and Engineering, Southeast University, Dhaka, Bangladesh
Email: gazi.islam@seu.edu.bd (G.Z.I.); amotakabber@iium.edu.my (S.M.A.M.)
*Corresponding author

***Abstract*—The Internet of Things (IoT) is becoming increasingly important due to its pervasive impact on various aspects of modern society and its potential to drive significant advancements in technology, industry, and everyday life. IoT relies on various technologies, including wireless communication protocols (e.g., Wi-Fi, Bluetooth, cellular), sensors and actuators, cloud computing, and data analytics. Researchers all around the world are working to improve the performance of the IoT network. Until now, the realization of full IoT has not been achieved and is not satisfactory according to its vision. Still, IoT technologies are emerging and expanding to meet the requirements of evolving new use cases. This paper reviews state-of-the-art developments on IoT by researchers, professionals, and IoT organizations. The article also focuses on the economical, regulatory, and ethical perspectives regarding the deployment of IoT. The paper also evaluates and contrasts several IoT research tools such as the testbed and simulator. At last, the article explores the path of research on IoT that helps future researchers by providing useful resources and strategic guidelines.**

***Keywords*—smart system, internet of things, simulation, testbed, sensors**

I. Introduction

The Internet of Things refers to the network of physical objects or 'things' embedded with sensors, software, actuators, and other technologies that enable them to connect and exchange data with other devices and systems over the Internet. These devices collect and exchange data with each other, often with a central server or cloud platform, enabling them to communicate, interact, and perform various tasks. The concept behind IoT is to enable everyday objects to connect and communicate with each other and the internet, creating a smart and interconnected ecosystem. These objects can include a wide range of devices, such as home appliances (e.g., smart thermostats, refrigerators), wearable devices (e.g., fitness trackers, smartwatches), industrial equipment, vehicles, and more.

IoT technology enables these devices to gather and analyze data, monitor and control physical processes, and automate tasks, leading to improved efficiency, convenience, and decision-making. IoT relies on various technologies, including wireless communication protocols (such as Wi-Fi, Bluetooth, and cellular networks), sensors and actuators, cloud computing, and data analytics [1, 2]. It has applications in various domains, including smart homes, smart cities, healthcare, agriculture, transportation, manufacturing, and more.

Researchers all around the world are working to improve the performance of the IoT network. Until now, the realization of full IoT has not been achieved and is not satisfactory according to its vision. Still, IoT technologies are emerging and expanding to meet the requirements of evolving new use cases. This paper thoroughly investigates the current state-of-the-art of the Internet of Things. The article delineates and evaluates several IoT research tools and techniques that would help the researchers to innovate and validate their model for IoT networks. The contents of the paper are organized as below.

Section I introduces the Internet of Things networks and also discusses the contributions of the paper. Section II describes the challenges and smart use cases of the IoT. Section III discusses different IoT connectivity technologies, requirements, and standards. Section IV reviews the state-of-the-art of recent development of the IoT and futuristic network. Section V focuses on the economical, regulatory, and ethical perspectives for feasible IoT deployment. Section VI discusses research tools and techniques for the IoT network. Finally, Section VII concludes the paper.

II. Challenges and Prominent Applications

This section elaborates on the challenges and modern use cases of the Internet of Things. Section II-A investigates some challenges to deploying the IoT, Section II-B summarizes prominent IoT use cases, and Section II-C overviews the key technologies used for different IoT applications.

A. Major Challenges

Massive deployment of IoT networks brings numerous opportunities and advancements for the Internet of Things

Manuscript received November 11, 2024; revised December 30, 2024, accepted January 30, 2025; published February 28, 2025.

(IoT). However, it also introduces several challenges that need to be addressed. Here are some of the key challenges that are worth investigating in the future.

Security: With the massive increase in connected devices, the security of the IoT ecosystem becomes a critical concern. Future IoT networks (e.g., using 5G, 6G) need to ensure robust authentication, encryption, and data privacy mechanisms to protect against cyber threats, unauthorized access, and data breaches.

Case Study: Securing Smart Home IoT Devices

Smart homes are equipped with IoT devices such as smart locks, cameras, thermostats, and voice assistants, which enhance convenience and efficiency. However, these devices are vulnerable to cyberattacks due to weak security measures, creating risks for users.

Example: To secure smart home IoT devices users can take several measures such as using a strong and unique password, enabling two-factor authentication, keeping updated the firmware, and monitoring for unusual activity [3].

Concerns: In smart homes, IoT devices often lack robust security mechanisms and are vulnerable to:

- Unauthorized access due to weak or default credentials.
- Man-in-the-middle attacks on unencrypted communication.
- Data breaches and stealing sensitive user information.

Mission-critical applications: Some IoT applications, such as autonomous vehicles, remote surgery, or industrial automation, require ultra-low latency and real-time communication. Future IoT networks must provide extremely low latency and high reliability to support these mission-critical applications [4, 5].

Case Study: IoT in Mission-Critical Healthcare – Remote Patient Monitoring

Mission-critical IoT applications are systems where failures can lead to severe consequences, such as loss of life, significant financial loss, or operational disruptions. In healthcare, IoT plays a vital role in Remote Patient Monitoring (RPM), ensuring continuous observation of patients with chronic conditions or during recovery from surgeries [6].

Example: A hospital has partnered with an IoT vendor to implement an RPM system for serving patients with cardiovascular conditions.

Concerns:

- Traditional monitoring is resource-intensive and also not convenient for patients.
- Early signs of critical conditions are often missed without real-time monitoring.
- Manual data collection is tedious and prone to errors that lead to suboptimal treatment.

Data Management and Analytics: The massive influx of data generated by IoT devices poses challenges in terms of data storage, processing, and analytics [7]. Robust IoT networks should have efficient data management systems, edge computing capabilities, and advanced analytics tools to derive valuable insights from the data deluge.

Case Study: IoT Data Management and Analytics in Smart Agriculture

Agriculture is increasingly employing IoT to increase productivity, resource utilization, and crop quality. IoT devices produce a large volume of data, such as weather conditions, soil quality, temperature, crop health, etc. Managing and analyzing vast amounts of data effectively is crucial for decision-making [8].

Example: In order to solve problems like crop diseases, water shortages, and operational inefficiencies, an agricultural company in Florida deploys an Internet of Things-based precision farming system.

Concerns:

- Overwatering and underwatering cause reduced yields and wasted water.
- Responding to unfavorable weather conditions or insect outbreaks is difficult due to the lack of real-time information.
- The lack of integration between disparate data sources, such as sensors, drones, and weather stations cause missing opportunities.

These challenges highlight the complexity and multifaceted nature of implementing 5G and 6G-based IoT networks. Addressing these issues will require collaboration between stakeholders, including network providers, device manufacturers, policymakers, and security experts, to ensure a secure, reliable, and efficient IoT ecosystem. Since IoT technologies and communication networks are evolving, it is crucial to establish standardized protocols, frameworks, and policies that ensure interoperability, security, and compliance.

B. Prominent Applications

The Internet of Things (IoT) has a wide range of major applications across various industries and sectors. Fig. 1 shows several smart applications of the Internet of Things. These applications highlight the versatility and transformative potential of IoT across multiple sectors, improving efficiency, safety, and quality of life.

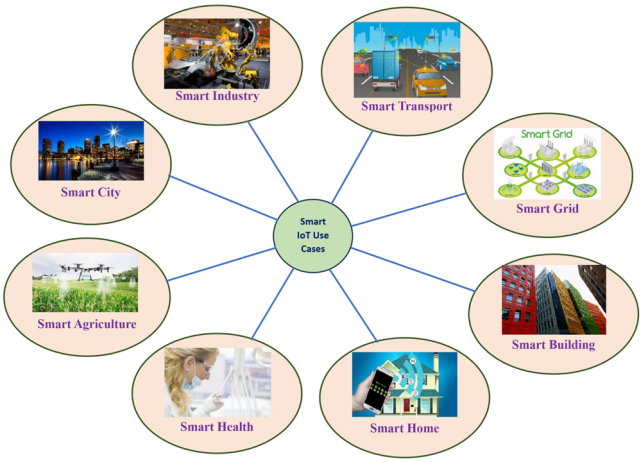

Fig. 1. Internet of things applications.

C. Key Technologies

The applications of IoT are continuously evolving and expanding as technology advances, providing new opportunities for efficiency, data-driven decision-making, and improved quality of life across various sectors. A

variety of wireless communication technologies and sensors are used to implement IoT applications. Table I shows key technologies and sensors for different IoT smart applications [9–11].

TABLE I. KEY TECHNOLOGIES FOR DIFFERENT IOT APPLICATIONS

Smart Applications	Typical Uses	Types of Networks	Key Technologies	IoT Sensors
Smart City	–Monitoring air quality and controlling pollution –Traffic management and congestion reduction	MAN, WRAN	5G, Wi-Fi, Satellite	Humidity, Air & Gas, Level, Water quality
Industrial IoT	–Quality control in manufacturing –Supply chain and inventory management	WPAN, WLAN	Zigbee, Wi-Fi	Chemical & Gas, Smoke, Proximity, Image, Motion
Transportation	–Vehicular communication for road safety –Tracking for logistics and delivery services	WRAN, MAN, WAN	5G, Wi-Fi, Satellite	Proximity, Piezoelectric, Ultrasonic, GPS
Smart Grid	–Optimize energy distribution –Monitoring power transmission lines	WLAN, WAN	5G, Satellite	Voltage, Temperature, Outage Detection, Dynamic Line Rating
Smart Building	–Utility service management –Security, parking, and space management	WLAN	Wi-Fi	Temperature, Image, Motion, Contact
Smart Home	–Security & surveillance – Regulate home appliances	WLAN, WPAN	Wi-Fi, Bluetooth	Temperature, Gas & Smoke, Image, Infrared
Healthcare	–Remote patient monitoring –Smart medical devices	WAN, WLAN	5G, Satellite, Wi-Fi	Image, Temperature, Pressure, Biomedical
Agriculture	–Monitoring soil conditions and crop health –Livestock tracking	WAN, WRAN	LoRaWAN, 5G	Temperature, Water Quality, Humidity, Image

III. IOT TECHNOLOGIES, REQUIREMENTS, AND STANDARDS

In this section, different IoT connectivity technologies, cellular requirements, and standards for the IoT are discussed elaborately.

A. Connectivity Technologies

IoT technologies for connectivity are essential for enabling communication between IoT devices and systems. These technologies vary in terms of range, bandwidth, power consumption, and application suitability. There are several IoT technologies available for connectivity, each with its own set of advantages and use cases. Here are some popular IoT connectivity technologies:

Wi-Fi: Wi-Fi is a widely adopted wireless networking technology that provides high-speed data transmission over short distances [12, 13]. It is commonly used for IoT applications within buildings or local areas where power consumption is not a major concern.

Cellular networks: Cellular networks, such as 2G, 3G, 4G, 5G, and emerging 6G, provide wide-area connectivity for IoT devices. Cellular networks offer good coverage and reliability but may have higher power consumption compared to other technologies [14].

Bluetooth: Bluetooth is a short-range wireless technology commonly used for connecting IoT devices to smartphones, tablets, or other nearby devices. Bluetooth Low Energy (BLE) is particularly suited for low-power IoT applications, such as wearable devices or sensors [15].

Zigbee: Zigbee is a low-power, low-data-rate wireless technology designed for short-range communication in home automation, smart lighting, and industrial applications [16]. It operates on the IEEE 802.15.4 standard and supports mesh networking, enabling devices to form self-healing networks.

Z-Wave: Z-Wave is a wireless communication protocol designed specifically for home automation applications. It operates in the sub-GHz range, providing good range and reliability [17]. Z-Wave devices form a mesh network, allowing for easy expansion and coverage across a home.

LoRaWAN: LoRaWAN (Long Range Wide Area Network) is a low-power, wide-area networking technology that enables long-range communication for IoT devices. It operates in unlicensed ISM bands (e.g., 868 MHz in Europe, 915 MHz in the US) and provides an adaptive data rate (i.e., 0.3 kbps to 50 kbps) based on the distance. It employs a Chirp Spread Spectrum (CSS) that facilitates high interference resistance and extended range. The range of LoRaWAN in urban areas is 2–5 km and in rural areas is 15–20 km. This technology is optimized for low-power devices that can operate on batteries for 5–10 years. Its payload size is 51–242 bytes and uses AES-128 encryption for secure data transmission. Some use cases of the LoRaWAN are smart metering, agriculture, environmental monitoring, and asset tracking [18].

NB-IoT and LTE-M: Narrowband IoT (NB-IoT) and LTE-M (Long-Term Evolution for Machines) are cellular technologies specifically designed for IoT devices. They offer low power consumption, extended coverage, and support for a massive number of connected devices. They cater to the requirements of LPWAN applications but differ in features, capabilities, and ideal use cases. The bandwidth of NB-IoT and LTE-M are 180 kHz and 1.4 MHz respectively. While LTE-M provides a data rate of up to 1 Mbps, NB-IoT provides only 20–60 kbps. The latency of LTE-M is very low (i.e., 10–15 ms) comparing NB-IoT (i.e., 1.6–10 seconds). NB-IoT provides limited mobility (no handover support) and LTE-M provides seamless handover support.

NB-IoT is ideal for applications requiring low data rates, extended battery life, and deep indoor or rural coverage such as environmental monitoring, agriculture and smart farming, smart metering, asset and goods tracking, utility management, smart cities, healthcare, etc. [19]. LTE-M is designed for applications that require higher data rates, mobility, lower latency, and voice support such as smart

transportation and logistics, wearable devices, healthcare and medical devices, connected vehicles, consumer electronics, industrial IoT (IIoT), Point-of-Sale (POS) terminals, public safety and emergency services, etc. [20]. Sigfox: Sigfox is a Low-Power Wide-Area Network (LPWAN) technology that operates on a dedicated global network. It provides long-range coverage with low power consumption, making it suitable for applications requiring low data rates and long battery life.

TABLE II. COMPARISON OF PERFORMANCE OF DIFFERENT CONNECTIVITY TECHNOLOGIES

Performance Criteria	Zig-Bee	Blue-tooth	Wi-Fi	Sigfox	LoRaWAN	NB-IoT	LTE-M	References
Primary Use Case	Smart homes, IoT networks	Short-range communication, IoT devices	High-speed internet	Low-power, wide-area IoT	Low-power, wide-area IoT	Cellular IoT applications	Cellular IoT with mobility support	[21–23]
Data Rate	Up to 250 kbps	1–3 Mbps	Up to 1 Gbps	~100 bps	~50 kbps	~250 kbps	Up to 1 Mbps	[7, 24, 25]
Latency	Low (~30 ms)	Very low (~10 ms)	Very low (~10 ms)	High (seconds)	Moderate (~1–10 s)	Low (~1 s)	Very low (~50 ms)	[11, 25]
Range	10–100 m	10–100 m	Up to 100 m (indoor), >200 m (outdoor)	~10 km (urban), ~40 km (rural)	~5 km (urban), ~20 km (rural)	~10–15 km	~10–15 km	[22, 23, 26]
Coverage	Local	Local	Local/ Building	Nationwide	Regional to nationwide	Nationwide	Nationwide	[24, 27, 28]
Frequency Band	2.4 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz	ISM bands (868 MHz/915 MHz)	ISM bands (868 MHz/915 MHz)	Licensed LTE spectrum	Licensed LTE spectrum	[22, 23, 26]
Mobility	Fixed devices	Limited	Limited	No	Limited	Yes	Yes	[29, 30]
Energy Consumption	Low	Moderate	High	Ultra-low	Ultra-low	Low	Moderate	[7, 29]
Deployment Cost	Low	Low	Medium	Low	Low	High (requires carrier support)	High (requires carrier support)	[11, 21]
Device Cost	Low	Low	Medium	Very low	Low	Moderate	Moderate	[11, 31]
Network Topology	Mesh	Point-to-point, star	Star	Star	Star	Cellular	Cellular	[21, 22, 26]
Scalability	High	Limited	Medium	Very high	Very high	High	High	[32, 29]
Security	AES encryption, network-specific keys	Strong encryption (AES)	WPA/WPA2/WPA3	Limited	AES encryption	Strong encryption	Strong encryption	[25, 29, 33]

These are just a few examples of IoT connectivity technologies. The choice of technology depends on factors such as range, power consumption, data rate, scalability, and cost requirements of the specific IoT application. Table II shows the comparison of the performance of different connectivity technologies. Fig. 2 compares the performance of different protocols graphically using bar charts. Each bar chart represents one feature with a normalized score of 0 to 1.

B. 3GPP Cellular MTC

Within the cellular context, the IoT connectivity solution is referred to as Machine-to-Machine (M2M), and within the 3GPP standardization body, it is referred to as Machine-Type Communications (MTC) [29]. 3GPP Cellular MTC (Machine Type Communication) refers to the set of specifications developed by the 3rd Generation Partnership Project (3GPP) for cellular networks to support IoT devices and Machine-to-Machine (M2M) communication. These specifications enable cellular networks to efficiently handle the unique requirements of IoT applications, such as low-power devices, low data rates, and massive device scalability. The 3GPP Cellular MTC technologies include:

NB-IoT (Narrowband Internet of Things): NB-IoT is a Low-Power Wide-Area Network (LPWAN) technology that operates within existing cellular networks [33]. It offers excellent coverage, long battery life, and the ability to connect a large number of devices cost-effectively. NB-IoT is designed for applications such as smart metering, asset tracking, and agriculture.

LTE-M (Long-Term Evolution for Machines): LTE-M, also known as Cat-M1, is another LPWAN technology within the LTE standard [11]. It provides a balance between data rates, power consumption, and coverage. LTE-M supports voice, mobility, and other advanced features, making it suitable for IoT applications like wearables, industrial monitoring, and tracking devices.

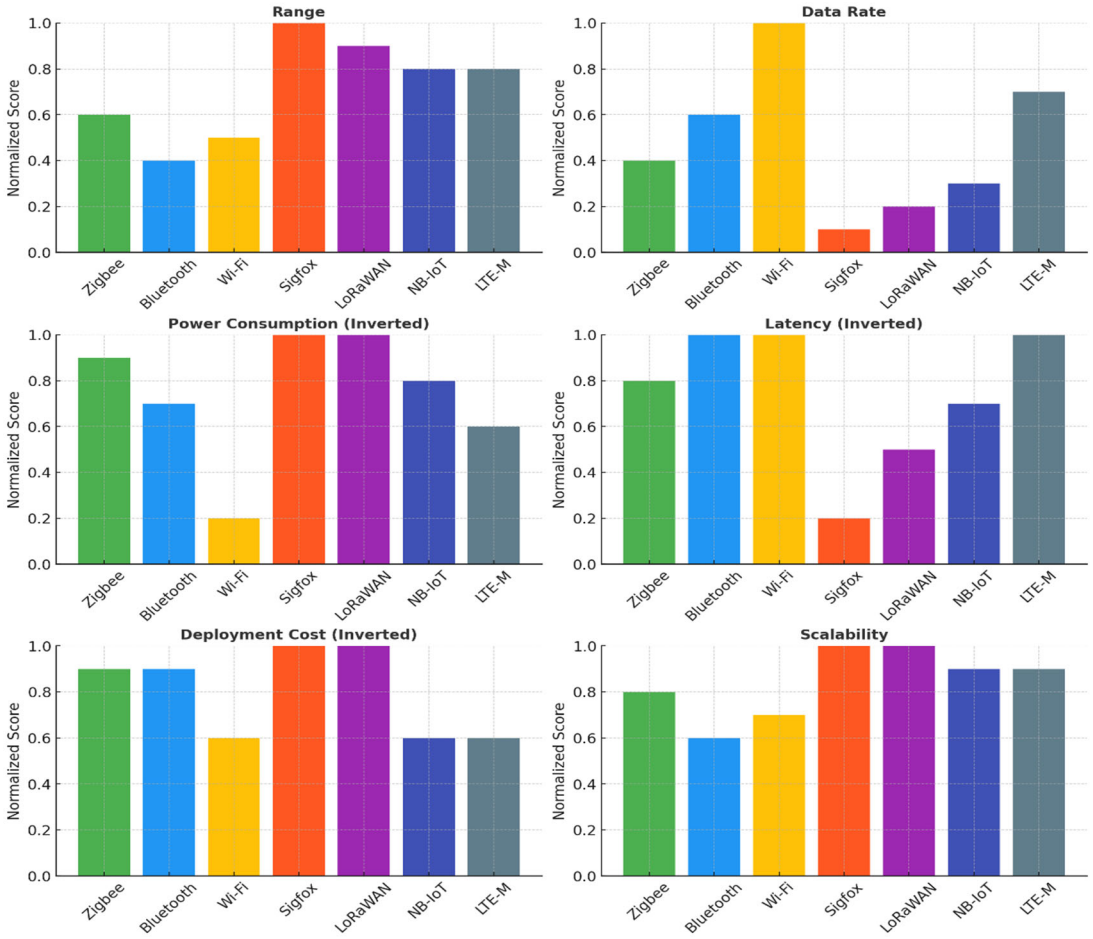

Fig. 2. Graphical comparison of different wireless protocols.

Both NB-IoT and LTE-M technologies operate in licensed spectrum, offering secure and reliable connectivity with cellular network infrastructure. 3GPP Cellular MTC technologies benefit from the existing cellular infrastructure, including coverage, security, and network management capabilities. They leverage the wide-area coverage of cellular networks, making them ideal for IoT deployments that require connectivity over large geographic areas or in remote locations.

These technologies are continually evolving within the 3GPP standards to address the diverse needs of IoT applications. As a result, cellular networks are becoming more capable of supporting a wide range of IoT use cases, enabling seamless connectivity, improved efficiency, and interoperability in the IoT ecosystem.

C. MTC Requirements and Standards

MTC (Machine-Type Communication) refers to communication between machines or devices in the context of the Internet of Things (IoT).

D. MTC Requirements

MTC has specific requirements due to the characteristics and needs of IoT devices. Here are some common requirements for MTC:

Low Power Consumption: Many IoT devices operate on limited battery power or have power constraints. Therefore, MTC solutions need to optimize power consumption to ensure long battery life or efficient use of power sources [11, 34]. This can be achieved through low-power communication protocols, energy-efficient hardware design, and power management techniques.

Wide Area Coverage: MTC devices may be deployed in various locations, including remote or rural areas. To support widespread IoT deployments, MTC solutions should provide reliable coverage over a wide area, including both urban and rural environments [35].

Scalability: IoT deployments often involve a massive number of devices. MTC solutions need to support scalability to accommodate a large number of connected devices, ensuring efficient management, communication, and data processing [36, 37].

Low Device Cost: IoT devices are often cost-sensitive, particularly when deployed in large numbers. MTC solutions should consider cost-effective hardware designs, efficient communication protocols, and optimization techniques to reduce the device cost and enable widespread adoption.

Security and Privacy: MTC solutions need to address the security and privacy concerns associated with IoT devices. This includes robust authentication, encryption, and access control mechanisms to protect against unauthorized access, data breaches, and tampering [38].

Quality of Service (QoS): Depending on the application, certain MTC use cases may require specific quality of

service parameters such as reliability, latency, and throughput [39, 40]. For example, applications like remote monitoring or industrial automation may require low latency and high reliability. MTC solutions should provide the necessary QoS capabilities to meet the requirements of different applications.

Interoperability: The IoT ecosystem comprises devices and platforms from various vendors and manufacturers. Interoperability is crucial to ensure seamless communication and integration between different devices and platforms. Standardized protocols and interfaces play a significant role in achieving interoperability in MTC [41].

Data Management and Analytics: MTC generates a massive amount of data, which needs to be efficiently managed, processed, and analyzed [42]. MTC solutions should include data management systems, edge computing capabilities, and analytics tools to derive meaningful insights from the collected data.

Regulatory Compliance: MTC solutions need to comply with local regulatory requirements regarding spectrum allocation, data privacy, security regulations, and other legal considerations. Compliance with regulations ensures that MTC deployments adhere to the relevant legal frameworks.

Addressing these requirements is crucial for the successful implementation and operation of MTC solutions in IoT deployments. It requires collaboration between stakeholders, including network providers, device manufacturers, standardization bodies, and regulatory authorities, to develop and adopt MTC technologies that meet the diverse needs of IoT applications.

E. 3GPP MTC Standardization

3GPP (Third Generation Partnership Project) is a global standardization organization that develops specifications for mobile communication systems, including MTC (Machine-Type Communication) in the context of the Internet of Things (IoT). 3GPP has played a significant role in defining the standards for MTC to ensure interoperability and efficient communication between IoT devices. Here are some key aspects of 3GPP's MTC standardization efforts:

Release 13: 3GPP Release 13, published in 2016, introduced significant enhancements and features specific to MTC. It included the introduction of Narrowband IoT (NB-IoT), a low-power, wide-area network technology designed for IoT devices with low data rate requirements. NB-IoT provides improved coverage, extended battery life, and support for a massive number of devices [43].

MTC in LTE: 3GPP has introduced several features and optimizations in LTE (Long-Term Evolution) networks to support MTC requirements. This includes power-saving modes, extended coverage, reduced signaling overhead, and optimized access schemes for low-data-rate IoT devices.

MTC in 5G: With the advent of 5G technology, 3GPP has continued to enhance MTC capabilities. 5G networks provide enhanced support for massive IoT deployments, including higher device density, Ultra-Reliable Low-Latency Communication (URLLC), and network slicing [44]. 3GPP has developed specifications for 5G New Radio (NR) to support MTC use cases effectively.

Coexistence with other services: 3GPP standardization ensures that MTC can coexist with other mobile communication services, such as voice and data services for human users. This requires efficient sharing of network resources, spectrum management, and coordination mechanisms between MTC and other services to avoid interference and provide reliable connectivity.

Security and Privacy: 3GPP has also focused on addressing the security and privacy challenges in MTC deployments. It has defined security mechanisms, authentication protocols, encryption algorithms, and access control mechanisms to protect MTC devices and their data from unauthorized access and threats.

Interoperability: 3GPP standardization ensures interoperability between different MTC devices, networks, and platforms. It defines common protocols, interfaces, and data formats, allowing MTC devices from different vendors to communicate seamlessly and interoperate with various networks and services.

Continued Evolution: 3GPP's work on MTC standardization is an ongoing process. The organization continues to evolve the specifications and releases new versions to address emerging requirements, technology advancements, and industry needs [45].

The standardization efforts by 3GPP have been instrumental in enabling the deployment of MTC solutions worldwide. They provide a foundation for the interoperability, reliability, and scalability of IoT networks, facilitating the growth of IoT applications across various industries and sectors.

IV. Researches for Futuristic Network

Research endeavors are instrumental in shaping the future landscape of IoT, ensuring its seamless integration into advanced network infrastructures and addressing the associated challenges. Research efforts highlight the multidisciplinary nature of IoT research, spanning protocol design, data science, and hardware design to build robust, intelligent, and scalable future networks. The IoT is rapidly evolving, with current research focusing on enhancing its integration into futuristic networks. This section highlights current research on IoT protocol design and integration of IoT with other technologies for futuristic networks.

A. Research on IoT Communications

A lot of recent articles have been reviewed to get insight into the recent progress of the IoT. Table III summarizes some selected articles on the IoT. These articles primarily focused on the communication technologies and protocols for the IoT.

B. Futuristic Network

The Internet of Things (IoT) continues to evolve, integrating advanced technologies and expanding its applications across various sectors. Table IV portrays key emerging trends in the IoT. These trends indicate a future where IoT systems are more intelligent, efficient, and

integral to daily life, driving innovation across industries and enhancing user experiences. Addressing these trends can help researchers navigate the evolving landscape of IoT technologies.

TABLE III. PROMINENT RESEARCH ON THE IOT

References	Key Issues
Fuqaha *et al.* (2015) [46]	-Focuses on access networks and enabling technologies -Covers reliability, latency, security, and privacy
Motlagh *et al.* (2016) [47]	-Emphasizes the needs and prospects of satellite communications -Coalesces aerial/satellite technologies with cellular technologies for the future IoT
Xu *et al.* (2018) [48]	-Discusses the efficient usage of the NB-IoT for the access networks -Emphasizes LPWA solutions to achieve super coverage, low power, low cost, and massive connection.
Wang *et al.* (2017) [49]	-Surveying client-controlled heterogenous networks for 5G -Reviewing Radio Access Technologies (RATs)
Vangelista *et al.* (2015) [50]	-Focuses LPWAN communication as a key enabling technology -Highlights LoRaWAN as a promising technology for the wide-area IoT.
Akpakwu *et al.* (2017) [51]	-Outlines the prospects and challenges of 5G for the IoT -Presents a comprehensive review of emerging enabling technologies
Vaezi *et al.* (2022) [7]	-Proposes 6G visions to enhance energy and spectral efficiency, reliability, security, and privacy -Elaborates satellite communication and access networks
Almeida *et al.* (2019) [52]	-Studies the physical layer characteristics of recent technologies -Advanced 5G waveforms such as OFDM, UFMC, FBMC, and GFDM are analyzed
Buurman *et al.* (2020) [53]	-Designs an architecture of the LPWAN for the IoT -Delineates several use cases for the smart IoT using the LPWAN
Kanj *et al.* (2020) [54]	-Provides a tutorial on the physical layer (PHY) design of the NB-IoT -Focuses on the scheduling of downlink and uplink physical channels of the NB-IoT base station (BS) side and the user equipment (UE) side
Maraqa *et al.* (2020) [55]	-Outlines the prospects of non-orthogonal multiple access (NOMA) for the future wireless networks -Achieves power efficiency using the NOMA technology
Wijethilaka *et al.* (2021) [56]	-Presents a comprehensive analysis of the exploitation of network slicing in IoT realization -Discusses the role of emerging technologies and concepts, such as blockchain and AI/ML in network slicing and IoT integration
Shahab *et al.* (2020) [57]	-Highlights grant-free non-orthogonal multiple access for the IoT -Presents various NOMA schemes, their potential, and related practical challenges
Elbayoumi *et al.* (2020) [58]	-Promises for the NOMA for machine-type communications (MTC) -Provides a comprehensive survey and illustrative simulation results on the application of NOMA to support MTC in a UDN environment

TABLE IV. KEY EMERGING TRENDS IN THE IOT

Emerging Trends	Role of IT	Related Articles
Integration of Artificial Intelligence (AI)	AI improves IoT systems by facilitating autonomous decision-making and real-time data processing. IoT applications like predictive maintenance and customized user experiences become more intelligent and responsive as a result of AI integration.	[6, 59–62]
6G Connectivity	The interaction between devices, systems, and applications is expected to be completely transformed by the integration of 6G with IoT networks. 6G-based IoT is expected to provide reduced latency, improved reliability, intelligent computing, seamless communication, and other advantages. Moreover, this integration spurs advances in automation, intelligence, and ubiquitous networking, opening up new opportunities for businesses, governments, and people.	[63–66]
Edge Computing	Latency and bandwidth consumption can be decreased by processing data closer to its source. Edge computing enhances real-time analytics and the performance of IoT devices, which is very important for certain applications such as driverless cars, industrial automation, etc.	[64–68]
Machine Learning (ML)	The Internet of Things benefitted from machine learning by allowing devices to analyze and learn from data, thereby improving automation and decision-making. The synergy of IoT and ML creates intelligent, self-governing, and effective systems that are revolutionizing industries. The foundation for a smarter and more connected future is being laid by this integration, which is propelling innovation in real-time analytics, automation, customization, and security.	[61, 69–71]
Digital Twins	Digital twins are virtual objects of real-world systems or gadgets that are updated in real time using data from the Internet of Things. Digital twins improve troubleshooting, performance monitoring, and system design. These agents can be deployed to healthcare simulation, urban planning, and industrial processes.	[72–75]

Security and Privacy	Improving security is necessary as IoT devices gather a huge volume of sensitive information. The goal of cutting-edge technologies like blockchain, AI-based security, and sophisticated encryption methods is to keep safe IoT networks from cyber-attacks. Moreover, Quantum-resistant cryptography can be employed to remain secure against attacks from both classical and quantum computers.	[69, 71, 76, 77],
Software-defined Internet of Things (SD-IoT)	It refers to an approach to managing and deploying IoT systems using principles of Software-Defined Networking (SDN) and virtualization. SD-IoT separates the control logic from physical devices, providing flexibility, scalability, and centralized control over IoT networks. SD-IoT extends the traditional IoT framework by introducing programmability, centralized control, and better resource management.	[77–81, 40]
Integration of SDN and Fog-IoT	The coalescence of Software-Defined Networking (SDN) and Fog-Internet of Things (IoT) networks offers an efficient and scalable approach to managing computational and network resources. An SDN-based task scheduling method can significantly improve performance (e.g., latency, energy consumption, resource utilization) when combined with optimization techniques like the Arithmetic Optimization Algorithm (AO) and the Whale Optimization Algorithm (WOA).	[79, 81–83]
Software-defined Internet of Vehicles (SD-IoV)	Efficient resource allocation for multimedia streaming in Software-Defined Internet of Vehicles (SD-IoV) is crucial to ensure a seamless user experience. Multimedia streaming in SD-IoV is highly demanding due to dynamic vehicular environments, mobility, and heterogeneous Quality of Service (QoS) requirements.	[78, 79, 84–87]

Software-Defined Networking (SDN) has a profound impact on the Internet of Things [87, 88]. SDN separates the network's control plane (decision-making) from the data plane (packet forwarding). This decoupling enables centralized control and programmability of the network through controllers, facilitating automation, optimization, and dynamic configuration. The coalescence of SDN and IoT networks opens new opportunities and facilities regarding management, security, scalability, and resource optimization [89, 90]. However, addressing challenges such as interoperability and latency is key to realizing the full potential of SDN in IoT applications. Efficient task scheduling can improve network efficiency and reduce latency, which are critical for IoT applications [88]. The authors in Ref. [88] focus on the SDN-based optimal task scheduling method in the Fog-IoT network using a combination of Aquila Optimizer (AO) and Whale Optimization Algorithm (WOA).

Software-Defined Internet of Vehicles (SD-IoV) is a paradigm that applies the concepts of SDN to the Internet of Vehicles (IoV), enabling more flexible, intelligent, and efficient management of vehicular networks [91]. The term 'IoV' refers to a network framework connecting vehicles, infrastructure, and cloud-based services, facilitating real-time communication and data exchange for improved safety, traffic control, and enhanced driving experiences [92]. Ref. [87] focuses on SDN-based resource allocation techniques for multimedia streaming for the Internet of Vehicles. Imanpour *et al.* [84] proposed an algorithm termed LSTM (long short-term memory) for load-balancing servers in software-defined Internet of multimedia things.

V. Economic, Regulatory and Ethical Aspects

Deploying IoT solutions involves many implications across economic, regulatory, and ethical domains. IoT deployment has to comply with laws, regulations, and ethics that vary across regions and industries. In this regard, the collaborative efforts of all stakeholders are crucial to maximize benefits while minimizing risks. Section V-A describes the economic impacts, Section V-B illustrates the regulatory frameworks, and V-C focuses on ethical issues for IoT deployment.

A. Economic Perspectives

Economically, the rollout of the Internet of Things has the potential to revolutionize different industrial sectors by promoting productivity, creativity, and value generation [93]. The following are the main financial effects of IoT deployment:

1) Improved resource management: By applying predictive maintenance, IoT can prevent downtime in manufacturing, utilities, and transportation [94]. In areas like agriculture and energy, IoT optimizes resource usage, reducing waste and operational costs by leveraging smart irrigation and smart grids respectively.
2) Cost and Labor Savings: The Internet of Things helps businesses to reduce operational costs. IoT-enabled system or businesses reduces operational costs by optimizing resource use and improving efficiency [95]. For instance, energy efficiency in smart grids and optimizing routes for IoT-enabled logistics companies contribute to economic savings. Again, by automating repetitive tasks, organizations can focus human resources on higher-value activities thereby decreasing labor costs.
3) Market Expansion: IoT creates new markets and ventures for connected devices, software, and services. IoT enables new business models such as subscription-based services (e.g., smart home devices), mobility as a service (e.g., dynamic ride-sharing), and pay-as-you-go systems (e.g., smart utilities). The global IoT market is projected to grow exponentially, contributing to GDP growth.
4) Automation and Optimization: IoT devices enable real-time monitoring and control that leads to improved process efficiency. For example, in transportation, Software-Defined Internet of Vehicles (SD-IoV) can reduce downtime of devices, saving costs and enhancing durability [93].
5) Business Transformation: IoT transforms industries like transportation (e.g., autonomous vehicles), healthcare (e.g., smart medical devices), retail (e.g., inventory tracking), and energy (e.g., smart grids), improving efficiency and reshaping competitive landscapes. IoT propels Industry 4.0 by automating

production lines and enabling real-time monitoring. The projected productivity gains can add 1.5–2 trillion US$ to the global economy annually.

6) Data Economy: IoT produces a large volume of data, leading the growth of data analytics, artificial intelligence, and cloud computing industries. Insights derived from IoT data drive business innovations and customer-centric solutions. Companies collecting and analyzing IoT data can sell valuable information to other organizations [96].
7) Emerging Business Models: IoT drives innovation by enabling businesses to move from product-based to service-based models. For instance, mobility as a service solution for dynamic ride-sharing, smart agriculture service for weather and soil analysis, etc.
8) Job Creation: As IoT expands, it creates new job opportunities across various areas such as firmware development, security, and data analysis [96]. Many IoT Engineers are required for designing, implementing, and maintaining IoT devices and systems. Data analysts analyze data collected from different sensors to derive valuable insights. Firmware developers are required to write and update software for IoT devices. IoT security specialists are responsible for ensuring the security of connected devices and preventing cyberattacks.
9) Long-Term Economic Impact: The long-term economic impact of IoT deployment spans various dimensions such as urban development, economic sustainability, global supply chains, etc. Smart cities driven by IoT can improve urban efficiency, reduce costs, and attract investment. Enhanced visibility, tracking, and transparency in supply chains reduce costs and improve efficiency and resilience. Moreover, IoT fosters economic sustainability by enabling smarter energy usage, reducing carbon footprints, and promoting the circular economy [95].

B. Regulatory Frameworks

An effective regulatory framework for IoT deployment is crucial to address challenges related to data security, privacy, interoperability, and ethical use. The framework focuses on a balance between enabling innovation and ensuring safety, fairness, and accountability. Here are the key elements and considerations in a regulatory framework for IoT deployment:

1) Data Privacy and Security: Clear policies are required to recognize the owner (i.e., users, device manufacturers, or service providers) of the IoT data. Policies must ensure that owners are informed about how their data is collected, stored, and used. IoT deployments must comply with existing data protection laws, such as the GDPR (General Data Protection Regulation) in the EU, CCPA (California Consumer Privacy Act) in California, and similar regulations globally [97]. Non-compliance with regulations is subject to fines, reputational damage, and legal challenges. Again, policies should encourage IoT deployers to collect only the data necessary for their functions.
2) Spectrum Allocation: As IoT devices rely on wireless communication, efficient spectrum management is necessary to prevent interferences. It is necessary to provide reliable connectivity for critical applications like healthcare and transportation. There are national and international organizations to regulate and allocate wireless spectrum for efficient and uninterrupted communication. Now, international regulatory bodies allocate unlicensed (e.g., ISM bands) and licensed spectrum (e.g., NB-IoT) to avoid interference of wireless signals.
3) Interoperability and Standardization: A universal standard for communication, data formats, and protocols helps interoperability between devices and technologies. On the other hand, fragmented standards hinder innovation and market growth. Therefore, collaboration between governments and industry bodies is important to provide common standards globally for IoT communication [98]. Open standards initiatives can promote open-source frameworks and APIs for IoT systems. Nowadays, several international organizations namely, International Telecommunication Union (ITU), International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), World Economic Forum (WEF) are working for setting and developing global standards for IoT.
4) Liability and Accountability: Regulations should clearly define the rules of product liability so that the stakeholders (e.g., device manufacturers, service providers, software developers, network operators) can bring under accountability for device failures, security vulnerabilities, or harm caused by their products. The regulations should address legal implications for IoT-related accidents, especially in high-risk sectors like autonomous vehicles or industrial IoT. Regulations should require manufacturers to provide clear documentation on device use, risks, and maintenance. AI-based IoT systems (e.g., autonomous vehicles) raise ethical and legal concerns about accountability for decisions made without human intervention [99].
5) Environmental Sustainability: Deploying IoT devices raises several environmental sustainability concerns. These include e-waste generation, carbon footprint, global energy demands, resource depletion (for mining raw materials e.g., cobalt, lithium), electromagnetic pollution, and biodiversity impact. Enforcing eco-friendly manufacturing and energy-efficient IoT devices can enhance environmental sustainability [94]. In this regard, EU's Ecodesign directives mandate energy-efficient IoT devices to reduce environmental impact. IoT regulations can also include provisions for recycling and safe disposal of IoT devices to minimize environmental impact. IoT researchers and engineers should focus on the circular economy so that IoT devices can be repairable, upgradable, and recyclable.

C. Ethical Aspects

IoT, connecting billions of devices worldwide, is transforming the way we live and work. The rapid growth of IoT devices raises remarkable ethical challenges that must be addressed to ensure a technology-blessed society while minimizing adversity [97]. Here is an overview of the key ethical issues:

1) Privacy Concerns: IoT devices collect a huge volume of personal and sensitive data and consumers are often not fully aware of the purpose of data collection. Ethical IoT systems must inform users about what data is collected, how it is used, and with whom it is shared. The systems should collect minimum personal data and acquire only those data that are essential. The IoT systems should focus on anonymization for data collection and adhere to the relevant laws such as GDPR in Europe. IoT devices in homes, offices, and public places can be used for intrusive monitoring which is also a great concern. Users should use IoT devices carefully and must respect other's privacy.
2) Data Security and Misuse: IoT systems are vulnerable to hacking, creating risks of data breaches, misuse, or manipulation. It is necessary to address who (e.g., manufacturers, users, service providers, etc.) is ethically responsible for securing IoT devices. Behavioral data collected by IoT devices can be used to influence decisions without users' awareness. Organizations and businesses may use IoT data unethically (e.g., discriminatory pricing, and manipulation).
3) Digital Divide: The extensive use of IoT may exacerbate existing disparities and raise ethical concerns about inclusivity. People of different socio-economic groups have not equal access to IoT technologies which creates a digital divide. IoT solutions designed for developed nations may not address the unique needs of developing regions or countries. Thus, High costs of IoT devices and services can exclude low-income populations. Developing cost-effective solutions is required to ensure equitable access.
4) Ethical AI in IoT: Ethical AI in the IoT is an important issue that focuses on the adoption of AI into IoT infrastructure in a manner that is responsible, transparent, and respectful of human rights [99]. Nowadays, a lot of IoT systems employ artificial intelligence for analytics and automation which raises unique ethical challenges. In many cases, AI-based IoT system presents a 'black box' effect to users and others as they do not know how the system makes decisions. Decision-making in IoT systems should be explainable and algorithms must be transparent and free of bias. It is urged to involve stakeholders in decision-making processes. Collaboration between governments, corporations, and society is necessary for the ethical deployment of IoT in order to establish a balance between innovation, accountability, and equality.
5) Other Concerns: IoT technologies can affect human autonomy in different ways. IoT gadgets aimed at older people or youngsters (such as smart toys) may take advantage of their limited ability to consent or understand the technology. Some IoT systems (e.g., driverless cars, and smart thermostats) make decisions without human input. Ethically, this raises questions about accountability and user control. The fast and enormous growth of IoT also contributes to ethical concerns about environmental sustainability. Ethical designs should focus on environment-friendly materials in device manufacturing as well as repairing and recycling products [94]. IoT systems deployed in mission-critical applications such as healthcare, transportation, industrial control systems, public safety, etc. must meet higher ethical standards. For example, a compromised industrial IoT system hacked by malicious actors can cause accidents or disasters. IoT solutions designed for beneficial purposes may also be used maliciously, raising ethical dilemmas about development and deployment.

IoT companies face ethical obligations regarding transparency, fairness, and societal impact [93]. Large IoT ecosystems controlled by several business giants may limit consumer choices and stifle competition. Organizations should consider the broader social impact of IoT deployments, such as the displacement of jobs through automation. International bodies may establish ethical standards and encourage fair IoT deployment worldwide. As IoT systems often operate across jurisdictions, it is also challenging to enforce ethical practices globally.

VI. IoT Research Tools

Researching the Internet of Things (IoT) involves a multidisciplinary approach, combining aspects of hardware, software, networking, simulation, prototyping, and data analysis. A lot of tools and techniques are used for IoT research. Section VI-A summarizes popular hardware and Section VI-B describes common software used for IoT research. Section VI-C describes and compares some widely used simulators and testbeds for the IoT.

A. Hardware Tools

Arduino and Raspberry Pi: Arduino and Raspberry Pi are two popular platforms in the world of electronics and DIY (i.e., do it yourself) projects. These are the micro-controller-based platforms/kits that are widely used for prototyping and building IoT devices. Arduino which is a low-price kit is suitable for simple projects. Raspberry Pi provides more computing power and is comparatively expensive.

Sensors and Actuators: Various sensors and actuators are the heart of the wireless sensor network (WSN) and IoT. These are usually simple and low-price circuitry/chips that form the basic building block of the IoT hardware. Sensors (temperature, humidity, pressure, etc.) and actuators (motors, relays, etc.) are crucial for collecting data and performing actions in the physical world. Table 1 explores many sensors for IoT research.

Microcontrollers and Development Boards: ESP8266 and ESP32 developed by Espressif Systems are very popular microcontroller platforms designed for IoT applications. Both can be programmed using Arduino IDE and support various programming languages. ESP8266 has a low-cost microcontroller that makes it suitable for IoT projects. It is very popular because of its affordability, ease of use, and built-in Wi-Fi facility. ESP32 is an advanced version of ESP8266 with more features and capabilities. It provides Bluetooth along with Wi-Fi connectivity. Besides these, kits provided by some companies like Intel, Microsoft, etc. often include a set of tools and hardware components for IoT development.

B. Software and Protocols

MQTT and CoAP: MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) are two IoT communication protocols designed for resource-constrained environments. Both are lightweight transport layer protocols. However, MQTT operates on top of TCP/IP which ensures reliable communication and CoAP operates over UDP which provides a connectionless communication mechanism. CoAP is suitable for applications where simplicity, low overhead, and scalability are important. On the other hand, MQTT is efficient for ensuring the quality of service, persistent, and real-time communication.

Node-RED: Node-RED originally developed by IBM is a visual programming tool for wiring together devices, APIs, and online services as part of the IoT. It provides a browser-based canvas that allows connecting different nodes to create flows, which can be deployed to a runtime to be executed. It provides a dashboard UI for monitoring and controlling IoT devices. Node-RED has built-in support for popular IoT protocols (e.g., MQTT) to design IoT applications. It has an active online community that contributes nodes, flows, and ideas. Node-RED is well-documented, and there are many resources available, including tutorials, forums, and a library of contributed nodes.

Operating systems: IoT operating systems are specialized operating systems designed to run on resource-constrained devices in the IoT, embedded, and similar systems. These operating systems cater to the unique requirements of IoT devices, which often have limited processing power, memory, and storage. Contiki [100] and RIOT [101] are two widely used open-source IoT operating systems. Contiki supports cooperative multitasking and requires very low memory to run. It has built-in support for several IoT protocols like CoAP and MQTT. RIOT supports real-time functions and consumes very low energy. It also supports numerous IoT protocols and IPv6 networking. On top of Contiki and RIOT, there are some other IoT operating systems namely, Zephyr, Tizen, TinyOS, FreeRTOS, etc.

Network and security tools: Wireshark [102] is a powerful network protocol analyzer that allows you to capture and inspect the data traveling over a network. It is open-source software used for network troubleshooting and traffic analysis in real time. Wireshark is also a valuable tool for analyzing and troubleshooting network communication between IoT devices. It is a multi-purpose networking tool and may require complementary tools, plugins, or techniques for a comprehensive analysis of the IoT network. The efficiency of Wireshark in the IoT context depends on the specific devices and corresponding protocols.

C. Simulators and Testbeds

1) IoT Simulators

An IoT simulator is a software tool that plays an important role in the development and testing of IoT applications and devices. It allows the developers and researchers to emulate various IoT scenarios, test different conditions, and ensure the reliability and efficiency of their solutions. There are a variety of IoT simulators each having its own scopes, features, and capabilities. It is noted that most of the IoT simulators are originally developed for network and communication simulation [103, 104]. As IoT technology emerges legacy network simulators incorporate IoT features and plugins to extend their services. A brief description of the popular simulators is given below.

TABLE V. COMPARISON OF THE POPULAR IOT SIMULATORS

Names and Web References	IoT Layers and Scales	Open Source and Languages	Mobility and Types	Best Use Cases
Cooja, [105]	Perceptual Network, Small	Yes, C/Java	Yes, Discrete Event	IoT and WSN-specific research
NS-3, [106]	Perceptual Network, Large	Yes, C++	Yes, Discrete Event	Protocol development, IoT and IP-based systems
MATLAB/ Simulink, [107]	All IoT layers, Large	No, MATLAB	Yes, Continuous and Discrete Event	IoT system design, data analytics
QualNet, [108]	Perceptual Network, Large	No, C/C++	Yes, Discrete Event	Enterprise-level network modeling
OMNeT++, [109]	Perceptual Network, Large	Yes, C++	Yes, Discrete Event	Academic and custom research projects

Cooja: Cooja [105] is part of the Contiki OS (Operating System), an open-source operating system designed for the IoT. It is a network simulator that supports various IoT platforms, making it useful for testing and debugging IoT applications. It is a popular simulator for the WSN (wireless sensor networks) community. Cooja is basically written in C programming language and its GUI is developed with Java.

Network Simulator-3: It is a widely used powerful network simulator that supports IoT simulations [106], [110]. Installation of NS-3 in the operating system on a personal computer is quite complex and tedious as lots of software modules need to be integrated and set up. Since

NS-3 is an open-source network simulator, it can be deployed on cloud infrastructure to take advantage of its scalability and distributed computing capabilities. NS-3 is written in C++ programming language and Python is used to write scripts and extensions.

OMNeT++: It is a component-based, modular, and extensible simulation framework designed for mobile, wireless communication, and WSN research [108]. This simulator is suitable for simulating communication protocols in IoT networks. The framework is extensible and suitable for various scales of network simulations. It supports various types of networks and provides numerous visualization tools to observe and analyze the simulation results.

QualNet: It is a commercial simulator suitable for networks comprising heterogeneous components. IoT-specific simulations can be achieved by using additional library extensions. QualNet provides a realistic simulation environment considering various factors such as network topology, traffic patterns, and application behavior [108]. It has a GUI for designing the model and analyzing simulation results.

MATLAB/Simulink: Simulink is a MATLAB-based graphical programming environment for modeling, simulating, and analyzing dynamic systems [107]. Simulink is an efficient tool that provides a block diagram interface for building IoT models. MATLAB supports cloud integration and automated testing that ensure the reliability and robustness of IoT applications. MATLAB provides graphical tools for data visualization and analysis.

On top of the above popular simulators, there are some other simulators used for IoT research such as [111] Azure IoT Edge Simulator, ThingsBoard, SimulIDE, FIWARE IoT Agent, and Eclipse Ditto. Table V shows the comparison of different IoT simulators.

2) IoT testbeds

IoT testbed comprises hardware and software that simulates real-world scenarios for testing and validating the performance of IoT systems and applications. It provides a controlled environment for IoT researchers and developers to deploy a prototype of their design. The result or outcome of the testbed is expected to be the target environment or close to the target environment. Thus, IoT researchers and professionals can measure the performance of their intended service/solution and identify critical issues before implementing their IoT project.

IoT researchers use simulators, testbeds, or both for measuring, evaluating, and validating the performance of their concepts, ideas, designs, or models. Network researchers perform computer simulations with network simulators for a long time to validate their protocols and models. Nowadays, IoT, network, and communication researchers initially use simulators as a proof-of-concept in the virtual domain. In the next step, they use the testbeds to design and implement the prototypes of their model/work/project using real hardware and software, unlike the simulators.

The IoT testbed serves as a platform for testing the interoperability, security, scalability, and efficiency of IoT devices, applications, systems, and solutions. It plays an important role in fostering innovation, standardization, and the development of robust and interoperable IoT systems and solutions.

VII. Conclusion

The Internet of Things Network holds immense potential for various industry sectors. Research in this area can explore specific use cases and applications of IoT, such as smart cities, industrial automation, healthcare, transportation, and agriculture. By developing innovative solutions and understanding the economic impact of IoT deployments, researchers can drive technological advancements and foster economic growth. As IoT technologies evolve, it is crucial to establish standardized protocols, frameworks, and policies that ensure interoperability, security, and compliance.

In summary, research on IoT plays a vital role in unlocking the full potential of these technologies. It enables advancements in connectivity, resource utilization, security, decision-making, industry applications, and standardization, ultimately shaping the future of IoT and contributing to the development of smart and connected environments. In this paper, the authors explore research areas, research potentials, research tools and techniques, and related aspects within the scope of IoT. The authors also highlight the economical, regulatory, and ethical aspects of IoT for the successful deployment of IoT solutions. In the future, the researchers implement an efficient model for the IoT network that significantly enhances the performance of IoT networks.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

The main credit goes to the first author, Gazi Zahirul Islam who contributes to every step of the research from the literature review to the submission of the article. During the literature review and survey, he collects and accumulates data and contents from a lot of primaries, secondary, and tertiary sources. He organizes, analyzes, compares, and presents the data and related information for the manuscript. After studying all recent contributions and developments on the Internet of Things, he designs and organizes the contents and framework of this manuscript. S. M. A. Motakabber supervises the work thoroughly and provides support and guidance throughout the research. He critically analyzes the contents, examines the information and data, provides valuable resources, and monitors the progress of the work from the very beginning of the research. Both authors had approved the final version.

References

[1] I. Kahraman, A. Köse, M. Koca, and E. Anarim, "Age of Information in internet of things: A survey," *IEEE Internet of Things Journal*, vol. 1, no. 6, pp. 9896–9914, Mar. 2024.

[2] A. Hazra, A. Kalita, and M. Gurusamy, "Meeting the requirements of Internet of Things: the promise of edge computing," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7474–7498, Mar. 2024.

[3] P. Sun *et al.*, "A survey of IoT privacy security: Architecture, technology, challenges, and trends," *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34567–34591, Nov. 2024.

[4] S. N. Mishra and M. Khatua, "Reliable and delay efficient multi-path RPL for mission critical IoT applications," *IEEE Transactions on Mobile Computing*, vol. 23, no. 6, pp. 6983–6996, June 2024.

[5] S. N. Mishra and M. Khatua, "Game theoretic congestion control to achieve hard reliability in mission-critical IoT," *IEEE Transactions on Mobile Computing*, vol. 23, no. 12, pp. 14159–14170, Dec. 2024.

[6] F. Al-Turjman and B. D. Deebak, "A proxy-authorized public auditing scheme for cyber-medical systems using AI-IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5371–5382, Aug. 2022.

[7] 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 Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1117–1174, Febr. 2022.

[8] M. E. Latino, M. Menegoli, and A. Corallo, "Agriculture digitalization: A global examination based on bibliometric analysis," *IEEE Transactions on Engineering Management*, vol. 71, pp. 1330–1345, 2024.

[9] 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, Jan. 2020.

[10] G. Z. Islam et al., "IoT-based automatic gas leakage detection and fire protection system," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 21, pp. 49–70, 2022. https://doi.org/10.3991/ijim.v16i21.30311

[11] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[12] G. Z. Islam and M. A. Kashem, "Efficient resource allocation in the IEEE 802.11ax network leveraging OFDMA technology," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, Part A, pp. 2488–2496, June 2022.

[13] A. A. Abbood, Q. M. Shallal, and M. A. Fadhel, "Internet of things (IoT): A technology review, security issues, threats, and open challenges," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 3, pp. 1685–1692, 2020.

[14] B. Ahlgren, M. Hidell, and E. C.-H. Ngai, "Internet of Things for smart cities: Interoperability and open data," *IEEE Internet Computing*, vol. 20, no. 6, pp. 52–56, Dec. 2016.

[15] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10474–10498, July 2021.

[16] C. W. Chen, "Internet of video things: Next-generation iot with visual sensors," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6676–6685, Aug. 2020.

[17] M. Weyrich, and C. Ebert, "Reference Architectures for the internet of things," *IEEE Software*, vol. 33, no. 1, pp. 112–116, Feb. 2016.

[18] L. Vangelista and G. Calvagno, "On the channel activity detection in LoRaWAN networks," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 5598–5607, Aug. 2024.

[19] J.-C. Lin, "NB-IoT physical random-access channels (NPRACHs) with Intercarrier Interference (ICI) reduction," *IEEE Internet of Things Journal*, vol. 11, no. 3 pp. 5427–5438, Feb. 2024.

[20] G.A. Medina-Acosta *et al*., "3GPP release-17 physical layer enhancements for LTE-M and NB-IoT," *IEEE Communications Standards Magazine*, vol. 6, no. 4, pp. 80–86, Dec. 2022.

[21] J. S. Yalli, M. H. Hasan, and A. A. Badawi, "Internet of Things (IoT): Origins, embedded technologies, smart applications, and its growth in the last decade," *IEEE Access*, vol. 12, pp. 91357–91382, June 2024.

[22] S. F. Ahmed *et al*., "Toward a secure 5G-enabled Internet of Things: A survey on requirements, privacy, security, challenges, and opportunities," *IEEE Access*, vol. 12, pp. 13125–13145, Jan. 2024.

[23] Z. M. Iqal, A. Selamat, and O. Krejcar, "A comprehensive systematic review of access control in IoT: Requirements, technologies, and evaluation metrics," *IEEE Access*, vol. 12, pp. 12636–12654, Dec. 2023.

[24] G. Z. Islam and M. A. Kashem, "A proportional scheduling protocol for the OFDMA-based Future Wi-Fi Network," *Journal of Communications*, vol. 17, no. 5, pp. 322–338, May 2022.

[25] P. Levchenko, D. Bankov, E. Khorov, and A. Lyakhov, "Performance comparison of NB-Fi, Sigfox, and LoRaWAN," *Sensors*, 22, 9633, pp. 1–21, 2022.

[26] A. Kaushik et al., "Integrated sensing and communications for IoT: Synergies with key 6G technology enablers," *IEEE Internet of Things Magazine*, vol. 7, no. 5, pp. 136–143, Sep. 2024.

[27] Z. Wang, H. Li, H. Wang, and S. Ci, "Probability weighted based spectral resources allocation algorithm in HetNet under cloud-RAN architecture," in *Proc. Int. Conf. Commun. China Workshops*, China, 2013, pp. 88–92.

[28] D. Solomitckii, M. Gapeyenko, V. Semkin, S. Andreev, and Y. Koucheryavy, "Technologies for efficient amateur drone detection in 5G, millimeter-wave cellular infrastructure," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 43–50, Jan. 2018.

[29] 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 Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510– 527, Mar. 2016.

[30] C. Sexton, Q. Bodinier, A. Farhang, N. Marchetti, F. Bader, and L. A. DaSilva, "Enabling asynchronous machine-type D2D communication using multiple waveforms in 5G," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1307–1322, Apr. 2018.

[31] N. Al-Falahy and O. Y. Alani, "Technologies for 5G networks: Challenges and opportunities," *IT Professional*, vol. 19, no. 1, pp. 12–20, Jan./Feb. 2017.

[32] Z. Dawy, W. Saad, A. Ghosh, J. G. Andrews, and E. Yaacoub, "Toward machine type cellular communications," *IEEE Wireless Communications*, vol. 24, no. 1, pp. 120–128, Feb. 2017.

[33] Y.-P. E. Wang, "A primer on 3GPP narrowband Internet of Things (NB-IoT)," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 117–123, Mar. 2017.

[34] X. Liu and X. Zhang, "Rate and energy efficiency improvements for 5G-based IoT with simultaneous transfer," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 5971–5980, Aug. 2019.

[35] J. Voas, B. Agresti, and P. A. Laplante, "A closer look at IoT's things," *IT Professional*, vol. 20, no. 3, pp. 11–14, June 2018.

[36] Y. Liu, M. Peng, G. Shou, Y. Chen, and S. Chen, "Toward edge intelligence: Multiaccess edge computing for 5G and internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6722–6747, Aug. 2020.

[37] A. Ijaz, L. Zhang, M. Grau, A. Mohamed, S. Vural, A. U. Quddus, M. A. Imran, C. H. Foh, and R. Tafazolli, "Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations," *IEEE Access*, vol. 4, pp. 3322–3339, June 2016.

[38] T. M. Fernández-Caramés, "From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, July 2020.

[39] T. Qi et al. "Double QoS guarantee for NOMA-enabled massive MTC networks," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22657–22668, Nov. 2022.

[40] A. Montazerolghaem and M. H. Yaghmaee, "Load-balanced and QoS-aware software-defined Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3323–3337, Apr. 2020.

[41] W. Wang, N. Kumar, J. Chen, Z. Gong, X. Kong, W, Wei, and H. Gao, "Realizing the Potential of the Internet of Things for Smart Tourism with 5G and AI," *IEEE Network*, vol. 34, no. 6, pp. 295–301, Dec. 2020.

[42] S. Dama, V. Sathya, K. Kuchi, and T. V. Pasca, "A feasible cellular internet of things: Enabling edge computing and the IoT in dense futuristic cellular networks," *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 66–72, Jan. 2017.

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

[44] 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, Mar. 2020.

[45] Z. Piao, M. Peng, Y. Liu, and M. Daneshmand, "Recent advances of edge cache in radio access networks for internet of things:

Techniques, performances, and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 1010–1028, Feb. 2019.
[46] A. A. Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
[47] N. H. Motlagh, T. Taleb, and O. Arouk, "Low-altitude unmanned aerial vehicles-based Internet of Things services: Comprehensive survey and future perspectives," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 899–922, Dec. 2016.
[48] J. Xu, J. Yao, L. Wang, Z. Ming, K. Wu, and L. Chen, "Narrowband Internet of Things: Evolutions, technologies, and open issues," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1449–1462, Jun. 2018.
[49] M. Wang, J. Chen, E. Aryafar, and M. Chiang, "A survey of client-controlled HetNets for 5G," *IEEE Access*, vol. 5, pp. 2842–2854, 2017.
[50] L. Vangelista, A. Zanella, and M. Zorzi, "Long-range IoT technologies: The dawn of LoRaTM," *Future Access Enablers for Ubiquitous and Intelligent Infrastructures*, vol. 159, V. Atanasovski and A. Leon-Garcia, Eds. Cham, Switzerland: Springer, 2015, pp. 51–58.
[51] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. A. Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2017.
[52] I. B. F. de Almeida, L. L. Mendes, J. J. Rodrigues, and M. A. da Cruz, "5G waveforms for IoT applications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2554–2567, 2019.
[53] B. Buurman, J. Kamruzzaman, G. Karmakar, and S. Islam, "Low-power wide-area networks: Design goals, architecture, suitability to use cases and research challenges," *IEEE Access*, vol. 8, pp. 17179–17220, 2020.
[54] M. Kanj, V. Savaux, and M. Le Guen, "A tutorial on NB-IoT physical layer design," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2408–2446, 2020.
[55] O. Maraqa, A. S. Rajasekaran, S. Al-Ahmadi, H. Yanikomeroglu, and S. M. Sait, "A survey of rate-optimal power domain NOMA with enabling technologies of future wireless networks," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 4, pp. 2192–2235, 2020.
[56] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5G networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 957–994, Mar. 2021.
[57] M. B. Shahab, R. Abbas, M. Shirvanimoghaddam, and S. J. Johnson, "Grant-free non-orthogonal multiple access for IoT: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1805–1838, 2020.
[58] M. Elbayoumi, M. Kamel, W. Hamouda, and A. Youssef, "NOMA-assisted machine-type communications in UDN: State-of-the-art and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1276–1304, 2020.
[59] A. Joshi, S. Agarwal, D. P. Kanungo, and R. K. Panigrahi, "Empowering IoT with generative for landslide monitoring and prediction," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 3, pp. 4246–4258, Mar. 2024.
[60] S. Sai, M. Kanadia, and V. Chamola, "Empowering IoT with generative AI: applications, case studies, and limitations," *IEEE Internet of Things Magazine*, vol. 7, no. 3, pp. 38–43, May 2024.
[61] N. Quadar, M. Rahouti, M. Ayyash, S. K. Jagatheesaperumal, and A. Chehri, "IoT-AI/Machine learning experimental testbeds: the missing piece," *IEEE Internet of Things Magazine*, vol. 7, no. 1, pp. 136–143, Jan. 2024.
[62] S. M. Alrubei, E. Ball, and J. M. Rigelsford, "The use of blockchain to support distributed AI implementation in IoT systems," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 14790–14802, Aug. 2022.
[63] U. M. Malik, M. A. Javed, S. Zeadally, and S. U. Islam, "Energy-efficient fog computing for 6G-enabled massive IoT: Recent trends and future opportunities," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14572–14594, Aug. 2022.
[64] M. A. Ferrag et al., "Edge learning for 6G-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 4, pp. 2654–2713, Sep. 2023.
[65] Z. Liwen, F. Qamar, M. Liaqat, M. N. Hindia, and K. A. Z. Ariffin, "Toward efficient 6G IoT networks: A perspective on resource optimization strategies, challenges, and future directions," *IEEE Access*, vol. 12, pp. 76606 –76633, May 2024.
[66] P. Valsalan *et al*., "Unleashing the potential: The joint of 5G and 6G technologies in enabling advanced IoT communication and sensing systems: A comprehensive review and future prospects," *Journal of Communications*, vol. 19, no. 11, pp. 523–535, Nov. 2024.
[67] H. Baghban *et al*., "Edge-AI: IoT request service provisioning in federated edge computing using actor-critic reinforcement learning," *IEEE Transactions on Engineering Management*, vol. 71, pp. 12519–12528, May 2022.
[68] J. Li *et al.*, "Service home identification of multiple-source IoT applications in edge computing," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 1417–1430, Apr. 2023.
[69] A. I. E. Sayed *et al*., "DDoS Mitigation in IoT Using Machine Learning and Blockchain Integration," *IEEE Networking Letters*, vol. 6, no. 2, pp. 152–155, June 2024.
[70] E. Ozdogan *et al.*, "A Comprehensive Analysis of the Machine Learning Algorithms in IoT IDS Systems," *IEEE Access*, vol. 12, pp. 46785–46811, Mar. 2024.
[71] E. Bout, V. Loscri, and A. Gallais, "How machine learning changes the nature of cyberattacks on IoT networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 248–279, 2022.
[72] J. Li *et al.*, "AoI-aware, digital twin-empowered IoT query services in mobile edge computing," *IEEE/ACM Transactions on Networking*, vol. 32, no. 4, pp. 3636–3650, Aug. 2024.
[73] J. Tan *et al.*, "Adaptive caching scheme for jointly optimizing delay and energy consumption in heterogeneous digital twin IoT," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 6, pp. 4020–4032, May 2023.
[74] J. Li *et al*., "An IoT architecture leveraging digital twins: Compromised node detection scenario," *IEEE Systems Journal*, vol. 18, no. 2, pp. 1224–1235, June 2024.
[75] Q. Guo, F. Tang, and N. Kato, "Federated reinforcement learning-based resource allocation for D2D-aided digital twin edge networks in 6G industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 5, pp. 7228–7236, May 2023.
[76] H. Wang *et al*., "An intelligent digital twin method based on spatio-temporal feature fusion for IoT attack behavior identification," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 11, pp. 3561–3572, Nov. 2023.
[77] J. Bhayo *et al*., "A time-efficient approach toward DDoS attack detection in IoT network using SDN," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3612–3630, Mar. 2022.
[78] K. I. Qureshi *et al*., "Asynchronous federated learning for resource allocation in software-defined internet of UAVs," *IEEE Internet of Things Journal*, vol. 11, no. 12, pp. 20899–20911, June 2024.
[79] M. U. Ghazi *et al*., "Emergency message dissemination in vehicular networks: a review," *IEEE Access*, vol. 8, pp. 38606–38621, Feb. 2020.
[80] Q. Liu *et al*., "CLB-LB: Controller load balancing based on load prediction using deep learning for software-defined IoT networks," *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 1, pp. 173–185, Feb. 2025.
[81] S. Javanmardi *et al*., "An SDN perspective IoT-Fog security: A survey," *Computer Networks*, vol. 229, 109732, June 2023.
[82] M. Snehi, A. Bhandari, and J. Verma, "Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems," *Computers & Security*, vol. 139, 103702, Apr. 2024.
[83] Y. Salami, V. Khajehvand, and E. Zeinali, "A new secure offloading approach for internet of vehicles in fog-cloud federation," *Scientific Reports*, vol. 14, 5576, Mar. 2024.
[84] S. Imanpour *et al*., "Load balancing of servers in software-defined internet of multimedia things using the long short-term memory prediction algorithm," in *10th International Conference on Web Research (ICWR)*, Iran, pp. 291–296, May 2024.
[85] M. M. Karim *et al*., "CIC-SIoT: Clean-slate information-centric software-defined content discovery and distribution for Internet of Things," *IEEE Internet of Things Journal*, vol. 11, no. 22, pp. 37140–37153, Nov. 2024.
[86] J. Cui *et al.*, "LISP-MM: Efficient LISP-based mobility management in software defined vehicular networks," *IEEE*

Transactions on Network Science and Engineering, vol. 11, no. 3, pp. 3222–3236, Feb. 2024.
[87] A. Montazerolghaem, "Efficient resource allocation for multimedia streaming in software-defined internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 14718–14731, Dec. 2023.
[88] T. Salehnia *et al*., "SDN-based optimal task scheduling method in Fog-IoT network using combination of AO and WOA," *Handbook of Whale Optimization Algorithm: Variants, Hybrids, Improvements, and Applications*, Academic Press, 2024, pp. 109–128.
[89] M. R. Rezaee *et al*., "Fog offloading and task management in IoF-fog-cloud environment: Review of algorithms, networks, and SDN application," *IEEE Access*, vol. 12, pp. 39058–39080, Mar. 2024.
[90] H. M. Belachew *et al*., "Design a robust DDoS attack detection and mitigation scheme in SDN-edge-IoT by leveraging machine learning," *IEEE Access*, pp. 2169–3536, Jan. 2025.
[91] T. Zhang *et al*., "How to mitigate DDoS intelligently in SD-IoV: A moving target defense approach," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1097–1106, Jan. 2023.
[92] R. Chaudhary and N. Kumar, "SecGreen: Secrecy ensured power optimization scheme for software-defined connected IoV," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 2370–2386, Apr. 2023.
[93] K. S Awaisi, Q. Ye, and S. Sampalli, "A survey of industrial AIoT: Opportunities, challenges, and directions," *IEEE Access*, vol. 12, pp. 96946–96996, July 2024.
[94] N. Alhussien and T. A. Gulliver, "Toward AI-enabled green 6G networks: A resource management perspective," *IEEE Access*, vol. 12, pp. 132972–132995, Sep. 2024.
[95] A. Montazerolghaem, "Software-defined internet of multimedia things: energy-efficient and load-balanced resource management," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2432–2442, Feb. 2022.
[96] F. Firouzi *et al*., "AI-driven data monetization: The other face of data in IoT-based smart and connected health," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5581–5599, Apr. 2022.
[97] M. Rajagopal *et al.*, "A conceptual framework for AI governance in public administration – a smart governance perspective," in *Proc. 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Nepal, pp. 488–495, Oct. 2023.
[98] A. Sedrati, A. Mezrioui, and A. Ouaddah, "IoT-gov: A structured framework for internet of things governance," *Computer Networks*, vol. 233, 109902, Sep. 2023.
[99] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet of Things*, vol. 15, 100420, Sep. 2021.
[100] Contiki operating system. [Online]. Available: https://www.contiki-os.org/
[101] RIOT operating system. [Online]. Available: https://www.riot-os.org/
[102] Wireshark protocol analyzer. [Online]. Available: https://www.wireshark.org/
[103] M. Chernyshev *et al*., "Internet of Things (IoT): Research, simulators, and testbeds," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637–1647, June 2018.
[104] Gazi Zahirul Islam et al., "Achieving robust global bandwidth along with bypassing geo-restriction for internet users," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 1, pp. 112–123, 2020.
[105] Cooja network simulator. [Website]. [Online]. Available: https://github.com/contiki-os/contiki/wiki/An-Introduction-to-Cooja
[106] The ns-3 network simulator. [Online]. Available: http://www.nsnam.org/
[107] MATLAB/Simulink simulator. [Online]. Available: https://www.mathworks.com/products/simulink.html
[108] QualNet simulator. [Online]. Available: https://www.qualnet.fr/
[109] OMNeT++ discrete event simulator. [Online]. Available: https://omnetpp.org/
[110] G. Z. Islam and M. A. Kashem, "An OFDMA-based hybrid MAC protocol for IEEE 802.11ax," *Infocommunications Journal*, vol. 11, no. 2, pp. 48–57, June 2019.
[111] S. Zhu, S. Yang, X. Gou, Y. Xu, T. Zhang, and Y. Wan, "Survey of testing methods and testbed development concerning Internet of Things," *Wireless Pers. Commun.*, vol. 2021, pp. 1–30, Sep. 2021.