

A Brief Study on Evolution of IoT Protocols and Applications

Balaiah Miska

Tata Communications Transformation Services Ltd. Pune, India

email: balaiah.miska@tatacommunications.com

Open Access Review Article

Received : 10/06/2024

Accepted : 21/08/2024

Published : 01/09/2024

Corresponding author email:

balaiah.miska@tatacommunications.com

Citation:

Balaiah M, "A Brief Study on Evolution of IoT Protocols and Applications," *Ci-STEM Journal of Digital Technologies and Expert Systems*, Vol. 1(2), pp. 57-65, 2024, doi: 10.55306/CJDTEs.2024.1201

Copyright:

©2024 Balaiah.M.

This is an open-access article distributed under the terms of the Creative Commons Attribution License which grants the right to use, distribute, and reproduce the material in any medium, provided that proper attribution is given to the original author and source, in accordance with the terms outlined by the license.

(<https://creativecommons.org/licenses/by/4.0/>).

Published By:

Ci-STEM Global Services Foundation, India.

Abstract:

By connecting things, the Internet of Things (IoT) is part of the next stage of the interconnected world, where different devices, platforms, and infrastructures can exchange data. With its diverse range of use cases, including but not limited to smart homes, industrial automation, healthcare, and environmental monitoring, IoT has emerged as a crucial element of contemporary technology landscapes. Thus, it first identifies the several significant aspects of IoT, the protocols of communication, and platforms, and finally assesses the applicability of IoT to numerous fields. But widespread adoption is facing several critical challenges, such as security issues, privacy concerns, interoperability issues, and scalability challenges. Advanced encryption, haltered frameworks and adaptive organization architecture can tackle these issues. In addition, emerging technologies like edge computing, AI-powered analytics and next-generation connectivity (e.g. 5G) are being utilized to reshape the capabilities of IoT. This paper summarizes the latest advancement achieved on IoT during the recent year and presents the empirical evidence on emerging trends, existing problems, and possible future work of IoT evolution.

Keywords: AI-driven analytics, Data exchange, Edge computing, Industrial automation, Interconnected world, Internet of Things (IoT), Smart homes, Security vulnerabilities.

1. INTRODUCTION

The Internet of Things is a new technological paradigm that connects networks of physical devices equipped with embedded software, sensors, and advanced communication technologies. It means that we can collect, analyze, and exchange information on the web seamlessly. But in doing so, it also leaves itself open to new avenues of automation and innovation across a myriad of industries. From healthcare to automotive systems, precision agriculture, industrial automation, and smart city projects [1], [2], the Internet of Things (IoT) is revolutionizing established processes and promoting data-driven decisions.

The increasing rate of AI and ML incorporation within the IoT sector has broadened IoT systems analytical capabilities enabling functions like predictive maintenance, real-time decision making and enriched user personalization [3]. In addition, the improvements to IoT by the advent of 5G networks and edge computing have nearly refined the latter as low latency and high data throughput are needed for real-time applications including autonomous vehicle and remote healthcare [4]. The adoption of blockchain has entered the IoT ecosystem to make the ecosystem secure and to authenticate [5].

While IoT can have a critical impact, there are also various challenges involved in IoT. With the enormous amounts of sensitive data transmitted over networks, the safety and privacy of data have become matters of serious concern [6].

Absence of standard protocols for communication gives rise to device interoperability problems and IoT network scalability in terms of sheer numbers as they scale exponentially [7]. Interdisciplinary collaboration and innovation in areas such as cybersecurity, protocol standardization, and energy-efficient system design are necessary to address these challenges.

This paper provides an extensive review of present-day IoT technologies. The content is targeted to be focused on basic elements such as sensors, communication protocols, and cloud infrastructures. The paper also elaborates upon the application domains of IoT and analyses the obstacles that hinder its developmental process. This paper tries to construct a deeper understanding of the technologies driving the evolution of IoT and their ability to transform industries worldwide through recent innovations and trends in IoT research.

2. KEY COMPONENTS OF IOT

IoT systems utilize various core elements, which have allowed the collecting, transmitting, and analysis of data for many applications. The elements include sensors, connectivity protocols, data platforms, and security mechanisms, and all of these have played their own role in IoT systems being so functional and efficient.

2.1. Sensors and Actuators

Sensors are devices that detect physical conditions such as temperature, humidity, light, and motion and convert them into digital signals for further processing [8]. Examples of sensors in IoT applications include temperature sensors in HVAC systems, motion sensors for security systems, and environmental sensors for smart agriculture. Recent advancements in sensor technology include nano-sensors and edge artificial intelligence, which make real-time analysis of data even better [9]. Such sensors can collect instantaneous data from the immediate physical environment surrounding them.

Actuators are devices that achieve specific tasks depending on the data they receive from sensors. For instance, an actuator may open a valve to control temperature in a process for industry or set the presets of a smart thermostat according to the conditions in the surrounding environment. Advancements in soft robotics and adaptive actuators enable modern IoT implementations to interact more intimately with the physical world [10]. Together, sensors and actuators allow continuous interaction between the physical world and IoT networks.

2.2. Connectivity Protocols

Connectivity is essential for enabling communication between devices and systems within IoT networks. Several protocols support IoT communication, each tailored to specific use cases.

Wi-Fi: It is commonly used at home and in the workplace as Wi-Fi allows high data transfer rates and is ideally suited for IoT applications that require substantial bandwidth, including smart home devices and wearable technology [11]. The availability of Wi-Fi 6, with its benefits like reduced latency and greater capacity, makes IoT connectivity even better [12].

Bluetooth Low Energy (BLE): BLE is optimized for low power consumption and short-range communication. It is being used in almost all health and fitness trackers, smartwatches, and home automation devices [13]. BLE 5.2 adds audio support at data link layer and enables mesh networking for all IoT applications [14].

Zigbee: Zigbee is a low energy consumption and short range dominated protocol that usually supports in IoT based devices, including smart lighting and security systems. This technology is suitable for applications where devices need to communicate over a local mesh network [15]. Recent developments include support for Matter, a unified protocol that enables cross-over between IoT ecosystems [16].

LoRaWAN (Long Range Wide Area Network): LoRaWAN is a long-range communication protocol for IoT devices transmitting tiny amounts of data. The authors provide a relevant technology to be applied in agriculture, environmental, and smart cities [17]. LoRaWAN has also extended the scope of its use cases by providing support for hybrid satellite-terrestrial networks [18].

5G technology can provide fast and low-latency communication, which makes it the main enabler of the Internet of Things (IoT) applications that require immediate data exchange (e.g., autonomous vehicles and remote surgical procedures) [19]. The emergence of 5G networks and the network slicing technique led to efficient IoT deployments [19].

IOT Protocols comparison:

It's hard to give a "best" table — the best protocol will vary widely depending on the particular use case for the IoT device. However, here's a breakdown against some of the major contenders, focusing on aspects relevant to a lot of projects:

Table 1: Comparison Table of IoT Protocols

Feature	MQTT	CoAP	HTTP	AMQP	Bluetooth LE	Zigbee	LoRaWAN
Typical Use Case	Sensor networks, industrial automation, mobile apps	Resource-constrained devices, simple sensor data	Web-connected devices, existing web infrastructure	Complex enterprise systems, financial transactions	Short-range communication, wearables, beacons	Home automation, mesh networks	Long-range, low-power wide area networks (LPWANs)
Transport Protocol	TCP	UDP (can use DTLS for security)	TCP	TCP	Bluetooth protocol stack	IEEE 802.15.4	LoRaWAN protocol stack
Messaging Model	Publish/Subscribe	Request/Response	Request/Response	Message queuing	Point-to-point, broadcast	Mesh networking	Star-of-stars
Message Size	Small to medium	Small	Large	Large	Small	Small	Very small
Overhead	Low	Very low	High	High	Low	Low	Very low
Power Consumption	Low	Very low	High	High	Very low	Low	Very low
Range	Depends on network (cellular, Wi-Fi, etc.)	Depends on network (cellular, Wi-Fi, etc.)	Depends on network (cellular, Wi-Fi, etc.)	Depends on network (cellular, Wi-Fi, etc.)	Short (up to 100m)	Short to medium (up to 100m)	Long (up to 10km)
Security	TLS/SSL	DTLS, Object Security	TLS/SSL	TLS/SSL	Encryption, authentication	Encryption, authentication	Encryption, authentication
Scalability	High	High	Moderate	High	Moderate	High	High
Complexity	Low	Very low	High	High	Low	Medium	Medium

Key Considerations When Choosing a Protocol

Resource-constrained Devices: Lightweight protocols like CoAP or MQTT are better suited to low memory, processing power, and battery life. Lossy or low-bandwidth networks are better served by lightweight protocols with minimal overhead and retry mechanisms (e.g. MQTT, LoRaWAN).

Transmission (Data Type And Frequency) Depending on the size and frequency of the data transmissions, different protocols can be selected. LoRaWAN is great for low throughput infrequent data packet transfers. For an often more giant stream of data, MQTT or even HTTP would probably be better suited. **Security Requirements:** Consider the sensitivity of the data being transmitted and choose a protocol with appropriate security mechanisms (encryption, authentication).

Existing Infrastructure: If you're integrating with existing web systems, HTTP might be the easiest option.

Range and Coverage: Bluetooth LE is suitable for short-range communication, while LoRaWAN is designed for long-range, wide-area coverage.

This table is not exhaustive. Many other IoT protocols exist, such as XMPP, DDS, and various proprietary protocols. Some protocols can be combined. For example, CoAP can be used over SMS for very constrained devices. The "best" protocol is highly context dependent. Carefully evaluate your specific requirements before making a decision.

2.3. Cloud Computing and Data Analytics

Cloud platforms are extremely central to IoT ecosystems, which enable scalable infrastructures used for data storage, processing, and analysis. The most recognizable of the existing cloud platforms that support the central management of tremendous amounts of data generated by the IoT devices are AWS, Microsoft Azure, and Google Cloud [20]. In integrating edge computing with cloud platforms, analytics can be done closer to the source location of the data, hence bringing down latency as well as reducing bandwidth use [21].

It is possible to draw actionable insights using the power of machine learning and artificial intelligence with IoT data. Techniques like federated learning help to do distributed data analysis without sacrificing any aspect of privacy [22]. It can analyze trends and patterns, thus helping organizations optimize their operations, predict equipment failures, and make decisions based on data [23].

2.4. IoT Platforms

IoT platforms enable the integration, management, and orchestration of devices and data across an IoT ecosystem. Some of the leading platforms include:

ThingSpeak:

An open-source platform that facilitates data collection and analysis in real time. It is now enhanced with built-in MATLAB analytics for IoT.

IBM Watson IoT:

A cloud-based platform designed for industrial IoT, offering device management, data analytics, and real-time insights. Recent developments include enhanced predictive maintenance capabilities through AI-driven insights.

Microsoft Azure IoT Hub:

A highly scalable platform that supports secure device connectivity and data analytics for IoT applications across industries. Its integration with Azure Digital Twins enables detailed modeling of physical environments.

Google Cloud IoT Core:

A platform that provides end-to-end IoT solutions, including secure device management and data processing capabilities. With BigQuery ML, it now supports integrated AI-driven analytics.

2.5. Security Mechanisms

IoT platforms integrate, manage, and orchestrate large numbers of devices and data streams across an IoT ecosystem. Examples include:

ThingSpeak: A free, open-source platform used for real-time data collection and analysis. Analytics for IoT is natively integrated with it.

IBM Watson IoT: A cloud-based industrial IoT platform that enables device management, data analytics, and real-time insights. The latest innovations include AI-driven predictive maintenance.

Microsoft Azure IoT Hub: A highly scalable framework that enables secure connectivity to devices and analyzes data for Internet of Things applications in every sector. As part of Azure Digital Twins, it enables extensive modeling of the physical environment.

Google Cloud IoT Core is an all-in-one platform offering full-fledged IoT solutions that encompass secure device management and data processing capabilities, along with new features of BigQuery ML that integrate AI-powered analytics.

3. APPLICATIONS OF IOT

Internet of Things (IoT) technologies range over a vast set of areas that enhance efficiency, create new business models, and improve life.

3.1. Smart Homes

Smart home technology connects all the devices from thermostats, lighting, to security systems through a network, which can be controlled from anywhere. All these devices improve comfort, reduce energy consumption, and enhance safety in homes for residents [24]. The latest trends include the use of artificial intelligence in streamlining energy consumption and achieving maximum automation. Devices such as smart speakers and voice assistants such as Amazon Alexa and Google Home have greatly impacted the smart home because they introduced natural language interfaces [25].

3.2. Healthcare

The use of IoT in healthcare systems allows distant monitoring and control of patient's health. Wearable technologies and medical devices monitor heart rate, blood glucose levels, and other similar metrics that communicate to the clinician for review [26]. The most advanced IoT-enabled medical devices nowadays contain artificial intelligence to ensure early diagnosis of diseases like diabetes and cardiovascular diseases [27]. The advent of remote patient monitoring technologies, such as smart inhalers and IoT-enabled insulin pumps, has significantly improved patient health outcomes [28].

3.3. Industrial IoT (IIoT)

Industrial IoT (IIoT) applies IoT technologies to monitor, control, and optimize industrial operations. Its uses include predictive maintenance, supply chain optimization, and real-time asset tracking, thus increasing efficiency and reducing operational costs [29]. It is through the integration of digital twins and edge computing that IIoT systems will provide support across industries for real-time simulations, decentralised decision-making in, among others, manufacturing and energy [30]. Moreover, IIoT-based autonomous robots and drones improve productivity in logistics and inventory management.

3.4. Smart Cities

IoT is at the core of smart cities. Here, sensors and devices are used to optimize urban operations in areas such as traffic management, waste collection, and energy use [31]. Among the latest innovations is smart parking, where drivers are directed to available parking spaces using IoT sensors. Other recent innovations include IoT-enabled streetlights, which automatically dim based on the level of pedestrian activity to minimize energy usage [32]. In addition, water quality monitoring systems and pollution sensors provide a sustainable way of urban living through real-time environmental data [33]. Also, the smart grid resulting from IoT technology enhances the reliability and effectiveness of energy supply by allowing dynamic demand-response.

3.5. Agriculture

IoT technology transformed the agricultural sector, especially in implementing precision farming techniques, which allows for the optimal use of inputs and crop yield maximization. IoT sensors in smart irrigation systems track soil moisture and weather conditions to ensure the right amount of water usage [34]. Livestock monitoring solutions with IoT devices monitor the health and behavior of animals to increase farm productivity. The latest innovations include IoT-enabled drones for crop monitoring and automated pest control, as well as blockchain for supply chain transparency [35].

3.6. Transportation and Logistics

IoT is transforming transportation and logistics through solutions such as fleet management systems, real-time tracking, and predictive maintenance [36]. Connected vehicles equipped with IoT sensors provide telemetry data to enhance driver safety and optimize fuel efficiency. IoT-enabled smart ports and warehouses streamline cargo handling and inventory management, reducing operational delays [37]. Autonomous vehicles and drone deliveries are also being realized through IoT integrations, revolutionizing last-mile delivery services.

4. CHALLENGES OF IOT

Despite its transformative potential, the Internet of Things (IoT) faces several challenges that impede its widespread adoption.

4.1. Interoperability

The IoT ecosystem is made up of a diverse range of devices, platforms, and communication protocols, many of which struggle to work together seamlessly. Achieving interoperability is a major hurdle for developers and necessitates the establishment of standardized protocols and interfaces [38]. New technologies, such as the Matter protocol and advancements in middleware frameworks, are being developed to tackle these challenges by facilitating smooth communication across various IoT ecosystems [39].

4.2. Security and Privacy

The sheer number of interconnected devices in IoT systems expands the potential attack surface, making them attractive targets for cyberattacks. Additionally, data privacy issues arise as sensitive information is shared between devices, often over unsecured networks [40]. Modern strategies like zero-trust architecture, blockchain-based security, and post-quantum cryptography are being implemented to reduce these risks [41]. Privacy-preserving machine learning methods, such as federated learning, also contribute to enhancing security without compromising user data [42].

4.3. Scalability

As IoT networks grow, it becomes increasingly challenging to ensure that systems can scale to accommodate a rising number of devices and larger data volumes. This necessitates a strong infrastructure and effective data management solutions [43]. Edge computing and distributed ledger technologies are emerging as crucial enablers for scalability by decentralizing data processing and lessening dependence on centralized cloud systems [44].

4.4. Energy Efficiency

Many IoT devices, especially those located in remote areas, depend on battery power. Therefore, designing energy-efficient devices and minimizing power consumption is essential for ensuring long operational lifespans [45].

4.5. Energy Efficiency

Many IoT devices, especially those used in remote areas, depend on battery power. It's essential to design energy-efficient devices and reduce power consumption to ensure they can operate for extended periods [46]. Recent advancements include energy-harvesting technologies like photovoltaic cells and kinetic energy converters, as well as low-power wide-area networks (LPWANs) such as LoRaWAN [47]. Furthermore, improvements in ultra-low-power processors and AI-driven power management systems significantly boost energy efficiency in IoT applications [48].

5. CONCLUSION

This web of connected devices, often referred to as the Internet of Things (IoT), is revolutionizing industries like never before while making our daily lives easier and more efficient. IoT systems harness the power of innovative sensors, robust communication methods, cloud and edge computation, and complex data analysis, resulting in incredible prospects in many fields. The IoT has unprecedented effects on the economy and society as it powers intelligent homes, streamlined industrial processes, and innovative healthcare interventions, as well as forward-looking solutions to urban management issues.

However, challenges such as security vulnerabilities, scalability problems, and interoperability gaps present significant obstacles. Addressing these challenges will require a holistic approach, including the creation of next-generation encryption techniques, standardized communication protocols, and AI-powered platforms to orchestrate complex IoT environments. Emerging technologies such as 6G communication, blockchain, and quantum computing will also be instrumental in addressing current constraints and enabling the future of the IoT to evolve.

Future Research and Application of IoT Will Focus on:

- **Energy Efficient Technologies:** Developing ultra-low-power devices and suitable energy harvesting technologies to enable sustainable operation of IoTs in remote areas where power resources are scarce.
- **Enhanced Security:** Development of zero-trust architectures, post-quantum cryptographic solutions, and decentralized identity management systems for safe and resilient IoT networks.
- **Device Interoperability:** Promoting universal standards and protocols, such as Matter and IPv6, to enable devices of all types to communicate and integrate with each other seamlessly.
- **Scalable Infrastructure:** Utilizing edge computing, fog computing, and advanced network slicing techniques to handle the increasing complexity and data demands of large-scale IoT implementations.

By focusing on these priorities, IoT systems can achieve greater sustainability and efficiency.

DECLARATIONS:

Acknowledgments	: Not applicable.
Conflict of Interest	: The author declares that there is no actual or potential conflict of interest about this article.
Consent to Publish	: The authors agree to publish the paper in the Global Research Journal of Social Sciences and Management.
Ethical Approval	: Not applicable.
Funding	: Author claims no funding was received.
Author Contribution	: Both the authors confirms their responsibility for the study, conception, design, data collection, and manuscript preparation.
Data Availability Statement	: The data presented in this study are available upon request from the corresponding author.

REFERENCES

1. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

2. P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–25, 2017, doi: 10.1155/2017/9324035.
3. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.
4. T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657–1681, Jul. 2017, doi: 10.1109/COMST.2017.2705720.
5. O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet Things J*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.
6. Y. I. Alzoubi, A. Al-Ahmad, and A. Jaradat, "Fog computing security and privacy issues, open challenges, and blockchain solution: An overview," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, p. 5081, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5081-5088.
7. J. SathishKumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues," *Int J Comput Appl*, vol. 90, no. 11, pp. 20–26, Mar. 2014, doi: 10.5120/15764-4454.
8. S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," in *2016 IEEE Smart Energy Grid Engineering (SEGE)*, IEEE, Aug. 2016, pp. 381–385. doi: 10.1109/SEGE.2016.7589556.
9. [V. Gupta and M. K. I. Rahmani, "IoT-based nano wireless sensor approach for detection of ships using mixed convolutional neural network approach," *Signal Image Video Process*, vol. 18, no. 11, pp. 8185–8194, Nov. 2024, doi: 10.1007/s11760-024-03460-2.
10. A. Salam, "IoT in Adaptive Control Systems," 2024, pp. 365–383. doi: 10.1007/978-3-031-62162-8_14.
11. I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, Aug. 2002, doi: 10.1109/MCOM.2002.1024422.
12. E. Mozaffariahrar, F. Theoleyre, and M. Menth, "A Survey of Wi-Fi 6: Technologies, Advances, and Challenges," *Future Internet*, vol. 14, no. 10, p. 293, Oct. 2022, doi: 10.3390/fi14100293.
13. M. Cäsar, T. Pawelke, J. Steffan, and G. Terhorst, "A survey on Bluetooth Low Energy security and privacy," *Computer Networks*, vol. 205, p. 108712, Mar. 2022, doi: 10.1016/j.comnet.2021.108712.
14. A. Barua, M. A. Al Alamin, Md. S. Hossain, and E. Hossain, "Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251–281, 2022, doi: 10.1109/OJCOMS.2022.3149732.
15. M. Kumar, V. Yadav, and S. P. Yadav, "Advance comprehensive analysis for Zigbee network-based IoT system security," *Discover Computing*, vol. 27, no. 1, p. 22, Jul. 2024, doi: 10.1007/s10791-024-09456-3.
16. D. Belli, P. Barsocchi, and F. Palumbo, "Connectivity Standards Alliance Matter: State of the art and opportunities," *Internet of Things*, vol. 25, p. 101005, Apr. 2024, doi: 10.1016/j.iot.2023.101005.
17. B. TORGÜL, L. Şağbanşua, and F. B. Balo, "Internet of Things: A Survey," *International Journal of Applied Mathematics, Electronics and Computers*, pp. 104–104, Dec. 2016, doi: 10.18100/ijamec.267197.
18. N. C. Almeida, R. P. Rolle, E. P. Godoy, P. Ferrari, and E. Sisinni, "Proposal of a Hybrid LoRa Mesh / LoRaWAN Network," in *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, IEEE, Jun. 2020, pp. 702–707. doi: 10.1109/MetroInd4.0IoT48571.2020.9138206.

19. T. Car, L. Pilepić Stifanich, and N. Kovačić, “The Role of 5G and IoT in Smart Cities,” *ENTRENOVA - ENTERprise REsearch INNOVAtion*, vol. 8, no. 1, pp. 377–389, Nov. 2022, doi: 10.54820/entrenova-2022-0032.
20. W. Zhang, M. Dong, K. Ota, J. Li, W. Yang, and J. Wu, “A Big Data Management Architecture for Standardized IoT Based on Smart Scalable SNMP,” in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, IEEE, Jun. 2020, pp. 1–7. doi: 10.1109/ICC40277.2020.9149368.
21. B. T. Hasan and A. K. Idrees, “Edge Computing for IoT,” in *Learning Techniques for the Internet of Things*, Cham: Springer Nature Switzerland, 2024, pp. 1–20. doi: 10.1007/978-3-031-50514-0_1.
22. D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, “Federated Learning for Internet of Things: A Comprehensive Survey,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, Feb. 2021, doi: 10.1109/COMST.2021.3075439.
23. S. Aiswarya, K. Ramesh, and S. Sasikumar S, “IoT based Big data Analytics in Healthcare: A Survey,” in *Proceedings of the FIST International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISSET 2020*, 16-17 May 2020, Chennai, India, EAI, 2021. doi: 10.4108/eai.16-5-2020.2304020.
24. M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, “A review of smart home applications based on Internet of Things,” *Journal of Network and Computer Applications*, vol. 97, pp. 48–65, Nov. 2017, doi: 10.1016/j.jnca.2017.08.017.
25. M. N. Varadarajan, V. C. R. N., and M. A., “Integration of AI and IoT for Smart Home Automation,” *International Journal of Electronics and Communication Engineering*, vol. 11, no. 5, pp. 37–43, May 2024, doi: 10.14445/23488549/IJECE-V11I5P104.
26. S. Abdulmalek et al., “IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review,” *Healthcare*, vol. 10, no. 10, p. 1993, Oct. 2022, doi: 10.3390/healthcare10101993.
27. S. Aiswarya, K. Ramesh, and S. Sasikumar S, “IoT based Big data Analytics in Healthcare: A Survey,” in *Proceedings of the FIST International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISSET 2020*, 16-17 May 2020, Chennai, India, EAI, 2021. doi: 10.4108/eai.16-5-2020.2304020.
28. L. A. Szolga and T. Blaga, “Smart Healthcare device based on IoT,” in *2023 International Electrical Engineering Congress (iEECON)*, IEEE, Mar. 2023, pp. 381–386. doi: 10.1109/iEECON56657.2023.10126823.
29. B. Sivathanu, “Adoption of Industrial IoT (IIoT) in Auto-Component Manufacturing SMEs in India,” in *Research Anthology on Small Business Strategies for Success and Survival*, IGI Global, 2021, pp. 719–746. doi: 10.4018/978-1-7998-9155-0.ch036.
30. S. Attaran, M. Attaran, and B. G. Celik, “Digital Twins and Industrial Internet of Things: Uncovering operational intelligence in industry 4.0,” *Decision Analytics Journal*, vol. 10, p. 100398, Mar. 2024, doi: 10.1016/j.dajour.2024.100398.
31. I. Rafiq, A. Mahmood, S. Razzaq, S. H. M. Jafri, and I. Aziz, “IoT applications and challenges in smart cities and services,” *The Journal of Engineering*, vol. 2023, no. 4, Apr. 2023, doi: 10.1049/tje2.12262.
32. A. Castiglione, J. G. Esposito, V. Loia, M. Nappi, C. Pero, and M. Polsinelli, “Integrating Post-Quantum Cryptography and Blockchain to Secure Low-Cost IoT Devices,” *IEEE Trans Industr Inform*, vol. 21, no. 2, pp. 1674–1683, Feb. 2025, doi: 10.1109/TII.2024.3485796.
33. T. Cunin, S. McGrath, and C. MacNamee, “Environmental monitoring based on Internet of Things Technology,” in *2018 12th International Conference on Sensing Technology (ICST)*, IEEE, Dec. 2018, pp. 31–34. doi: 10.1109/ICSensT.2018.8603658.
34. S. V. Gaikwad, A. D. Vibhute, K. V. Kale, and S. C. Mehrotra, “An innovative IoT based system for precision farming,” *Comput Electron Agric*, vol. 187, p. 106291, Aug. 2021, doi: 10.1016/j.compag.2021.106291.
35. S. Awan et al., “IoT with BlockChain: A Futuristic Approach in Agriculture and Food Supply Chain,” *Wirel Commun Mob Comput*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/5580179.

36. Y. Song, F. R. Yu, L. Zhou, X. Yang, and Z. He, "Applications of the Internet of Things (IoT) in Smart Logistics: A Comprehensive Survey," *IEEE Internet Things J*, vol. 8, no. 6, pp. 4250–4274, Mar. 2021, doi: 10.1109/JIOT.2020.3034385.
37. Y. Yang, M. Zhong, H. Yao, F. Yu, X. Fu, and O. Postolache, "Internet of things for smart ports: Technologies and challenges," *IEEE Instrum Meas Mag*, vol. 21, no. 1, pp. 34–43, Feb. 2018, doi: 10.1109/MIM.2018.8278808.
38. D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," *Wirel Pers Commun*, vol. 58, no. 1, pp. 49–69, May 2011, doi: 10.1007/s11277-011-0288-5.
39. R. K. Lomotey, J. Pry, S. Sriramoju, E. Kaku, and R. Deters, "Middleware Framework for IoT Services Integration," in *2017 IEEE International Conference on AI & Mobile Services (AIMS)*, IEEE, Jun. 2017, pp. 89–92. doi: 10.1109/AIMS.2017.20.
40. P. M. Chanal and M. S. Kakkasageri, "Security and Privacy in IoT: A Survey," *Wirel Pers Commun*, vol. 115, no. 2, pp. 1667–1693, Nov. 2020, doi: 10.1007/s11277-020-07649-9.
41. H. Omrany, K. M. Al-Obaidi, M. Hossain, N. A. M. Alduais, H. S. Al-Duais, and A. Ghaffarianhoseini, "IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction," *Discover Cities*, vol. 1, no. 1, p. 2, Mar. 2024, doi: 10.1007/s44327-024-00002-w.
42. R. Lazzarini, H. Tianfield, and V. Charissis, "Federated Learning for IoT Intrusion Detection," *AI*, vol. 4, no. 3, pp. 509–530, Jul. 2023, doi: 10.3390/ai4030028.
43. G. M. and N. Vijayaraj, "Increasing Scalability, Data Management, and Processing for Internet of Things Applications in Cloud-based IoT," in *2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL)*, IEEE, Mar. 2024, pp. 524–528. doi: 10.1109/ICSADL61749.2024.00091.
44. H. Xue, B. Huang, M. Qin, H. Zhou, and H. Yang, "Edge Computing for Internet of Things: A Survey," in *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, IEEE, Nov. 2020, pp. 755–760. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00130.
45. S. Zhao et al., "Understanding Energy Efficiency in IoT App Executions," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, IEEE, Jul. 2019, pp. 742–755. doi: 10.1109/ICDCS.2019.00079.
46. Z. Almudayni, B. Soh, H. Samra, and A. Li, "Energy Inefficiency in IoT Networks: Causes, Impact, and a Strategic Framework for Sustainable Optimisation," *Electronics (Basel)*, vol. 14, no. 1, p. 159, Jan. 2025, doi: 10.3390/electronics14010159.
47. J. Dela Flora da Silveira, A. F. Da S. Veloso, J. V. dos Reis Junior, and V. Uchôa Oliveira, "Performance Study of LoRa WAN, LoRaMesh, and Hybrid Networks for a Smart Farming Scenario," in *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/WF-IoT58464.2023.10539497.
48. M. N. Al-Rawahi, T. Sharma, and P. Palanisamy, "Internet of nanothings: Challenges & opportunities," in *2018 Majan International Conference (MIC)*, IEEE, Mar. 2018, pp. 1–5. doi: 10.1109/MINTC.2018.8363165.