Volume (1) No (10), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Internet of Things (IoT) Systems: A Survey of Platforms, Protocols, and Application Frameworks

Dr. Bal Krishna Sharma
Professor, Mandsaur University, Mandsaur
Department of Computer Sciences and Applications
bksharma7426@gmail.com

***Abstract*—A new paradigm in information and communication technology, the Internet of Things (IoT) allows for the interconnection of previously siloed systems in many different fields, including transportation, healthcare, industry, and even the environment. Despite its potential, IoT development faces significant challenges, including architectural heterogeneity, interoperability constraints, data management complexity, and security vulnerabilities. This survey presents a structured overview of IoT architectures, focusing on layered system models that incorporate edge, fog, and cloud computing to optimize scalability, energy efficiency, and Quality of Service (QoS). It examines communication protocols and IoT platforms, emphasizing their role in achieving device interoperability and robust data exchange. Middleware and application frameworks are highlighted as critical enablers, bridging device-level interactions with application-layer functionalities while ensuring data processing, security, and privacy. A comprehensive literature review synthesizes recent advancements in IoT middleware design, platform evaluation, multi-protocol integration, and lightweight cryptography, identifying prevailing gaps such as the absence of standardized frameworks and persistent security concerns. The survey underscores the necessity for unified middleware standards, standardized platform evaluation methodologies, and resource-efficient security mechanisms. Future research directions include real-world implementation of sustainable architectures, enhanced protocol flexibility, and advanced privacy-preserving solutions to enable resilient, scalable, and secure IoT ecosystems.**

***Keywords*—Internet of Things (IoT), IoT Architecture, IoT Platforms, Middleware, LPWAN, Communication Protocols, Advantages of IoT, Sigfox, Z-wave.**

I. INTRODUCTION

In an increasingly connected world, the need for intelligent, automated, and responsive systems has become essential to manage complex processes, optimize resource utilization, and enhance decision-making. The Internet of Things (IoT) responds to such requirements and provides an opportunity to connect devices, environments, and users in any industry and society-related practice in a matter-of-course way.

Devices, sensors, and smart systems have created a new paradigm resulting in the Internet of Things (IoT), where the digital and real worlds come together [1]. It also allows distribution of data, its processing, and communication in real-time across infrastructures [2]. The number of use cases of IoT applications are growing in various fields including healthcare, manufacturing, agriculture, and city management, which results in a growing emphasis on frameworks and approaches that facilitate high abstraction levels of systems, interoperability, extreme flexibility, and easy connection of devices. The strategies are designed to address the increasing complexity associated with IoT implementation, while also providing organized support for managing related devices and services.

The architectural design has a significant impact on the structure of the IoT systems and its operation. The three dominant parts of an Internet of Things (IoT) design include, the sensing or hardware layer that establishes data to real devices, the software control layer that comes in to work the information and inject context into it, and the application layer which facilitates domain-specific services, and User interface [3]. All these layers are required to make IoT systems reliable, responsive, and scalable. Raw input is offered to the sensor layer; the decision-making is performed by the control layer and the end-users as well as other systems receive functional output through the application layer.

The platform that will be used to implement an Internet of Things (IoT) has an influence on the flexibility, speed, and scalability of an Internet of Things (IoT) system. Developers should decide whether to work with existing platforms that can provide all the necessary tools and a community or design a new platform that would suit particular needs. This choice usually depends on the availability of existing methods in meeting technical and functional challenges of the planned application. Where some special functionality is needed or a requirement over domain-specific constraints [4]. Specialised platforms are created to maximise performance and overcome weaknesses of general-purpose ones.

A communication protocol is the key to establishing data transmission and providing reliability in communication between devices in the IoT-type networks on heterogeneous platforms [5]. They are followed in multiple layers of OSI or TCP/IP model and they come with technologies like MQTT, CoAP, and HTTP among others [6]. Protocols describe the way data is formatted, delivered and received, and in this way paired devices with differing capabilities can communicate in a reliable and efficient way. They are particularly important in managing limited resources, facilitating low-latency communication, and ensuring the secure transfer of data.

Application frameworks in Internet of Things (IoT) applications provide standardised interfaces, development tools, and components for reusing in system development and deployment. They decrease the overhead of dealing with heterogeneous computer hardware[7], distributed computing

platforms and high-volume data transfers. Through abstraction and modularization, these frameworks support application design, implementation, testing, and deployment. A comparative analysis of existing frameworks provides valuable insights into their capabilities, limitations, and suitability for different application scenarios, ultimately guiding the selection of appropriate solutions for high-quality IoT system development.

A. Structured of the paper

The paper is organized as follows: Section II introduces the IoT architecture and system model. Section III covers communication protocols and IoT platforms. Section IV discusses middleware and application frameworks. Section V highlights key contributions from existing literature. The paper is concluded and future work is outlined in Section VI.

II. Internet Of Things (IoT) Architecture And System Model

The IoT is designed to facilitate the seamless acquisition, transmission, processing, and deployment of services through its perception, network, middleware, and application layers, which interoperable models back [8]. Various IoT models operate across applications like transport, security, facility, and medical management. Without communication between these models [9], manual intervention would be required for both routine and critical decisions.

A. Internet of things (IoT) Architecture

The absence of a single IoT standard has led to diverse, hard-to-integrate technologies. Standards bodies like IEEE, ITU-T, and oneM2M provide specifications, while industrial IoT uses OPC UA and IIoT consortium standards[10]. In Figure 1, the present IoT design is made up of three layers: the perception layer, the network layer, and the application layer. Earlier IoT designs ranged from simple three-layer models to complex multi-layer and abstract reference designs.

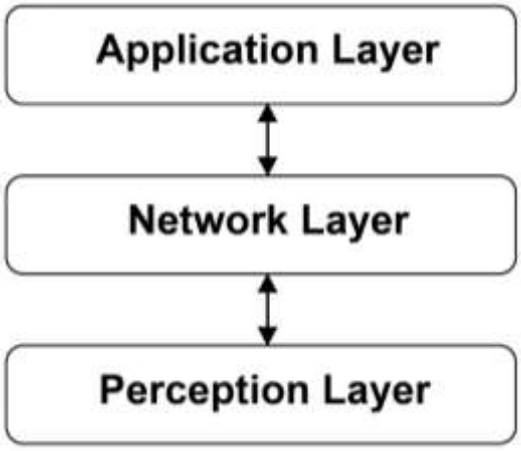

Fig. 1. IoT architecture

- **Perception Layer:** It is the physical layer in the IoT, on which the smart objects that have the computing capacities and sensors gather and analyze the information about the environment[11]. These devices are as basic as a smartphone and as complicated as a special sensor, and are the foundation of the systems of IoT.
- **Network Layer:** IoT networks allow communication between IoT devices and guarantee a secure data transfer. It presents such protocols as Wi-Fi, cellular, Bluetooth, and Zigbee, all compatible with different requirements[12]. The layer plays an important role in connectivity, data exchange and service delivery within IoT systems.
- **Application Layer**: The application layer is in charge of all Internet of Things apps and serves users over their needs [13]. It receives information at lower levels to facilitate such areas as smart homes, healthcare, and industrial automation.

B. System Elements of IoT architecture

IoT architecture consists of data-generating devices, intermediate nodes, and computing infrastructure, enabling data collection, transmission, and processing. Together, they form the core of IoT, ensuring efficient communication, scalability, and smart decision-making across various application environments, key elements include:

- **Data-generating devices:** IoT components referred to as data-generating devices include sensors and actuators[14] that scans real-time data of the physical world to provide it with further processing.
- **Intermediate nodes:** The intermediate nodes accept and pre-process data between the sensing devices and the computing infrastructure[15] facilitating effective communication within the IoT systems.
- **Computing infrastructure:** IoT data can be processed, stored, and analyzed through a computing infrastructure[16], empowering the notion of making rational decisions and service provision.

C. Advantages of IoT systems

Everyday life is improved in several ways by the Internet of Things.

- **Minimizing the human effort:** The interconnection and communication capabilities of IoT devices allow for the automation of formerly manual processes, which in turn allows us to enhance the standard of corporate services while decreasing the amount of time and effort required from humans.
- **Save time:** The time it saves is directly proportional to the amount of work it decreases, as we've already noted. A major benefit of an IoT platform is the time it saves.
- **Improved security:** The IoT is a network of interconnected devices that can improve security and personal safety by allowing smarter control of homes and communities through mobile phones [17].
- **Efficient resource utilization:** Increased and monitored resource utilization is made possible by the Internet of Things (IoT), which gains insight into device performance and operation.
- **Useful in the healthcare industry:** Direct, real-time patient treatment is superior to waiting for an appointment with a doctor. This empowers us to make decisions and deliver care based on solid facts.
- **Use in traffic systems:** The IoT enables efficient tracking, which in turn allows for more cost-effective delivery, asset[18], traffic, surveillance, transportation, individual order, inventory control, and customer management.

III. Communication Protocols And Internet Of Things Platforms

The IoT communication protocols are a collection of rules and guidelines for safely exchanging data between devices that are part of the network. While protocols encrypt the data being transmitted[19], platforms ensure their compatibility with other information. The IoT platform plays a crucial role in delivering business value by linking IoT endpoints with applications and analytics. It serves as the core of an IoT solution[20], enabling the data collected from devices to be processed and effectively utilized by end users.

A. Roles of IoT Platforms

The IoT platforms are at the core of the IoT system, which ensures connectivity, processing, and integration of devices, and coordination of services. They provide the foundational tools and interfaces, sourced from open or closed platforms, enabling secure, scalable, and efficient communication between devices, users, and enterprise systems. The platforms also condone important operations such as device management, data analytics[21], and system interoperability to facilitate the applications and development of IoT systems within organizations. There are two major types of IoT platforms, which are as follows:

1) Closed Source Platform:

Major IT companies have developed IoT platforms as extensions of their cloud services, typically offered as SaaS or PaaS. Ericsson's IoT Accelerator, based on the PaaS model, targets business partners by offering connectivity, security, APIs, and user management[22]. It supports REST, AMQP, CoAP, and LWM2M protocols and integrates with enterprise IT systems via service buses.

2) Open-Source Platform:

Open-source IoT platforms are fewer than closed-source ones, but several notable options exist. For a deeper comparison, the analysis extended beyond official documentation and surveys to include source code review and local installation on a Linux system. This enabled the assessment of additional aspects unique to open-source platforms [23], such as installation procedures and documentation quality. Table I compares the closed-source platform and the open-source platform.

TABLE I. Comparison of Closed-Source and Open-Source IoT Platforms

Aspect	Closed Source	Open Source
Ownership	Proprietary (e.g., Ericsson)	Community or organization-driven
Deployment	SaaS/PaaS	Self-hosted
Customization	Limited	Highly flexible
Protocol Support	REST, AMQP, CoAP, LWM2M	Varies; generally adaptable
Integration	Enterprise-ready via service buses	May require manual setup
Source Access	Not available	Fully accessible
Evaluation	Feature-based	Code review and real installation
Support	Vendor-backed	Community-based

B. IoT Communication Protocols

Each communication protocol is elaborated upon in full here [24]. Two prevalent categories of IoT communication protocols are long-range wide-area networks (LPWAN) and short-range networks (SRN), as seen in Figure 2.

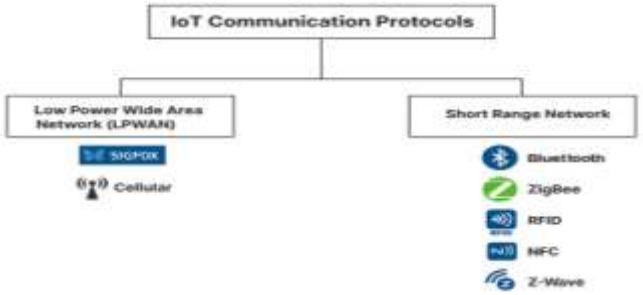

Fig. 2. IoT communication protocols

1) Low Power Wide Area Network (LPWAN)

LPWAN allows a long-range communication solution over a network with a low-power interface and with limited bandwidth, and is best suited to IoT environments. In this section[25]some important technologies, such as SigFox and cellular LPWANs and their maturity and present challenges are briefly discussed.

- **SigFox:** As an LPWAN (low-power wide-area network) that does not have a cutoff, Sigfox can be used for sparse Internet of Things (IoT) tasks, snap purchases [26], scrByteArray monitoring, and other similar applications.
- **Cellular:** Cellular networks support IoT, but they were designed for high-power devices[27]. New releases are more suitable for IoT demands.

2) Short Range Network

The IoT model is an essential element of connectivity, allowing the communication of smart objects and the provision of services with optimized use of low-power networks[28]. Important protocols are 6LoWPAN, Zigbee, Bluetooth, NFC, RFID and Z-Wave, each of which has its applicability.

- **6LoWPAN:** Designed for low-data Internet of Things applications, the 6LoWPAN protocol enables low-cost and low-power IPv6 communications using the IEEE 802.15.4 [29] standard.
- **Bluetooth Low Energy: The** Bluetooth SIG added to Bluetooth 4.0, BLE[30], provides a low-power communication protocol for IoT devices.
- **ZigBee:** ZigBee is an IoT protocol with a maximum range of 200 m[31] with increased security, that is, two times the range of Bluetooth.
- **Z-Wave:** Z-Wave is a wireless system for home automation that uses a dedicated radio frequency to avoid interference [32].
- **Radio Frequency Identification:** It is some kind of automatic identification system as it involves radio waves to track and capture items or data [33].
- **Near-Field Communication:** Near-Field Communication (NFC) is a form of short-range wireless communication that transmits data between proximate devices by employing radio frequency identification (RFID) principles.

IV. Internet Of Things (IoT) Middleware And Application Frameworks

Transport and logistics, healthcare, retail and supply chain, industry, and the environment are just a few of the many areas that have benefited from the development and implementation of Internet of Things applications. Even though they are everywhere, creating apps for the Internet of Things is still

difficult and takes a lot of time. Reason being, it necessitates handling a number of interconnected problems, such as inadequate stakeholder roles identification and an absence of suitable frameworks to handle the heterogeneity present in IoT systems on a big scale [34]. Striking good programming abstractions across many technological levels, from device software to middleware services and end-user apps, is another big obstacle. The development time and resources needed to overcome these challenges cause a delay in the implementation of IoT applications.

A. Role of Middleware

Managing data volumes is an integral part of IoT middleware, as trillions of objects generate and exchange hundreds of exabytes of data, leading to an "Exaflood" or "Data deluge." Novel methods are needed to find, fetch, and transfer data, with challenges in querying, indexing, process modelling, and transaction handling. Data may include identification, positional, environmental, historical, and descriptive information [35]. The purpose of middleware is to facilitate and coordinate cooperative processing by providing a software layer between application, operating system, and network communication layers. Middleware in the IoT should accommodate both viewpoints due to the great variety of communication and system-level technologies [36]. Key middleware and framework solutions are as follows.

B. Key Middleware and Framework Solutions

Middleware and framework solutions play a prominent role in IoT by serving as mediators between devices and data. They enable the development of scalable and efficient IoT systems by providing support (interoperability, data processing, security and application support) in the essential services. Key applications of Middleware and framework solutions are followed as:

- **EdgeX Foundry:** EdgeX Foundry is a microservices-based platform that aims to simplify edge application development by supporting container orchestrations, such as modern container orchestration[37], that of Kubernetes for scalable, fault-tolerant and efficient edge gateway deployment.
- **FIWARE:** FIWARE, which the European Commission has sponsored over the last several years, has been developed via multiple projects to develop and operate real-life pilots[38]. It is currently moving towards business-ready deployment.
- **Open IoT:** The OpenIoT ontology integrates sensors and the semantic web by adding IoT/cloud integration concepts[39] to existing sensor vocabularies concepts (units, raw values, and spatial points of interest).
- **AllJoyn:** An open-source software system, the AllJoyn framework facilitates the execution of applications [40] (apps) across a variety of device types.
- **IoTivity:** IoTivity is an open-source framework that allows safe access and communication between and among a variety of IoT devices and systems.

V. Literature Review

This literature review section presents a comprehensive overview of recent advancements in IoT integration, platform evaluation, architecture, and security. It synthesizes diverse methodologies and findings, identifies key challenges, and outlines future research directions across multiple application domains and sectors.

Meyo *et al.* (2025) propose a Sensors in IoT systems are vital when it comes to collecting data across various applications automatically. However, there is no standardized software architecture for collecting and processing data from IoT sensors, while also being able to aggregate other data sources. This is particularly evident in the context of managing asynchronous operations and streaming data, which are common in sensor-based systems. To address these issues, this paper proposes PD-MidI, a design pattern-based IoT middleware architecture that provides not only essential data collection, processing, and aggregation capabilities, but also incorporates comprehensive security, privacy, and anonymization features[41].

Fereira (2024) emphasizes that the IoT continues to expand and increasingly integrate into day-to-day life, supporting multiple applications ranging from smart homes and smart cities to autonomous vehicles and healthcare. Developing a sustainable IoT architecture to accommodate advanced applications presents a global challenge. A layered IoT architecture, encompassing edge, fog, and cloud layers, offers a viable solution to support these varied IoT applications. The frameworks have implemented ensure not only energy efficiency but also adherence to the network and application-specific QoS requirements. The proposed frameworks implemented in an event-driven simulation environment to validate their effectiveness in real-time network applications[42].

Rakshe and Dongre (2024) proposed that the Internet of Things (IoT) represents a network of distinct objects with embedded software for exchanging transient states and data, essential for activating actuators. To interact with a cloud conducting big data analytics and supporting business decisions, edge networking devices and protocols are integral. It is very significant to ensure data privacy, trust management, authentication and authorization in a heterogeneous environment. Addressing the vulnerabilities at edge and cloud service providers' sites is are critical aspect to be addressed, which extensively details security breaches and the protective mechanisms offered by IoT protocols[43].

Barros and Teixeira (2023) propose a Comparing IoT platforms has always been a challenge, for both academia and industry, due to the large number of platforms that exist and their huge heterogeneity. To address this problem, this work presents a precise methodology to define the common requirements that should be present in any IoT platform. After defining these requirements, a detailed survey is carried out among 32 specialists to prioritize these requirements, identifying which of them are essential. As a result, among a set of 64 mapped requirements, 26 are discussed regarding their relevance[44].

Fan *et al.* (2023) suggested that as the IoT sector grows, so does the variety of IoT devices and the protocols used to communicate with them. The diversity of IoT devices makes it more challenging and time-consuming to build a fully integrated IoT platform for real-world Internet of Things deployment implementation. Additionally, maintaining a consistently available platform has become increasingly difficult due to the proliferation of connected devices. developed and deployed an IoT platform multi-protocol access technique that addresses the present platform's

limitations in device access by allowing users to tailor the configuration of public and private protocols to specific purposes [45].

Garah, Mbarek, and Kirgizov (2022) note that the projected IoT data confidentiality is quickly becoming a key issue, causing users to have numerous worries. An often-used strategy for protecting sensitive information from prying eyes is the use of cryptographic techniques. To adapt and match the IoT device constraints of computing power and storage capacity, lightweight cryptographic algorithms have been designed to offer a scaled version of protection. It follows the traditional encryption modes that are energy and time consuming and utilise much CPU and memory [46].

Table 2 below summarizes recent literature dealing with the issue of integration of the Internet of Things, architecture, platforms, and security, feature major approaches and results, in addition to major obstacles and perspectives on further research in the different areas.

TABLE II. SUMMARY OF RECENT RESEARCH STUDIES ON IOT INTEGRATION, PLATFORMS, ARCHITECTURE, AND SECURITY

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Meyo et al., (2025)	IoT sensor data middleware	Design of PD-MidI architecture with security & anonymization	Handles asynchronous, streaming data efficiently	Lack of standardized software architecture	Develop unified middleware standards with built-in privacy features
Fereira, (2024)	Layered IoT architecture	Event-driven simulation of edge-fog-cloud models	Achieves energy efficiency and meets QoS needs	Sustainable architecture for advanced applications	Implement and optimize real-world use cases with simulation frameworks
Rakshe and Dongre, (2024)	IoT security in edge-cloud integration	Analysis of protocols and security mechanisms	Emphasizes the need for privacy, trust, and authentication in hybrid environments	Edge and cloud vulnerabilities	Strengthen protocol-level security and privacy-preserving techniques
Barros and Teixeira, (2023)	IoT platform comparison	Survey of 32 experts; identification of 64 requirements	26 essential requirements prioritized for platform design	Platform heterogeneity and lack of standard comparison metrics	Establish standardized IoT platform evaluation frameworks
Fan et al., (2023)	Protocol access in IoT platforms	Multi-protocol access method with public/private configuration	Addresses device heterogeneity, improves platform availability	Complex deployment and integration	Enhance flexibility and compatibility of access protocols
Garah, Mbarek and Kirgizov, (2022)	IoT data confidentiality	Use of lightweight cryptographic algorithms	Lightweight crypto ensures confidentiality with less resource usage	Traditional encryption is resource-heavy	Develop more efficient cryptographic methods for constrained devices

VI. CONCLUSION AND FUTURE WORK

The IoT has emerged as a technological game changer with the potential to bring intelligent decision-making, automation, and seamless data flow in numerous fields. Through this survey, the authors have analyzed the present situation in terms of IoT systems based on architectures, communication protocols, platforms, and middleware frameworks to provide an integrated picture in terms of what it can do and how they depend on each other. It was revealed that IoT architectures tend to adopt layered models, such as perception, network and application layers, to support ordered communication among devices, yet protocols and platforms are crucial when it comes to interoperability, scalability and integration of heterogeneous systems. Middleware frameworks such as EdgeX Foundry, FIWARE, OpenIoT, AllJoyn, and IoTivity are crucial for managing data flow in large systems, coordinating distributed resources, and adapting to diverse application requirements. Literature synthesis pointed to the progress in multi-protocol access mechanisms, standardised manner of platform evaluation and lightweight cryptography but challenges still prevail such as platform heterogeneity, absence of unified standard and the necessity of resource-efficient security solutions. The discussion highlights the importance of developing standardized evaluations and frameworks, as well as adaptive multi-protocol middleware, AI-based analytics, and energy-efficient structures.

Future work on cross-domain interoperability, dynamic resource allocation planning, and strategies, as well as advanced privacy-preserving mechanisms, should be carried out to provide resilient, scalable, sustainable IoT implementation in complex, evolving environments.

REFERENCES

[1] K. Seetharaman and M. Reddiar, "Internet of Things (IoT) Applications in SAP: A Survey of Trends, Challenges, and Opportunities," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 2, pp. 499–508, Mar. 2021, doi: 10.48175/ijarsct-6268b.

[2] C. Paniagua and J. Delsing, "Industrial Frameworks for Internet of Things: A Survey," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1149–1159, 2021, doi: 10.1109/JSYST.2020.2993323.

[3] M. M. Rahaman, "A Review on Internet of Things-IoT-Architecture , Technologies , Future Applications & Challenges," *Int. J. Sci. Bus.*, vol. 14, no. 1, pp. 80–92, 2022, doi: 10.5281/zenodo.7066810.

[4] L. De Nardis, A. Mohammadpour, G. Caso, U. Ali, and M.-G. Di Benedetto, "Internet of Things Platforms for Academic Research and Development: A Critical Review," *Appl. Sci.*, vol. 12, no. 4, p. 2172, Feb. 2022, doi: 10.3390/app12042172.

[5] D. D. Rao, "Systematic Analysis of threats, Machine Learning solutions and Challenges for Securing IoT environment," *J. Cybersecurity Inf. Manag.*, vol. 14, no. 2, pp. 367–382, 2024.

[6] A. Serianni and F. De Rango, "Application Layer Protocols for Internet of Things," *Lect. Notes Networks Syst.*, vol. 289, no. March, pp. 535–558, 2022, doi: 10.1007/978-3-030-87049-2_18.

[7] I. S. Udoh and G. Kotonya, "Developing IoT applications: challenges and frameworks," *IET Cyber-Physical Syst. Theory Appl.*, vol. 3, no. 2, pp. 65–72, 2018, doi: 10.1049/iet-cps.2017.0068.

[8] A. Q. Gill, V. Behbood, R. Ramadan-Jradi, and G. Beydoun, "IoT architectural concerns," in *Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing*, New York, NY, USA: ACM, Mar. 2017, pp. 1–9. doi: 10.1145/3018896.3025166.

[9] M. S. Pangtey and V. Gupta, "A Review of IoT Models," *CEUR Workshop Proc.*, vol. 3058, pp. 0–7, 2021.

[10] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, "An overview of IoT architectures, technologies, and existing open-source projects," *Internet of Things*, vol. 20, Nov. 2022, doi: 10.1016/j.iot.2022.100626.

[11] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," *Inf.*, vol. 12, no. 2, pp. 1–21, 2021, doi: 10.3390/info12020087.

[12] Aggarwal, "Cross-layer design in the Internet of Things (IoT) issues and possible solutions," *Researchgate.Net*, pp. 1–13, 2021, [Online]. Available: https://www.researchgate.net/publication/370400212_Cross-layer_design_in_the_Internet_of_Things_IoT_issues_and_possible_solutions

[13] N. Lata and R. Kumar, "Internet of Things: A Review of Architecture and Protocols," *2020 Int. Conf. Decis. Aid Sci. Appl. DASA 2020*, pp. 1027–1031, 2020, doi: 10.1109/DASA51403.2020.9317091.

[14] S. Mondal, P. P. Jayaraman, P. Delir Haghighi, A. Hassani, and D. Georgakopoulos, "Situation-Aware IoT Data Generation towards Performance Evaluation of IoT Middleware Platforms," *Sensors*, vol. 23, no. 1, pp. 1–7, Dec. 2022, doi: 10.3390/s23010007.

[15] A. Amjad, F. Azam, M. W. Anwar, and W. H. Butt, "A Systematic Review on the Data Interoperability of Application Layer Protocols in Industrial IoT," 2021. doi: 10.1109/ACCESS.2021.3094763.

[16] T. Kim, S. Yoo, and Y. Kim, "Edge/Fog Computing Technologies for IoT Infrastructure," *Sensors*, vol. 21, no. 9, p. 3001, Apr. 2021, doi: 10.3390/s21093001.

[17] H. S. Chandu, "A Review Of Iot-Based Home Security Solutions : Focusing On Arduino Applications," *TIJER*, vol. 11, no. 10, pp. a391–a396, 2024.

[18] Parteek, "A Review Paper on IOT Advantages and Disadvantages Parteek," *Int. J. Res. Anal. Rev.*, vol. 6, no. 1, pp. 441–443, 2019, [Online]. Available: http://ijrar.com/

[19] M. Jamuna and A. M. V. Prakash, "A Study of Communication Protocols for Internet of Things (IoT) Devices: Review," in *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, 2021, pp. 262–268. doi: 10.2991/ahis.k.210913.033.

[20] C. Macgillivray, "The Platform of Platforms in the Internet of Things," *Idc*, vol. February, no. February, pp. 32–46, 2016.

[21] M. Fahmideh and D. Zowghi, "An exploration of IoT platform development," 2020. doi: 10.1016/j.is.2019.06.005.

[22] A. Al-Sakran, M. H. Qutqut, F. Almasalha, H. S. Hassanein, and M. Hijjawi, "An Overview of the Internet of Things Closed Source Operating Systems," in *2018 14th International Wireless Communications and Mobile Computing Conference, IWCMC 2018*, 2018. doi: 10.1109/IWCMC.2018.8450314.

[23] A. Martikkala, J. David, A. Lobov, M. Lanz, and I. F. Ituarte, "Trends for low-cost and open-source IoT solutions development for industry 4.0," in *Procedia Manufacturing*, 2021. doi: 10.1016/j.promfg.2021.10.042.

[24] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *ICIT 2017 - 8th International Conference on Information Technology, Proceedings*, 2017. doi: 10.1109/ICITECH.2017.8079928.

[25] A. J. Onumanyi, A. M. Abu-Mahfouz, and G. P. Hancke, "Low power wide area network, cognitive radio and the internet of things: Potentials for integration," 2020. doi: 10.3390/s20236837.

[26] A. A. F. Purnama and M. I. Nashiruddin, "Sigfox-based internet of things network planning for advanced metering infrastructure services in urban scenario," in *Proceedings - 2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology, IAICT 2020*, 2020. doi: 10.1109/IAICT50021.2020.9172022.

[27] J. Zakaria, J. Kundu, and H. Rza, "A Review paper on The Internet of Things (IoT) & Its Modern Application," *AIP Conf. Proc.*, vol. 2851, no. 1, pp. 4–9, 2023, doi: 10.1063/5.0178765.

[28] A. A. Bahashwan, M. Anbar, N. Abdullah, T. Al-Hadhrami, and S. M. Hanshi, "Review on Common IoT Communication Technologies for Both Long-Range Network (LPWAN) and Short-Range Network," in *Advances in Intelligent Systems and Computing*, 2021. doi: 10.1007/978-981-15-6048-4_30.

[29] G. K. Ee, C. K. Ng, N. K. Noordin, and B. M. Ali, "A Review of 6LoWPAN Routing Protocols," *Proc. Asia-Pacific Adv. Netw.*, vol. 30, p. 71, 2010, doi: 10.7125/apan.30.11.

[30] D. Rani and N. S. Gill, "Review of various IoT standards and communication protocols," *Int. J. Eng. Res. Technol.*, vol. 12, no. 5, pp. 647–657, 2019.

[31] A. Zohourian *et al.*, "IoT Zigbee device security: A comprehensive review," 2023. doi: 10.1016/j.iot.2023.100791.

[32] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," 2023. doi: 10.1016/j.iotcps.2022.12.003.

[33] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings*, 2012. doi: 10.1109/CECNet.2012.6201508.

[34] A. Goyal, "Integrating IoT and Agile Methodologies for Smarter Engineering Solutions," *Int. J. Sci. Res. Arch.*, vol. 8, no. 2, pp. 754–766, Apr. 2023, doi: 10.30574/ijsra.2023.8.2.0284.

[35] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for Internet of things," in *Communications in Computer and Information Science*, 2011, pp. 288–296. doi: 10.1007/978-3-642-21937-5_27.

[36] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Cla, "Middleware for internet of things: A survey," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 70–95, 2016, doi: 10.1109/JIOT.2015.2498900.

[37] A. Dhulfiqar, M. A. Abdala, N. Pataki, and M. Tejfel, "Deploying a web service application on the EdgeX open edge server: An evaluation of its viability for IoT services," *Procedia Comput. Sci.*, vol. 235, pp. 852–862, 2024, doi: 10.1016/j.procs.2024.04.081.

[38] F. Cirillo, G. Solmaz, E. L. Berz, M. Bauer, B. Cheng, and E. Kovacs, "A Standard-Based Open Source IoT Platform: FIWARE," *IEEE Internet Things Mag.*, 2020, doi: 10.1109/iotm.0001.1800022.

[39] J. Soldatos *et al.*, "OpenIoT: Open source internet-of-things in the cloud," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015. doi: 10.1007/978-3-319-16546-2_3.

[40] O. Tomanek and L. Kencl, "Security and privacy of using AllJoyn IoT framework at home and beyond," in *Proceedings of the 2nd International Conference on Intelligent Green Building and Smart Grid, IGBSG 2016*, 2016. doi: 10.1109/IGBSG.2016.7539413.

[41] Z. Meyo, G. C. Ullmann, R. D. Makwana, and O. Gavaldà, "A Pattern-Driven Middleware Architecture for IoT Data," in *2025 IEEE/ACM 7th International Workshop on Software Engineering Research & Practices for the IoT (SERP4IoT)*, IEEE, Apr. 2025, pp. 32–39. doi: 10.1109/SERP4IoT66600.2025.00010.

[42] R. Fereira, "A Communication and Computation Converged Framework for Sustainable IoT Applications," in *2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, IEEE, Mar. 2024, pp. 366–367. doi: 10.1109/PerComWorkshops59983.2024.10503117.

[43] A. Rakshe and N. Dongre, "Survey on Security Protocols for IoT," in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, IEEE, Apr. 2024, pp. 1–5. doi: 10.1109/I2CT61223.2024.10544115.

[44] T. G. F. Barros and E. S. Teixeira, "Common Requirements for IoT Platforms," in *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, IEEE, Oct. 2023, pp. 1–8. doi: 10.1109/WF-IoT58464.2023.10539561.

[45] X. J. Fan, Z. Q. Huang, S. J. Huo, and X. B. Zhang, "Research on Multi-protocol Access Method for IoT Platform Based on Microservice Container Scheduling," in *2023 8th International Conference on Intelligent Computing and Signal Processing, ICSP 2023*, 2023. doi: 10.1109/ICSP58490.2023.10248790.

[46] A. Garah, N. Mbarek, and S. Kirgizov, "An architecture for confidentiality self-management in the Internet of Things," in *Proceedings - 16th International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2022*, 2022, pp. 472–478. doi: 10.1109/SITIS57111.2022.00078.

