Scientific Publications

Journal of Artificial Intelligence and Big Data, 2023, 3, 1382
www.scipublications.org/journal/index.php/jaibd
DOI: 10.31586/jaibd.2023.1382

Review Article

Networking Solutions for Large-Scale IoT Deployments: Architectures, Challenges, and Trends

Ajay Dasari [1,*], Venkata Kishore Chilakapati [2], Srikanth Reddy Keshireddy [3], Venkata Teja Nagumotu [4], Harsha Vardhan Reddy Kavuluri [5], Akhil Kumar Pathani [6]

[1] Senior Support Engineer, Microsoft, USA
[2] Technical Advisor, Microsoft, USA
[3] Senior Software Engineer, Keen Info Tek Inc, USA
[4] Sr Network Engineer, Techno-bytes Inc, USA
[5] Lead database administrator, Wissen infotech Inc, USA
[6] Sr Network Enginee, Ebay, USA

*Correspondence: Ajay Dasari (dasari.ajay50@gmail.com)

Abstract: The Internet of Things (IoT) is a network of linked items that can gather, exchange, and act on data thanks to sensors, software, and communication technologies. Networking solutions for large-scale IoT deployments have become a cornerstone in advancing smart applications across industries, cities, and healthcare ecosystems. With billions of connected devices generating vast amounts of data, efficient networking infrastructures are required to ensure seamless communication, reliability, and scalability. IoT architectures, ranging from layered models to advanced cloud–edge integration, offer structured approaches for managing heterogeneous devices and diverse communication protocols. Recent innovations, such as 5G connectivity, Software-defined networking and network function virtualization provide flexibility and programmability, enabling dynamic adaptation to evolving requirements. Edge and fog computing further enhance responsiveness by processing data closer to devices, while AI-driven approaches contribute to intelligent routing, predictive analytics, and self-optimizing network management. Blockchain-based frameworks add transparency and trust, securing data exchange in decentralized environments perspective on how networking continues to transform the capabilities of IoT, setting the foundation for sustainable growth and future adoption across multiple domains.

Keywords: IoT Networking, Large-Scale Deployments, 5G, communication technologies, AI-Driven IoT, SDN/NFV, Blockchain in IoT

How to cite this paper:
Dasari, A., Chilakapati, V. K., Keshireddy, S. R., Nagumotu, V. T., Kavuluri, H. V. R., & Pathani, A. K. (2023). Networking Solutions for Large-Scale IoT Deployments: Architectures, Challenges, and Trends. *Journal of Artificial Intelligence and Big Data, 3*(1), 102-112. DOI: 10.31586/jaibd.2023.1382

Received: September 10, 2023
Revised: October 26, 2023
Accepted: December 16, 2023
Published: December 27, 2023

1. Introduction

The Internet of Things (IoT) has become a paradigm shifter, bringing commonplace things into the digital realm through sophisticated processing, communication, and sensing [1]. IoT is changing a number of industries, including manufacturing, transportation, healthcare, and agriculture, and smart cities by empowering devices to gather, share, and act upon data. Its capacity to link disparate systems not only improves operational effectiveness but also facilitates the development of new business models powered by automation and data analytics. However, the proliferation of billions of devices worldwide introduces unprecedented complexity in managing connectivity, security, and scalability, emphasizing the importance of robust networking solutions.

The networking infrastructure is the most basic element of any IoT ecosystem and the foundation of a smooth flow of communication between the sensors, actuators, the gateway and the cloud platforms [2]. The performance of the system, latencies and power

consumption are directly influenced by the choice of the networking technologies, which vary between short-range options, including Wi-Fi, Zigbee, and Bluetooth Low Energy (BLE), and wide-area options, such as LoRaWAN, NB-IoT, and cellular networks [3,4]. As the number of IoT applications increases, networking solutions need to support a heterogeneous set of applications, including those with low power consumption and high data rates, as well as real-time responsiveness. Through the deployment of IoT, it can do more than a selection of appropriate communication technologies, it is a comprehensive strategy, with edge intelligence, data management, and security enforcement [5,6,7,8]. Large-scale deployments are expected to consider the heterogeneity of devices, geographical distribution and resource limits and still ensure interoperability and resilience [9,10,11]. The fact that edge and fog computing paradigms can process data closer to their origin has made them more desirable, thereby reducing the latency and bandwidth issues associated with centralized cloud paradigms. Onboarding is secured, updates delivered as OTA, and network configuration made dynamic, adding to the deployment robustness and contributing to sustainable and scalable IoT operations.

As IoT adoption accelerates, the focus shifts toward large-scale IoT networking, where millions of connected entities interact in real time to deliver mission-critical services. Such environments demand architectures that combine massive connectivity, low latency, and high reliability while preserving energy efficiency and data integrity. Emerging technologies, including 5G, network slicing, and software-defined networking (SDN), provide the agility required to orchestrate resources dynamically across diverse IoT domains.

Structure of the Paper

The paper is structured as follows: Section II presents IoT networking architectures, Section III discusses networking challenges; Section IV reviews emerging trends including 5G integration and AI-driven networking; Section V provides a literature review of key studies; and Section VI concludes with future research.

2. Iot Networking Architectures

A significant paradigm shifts in how devices interact with their physical surroundings has been brought about by the IoT. The four-layer architecture of IoT systems serves as the foundation for a popular paradigm for IoT system design and deployment [12]. Understanding the many parts of an IoT system and how they work together is possible through an organized method. Figure 1 depicts the four-layer construction.

- The perception layer also called the sensing layer or the physical layer—is the foundational element of the IoT architecture. The physical device layer of the data collecting system includes sensors and actuators. They gather information by observing their surroundings. This layer enables physical world gadgets to detect and perceive their surroundings, gathering data that is subsequently sent back to the network layer.
- In the network layer, the devices may access the internet and are linked to one another via Ethernet cables. Although the networking architecture consists of several levels, In the end, the network layer is in charge of setting up the communication and data storage infrastructure. The network layer can employ a variety of networks, including LANs, WANs, and PANs, to help devices communicate with one another.
- The two layers are connected by the middleware layer, bridging the gap between perception and application. It manages the IoT system's security features, data storage, and communication protocol. Device and network integration are handled by the middleware layer, which also offers a platform.

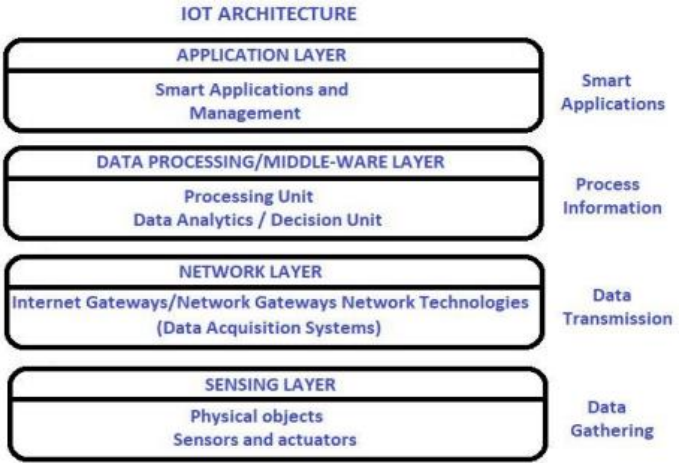

Figure 1. The Iot Architecture

2.1. Layered Architecture for IoT Communication

In general, the IoT architecture consists of four different levels, depending on the extent of this study [13]. Figure 2 below illustrates these levels, which are Perception, Network, Processing, and Application layers.

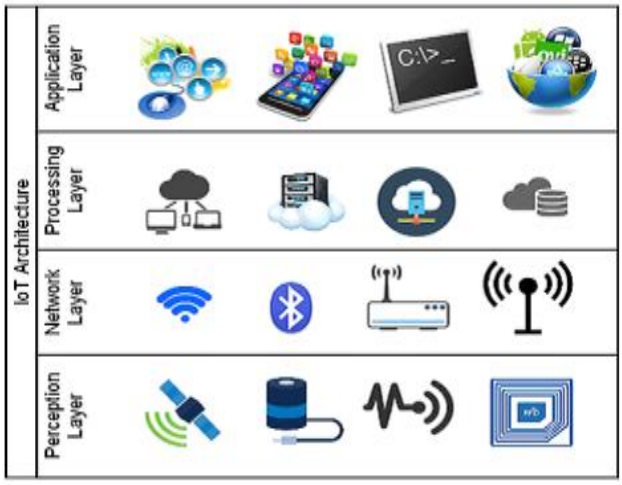

Figure 2. IoT Layer Architecture

- Perception/Device Layer: This layer is also known as the physical layer or the device layer. Through sensor nodes and other tangible devices, such as GPS, Arduino, barcodes, and RFID, it gathers data from the real world. Consequently, the layer makes it easier for different physical devices to communicate.
- Network Layer: In an IoT system, this layer is responsible for network administration, device connectivity, and information upkeep using many protocols, such as Constrained Application Protocol (CoAP) and MQTT 3.1.
- Processing Layer: The physical and network layers are connected (combined) via this layer. This layer utilizes intelligent computing to perform intelligent activities, such as data processing, autonomous information assessment, and ubiquitous computing.
- Application Layer: It is via this layer that end users have access to the pervasive support for context-aware services, often known as services between linked objects. IoT applications that meet client needs in various ways, such as smart homes and workplaces, are built on the data from this layer.

2.2. Communication Technologies for IoT

As seen in Figure 3, communication methods for IoT networks may be divided into two categories: cellular and non-cellular.

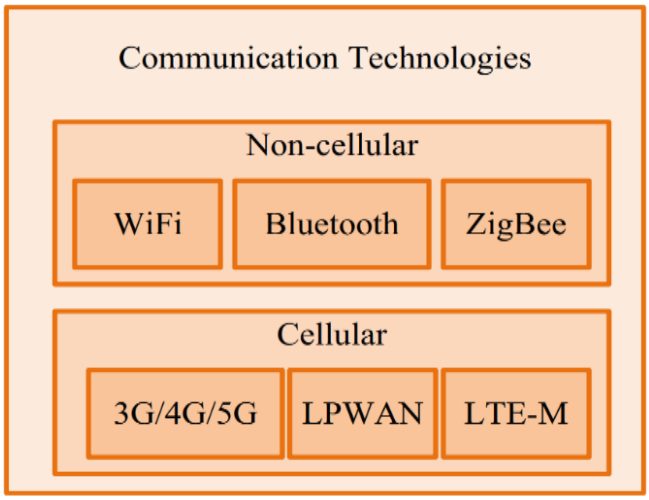

Figure 3. Communication Technologies for Iot Network

2.2.1. Non-Cellular Technologies

The most widely used Bluetooth, ZigBee, and WiFi are examples of IoT networks using non-cellular technology.

- **WIFI:** Wi-Fi devices are referred regarded as being on the Internet since they communicate via a full TCP/IP-based protocol [14]. This implies that any host with Wi-Fi is a member of a local area network by definition.
- **Bluetooth:** Bluetooth is only a reliable method of short-range communication when both ends are in the same room.
- **ZigBee:** A particular technology for wireless networking is the IEEE802.15.4 protocol, which is considered an industry standard, and serves as the foundation for ZigBee. ZigBee relies on data relaying between nodes to provide low data rates and short range.

2.2.2. Cellular Technologies

The unique features that have allowed protocols for cellular communication to compete on an equal footing with non-cellular technologies include:

- **3G/4G/5G:** The coverage of the third-generation (3G) network has not increased much, according to the Third Generation Partnership Project (3GPP). In contrast to 5G's ultra-low latency, increased bandwidth, and enormous connections for sophisticated applications, 4G LTE uses OFDMA technology, necessitating multi-mode devices.
- **Long-Term Evolution for Machines (LTE-M):** The current LTE features have been used to create a new IoT system design. It might share spectrum with current broadband LTE networks and be constructed using a single GSM channel (200 kHz).
- **Low-Power Wide-Area Network (LPWAN):** A system of wireless communication called LPWAN was created to link battery-operated devices across great distances while using the least amount of energy possible.

2.3. Software-Defined Networking (SDN) and Network Function Virtualization (NFV)

NFV is revolutionizing the field of computer and communication networks [15]. Through NFV, users may transition from proprietary and software housed on commercial off-the-shelf (COTS) platforms to vendor-specific hardware appliances for their networking operations. In cloud infrastructures, NFV offers network services for virtual machines (VMs), each of which performs unique network tasks.

- Adaptability in how network operations are distributed among general-purpose hardware.
- The prompt creation and deployment of new network services.
- Support for various tenancy circumstances and service versions.
- The decrease of capital expenditures through effective energy management.
- Operational process automation, which lowers OPEX expenses and increases efficiency.

The issue of developing and testing new protocols and solutions in production settings, SDN, a new network architecture, was developed as a result of the closed and proprietary underlying code of commercial switches and routers. Currently, the majority of commercial networking equipment include both control and data planes, making IP networks challenging to administer. As a result, operators must separately establish network rules for every device, frequently utilizing manufacturer-specific low-level instructions. Furthermore, modern networks lack automated reconfiguration capabilities, which are essential to adjust the network in the event of failures and changes in load. These problems impede development and innovation and limit the adaptability to adopt new network services and administration methods.

3. Networking Challenges in Large-Scale Iot Deployments

Large-scale IoT deployments face several vital networking challenges, with the high number of interconnected devices and disparate technologies involved. Scalability remains a significant concern for such networks because they may need to support billions of devices and transmit varied data types while remaining efficient. Energy efficiency is also a major concern because the majority of IoT devices run on batteries and need low-energy communication techniques [16]. Achieving low latency, high reliability, and consistent Quality of Service (QoS) in a dynamic, distributed IoT environment is difficult. There are also additional risks to security and privacy with the increased attack surface associated with massive amounts of connected IoT devices, making data protection even more difficult.

3.1. Low-Power Design Techniques for IoT

Designing energy-efficient circuits for IoT devices is essential to prolong battery life and guarantee sustained self-reliance. The power consumption issues with IoT devices have led to the development of an amount of low-power design strategies, especially those that rely on limited power sources or energy harvesting. Below are the key techniques used to minimize power usage [17].

- **Sub threshold:** Logic Design Sub-threshold logic operates transistors below their threshold voltage, reducing dynamic and leakage power consumption significantly. Despite this method decreasing the device's switching speed, it is highly effective for ultra-low-power IoT devices that do not require high performance.
- **Dynamic voltage:** and frequency scaling DVFS enables the system to dynamically modify the voltage and frequency of operation in real time in response to workload demands. DVFS lowers the processor unit's power consumption by reducing the voltage and frequency when computational demand is low.
- **Clock gating and power gating:** Clock gating reduces dynamic power usage by turning off the clock signal to particular circuit components when they are not

in use. Power gating, on the other hand, cuts off the power supply to unused sections of a circuit, significantly reducing leakage power. These techniques are widely used in IoT systems to conserve power during idle periods or when only certain functionalities are needed.

3.2. Security and Privacy Concerns

The Technologies are growing rapidly, and so are the machines. As technology advances, it also presents risks and raises concerns about privacy. Through a network, the smart devices may share data and communicate with one another. A machine being hacked puts the entire system at risk if any device becomes compromised. Some of the primary security issues include:

- **Integrity of Data:** A crucial consideration is the correctness of the data being sent between two nodes. Therefore, the data's accuracy needs to be preserved. For example, if a hacker instructs a manufacturing company to stop production, it is a very significant problem.
- **Confidentiality of Data:** The data sent back and forth between two nodes should be private. The data should be accessible only to the sender and the receiver. For example, Sensitive information may be made public if the infrastructure data is compromised, which might cause disruptions in operations or unauthorized access.
- **Authenticity of Data:** The authentication procedure guarantees that the supplied data is valid and reliable. In the medical and healthcare system, for instance, different medical institutions get a patient's parameters.
- **Availability of Data:** Data availability for consumers is a constant challenge in the IoT. The inability of the user to access the data is a serious problem. It has to be fixed as soon as feasible.

3.3. Interoperability and Standardization Issues

The networks on which IoT devices can function are still widely dispersed, heterogeneous, and multi-service and multi-vendor. IoT devices, in contrast to desktop PCs, frequently use a range of more irregular and unpredictable short-range wireless networking and communication techniques [18]. Network interoperability should handle issues like resource optimization, routing, addressing, and quality of service, security, and mobility assistance due to the IoT' dynamic and diverse network environment. standardization plays a vital role in ensuring consistency and compatibility across diverse IoT ecosystems. Various organizations such as IEEE, IETF, 3GPP, and ITU are actively working on defining communication protocols, security frameworks, and data models for IoT. Standardization not only enables seamless integration of devices from different vendors but also ensures scalability, reliability, and global adoption of IoT solutions.

4. Trends and Emerging Solutions in Iot Network

The potential of IOT in several industries, such as manufacturing, transportation, medical, and the arts, and agriculture. Nevertheless, there is still a conundrum when evaluating the current platforms and application services level in terms of worldwide market penetration [19]. The main cause, which has been recognized as the absence of standardization across smart devices, is the fragmented commitment to IOT solutions. A technical group working on modular standards for communication protocols known as machine-to-machine (M2M) mode has been prompted by numerous standard development organizations, including ETSI and ITU, to reduce the growing obstacle of the present modular shortcomings. AI-driven and edge computing solutions are being adopted to process data locally, reducing bandwidth usage and improving responsiveness. All these developments are geared towards addressing the current shortcomings to evolve the IoT to scalable, secure, and intelligent implementations.

4.1. 5G Networks and IoT Applications

The capability of living with 5G networks and IoT applications has entirely revolutionized several of its industries by providing network slicing of multiple services and applications, communication of a very large machine type, and highly reliable and low-latency connectivity. The use of 5G networks in industrial automation and driverless vehicles is one of the new ideas where the communication that is highly reliable and has low latency is essential to ensure the management of the traffic within the system and safety [20]. Smart cities and agriculture can also adopt 5G networks, which can facilitate data collection to the fullest extent possible, analysis, and decision-making through the facilitation of massive machine-type interfaces for a range of IoT devices, such as actuators and sensors. Furthermore, using network slicing, several services and applications may operate together on the same infrastructure while preserving their distinct latency, security, and dependability needs.

4.2. AI-Driven and Intelligent IoT Networking

The use of AI in IoT networking has emerged as a vital enabler for handling the size, diversity, and fluidity of extensive implementations [21]. ML, DL, and intelligent edge processing are utilized, IoT networks can become adaptive, secure, and autonomous, ensuring better performance and reliability.

- **Optimized Network Management:** AI models predict traffic patterns, optimize routing, and allocate resources dynamically to improve QoS.
- **Enhanced Security:** Anomaly detection, intrusion prevention, and proactive threat response are made possible by ML and DL algorithms.
- **Predictive Maintenance:** AI identifies potential device or network failures, reducing downtime and operational costs.
- **Real-Time Decision Making:** AI-driven edge computing supports local analytics, cutting latency and reducing reliance on cloud systems.
- **Autonomous Networks:** Self-learning IoT networks adapt to changing environments, improving scalability, resilience, and efficiency.

4.3. Edge and Fog Computing for Low-Latency Networking

As IoT devices expand exponentially, cloud-based architectures are no longer enough for applications that depend on delay [22]. Edge and fog computing let the application avoid depending entirely on distant cloud servers by enabling compute, data storage, and analytics to be relocated near the source of the data. In applications including medical monitoring, industrial automation, and driverless cars, having processing capacity close by lowers latency, improves bandwidth efficiency, and facilitates real-time decision-making.

- **Decreased Latency:** Analyzing data near the source allows for reduced response times that are critical to the success of services utilizing IoT applications.
- **Bandwidth Efficiency:** Since a proportion of the computing is being processed locally, there is less congestion as a result of less data being sent back to the central cloud.
- **Increased Reliability:** Localized computing means the IoT system continues to operate even when the cloud is intermittently available.
- **Security:** Data deemed sensitive can be processed without transmitting data to a cloud-based computer.
- **Scalability:** Compute resources can be distributed through the network, permitting the rollout of large-scale IoT solutions with workload being isolated to specific parts of the local compute as opposed to one central location.

The IoT network based on blockchain systems is turning into a secure and decentralized. The blockchain makes safe sharing of data possible through ensuring data

integrity, transparency and trust, control of access and tamper proof logging of data sharing amongst heterogeneous devices of the IoT. In addition, SDN and NFV technologies bring flexibility and programmability to IoT networks, which enables the dynamic configuration of networks, the orchestration of services, and the virtualization of network functions. These solutions are all oriented to flexibility, protection, and scalability of IoT application at a large scale.

5. Literature Review

It presents a summary of networking approaches to large-scale IoT, such as identifying devices, energy-efficient routing, LPWANs, hybrid architectures, convergence, and strengths, challenges, and future research of scalable, efficient, and resilient ecosystems.

Perdisci et al. (2020) The IoT Finder, a tool of effective passive identification of the IoT devices at the mass scale. The creation of an ML-based solution, which solely uses DNS fingerprints to locate a large variety of IoT devices, can be achieved through the use of distributed passive DNS data collection. The devices having IPv4, IPv6 addresses, or the place where the devices lie behind the NAT do not count in the system. In an effort to examine the precision of the IoT Finder, they deployed it as a multi-label classifier, which surmised the outcomes of detection of an IoT and DNS data collected at an ISP with more than 40 million customers in the US on third-party traffic [23].

Ouhab et al. (2020) present a new modelling paradigm to address this issue, grounded on a two-level control system. It could offer a new design of Low-Power and Lossy Networks Routing Protocol (RPL), which is built on the principles of multi-hop clustering strategy (MHC-RPL) at the initial level. It has been applied as a local control mechanism to cluster nodes in the IoT, aiming to minimize energy consumption. The second level is responsible for managing the global network through intelligence, utilizing the Q-routing algorithm in SDN. Compared to the state-of-the-art with regard to energy consumption, the ratio of packet delivery, and end-to-end latency, the results indicate that the proposed approach is superior [24].

Mekki et al. (2019) enhance the effective interconnectivity of intelligent, autonomous and heterogeneous devices by conducting a comprehensive and comparative study of diverse technologies. It can eventually work in favor of Sigfox and LoRa in the aspect of battery life, capacity and cost. Nonetheless, in terms of latency and quality of service, NB-IoT is even better. The success aspects of the different LPWAN technologies, such as the IoT, are also discussed, along with their application scenarios and the description of the best solution for each. Long-range radio communication (LWAN) is a low-rate, low-power technology that has become popular in the IoT. Three prominent LPWAN technologies are in competition for widespread IoT deployment: Sigfox, LoRa, and NB-IoT [25].

Rubio-Aparicio et al. (2019) Sigfox and LoRa are two IoT LPWAN technologies. It might be regarded as the most significant at the moment since it enables the creation of smart cities. It also suggests creating, deploying, and utilizing a hybrid IoT architecture called LoRa-Sigfox, which comprises open hardware and software components. In a real-world setting centered on remote water meter device monitoring, the architecture is assessed. Organizations can't even begin to comprehend the prospects that IoT presents. This means that they most likely have the option to create their own IoT network eventually [26].

Chowdhury et al. (2019) detailed explanations of how 5G/6G and IoT systems may function with using the use of optical wave communication, free space optics, optical camera, and visible light communication. The present fourth-generation communication system is expected to be significantly less competent than future 5G and 6G, respectively. 6G communication offers several times better performance than 5G communication in terms of minimal latency, excellent security, low energy use, and a great experience [27].

Mukherjee and Biswas (2018) proposed an exhaustive response that covers node placement, mobility patterns, protocols for networks, allocation of spectrum, MANET routing, and lastly, the running of Internet of Things (IoT) applications emulated with the Omnet++ simulator, with a demonstration of how well they function. When MANET and WSN are used together in smart environments that are everywhere, they make it possible to keep an eye on big cities and establish a new way for different Internet apps to conversation with each other. These applications can identify their surrounding and communicate the information to the gateway router. Data gathering is much facilitated when the information is sent from the gateway node to the MANET node [28].

Table 1 presents a concise comparative study of some networking solutions in the context of large-scale IoT implementation, including methods, key findings, limitations, and future research directions.

Table 1. Summary of a Study on Networking Solutions for Large-Scale IoT Deployments

Author	Technologies	Approach	Key Findings	Challenges	Future Directions
Perdisci et al. (2020)	IoT device identification	IoT Finder system using distributed passive DNS and ML-based multi-label classifier	NAT/IPv4/IPv6-independent DNS fingerprint-based precise large-scale identification of IoT devices	Scalability with increasing devices, evolving device behaviors	Extend detection to encrypted DNS and larger global datasets
Ouhab et al. (2020)	Energy-efficient and intelligent IoT routing	Two-level control: MHC-RPL for clustering + SDN with Q-routing	Enhanced efficiency in energy consumption, packet delivery ratio, and latency compared to cutting-edge	Integration complexity between SDN and RPL in real-world networks	Real-world deployment in large heterogeneous IoT environments
Mekki et al. (2019)	Comparative research on LPWAN technologies	Evaluation of Sigfox, LoRa, and NB-IoT	In terms of cost and battery life, Sigfox/LoRa is superior to NB-IoT, but QoS and latency are superior.	Trade-offs between coverage, capacity, and QoS	Hybrid LPWAN models for application-specific deployments
Rubio-Aparicio et al. (2019)	Mixed IoT LPWAN architecture	LoRa-Sigfox integration using open hardware/software	Successful deployment in smart city water monitoring	Limited interoperability and vendor dependencies	Broader deployment across other smart city applications
Chowdhury et al. (2019)	Optical Wireless Communication (OWC) for the IoT	Use of VLC, LiFi, OCC, FSO for 5G/6G IoT integration	OWC ensures high capacity, low latency, and reliable IoT connectivity	Environmental interference, infrastructure cost	Large-scale trials in real-world 5G/6G IoT systems
Mukherjee & Biswas (2018)	MANET-WSN convergence for IoT	Integration of MANET with WSN using Omnet++ simulations	Enhanced scalability and new communication platform for smart environments	High mobility management and dynamic topology issues	Develop robust mobility-aware protocols for large-scale IoT

6. Conclusion and Future Work

The increasing position of the IoT highlights the importance of networking solutions to facilitate the implementations of industries on large scale such as healthcare, transportation, and smart cities. The IoT architectures provide systematized approaches to managing the diversity of devices, scaling, interoperability, and security networking challenges are on the frontline. The emerging technologies such as 5G, AI-driven networking, SDN/NFV, blockchain, fog computing, edge computing, and others, are providing IoT systems with a boost by allowing them to become more adaptive, resilient, and intelligent infrastructure. The developments make performance and flexibility higher,

but the problem of latency, energy saving, standardization, and privacy of the information is burning. The limitations should be addressed so that they can be effectively incorporated between heterogeneous devices and communication protocols. The future emergence of the IoT networking depends on how well the networks can balance between the innovation and reliability, which can make the networks capable of supporting billions of devices, and meet the demands of security, efficiency and sustainability in the more complex environments.

The future work should focus on adaptive orchestration systems that can dynamically balance the computation and storage processes between the cloud, edge and device layers. Predictive traffic management, anomaly detection, and self-healing can be managed with the help of the integration of ML and reinforcement learning. Moreover, 6G and green networking are under investigation and are likely to redefine the IoT infrastructures in a global, safe, and sustainable adoption.

References

[1] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *J. Big Data*, vol. 6, no. 1, 2019, doi: 10.1186/s40537-019-0268-2.

[2] F. Pereira, R. Correia, P. Pinho, S. I. Lopes, and N. B. Carvalho, "Challenges in resource-constrained iot devices: Energy and communication as critical success factors for future iot deployment," *Sensors (Switzerland)*, vol. 20, no. 22, pp. 1–30, 2020, doi: 10.3390/s20226420.

[3] T. Gebremichael *et al.*, "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," *IEEE Access*, vol. 8, pp. 152351–152366, 2020, doi: 10.1109/ACCESS.2020.3016937.

[4] S. S. S. Neeli, "Serverless Databases: A Cost-Effective and Scalable Solution," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 6, p. 7, 2019.

[5] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 196–248, 2020, doi: 10.1109/COMST.2019.2933899.

[6] A. Kushwaha, P. Pathak, and S. Gupta, "Review of optimize load balancing algorithms in cloud," *Int. J. Distrib. Cloud Comput.*, vol. 4, no. 2, pp. 1–9, 2016.

[7] V. M. L. G. Nerella, "Observability-Driven SRE Practices for Proactive Database Reliability and Rapid Incident Response," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 7, no. 8, pp. 32–38, Aug. 2019, doi: 10.17762/ijritcc.v7i8.11710.

[8] D. D. Rao, "Multimedia Based Intelligent Content Networking for Future Internet," in *2009 Third UKSim European Symposium on Computer Modeling and Simulation*, 2009, pp. 55–59. doi: 10.1109/EMS.2009.108.

[9] N. H. Motlagh, M. Mohammadrezaei, J. Hunt, and B. Zakeri, "Internet of things (IoT) and the energy sector," *Energies*, vol. 13, no. 2, pp. 1–27, 2020, doi: 10.3390/en13020494.

[10] S. Gupta and S. Prakash, "QoS and load balancing in cloud computing-an access for performance enhancement using agent based software," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 11, pp. 641–644, 2019.

[11] G. Maddali, "Zero Trust Security Architectures for Large-Scale Cloud Workloads," *Gopikrishna Maddali*, vol. 5, no. 2, pp. 960–965, 2018.

[12] R. Kashyap, P. Bansal, S. Bharti, and A. Malyan, "Architecture, Features and Security Concern of IoT," vol. 10, no. 5, pp. 1125–1139, 2017.

[13] U. E. Chinanu, O. E. Oche, and J. O. Okah-edemoh, "Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures," *Guigoz. Sci. Rev.*, vol. 4, no. 10, pp. 80–89, 2018, doi: 10.32861/sr.410.80.89.

[14] W. Ejaz and A. Anpalagan, "Communication Technologies and Protocols for Internet of Things," 2019, pp. 17–30. doi: 10.1007/978-3-319-95037-2_2.

[15] M. S. Bonfim, K. L. Dias, and S. F. L. Fernandes, "Integrated NFV/SDN Architectures," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–39, Nov. 2018, doi: 10.1145/3172866.

[16] L. Farhan, R. Kharel, O. Kaiwartya, M. Quiroz-Castellanos, A. Alissa, and M. Abdulsalam, "A Concise Review on Internet of Things (IoT)-Problems, Challenges and Opportunities," *2018 11th Int. Symp. Commun. Syst. Networks Digit. Signal Process. CSNDSP 2018*, no. February 2019, 2018, doi: 10.1109/CSNDSP.2018.8471762.

[17] A. Thakkar, K. Chaudhari, and M. Shah, "A Comprehensive Survey on Energy-Efficient Power Management Techniques," *Procedia Comput. Sci.*, vol. 167, pp. 1189–1199, 2020, doi: 10.1016/j.procs.2020.03.432.

[18] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in Internet of Things: Taxonomies and Open Challenges," *Mob. Networks Appl.*, vol. 24, no. 3, pp. 796–809, 2019, doi: 10.1007/s11036-018-1089-9.

[19] S. Kumar and Z. Raza, "Internet of Things: Possibilities and challenges," *Fog Comput. Break. Res. Pract.*, no. August, pp. 1–24, 2018, doi: 10.4018/978-1-5225-5649-7.ch001.

[20] M. M. da Silva and J. Guerreiro, "On the 5G and Beyond," *Appl. Sci.*, vol. 10, no. 20, p. 7091, Oct. 2020, doi: 10.3390/app10207091.

[21] T. Adimulam, M. Bhoyar, and P. Reddy, "AI-Driven Predictive Maintenance in IoT-Enabled Industrial Systems," *Iconic Res. Eng.*, vol. 2, no. 11, pp. 398–410, 2019.
[22] Madhuri, "A review on Edge computing for Internet of Things," *Int. J. Res. Anal. Rev.*, vol. 5, no. 4, pp. 50–55, 2018.
[23] R. Perdisci, T. Papastergiou, O. Alrawi, and M. Antonakakis, "IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis," in *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2020, pp. 474–489. doi: 10.1109/EuroSP48549.2020.00037.
[24] A. Ouhab, T. Abreu, H. Slimani, and A. Mellouk, "Energy-efficient clustering and routing algorithm for large-scale SDN-based IoT monitoring," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6. doi: 10.1109/ICC40277.2020.9148659.
[25] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, Mar. 2019, doi: 10.1016/j.icte.2017.12.005.
[26] J. Rubio-Aparicio, F. Cerdan-Cartagena, J. Suardiaz-Muro, and J. Ybarra-Moreno, "Design and Implementation of a Mixed IoT LPWAN Network Architecture," *Sensors*, vol. 19, no. 3, 2019, doi: 10.3390/s19030675.
[27] M. Z. Chowdhury, M. Shahjalal, M. K. Hasan, and Y. M. Jang, "The Role of Optical Wireless Communication Technologies in 5G/6G and IoT Solutions: Prospects, Directions, and Challenges," *Appl. Sci.*, vol. 9, no. 20, p. 4367, Oct. 2019, doi: 10.3390/app9204367.
[28] S. Mukherjee and G. P. Biswas, "Networking for IoT and applications using existing communication technology," *Egypt. Informatics J.*, vol. 19, no. 2, pp. 107–127, 2018, doi: 10.1016/j.eij.2017.11.002.