ISSN: 2836-8495

Review Article

Journal of Current Trends in Computer Science Research

# Internet of Things Architectures, Protocols, And Standard Bodies: A Comprehensive Review

**Matendo Didas***

*Center for Information and Communication Technology, St. John's University of Tanzania*

***Corresponding Author**
Matendo Didas, Center for Information and Communication Technology, St. John's University of Tanzania.

**Submitted:** 2025, Aug 20; **Accepted:** 2025, Sep 15; **Published:** 2025, Sep 25

**Citation:** Didas, M. (2025). Internet of Things Architectures, Protocols, And Standard Bodies: A Comprehensive Review. *J Curr Trends Comp Sci Res, 4*(5), 01-11.

**Abstract**

*With the development of wireless sensor networks, ubiquitous computing, and machine-to-machine (M2M) communication, the idea of the Internet of Things (IoT) has grown steadily. Through the use of uniquely identifiable identifiers, the Internet of Things (IoT) links disparate physical things and permits communication between them. IoT has made it possible for digital systems and physical items to link seamlessly, revolutionizing modern computing. Nonetheless, knowledge about IoT designs, protocols, and standards is still sparse and disorganized. The available IoT architectures, communication protocols, and standardization initiatives are all thoroughly reviewed in this article. An overview of the Internet of Things is provided in this document along with information on its architecture, protocols, and associated standard organizations. In addition to analyzing important protocols like MQTT, CoAP, AMQP, and LoRaWAN, we look at layered architectural models, including three-tier and five-tier frameworks. We also talk about standardization efforts by groups like the IoT Alliance, IEEE, and IETF. Our study suggests future research areas while highlighting contemporary issues like scalability, security, and interoperability. Researchers and practitioners working on the design and implementation of IoT systems might use this paper as a reference.*

**Keywords:** IoT, Architecture, Protocols, Standards, MQTT, CoAP, Security

## 1. Introduction

A network of linked devices that gather, share, and process data to facilitate intelligent decision-making is known as the Internet of Things (IoT) [1]. A network of linked devices that communicate and share data to automate procedures and boost productivity across businesses is also known as the Internet of Things (IoT) [2]. IoT applications are changing modern life in a variety of ways, from smart cities and homes to manufacturing, healthcare, industrial automation, and agriculture.

The term "IoT" has gained popularity in the current wireless telecommunications era. Since it is a new field of study, more research into all related ideas and elements would be helpful for the development of the Internet of Things concept. According to, the core concept of the Internet of Things is to make ubiquitous computing possible by utilizing uniquely addressable items to detect information and improve information transmission with little to no human engagement [3]. Smart objects, which are created by integrating electronic components into common goods like mobile phones and household appliances, make this idea easier to understand. As they share their knowledge and access information created by other connected devices, the connected devices become identifiable inside the network and can make contextual decisions [4]. In actuality, IoT requires proactive operation based on several aspects (context-aware computation) and communication with existing networks. Since the Internet is now the foundation of numerous interconnected typical networks and networks of smart things for information sharing and circulation, the traditional explanation of the Internet has been transformed into an original concept [5].

The greatest obstacle to the development of IoT from the perspective of the research community can be attributed to the dispersed interests of researchers, which causes them to focus on certain areas rather than taking the IoT's overall growth into account. As a result, it undermines the idea's overall evolution and prevents the practical implementation of IoT [6]. Under a variety of interests, numerous studies have been carried out on the subject of IoT. Additionally, a survey on the Internet of Things was carried out by in order to elaborate on the primary communication technologies [6]. In their IoT findings, Gubbi et al. considered a cloud-centric architecture for IoT applications and enabling technologies [3].

In a similar vein, highlighted the difficulties in bridging the gap between research and practical applications [7]. Furthermore, a number of researchers have found numerous unresolved issues with the security of information sharing inside the Internet of Things [7]. Other issues that have been faced include enabling a complex sensing environment, power supply, various connectivity possibilities, privacy, changing architecture, and the complexity of the Internet of Things itself [8]. One of the biggest challenges in the Internet of Things is the unique addressing of items, as well as the storage and representation of the information that is transmitted [6]. In addition to the technological challenges, the absence of a well-defined and well-recognized business model that may draw in funding to encourage the use of these technologies is impeding the adoption of the IoT paradigm [9].

With the help of numerous wired and wireless connectivity alternatives, including Bluetooth, WIFI, Radio Frequency Identification (RFID), and Near-Field Communication (NFC), the aforementioned difficulties can be partially resolved. The current WI-FI networks should be adjusted to accommodate mesh networks and achieve broader coverage [10]. Furthermore, understanding the information flow within the Internet of Things requires a focus on its communication pathway. It disseminates information using a variety of standards, protocols, and methods. According to geographic coverage, the aforementioned connectivity alternatives can be divided into three main categories: personal area networks (PAN), local area networks (LAN), and wide area networks (WAN) [11]. Supporting device-to-device (D2D) communication, device-server architecture (D2S) interaction, and device data sharing among server architectures (S2S) are crucial for enabling information sharing in the Internet of Things (IoT) [12].

IoT communication involves several protocols and standards. Among these, IPv6 over Low Power Wireless Personal Area Network (6LoWPAN), IPv6 over Internet Protocol version 4 (IPv4), Constrained Application Protocol (CoAP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) are given precedence. However, because of its reduced size and performance, limited device developers have claimed that UDP is beneficial and economical [13]. A model that divides these protocols into confined and unconstrained stacks based on the TCP/IP network layer architecture was proposed.

Common standards like Extensible Markup Language (XML), Hypertext Transfer Protocol (HTTP), and IPv4 are found in the unconstrained stack, while protocols with comparable functionality but much lower complexity, such as Efficient XML Interchange (EXI), CoAP, and 6LoWPAN, are found in the constrained stack [9]. With the tremendous help of research institutes and businesses, IoT has grown quickly and been implemented in real life [14]. The most widely used IoT standards are IEEE 802.3, IEEE 802.11, and IEEE 802.15.4 [13]. Additionally, Sheng et al. assessed the Internet Engineering Task Force (IETF) protocol suite to identify the obstacles for IoT, and it has a significant contribution to IoT [15]. The quick expansion of IoT devices presents a number of securities, scalability, and interoperability issues. Strong designs, communication protocols, and standards are essential for resolving these problems. IoT device heterogeneity, however, calls for standardized frameworks, effective communication protocols, and clearly specified designs.

Reviewing the core elements and present status of IoT systems with an emphasis on their designs, protocols, and standardization initiatives is the goal of this article. To give readers a systematic understanding of IoT ecosystems, this article investigates IoT architectures, protocols, and standards. We go over standardization initiatives, assess important communication protocols, and talk about layered architectural models. The results enhance knowledge on the security, interoperability, and design of IoT systems.

## 2. Literature Review

Related work: Several paradigms and frameworks for structuring IoT systems are highlighted in the literature currently under publication. Early insights into IoT paradigms were offered by, who focused on the intersection of cloud computing, wireless sensor networks, and RFID [6]. A layered Internet of Things design including application, network, and sensing layers was proposed by [3]. A 2017 study by Lin et al. addresses the security issues with IoT communications. Other research examines communication protocols designed for limited contexts, as done by [16]. The significance of interoperability is highlighted in recent publications by writers such as, who examine standardization initiatives in various industries [17]. To offer a systematic understanding of IoT ecosystems, there is no exploration of IoT architectural models, protocols, or standardization initiatives.

## 3. Methodology

Using a methodical approach to literature review, this study collected information from technical reports, white papers, peer-reviewed journals, and standards publications. Key resources like ScienceDirect, IEEE Xplore, and ACM Digital Library were searched with phrases like "IoT architecture," "IoT protocols," and "IoT standards." Citations, recentness, and influence on the subject were taken into consideration when choosing pertinent papers. Three primary themes—architectures, protocols, and standards were then used to classify and examine the data.

The following were part of the systematic literature review approach:

**3.1. Data collection:** The following keywords were used to search academic databases (IEEE Xplore, Springer, and ACM): "IoT architecture," "IoT protocols," and "IoT standards."
**3.2. Selection criteria:** publications on architectures, protocols, and standards that were peer-reviewed between 2010 and 2025 were considered.
**3.3. Content analysis:** comparison of standardization trends, architectural models, and protocols.

## 4. Results and Discussion

IoT Architecture: After social networking and static pages (WWW), the Internet of Things (IoT) has emerged as the third wave of the web. It is the global network that uses IP to link different kinds of items at any time and from any location. When designing IoT architecture, scalability, interoperability, data storage dependability, and quality of service (QoS) are crucial factors to consider [18]. Several interest groups have tried to develop a uniform architecture for IoT to achieve these important objectives.

The traditional Internet of Things design has been separated into three levels, namely the perception layer, network layer, and application layer, out of numerous suggested architectures [19]. The bottom layer of the architecture, the perception layer, is in charge of taking information from objects and converting it into a digital representation. Digital signals are then carried across the network by the network layer, and their application in various settings is the responsibility of the application layer [20].

### 4.1. IoT Architectures

IoT architectures typically follow a layered design (Table 1):
**4.1.1. Perception layer:** in charge of gathering data with RFID and sensors. The perception layer, which is the first stage of the Internet of Things, gathers information from the environment, such as temperature, humidity, etc., as well as from various devices and objects. In the perception layer, wireless sensor networks (WSNs), which are made up of many tiny, resource-constrained sensors, are crucial for gathering and processing different kinds of data [21]. ZigBee, WI-Fi, and numerous other protocols designed for short-range communication are used by these sensors and other real-world IoT objects, such as actuators, cameras, GPS terminals, etc., to connect.

The Internet of Things is a vast network that links disparate devices. As a result, it is crucial to recognize and treat every item, gadget, or thing uniquely. In addition to communication, RFID, NFC, and Bluetooth are utilized as identification technologies. Furthermore, recent efforts on 6LoWPAN have made it possible for these devices to be addressed specifically within the network and integrate into it without any additional difficulties [18].

**4.1.2. Network layer:** Uses technologies such as Wi-Fi, ZigBee, LTE, and 5G to transmit data. This layer is regarded as the IoT architecture's brain. Between the perception layer and the application layer, it enables safe data transfer. Information gathered at the perception layer is sent to various servers and applications via the network layer. Actually, the Internet and communication networks have converged to form the network layer. The network layer is the most advanced layer of the Internet of Things architecture, according to a number of studies conducted on communication technologies and the Internet.

Because of IoT management and data centers, data processing occurs at the network layer. As a result, the Internet of Things' "core layer" (the network layer) enhances information operation capabilities. Furthermore, distinct addressing and routing capabilities guarantee the smooth integration of countless devices into a single cooperative network, achieving the IoT concept's universality. Wi-Fi, Bluetooth, xDSL, PLC, and other wired, wireless, and satellite technologies have all made significant contributions to this problem. In order to ensure that every connected device in the network has a unique address, the IETF has made significant efforts to establish the 6LoWPAN protocol, which forwards IPv6 traffic in IoT architecture.

**4.1.3. Application Layer:** provides user interfaces and services tailored to a particular application. This layer, which connects people and apps, is the highest in the Internet of Things architecture. IoT technology and industry knowledge are used to create a wide range of intelligent application solutions at the application layer [19]. For instance, it incorporates IoT system functions to create useful applications, like intelligent transportation, life medical and health monitoring, ecological environment and natural disaster monitoring, and building health monitoring for cultural dissemination and heritage conservation [22]. The application layer is primarily responsible for managing IoT applications globally [18]. As seen in Figure 2, the application layer does, in fact, adhere to certain standards and protocols. The assessment by found that HTML5's Web socket, which drastically lowers the communications overhead, is the second most lightweight protocol, behind IETF's CoAP, which is the only protocol that operates over UDP [23].

| S/N | Layer | Description |
|---|---|---|
| 1 | Perception | Gather data from several devices.<br>Short-range data processing and communication, such as RFID, sensors, and actuators |
| 2 | Network | A special addressing system to guarantee safe data transmission |
| 3 | Application | Real-world implementations of IoT technology, such as intelligent transportation, remote function control, and disaster monitoring |
| **Source:** Synthesized by the Author (2025) | | |

**Table 1: The IoT Architecture**

To allow for greater generality, authors have, however, recently talked about a five-layer design [6,19,20]. The five-layer design was defined in a number of ways, paying attention to various details. Nonetheless, the majority can be divided into application layer, business layer, service management, object abstraction, and objects.

Data collection from heterogeneous devices is the responsibility of the object layer. Additionally, it digitizes and processes the data that has been gathered. As a result, it moves the processed data to the higher layers [16,24]. In a three-layer architecture, this layer replicates the perception layer's services. Using communication technologies like RFID, 3G, and Wi-Fi, the object abstraction layer acts as a mediator between the objects layer and the service management layer [24]. The object abstraction layer manages the network layer functionalities.

In addition to supporting information processing and decision-making, the service administration is responsible for matching the requester with the requested applications [25]. Customers can request high-quality smart services from the application layer [24,25]. The topmost layer, the business layer, uses the data it receives from the application layer to create a business model and graphical representations. The duties of the service management layer, application layer, and business layer of the five-layer architecture are represented by the application layer in the three-layer design.

To handle latency and processing needs, sophisticated designs have been developed, such as cloud-centric and edge computing models. Decentralized processing nearer to data sources is provided via fog computing. The study's reviewed IoT architectural models are displayed in Table 2.

| S/N | IoT Architectures | Description | Ref. |
|---|---|---|---|
| 1 | Three-Tier Architecture | Consisting of the application, network, and perceptual layers | Gubbi et al., 2013 |
| 2 | Five-Tier Architecture | Extending to the transport, middleware, and business levels Better scalability is also provided, although complexity is increased. | Al-Fuqaha et al., 2015 |
| 3 | Fog/Edge Computing | Processing is decentralized to cut down on latency lowers latency as well, but presents security risks. | Bonomi et al., 2012 |
| **Source:** Synthesized by the Author (2025) | | | |

**Table 2: IoT Architectures Categorized into Layered Models**

### 4.2. IoT Communication Protocols

Data interchange that is both lightweight and energy-efficient must be supported by IoT communication protocols. There are trade-offs between complexity, scalability, and efficiency in every protocol. The study's synthesized IoT communication protocols are displayed in Table 3.

A variety of open and private communication protocols are supported by IoT. While some of the protocols were already in place, others were put into place expressly to increase the possibilities of the Internet of Things. State that there are four main categories into which IoT communication protocols can be divided: infrastructure protocols, application protocols, service discovery protocols, and other significant protocols [16]. Later in the next section, an overview of the associated infrastructure, application, and service discovery protocols will be covered. Additionally, Figure 3 provides a condensed overview of the stack of IoT communication protocols.

| S/N | IoT Communication Protocol | Latency | Power Usage | Use Case | General Description | Ref. |
|---|---|---|---|---|---|---|
| 1 | Message Queuing Telemetry Transport (MQTT) | Low | Medium | Real-time monitoring | Simple publish-subscribe methodology This publish/subscribe protocol is perfect for situations requiring little bandwidth. | Hunkeler et al., 2008 |
| 2 | Constrained Application Protocol (CoAP) | Medium | Low | Smart Sensors | RESTful protocol for devices with limited resources To put it another way, it is a web transmission protocol made for devices with limitations | Shelby et al., 2014 |
| 3 | Advanced Message Queuing Protocol (AMQP) | High | Medium | distributed IT environments | Business-class messaging | Ouaddah et al., 2016 |
| 4 | LoRaWAN | High | Very low | Wide-area IoT | Low-power, long-range, wide-area networks | Pham, 2016 |
| 5 | 6LoWPAN | Can be Low or High | Can be Low or High | Automation in wireless internet connectivity | Permits IPv6 over wireless personal area networks with low power consumption | Olsson, 2014 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | ZigBee and Bluetooth Low Energy (BLE) | Low | Low | Proximity sensors, heart rate monitors, and fitness devices | Make short-range communication available | Varol, 2019 |
| **Source:** Synthesized by the Author (2025) | | | | | | |

**Table 3: IoT Communication Protocols**

IoT Communication Protocols can also be classified as infrastructure, application, and Service Discovery:

**4.2.1. Infrastructure Protocols:** The physical, link, network, and routing layers are subcategories of the infrastructure layer. Each of these tiers has its own set of protocols. The IoT architectural layers discussed in Section 2 can be mapped onto these infrastructure levels. The perception layer of the Internet of Things is where the physical and connection layer protocols function. In the meantime, the generic IoT architecture's network layer is where the network and routing layer protocols operate. In Figure 1, the layer hierarchy is displayed.

The routing layer is where the infrastructure communication protocol, RPL, operates. The necessity for a lightweight routing system based on IPv6 for IP smart object networks was promptly identified by the IETF. The RPL specification was then developed by the IETF's ROLL working group. A distance vector protocol called RPL explains how to construct a DODAG [9]. It also employs four different kinds of control messages. DODAG Information Object (DIO) messages are the first kind of communication; they show the device's rank after taking matrices and computations into account. When the device rank is higher than the possible parent ranks, the DIO rank can be used to determine the preferred parent path. Both upward and downward traffic to a particular parent is supported by the Destination Advertisement Object (DAO) messages. DIOs are obtained from nearby nodes using DODAG Information Solicitation (DIS) messages.

DAO Acknowledgment (DAO-ACK), the final message type, is produced in response to a DAO message [26]. Both storing and non-storing modes are RPL's two modes of operation (MOP). While messages in the storing mode are routed according to the destination IP address, traffic in the non-storing mode is directed downward using source routing [27].

Another IETF-developed protocol that functions at the infrastructure's network layer is 6LoWPAN. Interoperability with other IP networks and other IEEE 802.15.4 wireless devices is made easier by 6LoWPAN's foundational use of IPv6. The administration tasks are made easier by 6LoWPAN, which enables each restricted device to be uniquely accessible within the network. Additionally, it is in charge of maintaining consistency with the top layers, enabling stateless addressing, reducing protocol stack headers, fragmenting and rearranging IPv6 packets, and supplying a foundation for "mesh-under" routing [28].

Additional header information is not required in IP routing over 6LoWPAN in order to minimize needless packet overhead and free up more space for data transfer [29]. Additionally, the mesh address header of 6LoWPAN facilitates packet routing in a mesh network; however, the link layer handles the specifics of routing [30]. The type field that is represented by the header's first two bits identifies the 6LoWPAN header. For 6LoWPAN communications, four header types are defined: (1) the header is set to No 6LoWPAN (00) if the packet is not for 6LoWPAN processing; (2) the header is set to Dispatch (01), which indicates that the packet is ready for IPv6 header compression; (3) the Mesh-Addressing (10) header-type forwards IEEE 802.15.4 frames to the link layer as needed, making multi-hop networks; and (4) the Fragmentation (11) header is used if the packet size exceeds IEEE 802.15.4 frame size [31].

16 channels between 2.4 and 2.48 GHz are defined by IEEE 802.15.4; each channel is 2 MHz wide and 5 MHz apart. Making sure that channels don't interfere with one another is the justification [32]. Both mesh and star topologies can be supported by this protocol [15]. Full functional devices (FFD) and restricted functional devices (RFD) are the two categories of IEEE 802.15.4 devices. The FFDs can communicate with any other device in the network and can establish, maintain, and coordinate the network (PAN Coordinator). Nevertheless, the RFDs are resource-constrained devices that can only speak with the coordinator. Nevertheless, IEEE 802.15.4 encounters MAC layer reliability problems.

The IETF released IEEE 802.15.4e after making changes to the MAC layer to address the shortcomings of IEEE 802.15.4. This protocol specifies how a schedule is carried out by the MAC layer. It is possible to execute the schedule in a distributed or centralized manner. A manager node creates the schedule in the centralized method. In a similar manner, the manager is periodically notified by the connected nodes about the other nodes that are producing data. The manager then uses the information that was obtained to establish the schedule. Since the manager is aware of all network activity, centralized scheduling is actually quite effective. Nodes locally decide the schedule with neighboring nodes in distributed scheduling, and the simplest method would be to plan a link for each neighbor. Distributed scheduling, however, works well with highly dynamic networks, such as those with numerous gateway nodes or mobile nodes [33].

Bluetooth Low Energy (BLE), which uses a short-range radio with lower power characteristics, was introduced to be active for a longer period of time. Because of its extremely low power consump-

tion and reduced latency compared to traditional Bluetooth, BLE is a promising IoT technology. A client connects to and accesses one or more servers using the client-server architecture used by the BLE. In this case, computers, smartphones, and other application devices serve as the clients, and data generators like sensors and actuators serve as the servers. During periods of inactivity, it keeps the radio off to minimize power consumption. In the same way, it activated the radio to transmit and receive smaller data packets.

**4.2.2. Application Protocols:** At the top of the architecture, the application layer connects the underlying platform with the Internet of Things application. The application layer has a large number of established communication protocols. Common protocols include HTTP-REST, XMPP, MQTT, CoAP, and DDS. An overview of the CoAP and MQTT application layer protocols is provided in the paragraphs that follow.

The IETF created the stateless CoAP protocol for Internet of Things applications. Since CoAP is built on the Representational State Transfer (REST) protocol, it is possible to translate a CoAP-REST proxy directly [16]. For devices that are lightweight and have limited resources, it was defined by substituting HTTP [34]. To achieve low power usage, minor changes were made to HTTP. It is a great fit for IoT communication because it is bound to UDP, which lowers TCP overhead and bandwidth needs [23].

IBM launched MQTT, intending to connect networks and embedded devices with middleware and applications. The transport layer protocol it employs is TCP. MQTT is straightforward and quick to install due to its lightweight broker-based architecture [35]. MQTT is suitable for devices with limited bandwidth that are linked to an unstable network. A publisher, a broker, and a subscriber make up MQTT. A device must be registered for a certain topic in order to become a subscriber. After that, the publisher creates content and uses brokers to distribute it to subscribers. The Quality of Service (QoS) is determined by MQTT based on the reliability of message delivery. From the three pre-established levels, it assigns a QoS value [36].

CoAP has established four message types: confirmable (CON), non-confirmable (NON), reset (RST), and acknowledgement (ACK). UDP does not offer dependability. Combining confirmable and non-confirmable communications with datagram transport layer security (DTLS) increases reliability. A CON message with a message ID is sent via the dependable CoAP transmission mechanism, and it is sent again to the recipient until the sender receives an ACK message with the same ID. When the receiving end fails to process the CON message, it sends an RST message rather than an ACK. When dependable transmission is not required for the message, non-confirmable messages are transmitted [37].

**4.2.3. Service Discovery Protocols:** In order to have an effective system for dynamically and efficiently registering and discovering devices and services, service discovery protocols are necessary. In this context, the two most used protocols are DNS Service Discovery (DNS-SD) and Multicast Domain Name System (mDNS). To work with the IoT's resource-constrained devices, these protocols should be adjusted appropriately.

Without a central DNS server, records in a local network can be resolved using mDNS [38]. The format of mDNS packets is 99% similar to that of DNS packets. Because mDNS does not require manual configuration, can function without infrastructure, and can continue to function even in the event of an infrastructure failure, it is appropriate for smart devices on the Internet of Things. Every node in the domain receives an IP multicast message from mDNS asking for a response from the node with the specified name.

As seen in Figure 1, the relevant node responds to the requestor and every other node in the domain, causing every other node to update its local cache with the answered IP address and the provided name. On a network, DNS-SD is used to find services. Although it is not dependent on mDNS, this protocol is compatible with it. Zero-conf networking point-to-point communication without the need for external configurations is made possible by DNS-SD. To connect new machines, DNS-SD doesn't need to be configured or administered externally. There are two steps involved in service discovery: Find the host names for the desired service and link the IP addresses with the host names. The IoT protocol stack summary is displayed in Figure 2.

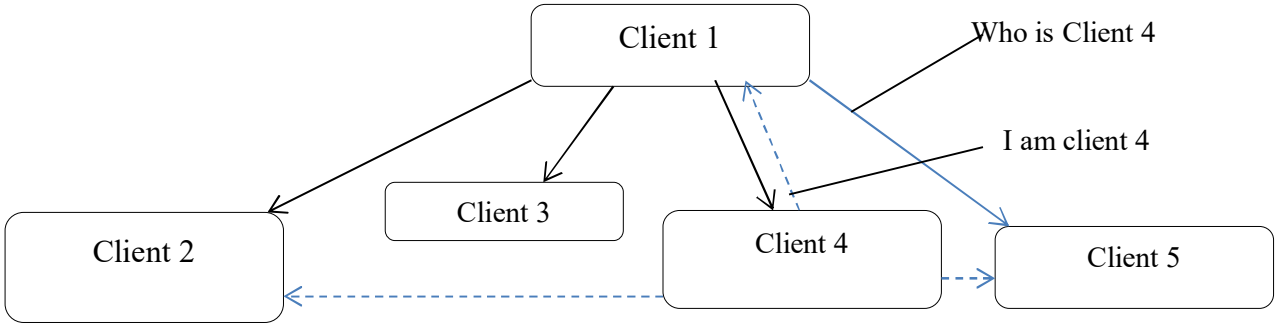


**Figure 1:** MDNS Protocol Request and Response Scenario
**Source:** Synthesized by the Author (2025)

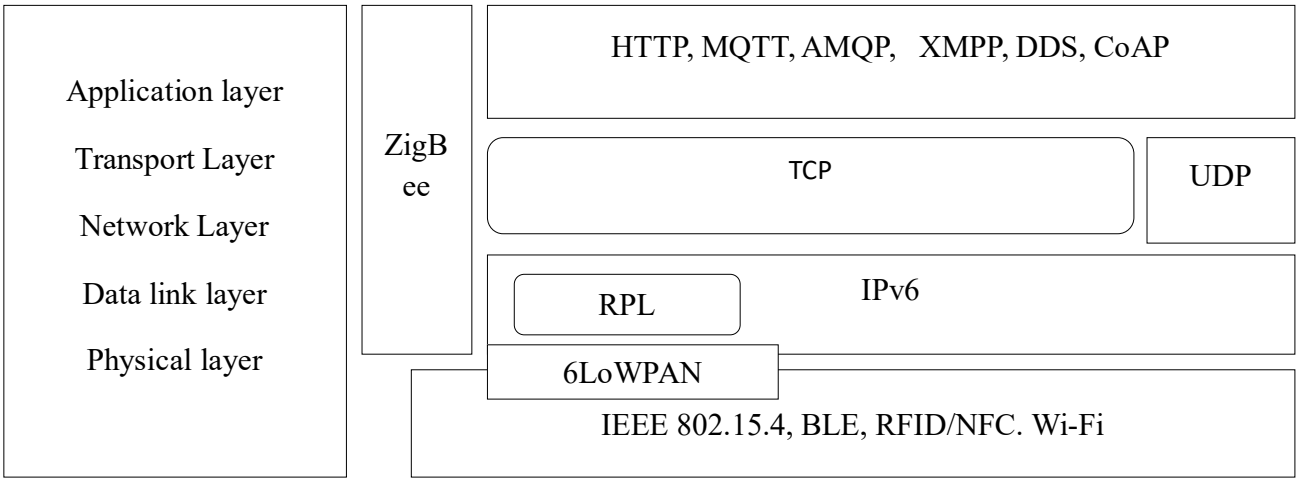


**Figure 2:** IoT Protocol Stack
**Source:** Synthesized by the Author (2025)

### 4.3. IoT Standards

The review identified several IoT standardization groups, including the IoT Alliance (oneM2M, OCF): Unified frameworks, IEEE: IoT standards for interoperability (IEEE P2413), IETF: CoAP, and 6LoWPAN for limited networks. The IoT standards are compiled in Table 4. It should be mentioned that other organizations are also creating IoT standards. These efforts aim to promote compatibility between various IoT systems and devices while guaranteeing strong security measures for widespread and secure implementation.

However, because TCP/IP is the industry standard for computer networking, it is thought to have promise for the realization of the Internet of Things. Nevertheless, IPv6's low power and bandwidth limitations limited its utility. Therefore, a lot of interest groups have worked to establish IoT standards to facilitate and streamline the development of IoT applications. The Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium (W3C), and EPC Global have made significant contributions to IoT standards. This section gives a summary of a few common standards.

IEEE 802.15.4, which is devoted to low-power, low-data-rate, low-cost, and short-range communications, is the result of the IEEE 802.15 PAN working group's expanded contribution [39,40]. According to, a greater proportion of mobile devices were created to comply with IEEE 802.15.4 [15]. For IPv6 packets, the maximum transmission unit (MTU) size permitted by the standard is 1280 bytes. However, there is a limit of 127 bytes for the maximum frame size of the physical layer, which is further limited by a maximum frame overhead of 25 bytes. According to, IPv6 packets cannot be accommodated within IEEE 802.15.4 packets [41]. This limits the amount of usable space for top-layer protocols to 86–116 bytes.

The studied literature demonstrates that there are gaps in IoT standardization, such as security, which is concerned with fragmented security frameworks, and interoperability, which is concerned with the lack of universal standards that result in vendor lock-in. DTLS for CoAP only reaches up to 250 kb/s at 2.4 GHz, which results in limited scalability and ineffective traffic load balancing, even though it guarantees a complete handshake protocol for data reliability [15,42]. Both the media access control (MAC) and physical (PHY) layers are specified in IEEE 802.15.4, albeit they can be changed to meet the needs of specific applications.

Nevertheless, because the MAC protocol is single-channel, its dependability becomes uncertain in multi-hop environments. The IEEE 802.15.4 MAC layer is vulnerable to failure because of interference and multi-path fading when an inherent frequency hopping method is not available. In order to use time-slotted access, multichannel communication, and channel hopping through Time Synchronized Channel Hopping (TSCH) in IEEE 802.15.4e, the MAC protocol of IEEE 802.15.4 has been improved. Accordingly, the IEEE 802.15.4e MAC layer improves the reliability problems that existed in the IEEE 802.15.4 MAC layer while reducing the negative impacts of interference and multi-path fading [34].

| Standard | Implemented by | Accessing layers | Influential Protocol | Features |
|---|---|---|---|---|
| ITU | ITU (Citaristi, 2022; Yang & Chang, 2019) | PHY and MAC layers | ITU | Emphasizes international telecom standards |
| IEEE 802.154 | IEEE (Citaristi, 2022; Yang & Chang, 2019; (Cooklev (2004) | PHY and MAC layers | IEEE 802.15 | Data transport with low power consumption Low rate of data Cheap |
| IEEE 802.15.4E | IEEE (Citaristi, 2022; Yang & Chang, 2019) | PHY and MAC layers | IEEE 802.154 | IEEE 802.15.4 MAC layer modification Excellent dependability in multi-hop environments |
| ZigBee | ZigBee Alliance (Xu et al., 2008) | Upper layers (Network, Transport, Application) | IEEE 802.15.4 | Built upon IEEE 802.15.4's PHY and MAC layers Self-healing and self-forming |
| 6LowWPAN | IETF (Works on IP-based networking protocols like 6LoWPAN and CoAP) (Halder et al., 2018; Yang & Chang, 2019) | Network layer | IPv6 | Transport IPv6 datagrams in overlapping broadcast domains using IEEE 802.15.4 neighbor discovery |
| IoT Alliance (oneM2M, OCF) | IoT Alliance (Kim et al., 2018), Wu et al., 2017) | PHY and MAC layers | oneM2M, OCF | Regarding unified frameworks |
| RPL | IETF (Works on IP-based networking protocols like 6LoWPAN and CoAP) (Halder et al., 2018; Yang & Chang, 2019) | Transport | IPv6 6LowPAN | Keep the route topology in place. Update the routing data. |
| ISO/IEC | ISO/IEC (Ganji et al., 2019) | PHY and MAC layers | ISO/IEC | Offers mechanisms for the security and interoperability of systems |
| **Source:** Synthesized by Author (2025) | | | | |

**Table 4: Standards Related to IoT**

In a nutshell, another crucial standard for Internet of Things applications is ZigBee. It belongs to the ZigBee Alliance, a collection of businesses that came together to develop and market the new standard. Because ZigBee is self-forming, self-healing, and supports mesh and star topologies, it resembles IEEE 802.15.4 [43]. On top of the IEEE 802.15.4 standard's PHY and MAC levels, it specifies the upper layers of the architecture. The ZigBee standard is specifically designed for applications including control and monitoring. As a result, it works well for applications including lighting and commercial control, industrial control, personal health care, and building automation.

With its IPv6-based 6LoWPAN standard, the IETF has advanced the Internet of Things. It stands for IPv6 over IEEE 802.15.4, a low-power wireless personal area network. Because of its stability, universality, and extensibility, IPv6 was regarded as the foundational model for 6LoWPAN [15]. The goal of the IETF's 6LoWPAN working group was to address the limitations of IPv6 datagrams when they were being transmitted over a low-power WPAN. In a network with overlapping broadcast domains, the considerations were how to carry IPv6 datagrams in 802.15.4 frames (because of the significant mismatch between IPv6's MTU and IEEE 802.15.4, as previously mentioned) and how to carry out essential IPv6 neighbor discovery functions, such as address resolution and duplicate address detection [44]. Header compression, fragmentation, and layer two forwarding are the three main components of 6LoWPAN [45].

For 6LoWPAN, routing is difficult for a variety of reasons. They are characterized by battery-powered nodes, low-power lossy networks (LLN), and constantly shifting mesh topologies brought on by mobility [33]. The Routing Protocol for LLN (RPL) was proposed by IETF, considering the 6LoWPAN mechanism and IPv6 behavior. In a lossy network, it facilitates the construction of a robust topology with low routing needs [16]. A Destination-Oriented Directed Acyclic Graph (DODAG) is the fundamental component of RPL. According to, every router in a converged LLN has identified a stable set of parents that may be the next hop on the road to the root [28]. For a wide range of application domains, RPL has decoupled packet processing and forwarding from routing optimization [27].

## 5. Conclusion and Recommendations

The Internet of Things (IoT) is a developing concept that seamlessly connects many kinds of devices to produce vast amounts of data that are shared among the devices. In order to enhance the quality of life, the processed information is utilized for both important and non-critical decision-making. In order to lay the groundwork

for future studies and industry acceptance, this article offers an organized summary of IoT topologies, protocols, and standards. The intricacy and variety of IoT ecosystems are highlighted in this review. Harmonized architectures, appropriate protocols, and internationally recognized standards are necessary for effective deployment. Scalable and safe deployments depend on IoT architectures, protocols, and standards. The following are some of the main conclusions: protocols: MQTT and CoAP predominate, although LoRaWAN is best for low-power applications and IoT standards; architectures: five-tier models are appropriate for large-scale deployments; and edge computing improves real-time processing. It is necessary for standards bodies to work together more closely. Enhancing security, improving interoperability, and creating scalable solutions to handle the expanding number of IoT devices should be the main goals of future research. For the Internet of Things to reach its full potential, cooperation between industry, academia, and standards organizations is crucial. Future developments may also involve improving cross-platform compatibility and creating unified security frameworks [46-57].

## References


1. Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., & Srinivasulu, T. (2015). The internet of things (iot): An overview. *International Journal of Engineering Research and Applications, 5*(12), 71-82.
2. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of computer and communications, 3*(5), 164-173.
3. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems, 29*(7), 1645-1660.
4. Vermesan, O., & Friess, P. (2015). *Building the hyperconnected society-internet of things research and innovation value chains, ecosystems, and markets* (p. 332). Taylor & Francis.
5. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications, and research challenges. *Ad hoc networks, 10*(7), 1497-1516.
6. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.
7. Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., & Razafindralambo, T. (2011). A survey on facilities for experimental Internet of Things research. *IEEE Communications Magazine, 49*(11), 58-67.
8. Ahmed, A. A. G. E. (2019). Benefits and Challenges of Internet of Things for. *Telecommunication Networks: Trends and Developments*, 105.
9. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal, 1*(1), 22-32.
10. Agnihotri, A., Puri, M., & Mahajan, A. (2024). IoT Based Recent Trends in Engineering and its Applications.
11. Gabrys, J. (2016). Re-thingifying the Internet of Things. In *Sustainable Media* (pp. 180-195). Routledge.
12. https://www.electronicdesign.com/home/whitepaper/21803072/understanding-the-protocols-behind-the-internet-of-things-pdf-download
13. El-Hadi, M. (2022). OVERVIEW OF THE IOT THAT MEET SOCIETAL CHALLENGES. Journal of the Egyptian Society for Information Systems and Technology, 28(28), 5-23.
14. Ganchev, I., Ji, Z., & O'Droma, M. (2021, December). A Service Tier Design for the EMULSION IoT Platform. In *2021 International Conference on Computational Science and Computational Intelligence* (CSCI) (pp. 1500-1504). IEEE.
15. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2014). A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities. *IEEE wireless communications, 20*(6), 91-98.
16. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE communications surveys & tutorials, 17*(4), 2347-2376.
17. Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless personal communications, 58*(1), 49-69.
18. Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on the Internet and underlying issues. *Ad Hoc Networks, 28*, 68-90.
19. Yun, M., & Yuxin, B. (2010, June). Research on the architecture and key technology of the Internet of Things (IoT) applied to the smart grid. In the *2010 international conference on advances in energy engineering* (pp. 69-72). IEEE.
20. Xiaocong, Q., & Jidong, Z. (2010, November). Study on the structure of the "Internet of Things (IOT)" business operation support platform. In *2010, IEEE 12th International Conference on Communication Technology* (pp. 1068-1071). IEEE.
21. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer communications, 54*, 1-31.
22. Shi, Y. R., & Hou, T. (2013). Internet of Things key technologies and architectures research in information processing. Applied Mechanics and Materials, 347, 2511-2515.
23. Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., & Alonso-Zarate, J. (2015). A survey on application layer protocols for the Internet of Things. *Transaction on IoT and Cloud computing, 3*(1), 11-17.
24. Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., & Liu, W. (2011, July). Study and application of the architecture and key technologies for IOT. In the *2011 International Conference on Multimedia Technology* (pp. 747-751). IEEE.
25. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of the Internet of Things. In *2010, the 3rd International Conference on Advanced Computer Theory and Engineering* (ICACTE) (Vol. 5, pp. V5-484). IEEE.
26. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis,

P., ... & Alexander, R. (2012). *RFC 6550-RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*.[online] Tools. ietf. Org.
27. Clausen, T., Herberg, U., & Philipp, M. (2011). A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL). In *2011 IEEE 7th international conference on wireless and mobile computing, networking and communications* (*WiMob*) (pp. 365-372). IEEE.
28. Hennebert, C., & Dos Santos, J. (2014). Security protocols and privacy issues in the 6LoWPAN stack: A synthesis. *IEEE Internet of Things Journal, 1*(5), 384-398.
29. Silva, B. N., Khan, M., & Han, K. (2018). Internet of things: A comprehensive review of enabling technologies, architecture, and challenges. *IETE Technical Review, 35*(2), 205-220.
30. Ott, A. (2012, November). Wireless Networking with IEEE 802.15. 4 and 6LoWPAN. In *the Embedded Linux Conference Europe*. Nov (Vol. 5).
31. Görmüş, S., Aydın, H., & Ulutaş, G. (2018). Security for the internet of things: a survey of existing mechanisms, protocols, and open research issues. *Journal of the Faculty of Engineering and Architecture of Gazi University, 33*(4), 1247-1272.
32. Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., & Dohler, M. (2012). Standardized protocol stack for the Internet of (important) things. *IEEE communications surveys & tutorials, 15*(3), 1389-1406.
33. De Guglielmo, D., Anastasi, G., & Seghetti, A. (2014). From ieee 802.15. 4 to ieee 802.15. 4e: A step towards the internet of things. In *Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful* (pp. 135-152). Cham: Springer International Publishing.
34. Castellani, A. P., Rossi, M., & Zorzi, M. (2014). Back pressure congestion control for CoAP/6LoWPAN networks. *Ad Hoc Networks, 18*, 71-84.
35. Locke, D. (2010). MQ Telemetry transport (MQTT) v3.1 protocol specification. *IBM developerWorks Technical Library, 15*.
36. Hunkeler, U., Truong, H. L., & Stanford-Clark, A. (2008, January). MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks. In *2008, the 3rd International Conference on Communication Systems Software and Middleware and Workshops* (*COMSWARE'08*) (pp. 791-798). IEEE.
37. Shelby, Z., Hartke, K., & Bormann, C. (2014). *The constrained application protocol* (*CoAP*) (No. RFC7252).
38. Strotmann, C. (2007). New DNS technologies in the LAN.
39. Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals.
40. IEEE 802.15 Work Group. (2006). Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs). *ANSI/IEEE Std, 802*(4).
41. Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016). A survey on secure communication protocols for IoT systems. In *2016 international workshop on Secure Internet of Things* (*SIoT*) (pp. 47-62). IEEE.
42. Jose, D., & Gutierrez, A. (2005). IEE Std. 820.15. 4 Enabling Pervasive Wireless Sensor Networks. Innovation Centre, 2-54.
43. Xu, X., Yuan, D., & Wan, J. (2008, December). An enhanced routing protocol for ZigBee/IEEE 802.15.4 wireless networks. In *2008, Second International Conference on Future Generation Communication and Networking* (Vol. 1, pp. 294-298). IEEE.
44. Ko, J., Terzis, A., Dawson-Haggerty, S., Culler, D. E., Hui, J. W., & Levis, P. (2011). Connecting low-power and lossy networks to the internet. *IEEE Communications Magazine, 49*(4), 96-101.
45. Hui, J. W., & Culler, D. E. (2008). Extending IP to low-power, wireless personal area networks. *IEEE Internet Computing, 12*(4), 37-45.
46. Yang, Z., & Chang, C. H. (2019, February). 6LoWPAN Overview and Implementations. In *EWSN* (pp. 357-361).
47. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16).
48. Citaristi, I. (2022). International telecommunication union—itu. In *The Europa Directory of International Organizations 2022* (pp. 365-369). Routledge.
49. Cooklev, T. (2004). *Wireless communication standards: A study of IEEE 802.11, 802.15, 802.16*. IEEE Standards Association.
50. Ganji, D., Kalloniatis, C., Mouratidis, H., & Gheytassi, S. M. (2019). Approaches to develop and implement iso/IEC 27001 standard information security management systems: A systematic literature review. *Int. J. Adv. Softw, 12*(3).
51. Halder, M., Sheikh, M., Rahman, M., & Rahman, M. (2018). Performance analysis of CoAP, 6LoWPAN, and RPL routing protocols of IoT using COOJA simulator. *Int. J. Sci. Eng. Res, 9*(6), 1670-1677.
52. Kim, J., Choi, S. C., Yun, J., & Lee, J. W. (2018). Towards the oneM2M standards for building IoT ecosystem: Analysis, implementation, and lessons. *Peer-to-Peer Networking and Applications, 11*(1), 139-151.
53. Olsson, J. (2014). 6LoWPAN demystified. *Texas Instruments, 13*, 1-13.
54. Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ait Ouahman, A. (2016, September). Access control in IoT: Survey & state of the art. In *2016, the 5th International Conference on Multimedia Computing and Systems (ICMCS)* (pp. 272-277). IEEE.
55. Pham, C. (2016, June). Building low-cost gateways and devices for open LoRa IoT test-beds. In *International Conference on Testbeds and Research Infrastructures* (pp. 70-80). Cham: Springer International Publishing.
56. Varol, A. B. (2019, September). Compilation of data link protocols: Bluetooth low energy (BLE), Zigbee, and Z-Wave. In *2019, the 4th International Conference on Computer Science and Engineering (UBMK)* (pp. 85-90). IEEE.

57. Wu, C. W., Lin, F. J., Wang, C. H., & Chang, N. (2017, September). OneM2M-based IoT protocol integration. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)* (pp. 252-257). IEEE.