Internet of Things 25 (2024) 101005

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

Connectivity Standards Alliance Matter: State of the art and opportunities

Dimitri Belli, Paolo Barsocchi, Filippo Palumbo *

Institute of Information Science and Technologies "A. Faedo", National Research Council (ISTI-CNR), Via G. Moruzzi, 1 - 56124, Pisa, Italy

ARTICLE INFO

Keywords:
Matter
Thread
IoT
Home and building automation
Ambient intelligence

ABSTRACT

Matter is an open-source, royalty-free connectivity standard developed by the Connectivity Standards Alliance (CSA-IoT). It aims to unify smart home devices and increase their compatibility across various ecosystems. Backed by major tech companies like Apple, Google, Amazon, and the Zigbee Alliance, Matter simplifies the development of IoT devices by providing a unified approach to connectivity. It offers a secure, reliable, and seamless way for devices to communicate and interact, regardless of the manufacturer.

This paper aims to present the current state of adoption of the Matter specification by devices available on the market, and the certification process by the available software. It describes the main characteristics of Matter in its Specification 1.0 state, reviewing the features and functionalities of the Matter protocol, as well as the opportunities for its use and the challenges for its large-scale adoption in Matter-compliant IoT devices.

We discuss the impact of Matter on IoT technologies and ecosystems, providing guidance for manufacturers and consumers. We analyze the emerging research challenges in its adoption and propose our recommendations on how to improve and extend this protocol for better use in the future.

1. Introduction

Matter is a novel application framework and royalty-free standard for home automation based on IP. The project was launched in December 2019 under the name Connected Home over IP (CHIP) with the goal of creating a new standard that enables IP-based communication between smart home devices, mobile apps, and cloud services.[1] At the base of the project stands the Connectivity Standards Alliance (CSA), with the initial Working Group including partners such as Amazon, Apple, and the Zigbee Alliances, in addition to some minor realities [1]. Over time, it has grown to include more than 280 companies to develop plug-and-play devices for smart building automation. This has always been a problem because each device family speaks its own language, for example, Google Home, Amazon Alexa, Samsung Smart Things, and Apple HomeKit have their own protocols and do not communicate with each other. As a global industry-wide effort, Matter introduces a single, stable, and open language that allows devices from different families to easily communicate with each other.

The strengths of Matter encompass a wide range of features and benefits. It unifies already existing technologies by guaranteeing compatibility between heterogeneous ecosystems, ensuring a seamless connection across various platforms. Interoperability is a core strength, allowing all Matter-blazoned devices to work together without conflict. Safety and security are prioritized, with communication between devices safeguarded by a Certificate Authority (CA) system based on reliable practices and protocols. Users

* Corresponding author.
E-mail address: filippo.palumbo@isti.cnr.it (F. Palumbo).

[1] https://csa-iot.org/newsroom/connectedhomeip/.

https://doi.org/10.1016/j.iot.2023.101005
Received 11 September 2023; Received in revised form 20 October 2023; Accepted 16 November 2023
Available online 25 November 2023
2542-6605/

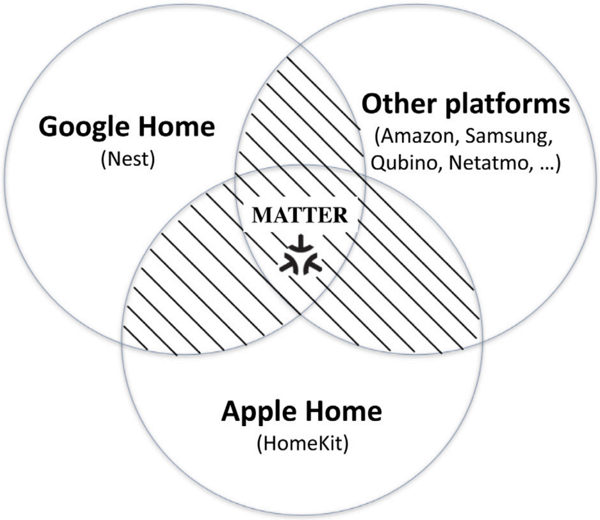

Fig. 1. Matter as a point of convergence for the various existing standards.

are provided with clear visibility of the system's status, enhancing their understanding and control. The life-cycle of each Matter device is clearly defined according to the Specification format, making each device easily manageable and maintainable, even in the face of changes to the Specification. Matter also focuses on overhead reduction, ensuring smooth operation between devices, even those with restricted computational and energy resources. The pervasive availability and deployability of protocols are facilitated by IP addressing, allowing for a wide reach across various networks. Simple adaptation to ecosystems with diverse policies is another advantage, along with an out-of-box experience that is enhanced by a user-friendly approach. Finally, transparency is guaranteed through open access to the development of resources, fostering trust and collaboration within the Matter community.

For these reasons, significant efforts are being made by different manufacturers and product designers to align their solutions, such as Apple HomeKit, Google Home, and Amazon Alexa, with the goal of establishing a unified standard: Matter. The ancestor of this effort is precisely the ZigBee Alliance and its Project CHIP. Indeed, the CSA is nothing more than the ZigBee Alliance with other stakeholders involved, and the Project CHIP is nothing but the starting point of Matter. One of the possible competitors, Samsung, recently recognized the importance of Matter by conforming its home automation solution (i.e., Samsung SmartThings[2]) to the Matter protocol. Fig. 1 shows an ideal abstraction in which the various brands converge towards the standard.

Household appliances (like washing machines, HVAC systems, lights, and so forth) are equipped with short-range communication interfaces, such as Wi-Fi or BLE, that enable them to exchange information with each other. In spite of the interconnection opportunities provided by IoT technology, communication between devices is still limited. We can turn on/off the living room lights with a voice assistant like Siri, or Google Assistant, and you can control the HVAC temperature with the Amazon Alexa app, but we cannot allow two different ecosystem devices to communicate with each other without extra effort. Any device or network of devices that implement Wi-Fi, BLE, and 802.15.4-based communication interfaces (such as ZigBee and Thread) is potentially a Matter device or network. Although some current versions of the earlier protocols are not directly compatible with the Matter standard, the current Matter specification includes guidelines for setting up a bridge device that can act as a translator between non-Matter devices and the standard. Based on this assumption, this paper gives an overview of the current state of the art of the Matter specification and summarizes the opportunities that this new technology promises. Furthermore, to date, vendors, companies, and corporations are providing suites of tools for easing the development of Matter solutions in their ecosystems,[3] and those that decide not to allow the users to custom their code, embed it in their integrated development environment the certified Matter SDK in its entirety.[4]

In this context, surveying the available devices and software on the market that are compliant with the Matter protocol is of paramount importance. Such a survey provides a comprehensive understanding of the current technological landscape, identifying existing trends and potential areas for further research and development. By evaluating the range and capabilities of Matter-compliant devices, this survey aims to assist various stakeholders, including researchers, developers, manufacturers, and end-users, in making informed decisions that align with compatibility and efficiency goals. Moreover, this examination contributes to the collective technological understanding, fostering collaboration and innovation within the community. The insights derived from this survey will facilitate connections, inspire new ideas, and significantly impact the future of technology integration.

[2] https://www.smartthings.com/.
[3] https://developers.home.google.com/matter?hl=en.
[4] https://developer.apple.com/apple-home/matter/.

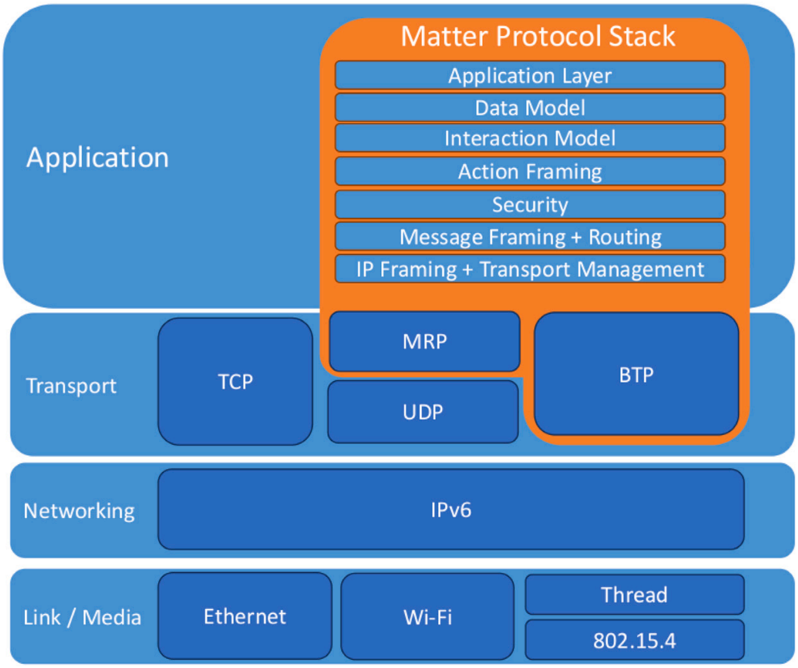

Fig. 2. Matter protocol stack with respect to the higher OSI layers.

In summary, the primary objectives of this work are: (i) to provide a concise yet comprehensive description of the current specifications of the Matter Stack; (ii) to examine the current state of the art in both the market and academic literature; (iii) to offer insights and recommendations on how to address the existing limitations of the framework, thereby facilitating the full adoption of the Matter specification.

The rest of the paper is structured as follows. Section 2 introduces the Matter protocol stack together with the main Matter architecture peculiarities. Section 3 thoroughly analyzes the state of the industry and the compliance with Matter of available IoT devices on the market. Section 4 describes the impact of Matter on the literature, giving insights on how it is currently adopted in research products with its outcomes. Section 5 poses some open questions related to the complete adoption of the Matter protocol stack and how to address those research challenges while Section 6 draws the conclusions.

2. Matter protocol stack

The Matter's protocol stack resides on the application layer as shown in Fig. 2. With respect to a home network device, the application layer contains the high-level contract logic, while the subsequent network stack, in turn, contains the three canonical sub-layers: the transport, the actual network, and the link (media) layer.

The stack standing on the application layer is organized as follows:

- *Data model* - This is where the informative and verbal elements that support the functionalities of the application layer reside. Each time there is a need to interact with a device, the application operates on this data first. As introduced in the Matter white paper (Chapter 7), the data model defines the first-order elements and namespace for endpoints, clusters, attributes, data types, and so on. An element in this context is a data construct that supports a data instance. Elements falls into several categories: first order, cluster first order, nested, dynamic, and semantic.
- *Interaction model* - The client–server interactions between devices are defined in this layer and operate on the elements defined in the first data model. The interaction model defines interactions, transactions, and actions between nodes. The purpose of this layer is to abstract interactions from all the other layers. An interaction is defined as a sequence of transactions, a transaction as a sequence of actions, and an action as a single logical communication established between nodes that are in a one-to-one or one-to-many relationship. One or more messages carry an action. Relationships between devices are established through the synergistic use of data model elements and interactions.
- *System Model and Action Framing* - To code and manage the network transmission process, the action is first defined and then serialized in binary format in this layer before being stored in a given packet. The system model defines the persistent relationships that are established and maintained between endpoints of nodes and clusters. An endpoint is an instance of one or more objects that follow one or more device-type definitions. While clusters are classes of objects instantiated on the endpoint. In short, clusters are the lowest, independent, functional elements of the data model and can be thought of as its

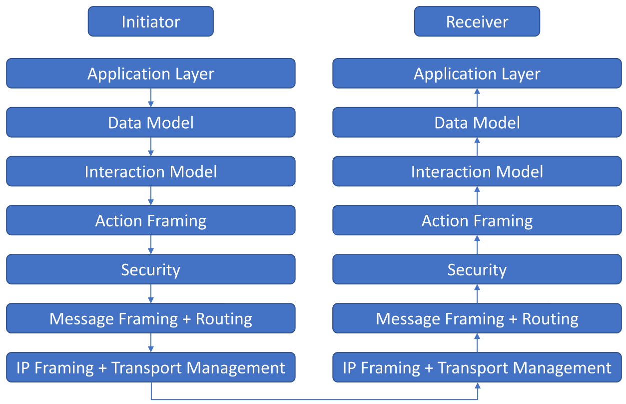

Fig. 3. Message routing from the initiator to the receiver through packing/unpacking layer by layer.

building blocks. Each is defined by a specification that details the mandatory or optional attributes, events, commands, and behaviors that the cluster must guarantee. The Specification defines both the client and server sides as well as their interactions. The network transmission process defines and serializes the action in binary format, which is then secured for storage in a given packet.

- *Security* - The security layer deals with the encryption of the message and its placement in the packet along with an authentication code. The Certificate Authenticated Session Establishment (CASE) provides a way to securely exchange authenticated keys between peers. The authenticity of the manufacturer and the hardware/software state of a device are guaranteed by a series of certificate chains, at the top of which stands the Device Attestation Certificate (DAC). The DAC allows only trusted devices to become part of a Fabric (see Section 4). Each Matter device is enabled with an Operational Node ID with an associated Node Operational Certificate (NOC). The NOC is released during the commissioning process of a device within a Fabric. Operational Node IDs are not permanent and can be removed by either factory or Fabric resets. To protect a Fabric Matter provides a number of security primitives, such as NIST-based elliptic curve cryptography for generating both public keys and digital signatures.
- *Message framing and routing* - Message framing constructs the payload. If necessary, an optional header is added to specify properties and logical routing information. The header field is optional and it is generally used to specify the properties of the message, as well as the routing information.
- *IP framing and transport management* - When the payload is ready to be attached to the packet, the message is sent to the transport layer, TCP or Matter Reliability Protocol (MRP), for IP management.

When an associated device begins to receive data, it moves backward up the protocol stack by performing a reverse of the operations performed for packaging and once delivered to the receiver's application layer, the information is ready to be consumed. Fig. 3 shows both sides (Initiator/Receiver) of the layering architecture as a one-way information flow.

The transport layer of the Matter protocol stack supports the two most common communication and datagram protocols, that is, TCP and UDP; the network layer includes the only IPv6 communication protocol; and the link layer works primarily with Ethernet, Wi-Fi, ZigBee, Thread, and other 802.15.4 standard protocols. As can be seen in Fig. 2, the two main characteristics are the decoupling of the application layer from the underlying layer and the absence of IPv4 in the network layer. In fact, the great ambition of Matter is to define a universal communication protocol based on IPv6, thus ensuring a larger address space with respect to those concurrent protocols that implement the IPv4. However, for the sake of coexistence, Specification 1.0 clarifies that all Matter devices should be tolerant of IPv4 addresses and may ignore them only for the purposes of Matter operations.

Matter does not undertake message profiling, but its message format provides support for several communication paradigms (e.g., unicast secure session, multicast group messaging, session establishment, etc.). Regardless of the type of application, the construction and encoding of messages are always handled by the message layer, which in the Matter protocol stack sits between the action framing and the transport management. Matter messages are used by applications to transmit application-specific data and/or commands. To date, Matter does not allow the definition of standard profiles to handle different application scenarios but leaves their management to communication interfaces (like ZigBee) and network protocols. Therefore, network designers can define heterogeneous network configurations to be adapted to several application domains. At the transport layer, instead, the Protocol introduces a security-enhanced UDP called Matter Reliable Protocol (MRP) and provides a TCP-like layer of connection-oriented data transfer on top of a generic attribute profile, which leverages the Bluetooth Transport Protocol (BTP) to define a Matter-over-BLE interface for device-to-device communication. These two hybrid protocols, represent a trade-off between the traditional TCP and UDP, and can be used in scenarios where there is a need to strike a better balance between time-driven and event-driven communication.

Fig. 4 shows in detail the composition of a Matter message. A Matter message consists of mandatory and optional information. The mandatory information consists of unsigned integer values identifying: the *Message Flags*, which specify the version of the

Header							
[Message Length]	Message Flags	Session ID	Security Flags	Message Counter	[Source Node ID]	[Destination Node ID]	[Message Extensions …]
2 bytes	*1 byte*	*2 bytes*	*1 byte*	*4 bytes*	*0/8 bytes*	*0/2/8 bytes*	*variable length*
Payload							
[Message Payload …] (Encrypted)							
variable length							
Footer							
[Message Integrity Checker]							
variable length							

Fig. 4. Matter Message format.

Matter message format used for the encoding; the *Session ID*, which identifies the keys used to encrypt the message and the integrity algorithm to be used for the encryption; the *Security Flags*, which specifies if the message is encoded with privacy enhancements, if the message is a control message, the presence or absence of the Message Extensions portion with non-zero length, and if the session associated to the message is Unicast or Multicast (Group Session); the *Message Counter*, eventually, uniquely identifies the message from the sending node perspective. The *Message Length*, the *Message Extensions*, the *Message Integrity Checker*, and the *Payload*, as well as the *Source* and *Destination Node ID* are all optional information identified by other unsigned integer values (in Fig. 4, the optional information is shown within square brackets). However, even for optional fields there exist exceptions. For instance, the message length, which indicates the overall length of the message in bytes, is required when transmitting a message over a stream-oriented channel like TCP. For the sake of conciseness, we do not report here details about the Protocol Message format definition, to which we refer to Section 4.4.3 et seq. of the official Matter Specification.[5]

2.1. Networking, data link, and physical layers

Regarding the Network layer, as a pivotal principle, any network that supports IPv6 standard cores is suitable for deploying Matter networks. Standard networks support standard structures, including wireless and/or wired subnetworks, and one or more Low-Power and Lossy subnetworks (LLNs). The most important communication protocols that are in use in the IoT domain are Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Hyper Text Transfer Protocol (HTTP), Advanced Message Queue Protocol (AMQP), and WebSocket. MQTT is a lightweight network protocol based on the publish–subscribe paradigm that allows one-to-many communication through brokering. It is widely used in many IoT sectors, particularly in Home and Building automation [2], smart grid [3], and healthcare [4]. CoAP is a client–server protocol offering a RESTful interface allowing a client node to directly command other nodes. CoAP solutions have been widely adopted in sensor networks for the Healthcare domain [5]. AMQP is a message-oriented application layer protocol that, like MQTT, leverages the publish–subscribe paradigm. Because of its peculiarities, it is usually employed for application-to-application integration at the enterprise level, even if some research efforts propose some AMQP-based network solutions in the Internet of Medical Things domain [6]. WebSocket is a protocol that has applications in various areas. Among the IT domain, WebSocket has also been tested to support smart home applications [7].

As the Link/Media layer, the current Matter specification supports three main protocols: Ethernet, Wi-Fi, and Thread. Thread is the default Matter LLN; it is an open, IPv6-based networking protocol designed specifically for the Internet of Things (IoT) and, in full, for home automation systems. It includes a low-power technology for mesh networks, where infrastructure nodes connect directly and dynamically to as many nodes as possible. Nodes cooperate with each other to efficiently route data through the network in a controlled flood. Like ZigBee, also the Thread protocol uses the IEEE 802.15.4 PHY and MAC (Media Access Control) layers operating at 250 kbps in the 2.4 GHz band for link layer communication. While under the application layer, the three main networking features of Thread are: UDP, IP routing, and the IPv6 over Low power Wireless Personal Area Networks (6LoWPAN). Many IPv6 subnets can be interconnected through backbone border routers, thus unifying multiple Thread networks and enabling a wider interconnection between Thread devices. The Thread Group recently published a white paper detailing the capabilities of the Border Router [8]. Another white paper from the Thread Group briefly outlines the benefits that the unified Matter standard combined with Thread can bring to Smart Buildings [9]. The main benefit emphasized is the use of the same technology in different environments, which reflects a major advantage in economies of scale, an increase in component capacity, a decrease in product prices, and an ever-widening choice of manufacturing sources from different suppliers.

A single Thread network should be able to manage approximately 250 devices. Fig. 5, which is an integrated picture of the latest version of the Thread white paper,[6] shows an overview of the current Thread stack. Thread is a royalty-free standard, but

[5] https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf.

[6] The Thread specification can be downloaded, previous request, at the following link https://www.threadgroup.org/ThreadSpec.

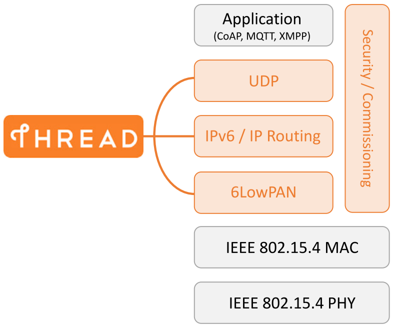

Fig. 5. Overview of the Thread stack as introduced in the Specification 1.1.1.

its documentation is closed. In response to this limitation, Nest Labs (by Google) has developed and released an open-source implementation called OpenThread. OpenThread implements all of the features presented in the official Thread Specification, defining an IPv6-based, low-power, trusted, and reliable communication protocol for consumer and commercial applications. Once a Thread device has discovered all networks in range, it can either attach to an existing network or create a new one if no networks are discovered.

Three unique identifiers spot a Thread network: a 2-byte Personal Area Network ID (PAN ID); an 8-byte eXtended Personal Area Network ID (XPAN ID); a human-readable Network Name. When creating or searching for an existing Thread network, the device performs the following two steps for each channel: an active scan for 802.15.4 networks in range, and broadcasting an 802.15.4 Beacon Request on a specific channel. Any routers or end devices eligible as routers in range broadcast a beacon containing their Thread network PAN ID, XPAN ID, and network name in response. The device repeats the previous two steps for each channel. Thread uses the Mesh Link Establishment (MLE) protocol to configure links and spread information about the network to third-party Thread devices. MLE operates below the routing layer and extends the capabilities of 802.15.4. It allows network devices to dynamically configure and secure wireless links, as well as allow network-wide changes to shared radio parameters and determine radio link quality prior to configuration. Note that MLE occurs only after a Thread device obtains Thread network credentials through Thread commissioning. Devices using Thread/802.15.4 networking technology must also support BLE for discovery and commissioning operations.

Thread is a key component of a Matter network because it uses a Zigbee-like, low-power, IP-based communication protocol. Zigbee-like means that Thread uses the same frequency as Zigbee, allowing in this way very low-power Matter-enabled end devices to communicate with each other. Like ZigBee, Thread is managed by the CSA with the goal of standardizing the smart home industry and ensuring full interoperability among Matter devices.[7] It has been extensively studied in the literature: Kim et al. [10] provided a comparative analysis between the Routing Protocol for Low-Power and Lossy Networks (RPL) and Thread, focusing on their respective technical aspects. Authors put in evidence affinities, divergences, and lacks in the two protocol performance in terms of scalability, reliability, and resource/energy efficiency. A comprehensive description of the Thread Architecture in terms of topology, routing, stack, and security considerations can be found in [11]. As highlighted in [12], Thread is an IP-based wireless standard that enables Thread devices to connect to the “cloud” and thus communicate with devices via the Internet Protocol.[8] Devices in a Thread network are connected with each other in a self-organizing mesh network, and multiple mesh networks can furthermore be connected with each other.

The protocol underlying Thread/ZigBee follows the IEEE 802.15.4 standard and specifies both the physical (PHY) and the Medium Access Control (MAC) layer for low-power wireless private area networks. It provides operability on different platforms, along with reliable and scalable communication with a high level of security and service authentication. IEEE 802.15.4 utilizes a direct sequence spread spectrum and supports three frequency channel bands (i.e., 250 kbps at 2.4 GHz, 40 kbps at 915 MHz, and 20 kbps at 868 MHz). IEEE 802.15.4 MAC utilizes the CSMA/CA protocol to reduce the likelihood of packet collisions and supports full- and reduced-function devices [13]. The standard topologies for IEEE 802.15.4, and in full Thread/ZigBee, are star, mesh (P2P), and tree. However, we must point out that Matter is agnostic to what is happening at the network, data link, and physical layers. It can ensure compatibility with all underlying technologies, but at the same time, it is subject to network performance that depends on the specifications of the technology in use in the different physical/datalink/network layers. It follows that in a Thread network, for example, the performance of Matter is contingent on the IEEE 802.15.4 payload length, 2.4 GHz band, 127 bytes frame at the PHY, Beacon or non-Beacon Mode at the MAC, and a link quality that depends on the strength of the link margin on incoming messages from the neighboring devices. While in an Ethernet network, the performance will vary depending on the category of physical infrastructure the network is composed of and its specifications. For those interested in a deep discussion on the topic, we refer to Kassab et al. [14], who surveyed architectures, applications, and future perspectives for IoT, comparing protocols at

[7] https://csa-iot.org/all-solutions/matter/.
[8] https://www.threadgroup.org/What-is-Thread/Overview.

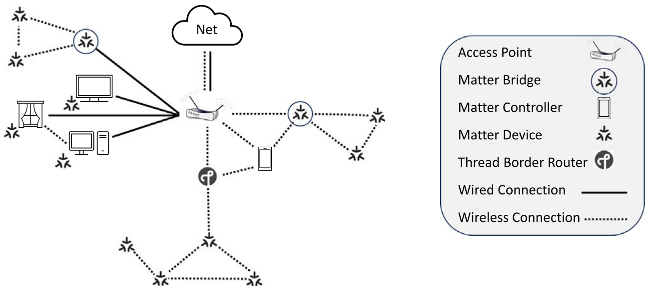

Fig. 6. An example of Matter network topology.

different OSI layers, and evaluating the pros and cons for their application in several scenarios (like home and building automation, agriculture, medical and healthcare, and smart grid).

As a final note on topology, Matter treats networks as shared resources, without considering the exclusive ownership of the network or its access. As a result, the protocol allows multiple Matter networks to overlap over the same set of network IPs. Being able to operate in the absence of a global IPv6 routing infrastructure, a Matter network works with complete autonomy and security from the global network. Because of this feature, a Matter network can operate even if the Internet Service Provider (ISP) does not support IPv6, or if such support is very limited (e.g. if addresses cannot cover all the networks and devices of the entire Matter network).

The protocol supports local communications over one or more IPv6 subnetworks. The current version of the specification considers two kinds of network topologies: single and multiple peripheral networks. In a single network topology, be it wireless or wired, the sole logical network connects all the devices. Canonical single-network topologies are star networks, mesh networks, ring networks, tree networks, and bus networks.

In the context of Matter, the main geometric models that aim to represent both physical and logical connectivity relationships between nodes are basically the star network topology and the mesh network topology, regardless of whether we are dealing with a single or multiple network. In a single network topology, all nodes are logically connected to a single Access Point (AP). A multiple or hybrid network topology is a combination of two or more single network topologies. Network segmentation is allowed for both wired and wireless configurations as long as they are bridged at the link layer. Here are some details about the three main network topology configurations mentioned above:

- *Star Network* - This topology is characterized by many child nodes connected to a common central parent node. The parent, which can be a hub or a switch (but always an access point), is responsible for managing all network functions, but most importantly for routing messages sent from one node to another. Child nodes can form peripheral networks themselves, but such networks must always connect directly to the central parent through one or more border routers implementing the Matter protocol. Border routers must meet a number of requirements, including address and route allocation, advertising, multicast support, and proxy discovery.
- *Tree Network* - This topology consists of a root node, which plays the role of coordinator, and child, sibling, and leaf nodes as routers and end devices. The standard wired solution considers the tree topology as a hybrid configuration, where routers are connected by buses, which is why it is also defined as a star-bus topology. The wireless solution, as adopted in ZigBee, considers a Personal Area Network (PAN) coordinator to which both routers and end devices are connected. In this type of topology, routers extend the network coverage and, equipped with the full set of MAC layer functionalities, they can play the dual role of subnetwork coordinator and end device.
- *Mesh Network* - all nodes are (potentially) connected to each other, so they can be reached in a single step. The main advantage over any other type of network topology is maximum fault tolerance. In a mesh network, if for some reason the direct link between two nodes fails, those nodes may still be able to communicate because of the link redundancy provided by third-party network nodes. In other words, there is always an alternative route to reach a given node, unless that node is completely disconnected from the others. A mesh network can be partially or fully interconnected. Mesh topology is in contrast to traditional star and tree local area network structures, where infrastructure nodes (switches and/or bridges) are directly interconnected in a limited subset.

Fig. 6 shows an example of a Matter network topology. The main Matter network components are those that allow the end user to manage all network devices and those that bridge all the sub-networks (be they Thread, Zigbee, Z-wave, or others) to the same root. The toy topology example also includes a Thread Border Router, an entity specifically designed for Thread mesh networks, as an alternative connection node that can be used instead of a generic Matter Bridge. The Matter Controller can exchange information directly with bridge nodes or the access point. In fact, a unique feature of Matter is that it allows the interconnection and the management of home network devices without necessarily relying on the global network.

2.2. Fabric

A Fabric in a Matter network is a set of nodes that interact with each other by accessing the elements of the data model as defined by the interaction model. Everything in a Matter network is organized into Fabrics, and a Fabric is a Matter network itself. All the nodes within a Fabric share a safety root, simply called Certificate Authority (CA), and a common distributed configuration state. More specifically, a Fabric is a safety domain that enables the identification of a set of nodes and communication links within their own context. A network node that is identified by a Fabric can interact with other nodes belonging to the same Fabric or different ones. An accessing fabric is a Fabric with at least one interaction. If a Fabric is supported by a node, it must be uniquely identified by a Fabric ID (or Fabric Index), which is a 64-bit number that uniquely identifies the Fabric within the scope of a given Root CA. When a Fabric is identified by an index, that index enables the lookup of information about the given Fabric. Conceptually, the Fabric ID is contained in a tuple, associated with the Root CA's public key. Since it is not the goal of this study, we do not go into the details of the establishment of a secure session between Matter nodes, for which we refer interested parties to Section 4.13 of the official Matter Specification.

A node, whether a Controller, Bridge, Border Router, or Terminal, is an instance of a Matter device available on an IP network within the Fabric. A Matter Node is a physical device or a logical instance that represents an addressable, unique resource with a set of functions and capabilities. The node is composed of services or virtual devices with properties called endpoints, each represented by a *device type* field, describing the semantic part of the communication architecture. The Matter node must possess at least hardware and firmware requirements to be recognized to other devices, and no additional functionality is required to be part of a Matter network. In concrete terms, Matter nodes are devices like plugs, switches, or refrigerators, and any one of them can potentially become a Matter Controller. A Matter *Controller* is a special device that enables the remote access of all Matter devices in the network. It is a Matter device itself, also possessing the capability to bridge the local network with the global one. The Matter Controller can discover both IPv6 addresses and ports for an already known Matter node and send commands to the appropriate clusters on one or more endpoints on the bridge node. The latter serves to allow the use of non-Matter IoT devices (e.g. devices on a Z-Wave network) in a Matter Fabric, with the goal to enable the consumer to keep using these non-Matter devices together with their Matter devices. A Matter *Bridge* enables non-Matter devices to be used by the Controller. In other words, a non-Matter device becomes compatible with Matter devices through the Bridge, which represents and enables the non-Matter nodes to communicate with the rest of the network entities. The Bridge is a hub and acts as an interpreter for the bridged devices, advertising them as Matter devices to the user interface. It can receive status, events, or commands from sensors or third-party devices and convert them from the native protocol of the non-Matter devices towards Matter protocol and vice versa. It also provides control of the bridged and Matter devices and is responsible for securing and certifying the communication link to each end device. Because of these peculiarities, the Bridge owns information on the network topology or logical grouping (and associated naming).

The primary responsibility of a Bridge is to ensure seamless interoperability between devices and provide a consistent user experience during the commissioning process. The commissioning process involves the integration of a device into a Fabric, essentially exposing the cluster that comprises third-party devices to the Fabric itself. This is achieved by designating one of these third-party devices as an "aggregator". The aggregator is equipped with a descriptor detailing all the endpoints (i.e., instances, services, or virtual devices) associated with the cluster and a parts list that contains information about each device within the ecosystem. In this vest, the aggregator can be interpreted as a Controller node of a non-Fabric ecosystem.

In the case of bridged devices acting as actuators (i.e., the Matter Controller is sending them commands), a Controller within the Fabric sends instructions to the associated cluster, which may be located on one or more endpoints on the Bridge. For example, it may send the command On to the On/Off cluster of a bridged device. The Bridge then manages the conversion between the Matter protocol and the native protocol of the non-Matter device, ensuring in this way the correct relay of the command to the relevant bridged device. *Vice versa*, in the case of bridged devices acting as sensors and switches (i.e., the Matter Controller receives from them messages), the Bridge is responsible for receiving updates in the form of values, events, or commands. After converting these data from the native protocol of the non-Matter devices to the Matter protocol, the Bridge represents them as attributes, events, or commands in the appropriate clusters on the associated endpoints. Interactions with these attributes, events, or commands on the Matter side, for example, when communicating with a Controller using the data from the sensor or switch, should ideally mirror interactions with the corresponding attributes, events, or commands in native Matter sensors and switches.

In addition to Controller, Bridge, and network terminal nodes, the other main type of node in a Matter architecture is the Border Router. A *Border Router* is a device that connects a Matter network to other IP-based networks. It is an entity specifically designed for Thread networks and in Matter is considered a Bridge itself. As introduced in the official Open Thread guidelines, for being a Border Router the device must at least support the following functions:

- Bidirectional IP connectivity between Thread and Wi-Fi/Ethernet networks.
- Bidirectional service discovery via mDNS (on Wi-Fi/Ethernet link) and SRP (on Thread network).
- Thread-over-infrastructure that merges Thread partitions over IP-based links.
- External Thread Commissioning (e.g., a mobile) to authenticate and join a Thread device to a Thread network.

Concisely, a Matter/Thread Border Router is an Edge Router that provides routing services between two IPv6 subnetworks, being them two hub networks or, more frequently, a hub network and a peripheral one.

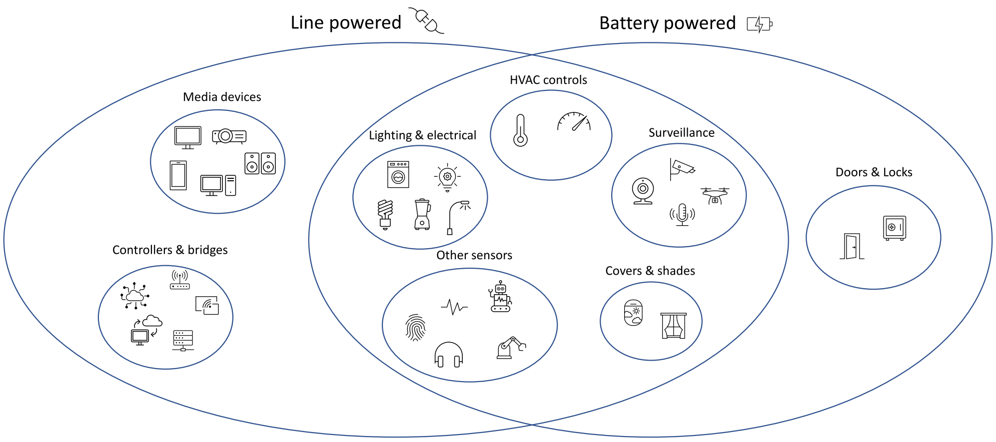

Fig. 7. Representation of the main families of devices supported by Matter 1.0.

3. Devices on the Market

Specification 1.0 includes a Device Library document that introduces the main modules managed by Matter, which are subdivided into Utility and Application categories. Each category contains a list of related modules. The Utility group comprises root nodes, power sources, Over-the-Air (OTA) requestors, OTA providers, aggregators, and bridged nodes. The Application subset, instead, comprehends:

- *lighting* - On/Off lights, dimmable lights, color temperature lights, and extended color lights;
- *smart plugs/outlets* - On/Off plug-in units, dimmable plug-in units and pumps;
- *switches and controls* - On/Off light switches, dimmer switches, color dimmer switches, control bridges, pump controllers, and generic switches.
- *sensors* - contact sensors, light sensors, occupancy sensors, temperature sensors, pressure sensors, flow sensors, humidity sensors and On/Off sensors;
- *closures* - door locks and door lock controllers, window coverings and window covering controllers;
- *HVACs* - heating/cooling units, thermostats and fans;
- *media* - basic video players, casting video players, speakers, content apps, casting video clients, video remote controls.

As of now, the range of devices currently available on the market, as well as those that comply with Matter Specification 1.0 and are being marketed, includes both line-powered and battery-powered devices. Each device is equipped with at least one of the communication interfaces required by the protocol. The primary categories of line-powered devices include lighting systems, plugs, media and mobile devices, bridges, and controllers. On the other hand, the main categories of battery-powered devices encompass HVAC systems, locks, shutters, roller blinds, and a variety of other sensors (e.g., scales, pressure, temperature, etc.). Line-powered devices can be further classified into two subcategories based on their network infrastructure membership (e.g., platforms, mesh extenders, border routers, home gateways, etc.) and the role played by the specific component (e.g., commissioner, controller, or bridge). Fig. 7 provides a summary representation of the device family sets supported by the Specification.

Coinciding with the release of the specification, reputable electronics retailers are introducing Matter-compatible boards, IoT development kits, and controllers to the market. These tools allow for the physical configuration of prototypical Matter-based device networks for testing purposes. Notable examples include the Silicon Labs Sparkfun Things Plus Matter MGM240P board[9] and various EFR32xG24 Development Kits.[10] Simultaneously, test labs have been made available to all vendors interested in developing Matter-certified products and solutions. Examples include Allions[11] and Eurofins Digital Testing by Resillion,[12] among others. To facilitate the development of these solutions, the CSA has provided reference open-source implementations and guidelines for updating the software of Matter products that meet the minimal hardware resource requirements.

In line with this, some partners have already made their code open source for developers, such as the Unify SDK by Silicon Labs[13] and OpenThread from Nest Labs by Google.[14] Recently, the CSA began issuing certification IDs for devices that comply with the Specification.

9 https://learn.sparkfun.com/tutorials/sparkfun-thing-plus-matter---mgm240p-hookup-guide.
10 https://www.silabs.com/development-tools/wireless/efr32xg24-pro-kit-10-dbm.
11 https://www.allion.com/certification/matter/.
12 https://www.eurofins-digitaltesting.com/.
13 https://www.silabs.com/developers/unify-sdk.
14 https://openthread.io/.

In this context, we conducted a survey of devices that currently conform to the specification, based on the list provided by the Standard Alliance. We considered devices that are currently certified, those that meet the requirements even if not certified, and those for which a software update has been provided.

We present our findings in three tables:

- Table 1 lists devices currently on the market and those about to be introduced;
- Table 2 details boards, bridges, gateways, hubs, and SoCs;
- Table 3 provides information on certified software.

Specifically, Tables 1 and 2 encompass the majority of certified/compatible Matter products currently available or soon to be released. Both tables are categorized based on device types, distinguishing between devices on the market and boards, bridges, controllers, etc. Each table includes the device Name, Manufacturer, Category, Wireless Protocols, and general Notes about the product's positive and/or negative features, along with its certificate ID. The device categories listed in Table 1 include air conditioners, contact sensors, curtains, lights, locks, motion sensors, plugs, smart TVs, switches, thermostats, and wireless modules (i.e., antennas). The light category encompasses bulbs, LEDs, and strips.

Note that some devices in both tables are listed without Matter certification. This is primarily due to two reasons: (i) some devices were already on the market before the first Specification was published and, meeting the requirements, manufacturers provided an upgrade to comply with the Matter protocol; (ii) some devices were already on the market, and neither the company provided information about the certificate ID (except to declare them as Matter devices), nor do the products appear on the current CSA's list of Matter-certified products.

Table 3 shows the current Matter-certified software. This table shares the columns Name, Manufacturer, Category, and Notes with the previous tables. Here, 'Name' includes both the device's name and the software it runs. The 'Wireless Protocol' field from Tables 1 and 2 is replaced with 'Firmware/Hardware' in this table, detailing the current version of the certified software product and the hardware it was developed for. As before, the 'Notes' field provides a brief description of the software along with its certificate ID. We chose to provide the full certificate ID, where possible, to facilitate readers in retrieving product detail sheets.

Please note that in all tables, some device names and certificate IDs are followed by an asterisk. The former indicates that multiple codes are associated with the given device name, while the latter signifies the presence of multiple certificate IDs associated with the same product from the same manufacturer. As for our selection criteria, we have omitted devices with inconsistent descriptions and those lacking requirement specifications from the complete list of certified products on the official site.

It is also worth noting that, to date, major manufacturers of home automation devices have not begun the certification process for their future commercial products. Instead, they have ensured partial compatibility for the products they have already launched. For instance, Matter-certified coordinators like Apple TV 4K, HomePod (2nd gen), Google Nest Hub V2, and many other devices that act as Bridges for third-party devices in a Matter network, have been upgraded to be compatible with a limited subset of components (e.g., HomeKit- or Matter-enabled Thread accessories only). This restricts full interoperability between different kinds of ecosystems.

All tables are sorted alphabetically by category and device name to facilitate comparison between similar products from different manufacturers.

Lastly, many products were already available before the release of the first Specification and became Matter-compliant through software upgrades. Compiling a complete list of these products is difficult, as the CSA has not yet established a section specifically for Matter-compliant products that predate the initial Specification. Consequently, these products are not included in the tables mentioned earlier. However, these tables merely represent the products that first achieved certification. The number of Matter-certified products, whether already on the market or forthcoming, continues to grow daily.

3.1. The Matter certification process

A product developer wishing to start the Matter certification process for its products can obtain a Vendor ID and a Product ID (i.e., codes that uniquely identify the vendor and its products) by joining the Alliance as an Adopter, Participant, or Promoter. This step requires the payment of an annual fee but is not mandatory. Those who do not wish to join the Alliance can still obtain the certification for their products by taking advantage of the Certification Transfer Program (CTP) as an Associate. The profile of an Associate does not require a subscription fee, but the certification process is not cost-free, and the subject must pay a one-time fee for each product he wishes to certify, in addition to a reduced annual fee to keep the certification active.

The certification process is carried out by the product developer through a CSA web tool. To be sure that the device on the cusp of being certified meets the required standards, the owner must produce the following documentation:

- Declaration of Conformity
- Protocol Implementation Conformance Statement (PICS)
- Final Test Report
- Dependent Transport Attestation
- Security Attestation

The Declaration of Conformity reports that the product has passed a conformity assessment with respect to the properties declared by the product developer. The PICS is a structured document detailing the requirements met by implementing the Protocol. The Final Test Report provides feedback on the overall state of the device to be marketed. The Dependent Transport Attestation confirms that

Table 1
Devices on the market.

Name	Manufacturer	Category	Wireless protocol	Notes
Haier air conditioner	Qingdao Haier Technology Co., Ltd.	Air Conditioner	Wi-Fi	Haier KFR-35GW/17EAA81U1 realizes ultra-wide Angle air supply. Energy efficiency value up to 5.28. Certificate ID: CSA22076MAT40076-24
Midea window air Conditioner	GD Midea Air-Conditioning Equipment Co., Ltd.	Air Conditioner	Wi-Fi	Provided with the MideaAir app on iOS or Android. Certificate ID: CSA22074MAT40074-24
Door window sensor	Tuya Global Inc.	Contact Sensor	Wi-Fi, Bluetooth	Monitor the opening and closing of doors and windows in real time. Certificate ID: CSA23398MAT40911-24
Eve door & Window	Eve Systems	Contact Sensor	Thread, BLE	Works with Apple HomeKit, Samsung SmartThings, Amazon Alexa and Google Home. Certificate ID: CSA22068MAT40068-24 *
Door and window sensor P2	Lumi United Technology Co., Ltd.	Contact Sensor	ZigBee	To date Aquara Hub is required. The associate App supports multiple platforms. Certificate ID: CSA22085MAT40085-24
Netatmo (2-in-1) smart security sensor	LEGRAND	Contact Sensor	Thread, Bluetooth	The sensor exclusively works with the Netatmo Smart camera. Certificate ID: CSA23163MAT40676-24 *
Smart door sensor	Shenzhen Heiman Technology Co., Ltd.	Contact Sensor	Z-Wave, Wi-Fi 802.11b/g/n 2.4 GHz	DC 3 V voltage, alarm current ≤ 30 mA, detection range >20 mm. Certificate ID: CSA23157MAT40670-24
Matter roller motor	Zemismart Technology Limited	Curtain	Wi-Fi	Wi-Fi roller motor for 36–38 mm tube; wiring required. Certificate ID: CSA23099MAT40612-24
MOTOR CM-03-E for roller blinds	Eve Systems	Curtain	Thread, BLE	MOTOR CM-03-E for Roller Blinds. Built-in rechargeable battery (USB-C). Certificate ID: CSA22221MAT40221-24
MT01 slide curtain	Zemismart Technology Limited	Curtain	Thread	It supports open,. close, stop, percent control and so on. Certificate ID: CSA23162MAT40675-24
LC 35/24V MTR SC PRE2	Zumbotel Group AG	Led Converter	Thread, Bluetooth	Dimmable driver LED, constant voltage 24 V. Thread Border Router required (e.g., Apple HomePod mini or Google NestHub). Certificate ID: CSA23171MAT40684-24 *
LED converter MTR	Zumbotel Group AG	Led Converter	Thread, Bluetooth	Dimmable driver LED, constant voltage 24 V. Available in 35 W, 60 W, 100 W, 150 W. Thread Border Router required (e.g., Apple HomePod mini or Google NestHub). Certificate ID: CSA23399MAT40912-24 *
Cync full color (Direct connect LED) A19	Savant Company	Light	Wi-Fi	Works with iOS 13 (and above) and Android 9 (and above). Certificate ID: CSA23180MAT40693-24 *
Groove LED strip light	Shenzhen Qianyan Technology Ltd.	Light	Wi-Fi, Bluetooth	Certificate ID: CSA22180MAT40180-24 *
Groove neon light	Shenzhen Qianyan Technology Ltd.	Light	Wi-Fi, Bluetooth	Neon Strip Light. Certificate ID: CSA23540MAT41053-24 *
Groove string light 0x703*	Shenzhen Qianyan Technology Ltd.	Light	Wi-Fi, Bluetooth	50ft LED bulb string light with 15 bulbs. Waterproof level IP65. Certificate ID: CSA23558MAT41071-24 *
Groove wall light	Shenzhen Qianyan Technology Ltd.	Light	Wi-Fi, Bluetooth	LED string wall light. Certificate ID: CSA23554MAT41067-24 *
Infineon thread light bulb	Infineon Technologies AG	Light	Thread	Light bulb over Thread on CYW30739A0. Certificate ID: CSA22471MAT40471-24
Motion and light sensor P2	Lumi United Technology Co., Ltd.	Light	Zigbee	To date Aquara Hub is required. The associate App supports multiple platforms. Certificate ID: CSA22084MAT40084-24
Nanoleaf essentials lightstrip	Nanoleaf	Light	Thread, Bluetooth	Work with major smart home platforms but do not support Apple's adaptive lighting. Certificate ID: CSA22087MAT40087-24 *
Sengled multicolor A19 bulb	Sengled Co., Ltd.	Light	Wi-Fi, Zigbee	Works with iOS 13 (and above) and Android 9 (and above). Certificate ID: CSA23113MAT40626-24 *
Smart color night light	Jiangsu Shushi Technology Co., Ltd.	Light	Wi-Fi, BLE	Build-in Motion and Light Sensor. Compatible with Apple HomePod, Google Nest Hub and Amazon Echo V4. Certificate ID: CSA23158MAT40671-24

(*continued on next page*)

Table 1 (*continued*).

Smart color night light	ubisystechnologies GmbH	Light	ZigBee	Certificate ID: CSA23145MAT40658-24
Smart wall lamp	Shenzhen Orvibo Electronics Co., Ltd.	Light	...	Certificate ID: CSA22104MAT40104-24
UA-RGBCW bulb	Uascent Technology Company Limited	Light	Wi-Fi	Range of 16 million colors and tunable white. Certificate ID: CSA23205MAT40718-24 *
Wall sconces	Shenzhen Qianyan Technology Ltd.	Light	Wi-Fi, Bluetooth	The product is made up of six RGBW wall sconces. Certificate ID: CSA23551MAT41064-24
Wi-Fi extended color light	Tuya Global Inc.	Light	Wi-Fi, Bluetooth	Support on/off, brightness control, col7or temperature control and color control, timer, schedule, music sync, and scene. Certificate ID: CSA23362MAT40875-24 *
WiZ LED luminaire - Full color	Signify	Light	Thread, Bluetooth	Dimmable lights scheduled brightness level via app or voice. Certificate ID: CSA23119MAT40632-24 *
WiZ LED luminaire dimmable	Signify	Light	Thread, Bluetooth	The device provides dimmable white lights scheduled brightness level via app or voice. Certificate ID: CSA23287MAT40800-24 *
WiZ LED lamp - Full color	Signify	Light	Thread, Bluetooth	The device provides dimmable white lights scheduled brightness level via app or voice. Certificate ID: CSA22208MAT40208-24 *
WiZ LED luminaire tunable white	Signify	Light	Thread, Bluetooth	Dimmable lights scheduled brightness level via app or voice. Certificate ID: CSA23095MAT40608-24 *
WiZ outdoor LED Strip - Full color	Signify	Light	Thread, Bluetooth	Dimmable lights scheduled brightness level via app or voice. Certificate ID: CSA23409MAT40922-24 *
Zemismart bulb	Zemismart Technology Limited	Light	Wi-Fi	Dimmerable, RGB Bulb E27. Compatible with any app certified by Matter. Certificate ID: CCSA23291MAT40804-24
Zemismart downlight	Zemismart Technology Limited	Light	Wi-Fi	Dimmerable. Compatible with any app certified by Matter. Certificate ID: CSA23292MAT40805-24
Thread door lock	Infineon Technologies AG	Lock	Thread	Certificate ID: CSA22474MAT40474-24
Yale matter smart module	Assa Abloy AB	Lock	Bluetooth	Matter Smart Module Upgrade for Yale Assure Lock. Certificate ID: CSA22465MAT40465-24
Eve motion	Eve Systems	Motion Sensor	Thread, BLE	Time & duration statistics, Rules, Adjust motion sensitivity & duration, firmware updates and many other functionalities are not available for third-party apps. Certificate ID: CSA23276MAT40789-24 *
Smart motion sensor	Shenzhen Heiman Technology Co., Ltd.	Motion Sensor	Z-Wave, Wi-Fi 802.11b/g/n 2.4 GHz	Certificate ID: CSA22153MAT40153-24
Cync indoor (Smart) plug	Savant Company	Plug	Wi-Fi (2.4 GHz), BLE	Works with iOS 13 (and above) and Android 9 (and above). Certificate ID: CSA23179MAT40692-24 *
EcoFlow smart plug	EcoFlow Inc.	Plug	Thread, BLE	The smart plug is specially designed by EcoFlow to work with the EcoFlow micro inverter seamlessly. Certificate ID: CSA23435MAT40948-24
Eve energy	Eve Systems	Plug	Thread, BLE	Input/Output: AC 120 V, 60 Hz, max. 15 A/1800 W. Certificate ID: CSA22064MAT40064-24 *
HooRii smart plug	HooRii Technology Co., Ltd.	Plug	Thread, Bluetooth	Certificate ID: CSA23159MAT40672-24
Kasa smart outdoor plug	TP-Link Corporation Limited	Plug	Wi-Fi, Bluetooth	Individual control two outdoor devices, Wi-Fi range up to 300 ft, Voice Control, Auto-off Timer, Away Mode. Certificate ID: CSA23176MAT40689-24
Smart plug mini	Chengdu Meross Technology Co., Ltd.	Plug	Wi-Fi (2.4 GHz), Bluetooth	MSS115 and MSS315 codes respectively stand for the EU and US/CA version of the product. Certificate ID: CSA22335MAT40335-24 *
Smart plug	Leedarson IoT Technology Inc.	Plug	Wi-Fi or ZigBee	Certificate ID: CSA23494MAT41007-24 *
Smart plug	Schneider Electric	Plug	Wi-Fi	A Wi-Fi Smart Plug which can be used for loads attaching, then switching loads on or off. Certificate ID: CSA22072MAT40072-24

(*continued on next page*)

Table 1 (*continued*).

Smart plug	Shenzhen NEO Electronics Co. Ltd.	Plug	IEEE 802.11b/g/n, ZigBee 3.0	A Smart socket based on Wi-Fi2.4G to control 220 V output. Certificate ID: CSA23408MAT40921-24
Tapo (Mini) plug	TP-Link Corporation Limited	Plug	Wi-Fi, Bluetooth	Works with Alexa, Google Home, SmartThings & IFTTT. Auto-off Timer, Compact Design and Away Mode. Certificate ID: CSA22165MAT40165-24
Tapo smart plug, Energy monitoring 0x010*	TP-Link Corporation Limited	Plug	Wi-Fi, Bluetooth	Smart Home Wi-Fi Plug, Energy Monitoring, Voice Control, Auto-off Timer, Away Mode. Certificate ID: CSA23542MAT41055-24 *
Tapo smart Wi-Fi outlet extender	TP-Link Corporation Limited	Plug	Wi-Fi, Bluetooth	9 in 1 (3 individually controlled smart outlet, 3 always on outlets, 1 USB-C, 2 USB-A fast charging ports). Certificate ID: CSA23583MAT41096-24
UA-SmartPlug	Uascent Technology Company Limited	Plug	Wi-Fi, Bluetooth	Certificate ID: CSA23275MAT40788-24 *
Wi-Fi plug	Tuya Global Inc.	Plug	Wi-Fi	Support remote switch and power-on state setting. On/Off Led notification status. Certificate ID: CSA22049MAT40049-24
Wi-Fi plug On/Off 0x200*	Espressif Systems Co., Ltd.	Plug	Wi-Fi, BLE	A Wi-Fi Plug implementation based on the ESP32-C2 SoC and Espressif's Matter SDK. Certificate ID: CSA23565MAT41078-24 *
55SD111-NA	Shenzhen TCL	Smart TV	Wi-Fi 6, Ethernet, Bluetooth	4K QLED Smart TV. Certificate ID: CSA23169MAT40682-00
D215S	Leviton manufacturing company	Switch	Wi-Fi 802.11 a/b/g/n 2.4 GHz, Bluetooth 5.0	DECORA Smart Wi-Fi (2nd gen) 15 A switch. Support for multiple platforms (IFTTT, Apple Home, Amazon Alexa, My Leviton, Hey Google, Schlage. Certificate ID: CSA23178MAT40691-24
D23LP	Leviton manufacturing company	Switch	Wi-Fi 802.11 a/b/g/n 2.4 GHz, Bluetooth 5.0	The DECORA Smart Wi-Fi (2nd gen) 600 W is a dimmerable light switch that works with my leviton, Apple Home, Hey Google, Alexa, IFTTT, Schlage. Certificate ID: CSA23581MAT41094-24
D26HD	Leviton manufacturing company	Switch	Wi-Fi 802.11 a/b/g/n 2.4 GHz, Bluetooth 5.0	Dimmer switch that works with Google Assistant, Apple Home, vera, Amazon Alexa, iOS, Android. Certificate ID: CSA23177MAT40690-24
LY-MW series	Longan Link Tech Co., Ltd.	Switch	Wi-Fi	Window Motor based on Wi-Fi 4. Certificate ID: CSA23458MAT40971-24 *
LY-switch-WIFI4-NL	Longan Link Tech Co., Ltd.	Switch	Wi-Fi	Generic switch based on Wi-Fi 4. Certificate ID: CSA23147MAT40660-24 *
Mixpad D1 (digital mixing console)	Shenzhen Orvibo Electronics Co., Ltd.	Switch	2.4 GHz Wi-Fi, Bluetooth 4.2	Smart Dimmer Switch with Touchscreen, ORVIBO Single Pole & 3 Way Wi-Fi Dimmable Light Switches, Neutral Wire Required. Certificate ID: CSA23557MAT41070-24 *
Smart dimmer switch	Leedarson IoT Technology Inc.	Switch	Wi-Fi	Certificate ID: CSA23450MAT40963-24 *
Smart dimmer switch	Shenzhen Orvibo Electronics Co., Ltd.	Switch	Wi-Fi	ORVIBO Smart Dimmer Switch, Single Pole, WiFi, With Wall Mount, Neutral Wire Required. Certificate ID: CSA22105MAT40105-24
Smart Plug-in unit	Shenzhen CoolKit Technology Co., Ltd.	Switch	Wi-Fi, Bluetooth	Certificate ID: CSA23192MAT40705-24 *
Smart Plug-in unit	Shenzhen Sonoff Technologies Co., Ltd.	Switch	Wi-Fi, Bluetooth	Certificate ID: CSA23293MAT40806-24
Smart Plug-in unit	Zhongshan QIHANG Electronic Technology Co.	Switch	Wi-Fi, Bluetooth	Certificate ID: CSA23556MAT41069-24
Wi-Fi Switch On/Off	Espressif Systems Co., Ltd.	Switch	Wi-Fi, BLE	A Wi-Fi Light Switch implementation based on the ESP32-C3 SoC and Espressif's Matter SDK. Transmit power of up to +21 dBm. Certificate ID: CSA23161MAT40674-24

(*continued on next page*)

Table 1 (*continued*).

Wireless module MTR	Zumbotel Group AG	Switch	Thread, Bluetooth	Wireless Matter to DALI module for luminaire in-built or stand-alone. Integrated DALI power supply (10 mA). Certificate ID: CSA23173MAT40686-24
Wireless module SR MTR	Zumbotel Group AG	Switch	Thread, Bluetooth	Wireless Matter to DALI module for luminaire in-built or stand-alone. Possible connection to max 25 DALI drivers. Certificate ID: CSA23172MAT40685-24
Nest thermostat	Google LLC	Thermostat	Wi-Fi 802.11 a/b/g/n (2. GHz/ 5 GHz), 802.15.4 (2.4 GHz), BLE	Implement temperature, humidity, proximity, motion, ambient light, and magnetic sensors; built-in rechargeable lithium-ion battery; less than 1 kWh/month power consumption. Certificate ID CSA22103MAT40103-24 *
BK7231	Beken corporation	Wireless Module	Wi-Fi 802.11n, BLE	BK7231 integrates Bluetooth Basic Rate and BLE features fully compliant with Bluetooth 5.2 specification. It supports both Access Point and Station mode. The chip supports multi-cloud connectivity with an 32-bit MCU running up to 120 MHz and 256 KB RAM. Certificate ID: CSA22077MAT40077-24
BK7235	Beken corporation	Wireless Module	Wi-Fi 6 (802.11 b/g/n/ax), BLE 5.2	BK7235 is a highly-integrated 1 × 1 single-band 2.4 GHz Wi-Fi 6 (802.11b/g/n/ax) and Bluetooth LE 5.2 combo solution. It integrates a 32-bit RISC-V MCU and a comprehensive set of peripherals. Certificate ID: CSA22078MAT40078-24
STM32 WB5MMG	STMicro-electronics	Wireless Module	Zigbee, Thread, BLE 5.3	Ultra low-power module compatible with Arduino. Among other features: 1-Mbyte Flash memory, 256-Kbyte SRAM, fully integrated BOM, including 32 MHz radio and 32 KHz RTC crystals and 68 GPIOs. Certificate ID not provided.

the product developer has obtained the certification for the transport platform in use for the Matter component. And the Security Attestation lists the requirements of security and the level of compliance the product must guarantee based on the Matter Core Specification.

The whole documentation confirms that the Matter component is meeting the protocol requirements. Once it has been submitted through the certification web tool, the CSA verifies the relevant criteria and, at the end of successful processing, the Matter component obtains the certification.

The crucial steps of the verification process are performed by authorized laboratories (i.e., test providers) contracted by the CSA. The most important certification institutes, spread all over the world, include: Allion Labs (Taiwan), Bureau Veritas (China, France, Germany, US), Cesi (China), DEKRA (China, Germany, Spain), Element Materials Technology (China, UK), Granite River Labs (Korea, US), Resillion (Belgium, China), TÜV Rheinland (Germany, Japan, Korea, Shenzen, Sweden), and UL Solutions (China, Taiwan, UK, US).

4. Matter in the literature

While Matter is primarily designed as a universal protocol for smart homes, its ability to enable communication between devices of various natures makes it adaptable for a broader range of application domains [15–17]. Indeed, many consortium members have expressed interest in potential applications of Matter beyond home automation, such as smart grids [18], building automation [19], and healthcare [6], to name a few.

Our approach emphasizes the practical implications of the protocol rather than its bibliographic impact. To achieve this, we analyzed numerous systematic reviews in accordance with the umbrella review methodology. Our goal is to introduce the protocol, summarize its key outcomes from current findings, and pinpoint unexplored areas for further implementation. The adopted *modus operandi* illuminates the challenges and future prospects of the protocol's evolution. This insight allows us to provide a series of recommendations, guiding developers and manufacturers in enhancing subsequent versions of the Matter protocol.

We surveyed the existing literature on the topic and explored potential application domains where Matter is expected to be utilized. The core set revolves around Matter in IoT, branching out into the following application domains: Healthcare, Home and Building Automation, Smart Grid, Industrial IoT, and Automotive. We grouped Home and Building Automation under the same application domain due to their close relationship. We also added two additional subdomains to the Healthcare subset: Internet of Medical Things (IoMT) and Ambient Assisted Living (AAL). The latter overlaps with Home and Building Automation as it can be considered part of both application domains. However, due to its closer affinity with the Healthcare domain, we chose to discuss it within the corresponding subset.

We could have also considered subdomains for the other application domains, but for the sake of clarity, we discuss the main subdomains within their respective sections without explicitly introducing them into the diagram, which would otherwise become difficult to read. Finally, since safety and security are aspects that concern all the aforementioned domains, particularly home automation, we decided to discuss the topic in a dedicated subsection within the Home and Building Automation section. Fig. 8

Table 2
Boards, Bridges, Hubs, Gateways, and SoCs.

Name	Manufacturer	Category	Wireless Protocol	Notes
AmebaD	PanKore Integrated Circuit Technology Co. Ltd.	Board	Wi-Fi, BLE	The AmebaD series combines the integrated CPU architecture of AmebaZ2 with maximum 54 configurable GPIOs including PCM, UART, I2S, I2C, ADC and PWM. Certificate ID: CSA22075MAT40075-24
LP-CC2652R7	Texas Instruments, Inc.	Board	Support for Thread, ZigBee, BLE 5.2, SimpleLink TI 15.4 stack	The SimpleLink Multi-standard LP-CC2652R7 Wireless MCU Development Kit support 6LoWPAN and other proprietary systems; programmable radio includes support for 2-(G)FSK, 4-(G)FSK, MSK, BLE 5.2, IEEE 802.15.4 PHY and MAC; support OTA upgrade. Certificate ID: CSA23110MAT40623-24
nRF52840 DK	Nordic Semiconductor	Board	BLE 5.2, Bluetooth mesh, NFC, Thread, Zigbee	The dongle supports Matter in nRF. Connect SDK. Toolchain and IDE need to be set from-scratch. Certificate ID not provided.
nRF5340 Prototyping Platform - Tingy:53	Nordic Semiconductor ASA	Board	BLE, Bluetooth mesh, NFC, Thread, Zigbee	Includes integrated sensors like environmental, color and light, accelerometer and magnetometer. The board is powered by a USB-C rechargeable Li-Po battery with a 1350 mAh capacity. Certificate ID: CSA23434MAT40947-24
NXP 88MW32X	NXP Semiconductors Netherland B.V.	Board	Wi-Fi	The development platform kit includes a set of IO headers that bring out SPI, I2C, UART, I2S, PWM, ADC, and DAC interfaces to connect to external sensor or other peripheral boards. Certificate ID: CSA23111MAT40624-24
NXP K32W061/41	NXP Semiconductors Netherland B.V.	Board	Zigbee, Thread, BLE 5.0	The NXP K32W061/41 wireless microcontroller family is ideal for IoT platforms since implement multiple low-power modes and ultra-low radio Tx and Rx power consumption. Certificate ID: CSA22048MAT40048-24
NXP i.MX 8M with 88W8987, K32W061/41, EdgeLock SE05x	NXP Semiconductors	Board	Zigbee, Thread, BLE 5.0	Ideal for implementing Matter Controllers, Matter Commissioners, advanced Matter Devices, and Thread Border Routers. Matter is supported over Wi-Fi, with the NXP Wi-Fi drivers included in the Yocto BSP. Certificate ID: CSA22086MAT40086-50
QPG6105 DK Matter Light	Qorvo	Board	Zigbee, Thread, BLE and Bluetooth Mesh	The QPG6105 natively implements Zigbee, Thread, Matter, Bluetooth Low Energy and Bluetooth Mesh protocols, and the Qorvo IoT Development Kit for QPG6105 provides a complete solution for building Matter applications. Certificate ID: CSA22002MAT40002-24
SparkFun Things plus Matter	SparkFun	Board	Zigbee, Thread, BLE 5.3, Multiple 802.15.4 Protocols	SDK MultiOS, suitable for prototyping Matter-based IoT devices. Certificate ID not provided.
M2D Bridge	Innovation matters iot GmbH	Bridge	Wi-Fi	Broadcast control of standard and TW (DT8) DALI LED-driver. Features: integrated DALI power supply (max. 8 DALI-driver), broadcast control of standard and TW (DT8) DALI LED-driver, dimensions (LxBxH): 53 × 30 × 21 mm. Certificate ID: CSA22001MAT40001-24
Philips Hue V2 Bridge	Signify	Bridge	Ethernet, ZigBee	The Bridge supports Matter with a software update. Certificate ID not provided.
QBEDFMB3 smart home gateway Ethernet	CAME S.p.a.	Gateway	Ethernet	QBEDFMB3 is a Matter (Ethernet) Bridge that exposes endpoints to on-off/dimmable lights, and window covering. Certificate ID: CSA23155MAT40668-00
Smart Home Control Gateway CRI4	Xiamen Intretech	Gateway	Bluetooth, Thread	Certificate ID: CSA22472MAT40472-24
Smart Wired Gateway Pro	Tuya Global Inc.	Gateway	Ethernet, Zigbee, Thread	It supports the communication protocol of Cable+Zigbee+Thread, that is, the uplink Ethernet connects to the cloud, and the downlink supports both Zigbee (compatible with the original Zigbee device ecology of Tuya) and Thread (Matter over thread) sub-devices. This gateway has powerful localized management capabilities and high stability of multi-device control. Certificate ID: CSA22071MAT40071-00

(*continued on next page*)

Table 2 (*continued*).

ubisys G1	ubisys technologies GmbH	Gateway	ZigBee 3.0, Ethernet, Matter	It acts as a bridge by transferring from the Zigbee network to the local network. Either 10/100 Base-T Ethernet PoE PD or 5 V/1 A power supply; BLE+MC (optional). Certificate ID: CSA22082MAT40082-00
Echo (series)	Amazon	Hub	Wi-Fi, BLE Mesh, ZigBee	The line includes Echo Dot series (3-5 gen.), Echo Studio, Echo Show 5-8-10-15, Echo Dot (3-5 gen with clock), Echo (v3), Echo Input, Echo Flex, Echo Plus (2ª gen.); support for Thread. Certificate ID not provided
Hub 2	Woan Technology (Shenzhen) Co., Ltd.	Hub	Wi-Fi, Bluetooth	Certificate ID: CSA23202MAT40715-24
Hub M2	Lumi United Technology Co., Ltd.	Hub	Wi-Fi, Ethernet, ZigBee	The Aqara Hub M2 can be connected via WiFi or Ethernet, and supports interaction and connection with Aqara Zigbee accessories. It is also provided with IR remote control functions. Certificate ID: CSA22083MAT40083-24
Wiser Hub - Mod. CCT501900 et seq.	Schneider Electric	Hub	Ethernet, ZigBee	Wiser Smart Home System controller. It implements Zigbee coordinator to commission Schneider Electric's Zigbee sub-device onto Wiser Platform. It also acts as the center controller to control any installed Zigbee sub-device remotely. Certificate ID: CSA22080MAT40080-00
AmebaZ2	PanKore Integrated Circuit Technology Co. Ltd.	SoC	Support for Wi-Fi, BLE	The AmebaZ2 series combines a Real-M300 (KM4) CPU based on ARMv8-M architecture, WLAN MAC, a 1T1R capable WLAN baseband, RF circuit, and Bluetooth Low Energy (BLE). Certificate ID: CSA23146MAT40659-24
ASR582x-HolaConWB01	ASR Microelectronics (Shenzhen) Co., Ltd.	SoC	Support for WiFi and Bluetooth 5.2	ASR Combo Soc with 32-bit MCU core and Security engine, for IOT market. Certificate ID: CSA22070MAT40070-24
EFR32MG24	Silicon Labs	SoC	Support for Zigbee, Thread, BLE 5.3 (Mesh)	The SoC empowers the EFR32MG24 pro kit +10/20 dBm. Certificate ID: CSA23152MAT40665-24
ESP32-C Series	Espressif Systems (Shanghai) Co., Ltd.	SoC	Support for ZigBee, Thread, 802.15.4 + Bluetooth 5 (LE)	Single-core, 32-bit RISC-V microcontroller for low power consumption and securely connected devices; provided with 256 KB SRAM and slots for external flash; it can be clocked up to 96 MHz; transmit power of up to +21 dBm. Certificate ID: CSA22107MAT40107-24
NXP i.MX8M MPU + IW612 Tri-Radio	NXP Semiconductors Netherlands B.V.	SoC	Wi-Fi 6, Bluetooth, Thread	IW612 includes a full-feature Wi-Fi subsystem powered by NXP's 802.11ax (Wi-Fi 6) technology, an independent Bluetooth/BLE and 802.15.4 subsystem that supports Thread mesh networks. Interfaces for connecting the IW612 to external host processors include SDIO 3.0 for Wi-Fi, UART for Bluetooth and SPI for 802.15.4. Certificate ID: CSA22098MAT40098-50
RS9116 Wi-Fi NCP SoCs	Silicon Labs	SoC	Support for Wi-Fi, dual-mode Bluetooth 5	Single band SoC that provides an ultra low-power comprehensive multi-protocol wireless connectivity solution, including 802.11 b/g/n (2.4 GHz), and dual-mode Bluetooth 5. Certificate ID: CSA23572MAT41085-24
RT58X	Rafael Microelectronics, Inc.	SoC	Support for Zigbee, Thread, Matter, BLE	Dual-core SOC for mesh IoT wireless connectivity, with key features likes high performance 2.4G/Sub-G RF, hardware accelerator and low current consumption. Certificate ID: CSA23397MAT40910-24

provides a quick overview of the main Matter application domains that we have divided into sets. In the following sections, we detail what we have surveyed in the literature.

4.1. Matter in IoT

IoT is nowadays considered a disruptive technology for solving most of society's issues such as efficiency in public transportation with more efficient scheduling of the routes, pollution through the constant monitoring of particulate matter and other contaminants, overcrowding of hospital buildings and nursing homes with the implementation of AAL, etc. The key idea behind IoT is to deploy billions of smart objects capable of sensing the surrounding environment, transmitting, process, and providing feedback based on the collected information [20]. Independently from the application domain where such technology can operate, what needs to be guaranteed is the interoperability between devices [21]. With this term, we intend the ability of different devices, sensors, platforms, and applications to communicate and exchange data with each other in a seamless and efficient manner. Interoperability aims at

Table 3
Certified software.

Name	Manufacturer	Category	FW/HW	Notes
AiDot Application for iOS	AiDot Inc.	App	1.16.0/1.16.0	User interface for dynamic control home automation devices. Certificate ID: CSA22032SWC60032-M1
Deco X55	TP-Link Corporation Limited	App	1.7.3/1.0	App for the management of the TP-Link Deco AX3000 WiFi 6. Certificate ID: CSA23025SWC60076-M2
Google Home for Android	Google LLC	App	2.62/Google Pixel	Android App that provides support for the setup of Nest, Chromecast, Google Home and Matter devices. Certificate ID: CSA22027SWC60027-M1
Google Home for iOS	Google LLC	App	2.62/Apple iPhone	IOS App that provides support for the setup of Nest, Chromecast, Google Home and Matter devices. Certificate ID: CSA22028SWC60028-M1
Google Home for iPadOS	Google LLC	App	2.62/Apple iPad	iPadOS App that provides support for the setup of Nest, Chromecast, Google Home and Matter devices. Certificate ID: CSA22030SWC60030-M1
LG ThinQ Application (Android)	LG Electronics	App	V4.1.38000/1.0	App Android enabling the management of all LG smart appliances and IoT devices in the smart home ecosystem. Certificate ID: CSA23006SWC60057-M1
LG ThinQ Application (iOS)	LG Electronics	App	v4.1.41000/IPhone 13 Pro Max	App iOS enabling the management of all LG smart appliances and IoT devices in the smart home ecosystem. Certificate ID: CSA23034SWC60085-M1
Smart Life Application (Android)	Tuya Global Inc.	App	V4.7.0/9.1.0.233 (C00E233R2P1) GPU Turbo	Device management Android App compatible with Wi-Fi, Bluetooth, Zigbee, NB-IoT, Thread and Matter certified devices. Certificate ID: CSA23003SWC60054-M3
Smart Life Application (iOS)	Tuya Global Inc.	App	V4.7.0/iPhone X/Alexa	Device management iOS App compatible with Wi-Fi, Bluetooth, Zigbee, NB-IoT, Thread and Matter certified devices. Certificate ID: CSA23001SWC60052-M3
SmartThings Application (Android)	Samsung Electronics Co., Ltd.	App	1.7.91/1.0	SmartThings App for Android can be used to onboard WiFi, Zigbee, ZWave, Thread and Matter certified devices, including voice assistants as Alexa, Bixby and Google Assistant. Certificate ID: CSA22021SWC60021-M3
SmartThings Application (iOS)	Samsung Electronics Co., Ltd.	App	1.6.94/1.0	SmartThings iOS App can be used to onboard WiFi, Zigbee, ZWave, Thread and Matter certified devices, including voice assistants as Alexa, Bixby and Google Assistant. Certificate ID: CSA22051SWC60051-M3
Brain-level Smart Pal 12	Qingdao Haier Technology Co., Ltd.	Broker	1.0.00/v17	Brain-level Smart Pal 12 is an AI butler for home automation. It integrates capabilities as decision-making, connection, interaction and distribution perception. Certificate ID: CSA23027SWC60078-M2
QuickSet	Universal Electronics, Inc.	Commis-sioner	5.5/60291-4227000 A01	This software solution supports multiple communication mediums ranging from HDMI to IP, as well as different wireless protocols as Zigbee, Bluetooth, Infrared and Matter. Certificate ID: CSA22050SWC60050-M2
Admin Software Component for FireOS	Amazon Lab126	Framework	1.0.1/PVT	Admin Software Component for FireOS. Certificate ID: CSA23026SWC60077-M2

(*continued on next page*)

Table 3 (*continued*).

Name	Manufacturer	Category	FW/HW	Notes
Google Home Framework	Google LLC	Framework	1,0/Google Home Framework Test Device 1.0	Google Home Framework is an integration of the Matter SDK into the Google codebase to be used for internal Smart Home integrations. Certificate ID: CSA22024SWC60024-M2
Google Home Framework and Services for Android	Google LLC	Framework	1.0/Android Pixel	Google Home Framework and Services for Android integrates the Matter SDK into the Google ecosystem, enabling it to be used with Android Applications. Certificate ID: CSA22025SWC60025-M2
SWAN Sagemcom middleware	Sagemcom SAS	Framework	swan-matter-r1.0/F5670	The architecture of Sagemcom middleware allows portability between hardware (Core chipset, front-end...) and regarding security (CAS, DRM...). Certificate ID: CSA23035SWC60086-M2
Alexa Commissioner for Android	Amazon Lab126	Software update	1.0.0/Android Phone	Alexa Commissioner Software Component for Android. Certificate ID: CSA23004SWC60055-M1
Amazon Casting Video Player	Amazon Lab126	Software update	1.0.0/FireOS	Amazon's Casting Video Player software component. Certificate ID: CSA23002SWC60053-M2
HomePod software	Apple Inc.	Software update	1.1.5.2/MacBook Pro	Update for the operating system that runs on HomePod to support Matter. Certificate ID: CSA23011SWC60062-M2 *
iOS	Apple Inc.	Software update	1.1.5.2/MacBook Pro	The operating system that runs on iPhone. Certificate ID: CSA23008SWC60059-M2 *
iPadOS	Apple Inc.	Software update	1.1.5.2/MacBook Pro	The operating system that runs on iPad. Certificate ID: CSA23009SWC60060-M2 *
macOS	Apple Inc.	Software update	1.1.5.2/MacBook Pro	The operating system that runs on Mac devices such as the MacBook Pro, MacBook Air, iMac, Mac mini, Mac Pro, and Mac Studio. Certificate ID: CSA23021SWC60072-M2 *
SmartThings Hub Software for Samsung Tizen	Samsung Electronics Co., Ltd.	Software update	0.45/Rev. A	SmartThings Hub Software for Tizen OS provides support for Matter and enables Tizen OS to act as SmartThings Hub. Certificate ID: CSA22020SWC60020-M2
SmartThings Hub Software on Hub V2/V3	Samsung Electronics Co., Ltd.	Software update	0.45/1.1	The SmartThings Hub Software for The SmartThings Hub V2 and SmartThings/Aeotec Hub V3 includes support for Matter, Zigbee, Z-Wave and other device protocols. Certificate ID: CSA22019SWC60019-M2
tvOS	Apple Inc.	Software update	1.1.5.2/MacBook Pro	The operating system that runs on Apple TV. Certificate ID: CSA23010SWC60061-M2 *
watchOS	Apple Inc.	Software update	1.1.5.2/MacBook Pro	The operating system that runs on Apple Watch. Certificate ID: CSA23022SWC60073-M2 *
webOS TV	LG Electronics	Software update	webOS TV 23/1.0	Software for LG Smart TV with Matter support. Certificate ID: CSA22022SWC60022-M2

improving many aspects of the communication between IoT devices like fast response time, reliability, security, power saving, and so forth. Nevertheless, interoperability is a long-standing problem in IoT, and in the literature, there are several examples of research efforts to solve it. Among the main virtuous interoperability solutions that paved the way to Matter it is worth mentioning SOAP-based Web Service solutions [22–24], semantic solutions [25,26], as well as OSGi-based and Atlas-based solutions leveraging the MQTT messaging service [27–29]. To overcome interoperability problems between heterogeneous devices in IoT, Bouloukakis et al. [30] suggest comprehensively abstract and represent the semantics of various middleware protocols. The strategy used by the authors leverages data exchange API and a connector model for connecting heterogeneous devices with each other. The framework supports the abstraction of the functional semantics of middleware IoT protocols such as CoAP, MQTT, and WebSocket. However, the solution proposed is not so generic as to guarantee interoperability with any type of IoT device. Newly proposed is TinyNet [31],

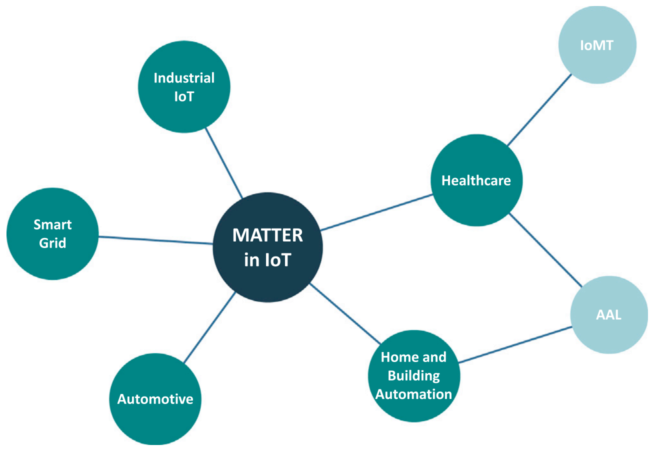

Fig. 8. Representation of the main IoT application domains in which Matter can bring benefits.

a lightweight network architecture that provides IP support to IoT radio technologies. In a Matter-competitive way, TinyNet traces the Matter behavior at the IP layer by providing interoperability between IoT devices mounting radio technologies such as 802.15.4, BLE, LoRa, Wi-Fi, Z-Wave, and ZigBee. To achieve the coexistence of such heterogeneous technologies and permit communication between network-layer routing protocols, TinyNet add to the protocol stack an additional layer that provides a unified (MAC) interface to a wide range of data link and physical layer.

Griffith et al. [32], instead, highlight three main strategic points that urgently require innovation in IoT: power consumption (e.g., with the introduction of BLE technology for Bluetooth), market expansion (e.g., with the introduction of smaller edge nodes for emerging IoT applications), and interoperability across connectivity protocols and technologies. The authors also point out how Matter can improve such three points using BLE for commissioning, providing a simplified development platform for manufacturers, and introducing an abstraction of the application layer that builds on top of IP protocols to overcome interoperability device-to-device issues.

However, due to its recent formalization to date not much literature provides potential application of Matter in practice and some just introduce it among other emerging technologies for IoT [33]. An exception, and to date the most representative research effort on the topic is given by Zegeye et al. [34], who introduce a smart home Testbed over Matter protocol by taking advantage of the Silicon Labs development kit,[15] other open-source software tools, libraries, and third-party applications. The core of the tested network is composed of a Thread Border Router built on a Raspberry Pi 3 B+ and connected through USB to an SLWSTK6000B, which is a Thread-capable Silicon Labs radio co-processor. The whole network is able to interconnect and remotely manage a smart door lock and other Thread devices of third-party. For ping tests, authors leverage Wireshark and set up a Thread protocol sniffer on a nRF52840-Dongle by Nordic Semiconductor. The sniffer indirectly demonstrates the inter-device communication peculiarity of Matter through the capture of the mesh network traffic.

In line with the above, Ortega [35] gives an initial evaluation of the Thread protocol in the framework of Matter. The dissertation focuses on the setup and configuration of a Thread network composed of Zolertia Re-Mote and Zolertia Firefly devices. The test scenario includes both the configuration of a Thread sniffer, whose purpose is to acquire and visualize the Thread messages exchanged between devices and the use of the Texas Instrument Wireshark Packet Converter to directly plot the data provided by the sniffer. Zolertia devices are configured by taking advantage of a virtual machine mounting the Contiki OS. The choice of the OS is justified by the fact that Contiki fully supports IPv6 and low-power wireless standards (i.e., 6LoWPAN, RPL, and CoAP) that the Thread protocol relies on. Performing tests the author observes the network performance, e.g., during the association/disconnection of one or more devices or through the detection of devices unable to decipher all the mesh link establishment messages that operate below the routing layer, and evaluates the end-to-end connectivity under multi-hop routing. The work includes a brief description of unsuccessful configurations of MakerDiary devices.

An informative study is carried out by Domınguez-Bolano et al. [36], which provides a comprehensive overview of the current IoT technologies and protocols. After framing Matter together with the most relevant (application) layer protocols for IoT (i.e., HTTP, CoAP, MQTT, and AMPQ), the authors highlight the use of tree, star, and mesh network topologies for the communication network and how Matter should necessarily rely on additional security rules (such as Datagram Transport Layer Security) during data transmission to ensure privacy, integrity, and authenticity of communications. Similarly, Tlili et al. [37] provide an overview of current IoT communication technologies, focusing on the most popular application domains and challenges. Comparing wired and wireless technologies, the authors emphasize that the latter actually holds more promise for the future of IoT, especially in the context of smart homes, and summarize the main improvements that ZigBee (and Matter as a whole) can bring in terms of

[15] https://www.silabs.com/developers/unify-sdk.

satisfying individual preferences and needs, convenience in daily activities, space savings, security and energy efficiency, as well as reducing human intervention. The authors state that this technology promises to strengthen the security and confidentiality of the transmitted and stored data in terms of protecting IoT environments against possible threats, implementing scalable solutions to meet the needs of networks that are currently experiencing exponential growth of interconnected objects in terms of network scalability and connectivity, and both compatibility and interoperability between multiple hardware and software installations from different vendors in terms of heterogeneity of implemented technologies.

Always in the IoT domain, some literature on the subject has been produced for Multi-access edge computing [38]. Shrivastwa et al. [39] propose a general-purpose IoT monitoring framework for smart intrusion detection systems that can be applied to edge-to-cloud applications. Among the possible protocol implementation, authors mention IP-based solutions like MQTT, CoAP, and other solutions considering the implementation of higher-level protocols such as Open Mobile Alliance Lightweight Machine-to-Machine (OMALwM2M) and Matter. Sidhardhan et al. [40], instead, propose a distributed edge service strategy to make any Personal Area Network (PAN) resilient to sudden access point disconnection. The solution aims to provide reliable internet services to generic IoT hubs or any other device at any given point in time with the support of third-party devices acting as hubs within the PAN. By doing so, the authors introduce the concept of the alternative access point (aka the border router), a role that can be played by any device within the PAN implementing the whole protocol stack, enabling a seamless connection between the Matter/Thread network and the Global network. However, it is worth remembering that based on the Matter Specification, the Matter protocol itself has been conceived to build an autonomous PAN, capable of operating in a detached way, locally, with respect to the Internet.

Last but not least, to date the level of adoption and backward compatibility with legacy devices still remain pending for Matter, IoT research continues to come up with alternative solutions, especially for tools enabling the discovery of devices across multiple protocols. An example is given by Gvozdenovic et al. [41], that propose a concurrent IoT network reconnaissance solution called IoT-Scan. IoT-Scan runs on a software-defined radio on the 900 MHz and 2.4 GHz bands and supports Zigbee, BLE, LoRa, and Z-Wave. Authors state that there is currently an effort by several vendors to create an IP-based IoT protocol to overcome interoperability issues between brand-different devices (i.e., Matter), but the evidence suggests that its level of adoption and backward compatibility is still uncertain.

4.2. Home and building automation

Today, the trend for homes and buildings is towards the implementation of IoT technology to automate lighting, doors and windows, heating, and air conditioning system, monitor and manage power consumption, and so forth [42,43]. However, as partly discussed in the introduction, such domains still suffer from inflexibility due to the excessive number of communication protocols, mostly incompatible with each other, and the lack of an effective standard capable of ensuring interoperability between devices. Moreover, as well explained in [44], in spite of the fact that the feasibility of home automation has existed for decades, other problems related to the high cost of ownership, poor manageability, and the difficulty of achieving security slow down its large-scale adoption. In this context, Matter is the most recent home automation protocol conceived for overcoming some of such issues. In line with the above-mentioned daily growth of new certified products, some research works are focusing on the implementation and testing of Matter with home automation products already on the market. An example is given by the thesis work of Ganassin [45], where is detailed the implementation of the Matter protocol on an already existing Vimar Wi-Fi Smart Thermostat. The author reports that has been necessary important work in terms of ecosystem understanding, logic connections, and implementation; in particular towards the firmware module, for its standardization and integration into other current compatible devices. While some authors focus on the benefits that Matter can bring to the home and building automation others, for the same application domain, propose alternative solutions. An example among all is the work of Sioutis et al. [46], which proposes a home automation solution that overcomes compatibility limitations between ECHONET lite, a well-known resource-saving framework for IoT, and the Z-wave protocol. As the authors highlight, soon Z-Wave will be replaced by technologies such as Thread and Matter. The work focuses on the extension of the Z-wave lifetime, by leveraging the open-standard nature of ECHONET lite and achieving a mapping of Z-Wave primitives into the corresponding ECHONET lite ones.

Recent research efforts, instead, introduce Matter within their smart home technology surveys. Dias et al. [47], for instance, give an overview of IoT ecosystems by surveying the state of the art in designing and developing the layers of the whole protocol stack. In doing so, authors introduce advantages and disadvantages (e.g., communication range, power, bandwidth needs, and so forth) that a system designer has to face during the development of specific scenarios and highlight how in the plethora of solutions for IoT smart home network the introduction of Matter eases the process of selecting a protocol for low-range communications, in virtue of its intrinsic feature of unifying the major and well-known low-power personal area network protocols (e.g., ZigBee, Thread/Matter, Wi-Fi, and BLE). Andraschko et al. [48], differently, propose a taxonomy of smart home technologies based on the Nickerson–Varshney–Muntermann method. Authors highlight the issues that Matter intends to overcome in the smart home domain, that is comfort in terms of communication expansion (e.g., consumption sensing devices that directly communicate with organizations), convenience in terms of simplification of the home automation and customization process (e.g., ease the implementation of technologies designed to decrease the effort to do chores by automating the user's tasks), benefits in terms of savings (e.g., responsible use of energy consumption and reuse of resources because of the possibility to build home networks composed of heterogeneous devices), healthcare in terms of facilitating the monitoring of user's health conditions (e.g., integration in the smart home physiological sensors and devices capable of monitoring the health status and provide recommendations or actions), security and safety through the introduction of a unified protocol to overcome the vulnerabilities of the layers underlying the stack. Lastly, it is worth noting that the entries of the taxonomy proposed in this paper fit most parts of the application domains introduced in the present survey.

4.2.1. Safety and security in home and building automation

Safety and security in smart home ecosystems have always been thematics of major interest. Safety and security are considered fundamental design tenets for Matter, and the protocol itself can be viewed as a valid incentive to overcome many weaknesses of the protocol stack [49]. In line with the above, to date, the majority of the literature produced on the subject focuses on safety and security in smart homes, and Matter is mentioned in synergy with the proposed security solutions. Shafqat et al. [50], for instance, present a retrospective about passive inference attacks on Zigbee-based smart home systems. Specifically, the authors introduce a tool capable of identifying and sniffing respectively ZigBee devices and the data they exchange with each other, thereby highlighting falls in the ZigBee-based home automation system. To face the problem they propose some feasible countermeasures, but they also point out the benefits that Matter (as a project of the ex-ZigBee alliance) can bring to ZigBee networks in terms of safety and security. Bauer et al. [51], instead, introduce a platform architecture that implements an IoT module based on openHAB[16] to enable the connection of different smart home ecosystems by preserving privacy and security. Authors also highlight that, because of the platform flexibility, the IoT module can be replaced with more proficient smart living middleware systems as universAAL,[17] HomeKit[18] or Matter. Salnikov's thesis [52] presents an overview of the Matter standard from a security perspective. The dilemma the bachelor candidate tries to unveil is whether or not Matter provides a sufficient degree of security and what kind of advantage it can bring to the smart home domain. The study interests the analysis of some security peculiarities such as strong encryption, signature process, and the use of certificates to verify the device identity. The analysis considers the generation of data traffic from and towards an ESP32 module. The ESP32 is subjected to TCP, UDP, SYN, and FIN scans. Results show that the sole open port detected is the one the controller used to ask for the IP address of the ESP32, by evidence that there are no fundamental weaknesses in the design of the security measures of the Matter protocol. Last, Akestoridis et al. [53] carry on experimentation with OpenThread-enabled devices to test the security of Thread networks and, in full, of Matter. To form the Thread network, the authors took advantage of the Adafruit Feather nRF52840 Express, flashed with OpenThread binaries. They aimed to study the Thread traffic susceptibility to a set of energy depletion attacks and online, low-entropy attacks, like jamming and spoofing, that during the commissioning process attempt to guess the password of Thread devices. The study of the susceptibility of the Thread networks with existing software tools, properly enhanced for the purpose and shared, opens up the opportunity of studying the safety and security of Matter-enabled Thread devices as well.

4.3. Industrial internet of things

Industrial Internet of Things (IIoT) is a subset of IoT, which covers the domains of M2M and industrial communication technologies with automation applications [54]. IIoT applications typically require small throughput per node and the capability for interconnecting a very large number of devices with limited hardware and energy resources. To date, an IIoT facility is mainly structured in automation units (or islands), whose mutual interoperability relies on TCP/UDP/IP-based Ethernet connections [55] (see also the Common Industrial Protocol network families for IIoT [56]), or is restricted by the diversification of wireless networking protocols [57]. In this context, Matter can bring benefits in terms of interconnection between intelligent assets, and reduction of the costs for renewed installations by facilitating the process of plant updates as technology advances.

Artetxe et al. [58] introduce the up to the minute Wireless Network Technologies applied to IoT Industry 4.0 and highlight that novel solutions like Random Phase Multiple Access, enhanced Machine-Type Communication, Extended Coverage GSM IoT, Weightless, DASH7, Wi-Sun, and Matter-or-Thread protocols are still in their infancy, and consequently less common. However, the authors continue, the core of Industry 4.0 is the ever-growing integration between cyber–physical units to satisfy operations like monitoring, maintenance, supervision, control, and so forth. By proposing a unified approach to IoT device development, Matter could bring lots of benefits in the sector in terms of enhanced efficiency, improvement of working conditions, cost saving, and economic sustainability.

Hou et al. [59] survey the current trends and challenges in different IoT subdomains, with a special focus on IIoT and device-to-device interoperability. Authors highlight that to guarantee effective and efficient interoperability between IIoT devices there are three main components that must be standardized and adopted, that is: the wireless physical layer, the communication protocol stack, and the application layer protocol. While the physical layer already relies on some well-known standards (e.g., BLE 5.x and IEEE802.15.4), the communication protocol stack and the application layer are always looking for ongoing accommodations and temporary solutions. However, one step towards standardization of IIoT, and in full the whole IoT domain, has been done since big IT players such as Google, Apple, Amazon, and Huawei are progressively adopting OpenThread and Matter for their IoT products.

4.4. Automotive

With the introduction of IoT applications into the transportation system, the automotive industry is moving towards a new way of interacting with our vehicles [60]. It is experiencing ever-increasing growth, leading to intelligent wireless network communication scenarios where vehicles are able to interact with drivers, passengers, and with each other. However, the industry still faces many challenges related to connectivity efficiency, security, and interoperability between components. The Automotive Open System

[16] https://www.openhab.org/.

[17] https://www.universaal.info/.

[18] https://developer.apple.com/homekit/.

Architecture[19] and the Connected Vehicle Systems Alliance[20] report that a common technology stack is not enough for automotive interoperability. Even if devices can communicate over IP, they are still not talking the same language because IP only provides a common baseline across many different types of devices and physical networks. As a result, the winning strategy in the short term is that of consolidated technologies such as ZigBee or WLAN. In this scenario, a common understanding of the application-level data and commands is required for different devices to work together. The challenge here is to find solutions that efficiently and effectively integrate IoT ecosystems into connected vehicles [61]. Matter provides the ability to easily build interoperable heterogeneous networks that are disconnected from the Global one. In this context, the Matter protocol can facilitate the development of local network infrastructures for automated vehicle systems. Sensors such as localization, RPM, acceleration, pressure, temperature, and flow can be combined together to streamline driving functionalities, predict periodic maintenance cycles, provide critical information to the vehicle's control system, and so on. To date, not much literature has been produced on the subject, but some research efforts are paving the way for future applications of this technology in the vehicular domain.

4.5. Smart grid

Smart Grid is a communications network that sits on top of the power grid to collect and process data from different parts of the grid and efficiently manage power supply and demand [62]. It is a concept that combines sustainability and smart energy. It focuses on monitoring, measuring, and managing energy generation and consumption. To effectively achieve these goals, smart grid solutions require interoperable components that can be easily adapted and expanded as technology advances. Designed as a protocol for interoperability, Matter in this domain can bring benefits in terms of communication network [63] (by providing a self-organizing, secure, and reliable mesh network of smart grid components) and energy efficiency [64] (by facilitating the process of balancing energy supply and demand for customers, thereby optimizing energy use during peak periods).

Some Matter-based research efforts have already been tempted in this direction. For instance, Fiastri et al. in [65] introduce a solution to tackle the variability of renewable energy generation by leveraging the Matter standard to enable implicit demand-response for privates. The proposal here is to dynamically adapt the behavior of household consumption by taking advantage of Matter's peculiarity in connecting devices belonging to different ecosystems. The focus is on the variability of energy demand in terms of its correlation with the price of electricity. Attention is given to currently available energy storage solutions and, since Matter works on top of the physical and network layer standards, the author describes a scenario in which any Matter-compliant energy retailer will be able to provide hubs that control energy-consuming devices, thus enabling demand response. Ultimately, the author highlights that a growing number of participants inside the CSA Group (like Tesla, Aclara, Schneider Electric, Voltalis, and ConnectedResponse, just to name a few) are focusing their efforts on energy management.

In line with the above, Nagashige et al. [66] recently extended their iHAC Hub to support the Matter protocol and laid the groundwork for the interconnection between Matter and the ECHONET Lite ecosystem [67]. The latter is a *de jure* home networking standard, ratified by the IEC and ISO, that enables resource-efficient devices to support the IoT and realize energy management and remote maintenance services. Provided the Matter extension, the iHAC Hub assumes the concept of a bridge device for different communication standards and opens up to the possibility of building systems in multi-vendor environments.

In affinity with the vehicular mobility domain, Hasan et al. [68] present an overview of the opportunities and challenges in the smart grid domain for electric vehicles. In doing so, they make comparisons between different communication networks applicable to the smart grid such as power line communication, fiber optical, Ethernet, cellular network, ZigBee, digital subscriber line, wireless, and radio frequency mesh. All the technologies are evaluated considering spectrum, data rate, coverage range, and limitations such as noisy channels, low data rate, lack of coverage, short range, etc.

It is also worth mentioning the work done by Choroszucho et al. [69] that introduces an air quality monitoring system for the improvement of working and learning conditions. The built sensor network takes advantage of an ESP32 microcontroller (see Table equipped with Bluetooth for discovery and commissioning, and Wi-Fi for peripheral operations, data acquisition, and wireless connectivity. The solution is capable of monitoring carbon dioxide concentration, temperature, humidity, and pressure, and enables the implementation of mesh technology (e.g., a Matter-based ZigBee network) to create a scalable measurement system.

4.6. Healthcare

The healthcare industry has evolved since the introduction of horizontal, system-level architectural paradigms (such as fog and edge computing) that seamlessly distribute computing resources, services, storage, and infrastructure control between the IoT and the Cloud [70,71]. However, still persist limitations in device-to-device communication. Most are related to high power consumption, scarce resources, security, and limited interoperability due to the heterogeneity of communication protocols. Among other challenges, interoperability plays a key role in promoting the expansion of this field beyond the niche of practical applications that have been realized so far. Some valuable solutions have already been attempted to overcome interoperability issues in heterogeneous IoT infrastructures for healthcare. Ullah et al. [26], for instance, propose an IoT-based semantic interoperability model to enable semantic interoperability among heterogeneous IoT devices using the Resource Description Framework for semantic annotation and SPARQL for data extraction. The goal is to track and monitor the patient's disease in relation to prescribed medicines.

[19] https://www.autosar.org/.

[20] https://www.covesa.global/.

The application of semantics to the context ensures that IoT devices from different vendors are interoperable. Ahmadi et al. [72], instead, expose a systematic review of challenges and opportunities in IoT healthcare systems. In doing so, the authors highlight that studies on interoperability issues in healthcare IoT architectures are still scarce, while the topic has a prominent aspect in terms of the efficiency of home care systems. In this context, two important areas have gained the attention of research and industry in recent years: IoMT and AAL. The benefits that Matter can bring to these areas are many. Devices operating on Matter-enabled networks can link individuals at home to physicians and healthcare facilities through robust and secure communications. The simplification enabled by the protocol can help improve both the quality of care and the quality of life for patients. For these reasons, we have decided to deal with the implications of introducing Matter into these areas in two separate subsections.

4.6.1. Internet of medical things

The power and performance of distributed products are growing, offering promising outcomes for patients, but also improving in terms of usability and accessibility for physicians. The IoMT in healthcare sometimes referred to as the Internet of Healthcare Things (IoHT), refers to all those medical devices associated with a facility or healthcare provider that enable the home management of chronic conditions [73]. Most of the IoMT systems integrate multiple technologies, devices, sensors, and systems connected via wired or wireless. Matter can bring lots of benefits in this domain, by widening the communication opportunities between heterogeneous physical objects, thus promoting both personalized medicine and optimization of available resources. Moreover, a universal communication protocol for things enables compliance with ever-changing regulatory requirements and allows one to easily upgrade and reuse expensive medical equipment. As in the previous area, there is a lack of interoperability between heterogeneous devices. To date, some solutions have been proposed to overcome incompatibilities between device components designed by heterogeneous vendors. In [74], for instance, are introduced six levels of conceptual interoperability that should be ensured to realize an effective and efficient device-to-device communication in healthcare and a framework based on such logical layers for managing numerous critical clinical scenarios with devices coming from different manufacturers. Vangimalla and El-Sharkawy [75], instead, aim at improving health care in poor rural areas by enhancing the interoperability between smart objects, through the implementation of a secured Thread network in Unmanned Aerial Vehicles (UAVs). Similarly, Shankar et al. [76] illustrate a remote-control Health Monitoring System (HMS) with the integration of a UAV Thread network, which enables the doctor to remotely access and analyze the patients' data. Specifically, they propose a UAV-based HMS capable of measuring and storing UAVs temperature, humidity, blood pressure, heart rate, and SpO2. Always in the healthcare domain, Tanwar et al. [77] propose a solution for human arthritis analysis by applying a Bayesian network classifier, specifically designed for anomaly detection, to a fog computing environment enhanced with Thread protocol. The platform gateway collects data sensed by sensors placed in the patient's gloves, and these smart devices implement Thread within their microcontrollers. The authors experienced that the Thread protocol together with fog computing architecture is able to overcome in performance a traditional core-based cloud computing infrastructure. With no specified application layer in the Thread-based architecture, the protocol manifests sufficient flexibility to support multiple protocols (e.g., Matter) in the application layer, an aspect that can further improve the performance of the proposed platform.

One branch of IoMT is aimed at measuring the vital parameters of the human body and analyzing the data to allow physiologists to assess the well-being of a patient in real-time. In this context, it is worth mentioning that Matter can bring advances in the Wireless Body Area Network (WBAN) and, specifically, in the medical body area network [78]. The benefits are in terms of interoperability, security, cost savings, and constrained deployment. Specifically, the protocol ensures seamless data transfer across standards, promotes information exchange, provides strong cryptography, and overcomes vulnerabilities of some protocols in the PHY layer. Moreover, it enables the production of low-cost health monitoring solutions and opens the door to cross-standard interaction, extending the quantity of WBAN devices and facilitating non-invasive patient monitoring. Ultimately, it is worth mentioning that with the pandemic situation created by COVID-19, the adoption of IoMT technologies has impacted domains other than healthcare, such as smart homes, smart buildings, smart cities, transportation, and industry [79]. Since the treatment of this topic could be misleading to the subject of this survey, for a systematic review of the potential of IoMT applications in building smart healthcare systems, we limit ourselves to referring interested parties to [80].

4.6.2. Ambient assisted living

AAL encompasses a range of home automation solutions that help improve our daily lives by enhancing the environments in which we spend most of our time with devices and sensors to monitor our health status and provide *ad hoc* (or tailored) solutions to promote an active and health aging. Consistently, an AAL system uses IoT technologies and services to support the independent living and well-being of older adults in their own homes or communities by monitoring environmental, health, and location parameters. An AAL system should be able to provide assistance, send alerts and reminders, and entertain and promote social interactions [81]. However, one of the biggest challenges for AAL systems is interoperability. This peculiarity is essential to ensure the reliability, scalability, security, and usability of any AAL system. The two main issues that affect interoperability in AAL are (i) the heterogeneity of devices and communication protocols present in different scenarios, and (ii) the lack of common standards and ontologies to represent and share data between different AAL components. To address these issues, the solutions presented so far have focused on the development of smart gateways that act as intermediaries between different devices and protocols [82,83], the use of semantic web technologies and ontologies to enable common understanding and reasoning across heterogeneous data sources and services [84,85], the application of service-oriented architectures and middleware platforms to facilitate the discovery, composition, and orchestration of different AAL services and applications [81,86].

An interesting case is presented by Sukaridhoto et al. [87] that surveys a conceptual Healthcare IoT system for monitoring outpatient and inpatient activities. In this context, the Matter protocol is used to increase the overall interoperability of the system. The Matter accessories collect some patient health information such as body temperature, blood pressure, and heart rate. Sensed data are then conveyed to a Thread border router (specifically a Google Nest Hub 2nd generation) that routes them to a health monitoring server for storage and analytics. The study highlights how the Matter protocol is suitable for local area monitoring or inpatient activities. While for outpatient healthcare monitoring authors propose MQTT as a data communication protocol. The system is a well-defined example of a potential Matter-based healthcare monitoring scenario that provides interoperability, flexibility, and security. Besides this example, there is still a conceptual gap on the topic, as there is a lack of literature that presents Matter-based interoperability solutions in AAL. However, given the affinity of AAL with the home automation domain, one would expect a large body of literature production on the subject in the near future.

5. Open questions

Below, we summarize some of the key questions that have emerged since the introduction of the Matter protocol. The answers we provide draw from lessons learned from implementing similar solutions in the past, expectations set by the Connectivity Standards Alliance, and the research evidence published on the topic to date.

- *Does the ZigBee protocol guarantee direct compatibility with Matter in the future?* Apparently not. To enable communication between Matter devices and native ZigBee devices, a properly configured bridge is required to interpose between the ZigBee hub and the Matter-enabled hub. This may improve ZigBee networks because, as highlighted in [50], ZigBee introduces unresolved vulnerabilities into IoT networks, which Matter can address.
- *Is the current Matter specification capable of directly managing IoT devices designed specifically for the energy sector?* The answer seems to be negative, as suggested by [88]. However, foundational work has been initiated for future advancements in this field [65,67].
- *Will Matter truly become an open standard like TCP?* While it is royalty-free and freely implementable for vendors adhering to the protocol specification, there is no assurance that Matter will not evolve into a proprietary standard controlled by a select group of stakeholders. The current Specification is publicly available, but, as noted in [89], accessing the version under development requires a project member status, obtainable with an annual subscription fee of 20,000 USD.[21]
- *Is full interoperability between different devices truly seen as beneficial by all consortium members?* In [90], Matter is cited as a standard technology addressing incompatibilities between smart home devices due to differing low-power radio technologies. However, the study also emphasizes how interoperability remains constrained, as manufacturers might not see a benefit in allowing competitors full control over their devices. This suggests a potential risk: if Matter becomes widely adopted as a standard, it might evolve into a protocol dominated by a few key players, potentially sidelining smaller IoT companies.

The future of Matter remains uncertain. Many manufacturers, having already standardized their new product lines—such as plugs, light bulbs, and locks—are still reserving advanced monitoring features for their official applications, not providing full access to third-party controllers. The hope is that as more companies have their devices Matter-certified, this trend will diminish.

5.1. Overcoming limitations

The primary challenges of the Matter protocol relate to handling resource-constrained devices, orchestrating complex scenarios with a diverse array of brand-specific platform devices, the still limited number of certified devices available, and the need to define standards distinct from the Thread protocol for various border routers.

Some Matter-certified devices, especially those powered by batteries, grapple with limitations in energy and computational resources. Recognizing the imperatives of energy conservation, a category of intermittently connected devices has been introduced. These devices conserve energy by predominantly remaining in a "sleepy" mode, periodically waking up to signify their active status. Such power-saving strategies can be inherent to the device's hardware, such as wake-up radios, or can be realized at the software level. For instance, OpenThread recently launched the Sleepy End Device (SED) operating mode. This mode capitalizes on specific protocol functions to intermittently deactivate the device's radio, thereby curtailing its overall power consumption. SED effectively augments the lifespan of energy-constrained Matter endpoints without mandating specialized hardware. However, these intermittently connected devices might face challenges during interactions with users or platforms, potentially being misidentified as offline. To counteract this, the latest specification furnishes an SDK and APIs designed to minimize the chances of SEDs being inaccurately reported as offline during interactions.

Currently, Matter does not offer explicit guidance on orchestrating complex scenarios that necessitate coordination and automation across heterogeneous devices and platforms. This challenge can be addressed by supplementing the updated Specification with insights from project partners, steering developers towards potential interoperability scenarios that incorporate a diverse device ecosystem.

[21] The CSA subscription plan details are available at https://csa-iot.org/become-member.

The relatively narrow spectrum of devices currently supported by the protocol, with a limited feature set, can largely be attributed to the protocol's nascent stage. Previous discussions have underscored potential bottlenecks that might hinder the broad-based adoption of certified products, alongside potential solutions that could expedite the protocol's mainstream acceptance.

Broadening support to encompass Zigbee, Z-Wave, and Bluetooth could obviate the need for distinct bridges, narrowing the requirement down to just the Matter bridge. This would simplify integration and reduce costs across a plethora of branded devices.

Given the potential to address these limitations with concerted efforts, it is plausible that as the standard matures, many of these challenges will either be ameliorated or completely resolved.

6. Conclusion

Matter emerges as a groundbreaking, royalty-free interoperability protocol tailored for smart homes, birthed through the collective effort of leading tech conglomerates under the banner of the Connectivity Standards Alliance. Its core proposition lies in offering a standardized suite of commands transmitted over local IP networks, ensuring seamless communication across diverse device ecosystems. In essence, devices that *speak* Matter adhere to a common command language.

Historically, new technologies have often spanned decades before achieving mainstream adoption. Matter, however, aspires to defy this norm, projecting its relevance beyond just home automation.

Throughout this research, we delved into Matter's salient features, anchored by its inaugural official specification. Our exploration spanned an inventory of current Matter-certified products and software, either already available or on the cusp of release. Concurrently, we gauged the academic landscape surrounding the protocol, spotlighting its inherent challenges and prospective potential. This analysis helped chart a trajectory for Matter's evolution and underscored its potential impact across a myriad of application domains.

Yet, it is essential to recognize that Matter is still in its nascent stages. The limited academic discourse on the topic attests to its novelty. As of this writing, the CSA has unveiled version 1.1 of the Matter specification, enhancing its compatibility with intermittently connected devices — predominantly energy-conserving, battery-driven devices like door locks, switches, and contact sensors.

While expectations soar, lingering apprehensions persist. There is a palpable concern that Matter might, over time, metamorphose into yet another rival to extant standards, rather than rise as the coveted universal standard poised to transcend the limitations of contemporary solutions.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This publication was produced with the co-funding of the European Union - Next Generation EU, in the context of The National Recovery and Resilience Plan, Investment 1.5 Ecosystems of Innovation, Project Tuscany Health Ecosystem (THE), CUP: B83C22003920001.

References

[1] C.S. Alliance, Amazon, Apple, Google, and the Alliance and its board members form industry working group to develop a new, open standard for smart home device connectivity, 2022, Retrieved April 4, 2022 from. URL: https://csa-iot.org/newsroom/connectedhomeip/.
[2] R.K. Kodali, S. Soratkal, MQTT based home automation system using ESP8266, in: 2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), IEEE, Agra, India, 2016, pp. 1–5.
[3] S. Blechmann, I. Sowa, M.H. Schraven, R. Streblow, D. Müller, A. Monti, Open source platform application for smart building and smart grid controls, Autom. Constr. 145 (2023) 104622.
[4] H.H. Alshammari, The internet of things healthcare monitoring system based on MQTT protocol, Alex. Eng. J. 69 (2023) 275–287.
[5] H.A. Khattak, M. Ruta, E.E. Di Sciascio, CoAP-based healthcare sensor networks: A survey, in: Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST), 14th-18th January, 2014, IEEE, Islamabad, Pakistan, 2014, pp. 499–503.
[6] M. Bansal, et al., Application layer protocols for internet of healthcare things (IoHT), in: 2020 Fourth International Conference on Inventive Systems and Control (ICISC), IEEE, Coimbatore, India, 2020, pp. 369–376.
[7] B. Soewito, F.E. Gunawan, I.G.P. Kusuma, et al., Websocket to support real time smart home applications, Procedia Comput. Sci. 157 (2019) 560–566.
[8] Thread Group, Thread Border Router, Technical Report, White Paper, 2022.
[9] Thread Group, Thread and Matter in Smart Buildings, Technical Report, White Paper, 2022.
[10] H.-S. Kim, S. Kumar, D.E. Culler, Thread/OpenThread: A compromise in low-power wireless multihop network architecture for the Internet of Things, IEEE Commun. Mag. 57 (7) (2019) 55–61.
[11] R. Herrero, Fundamentals of IoT Communication Technologies, Springer, Berlin, Heidelberg, 2022.
[12] F.R. Biallas, Analyse unterschiedlicher funkstandards des smart home sektors für den einsatz in vernetzten einzelraumregelungen, 2022.

[13] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376.
[14] W. Kassab, K.A. Darabkh, A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations, J. Netw. Comput. Appl. 163 (2020) 102663.
[15] M. Mihaeljans, A. Skrastins, IoT concept and SDN fusion in consumer products: Overview, in: 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), IEEE, 2023, pp. 1–6.
[16] M. Schenk, Matter and the Web of Things (Ph.D. thesis), Technische Universität Wien, 2023.
[17] K. Shashwat, F. Hahn, X. Ou, A. Singhal, Security analysis of trust on the controller in the matter protocol specification.
[18] A. Ghasempour, Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges, Inventions 4 (1) (2019) 22.
[19] M. Jung, J. Weidinger, C. Reinisch, W. Kastner, C. Crettaz, A. Olivieri, Y. Bocchi, A transparent ipv6 multi-protocol gateway to integrate building automation systems in the internet of things, in: 2012 IEEE International Conference on Green Computing and Communications, IEEE, Besancon, France, 2012, pp. 225–233.
[20] K. Rose, S. Eldridge, L. Chapin, The internet of things: An overview, Internet Soc. (ISOC) 80 (2015) 1–50.
[21] M. Noura, M. Atiquzzaman, M. Gaedke, Interoperability in internet of things: Taxonomies and open challenges, Mob. Netw. Appl. 24 (2019) 796–809.
[22] V. Miori, D. Russo, Domotic evolution towards the IoT, in: 2014 28th International Conference on Advanced Information Networking and Applications Workshops, IEEE, Victoria, BC, Canada, 2014, pp. 809–814.
[23] A. Gabillon, Q.Z. Sheng, W. Mansoor, T. Perumal, A.R. Ramli, C.Y. Leong, K. Samsudin, S. Mansor, Interoperability among heterogeneous systems in smart home environment, in: Web-Based Information Technologies and Distributed Systems, Vol. 2, Springer, 2010, pp. 141–157.
[24] T. Perumal, A.R. Ramli, C.Y. Leong, S. Mansor, K. Samsudin, Interoperability for smart home environment using web services, Int. J. Smart Home 2 (4) (2008) 1–16.
[25] J.E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, D. Mosse, Seamless integration of heterogeneous devices and access control in smart homes, in: 2012 Eighth International Conference on Intelligent Environments, IEEE, NW Washington, DC, USA, 2012, pp. 206–213.
[26] F. Ullah, M.A. Habib, M. Farhan, S. Khalid, M.Y. Durrani, S. Jabbar, Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare, Sustain. Cities Soc. 34 (2017) 90–96.
[27] P. Barsocchi, A. Calabrò, F. Lonetti, E. Marchetti, F. Palumbo, Leveraging smart environments for runtime resources management, in: Software Quality: Methods and Tools for Better Software and Systems: 10th International Conference, SWQD 2018, Vienna, Austria, January 16–19, 2018, Proceedings 10, Springer, Swiss, 2018, pp. 171–190.
[28] I. Froiz-Míguez, T.M. Fernández-Caramés, P. Fraga-Lamas, L. Castedo, Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes, Sensors 18 (8) (2018) 2660.
[29] A.E. Khaled, S. Helal, Interoperable communication framework for bridging RESTful and topic-based communication in IoT, Future Gener. Comput. Syst. 92 (2019) 628–643.
[30] G. Bouloukakis, N. Georgantas, P. Ntumba, V. Issarny, Automated synthesis of mediators for middleware-layer protocol interoperability in the IoT, Future Gener. Comput. Syst. 101 (2019) 1271–1294, http://dx.doi.org/10.1016/j.future.2019.05.064.
[31] W. Dong, J. Lv, G. Chen, Y. Wang, H. Li, Y. Gao, D. Bharadia, TinyNet: A lightweight, modular, and unified network architecture for the internet of things, in: Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services, Association for Computing Machinery, New York, NY, USA, 2022, pp. 248–260.
[32] D. Griffith, Innovation at the edge: IoT 2.0, in: 2022 IEEE Asian Solid-State Circuits Conference (A-SSCC), IEEE, Taipei, Taiwan, China, 2022, pp. 2–3.
[33] J. Wytrębowicz, K. Cabaj, J. Krawiec, Messaging protocols for IoT systems—A pragmatic comparison, Sensors 21 (20) (2021) 6904.
[34] W. Zegeye, A. Jemal, K. Kornegay, Connected smart home over matter protocol, in: 2023 IEEE International Conference on Consumer Electronics (ICCE), IEEE, Las Vegas, NV, USA, 2023, pp. 1–7.
[35] A. Ortega i Blasi, Evaluating Thread Protocol in the Framework of Matter (Master's thesis), Universitat Politècnica de Catalunya, 2022.
[36] T. Domínguez-Bolaño, O. Campos, V. Barral, C.J. Escudero, J.A. García-Naya, An overview of IoT architectures, technologies, and existing open-source projects, Internet Things 20 (2022) 100626.
[37] S. Tlili, S. Mnasri, T. Val, The Internet of Things enabling communication technologies, applications and challenges: a survey, Int. J. Wirel. Mob. Comput. 23 (1) (2022) 9–21.
[38] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, T. Taleb, Survey on multi-access edge computing for internet of things realization, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2961–2991.
[39] R.-R. Shrivastwa, Z. Bouakka, T. Perianin, F. Dislaire, T. Gaudron, Y. Souissi, K. Karray, S. Guilley, An embedded AI-based smart intrusion detection system for edge-to-cloud systems, in: Cryptography, Codes and Cyber Security: First International Conference, I4CS 2022, Proceedings, Springer, Casablanca, Morocco, 2023, pp. 20–39.
[40] S. Sidhardhan, D. Das, Reliable edge service for IoT home environment, in: 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), IEEE, Bengaluru, India, 2021, pp. 1–4.
[41] S. Gvozdenovic, J.K. Becker, J. Mikulskis, D. Starobinski, Multi-protocol IoT network reconnaissance, in: 2022 IEEE Conference on Communications and Network Security (CNS), IEEE, Austin, USA, 2022, pp. 118–126.
[42] C. Gomez, J. Paradells, Wireless home automation networks: A survey of architectures and technologies, IEEE Commun. Mag. 48 (6) (2010) 92–101.
[43] P. Domingues, P. Carreira, R. Vieira, W. Kastner, Building automation systems: Concepts and technology review, Comput. Stand. Interfaces 45 (2016) 1–12.
[44] A.B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, Home automation in the wild: challenges and opportunities, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, New York, NY, USA, 2011, pp. 2115–2124.
[45] A. Ganassin, Analysis of the Matter protocol and implementation of the Thermostat device type on a prototype, 2021, URL: http://hdl.handle.net/20.500.12608/29050.
[46] M. Sioutis, V.C. Pham, Y. Tan, S. Morooka, K. Kawanishi, ECHONET lite as an interface for Z-wave devices in a home automation system, in: 2022 IEEE 11th Global Conference on Consumer Electronics (GCCE), IEEE, Osaka, Japan, 2022, pp. 788–792.
[47] J.P. Dias, A. Restivo, H.S. Ferreira, Designing and constructing internet-of-Things systems: An overview of the ecosystem, Internet Things 19 (2022) 100529.
[48] L. Andraschko, P. Wunderlich, D. Veit, S. Sarker, Towards a taxonomy of smart home technology: a preliminary understanding, in: International Conference on Information Systems (ICIS) 2021, ICIS, Austin, Texas, 2021.
[49] J. Yang, L. Sun, A comprehensive survey of security issues of smart home system:"Spear" and "Shields", theory and practice, IEEE Access 10 (2022) 124167–124192.
[50] N. Shafqat, D.J. Dubois, D. Choffnes, A. Schulman, D. Bharadia, A. Ranganathan, Zleaks: Passive inference attacks on Zigbee based smart homes, in: Applied Cryptography and Network Security: 20th International Conference, ACNS 2022, Rome, Italy, June 20–23, 2022, Proceedings, Springer, Rome, Italy, 2022, pp. 105–125.
[51] J. Bauer, R. Wichert, C. Konrad, M. Hechtel, S. Dengler, S. Uhrmann, M. Ge, P. Poller, D. Kahl, B. Ristok, et al., ForeSight–user-centered and personalized privacy and security approach for smart living, in: 10th International Conference on Distributed, Ambient and Pervasive Interactions, (DAPI), Springer International Publishing, Cham, 2022, pp. 18–36.
[52] M. Salnikov, Smart Home Security: Betrachtung des IoT Standards Matter aus einer Security Perspektive (Ph.D. thesis), Hochschule Offenburg, 2022.

[53] D.-G. Akestoridis, V. Sekar, P. Tague, On the security of Thread networks: Experimentation with OpenThread-enabled devices, in: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, ACM, New York, NY, USA, 2022, pp. 233–244.
[54] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, Industrial internet of things: Challenges, opportunities, and directions, IEEE Trans. Ind. Inform. 14 (11) (2018) 4724–4734.
[55] P. Brooks, Ethernet/IP-industrial protocol, in: ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No. 01TH8597), Vol. 2, IEEE, Antibes-Juan les Pins, France, 2001, pp. 505–514.
[56] V. Schiffer, Common industrial protocol (CIP™) and the family of CIP networks, in: Industrial Communication Technology Handbook, CRC Press, Boca Raton, Florida, USA, 2017, 9–1.
[57] G. Veneri, A. Capasso, Hands-on Industrial Internet of Things: Create a Powerful Industrial IoT Infrastructure using Industry 4.0, Packt Publishing Ltd, Birmingham, 2018.
[58] E. Artetxe, O. Barambones, I. Calvo, P. Fernández-Bustamante, I. Martin, J. Uralde, Wireless technologies for industry 4.0 applications, Energies 16 (3) (2023) 1349.
[59] K.M. Hou, X. Diao, H. Shi, H. Ding, H. Zhou, C. de Vaulx, Trends and challenges in AIoT/IIoT/IoT implementation, Sensors 23 (11) (2023) 5074.
[60] E. Fantin Irudaya Raj, M. Appadurai, Internet of things-based smart transportation system for smart cities, in: Intelligent Systems for Social Good: Theory and Practice, Springer, New York, NY, USA, 2022, pp. 39–50.
[61] S.K. Datta, R.P.F. Da Costa, J. Härri, C. Bonnet, Integrating connected vehicles in Internet of Things ecosystems: Challenges and solutions, in: 2016 IEEE 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, Coimbra, Portugal, 2016, pp. 1–6.
[62] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid—The new and improved power grid: A survey, IEEE Commun. Surv. Tutor. 14 (4) (2011) 944–980.
[63] Q.-D. Ho, Y. Gao, T. Le-Ngoc, Challenges and research opportunities in wireless communication networks for smart grid, IEEE Wirel. Commun. 20 (3) (2013) 89–95.
[64] C.W. Gellings, The Smart Grid: Enabling Energy Efficiency and Demand Response, CRC Press, Boca Raton, Florida, USA, 2020.
[65] A. Fiastri, A solution to tackle the variability of renewable energy generation: using the Matter IoT standard to enable implicit demand response for private consumers, 2022.
[66] S. Nagashige, K. Tanaka, H. Suzuki, Extension of iHAC hub specification for supporting interconnectivity between matter and ECHONET lite, in: 2022 IEEE 11th Global Conference on Consumer Electronics (GCCE), IEEE, Osaka, Japan, 2022, pp. 779–780.
[67] S. Matsumoto, Echonet: A home network standard, IEEE Pervasive Comput. 9 (3) (2010) 88–92.
[68] M.K. Hasan, A.A. Habib, S. Islam, M. Balfaqih, K.M. Alfawaz, D. Singh, Smart grid communication networks for electric vehicles empowering distributed energy generation: Constraints, challenges, and recommendations, Energies 16 (3) (2023) 1140.
[69] A. Choroszucho, M. Sumorek, J. Żukowski, Air quality monitoring device to optimize working and learning conditions, in: The Problematic Aspects of Energy Efficiency '22, Bialystok University of Technology, Poland, 2022, pp. 38–48.
[70] A.M. Rahmani, T.N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, P. Liljeberg, Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach, Future Gener. Comput. Syst. 78 (2018) 641–658.
[71] P.P. Ray, D. Dash, D. De, Edge computing for Internet of Things: A survey, e-healthcare case study and future direction, J. Netw. Comput. Appl. 140 (2019) 1–22.
[72] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, M. Alizadeh, The application of internet of things in healthcare: a systematic literature review and classification, Univers. Access Inf. Soc. 18 (2019) 837–869.
[73] G.J. Joyia, R.M. Liaqat, A. Farooq, S. Rehman, Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain, J. Commun. 12 (4) (2017) 240–247.
[74] M. Robkin, S. Weininger, B. Preciado, J. Goldman, Levels of conceptual interoperability model for healthcare framework for safe medical device interoperability, in: 2015 IEEE Symposium on Product Compliance Engineering (ISPCE), IEEE, Chicago, Illinois, USA, 2015, pp. 1–8.
[75] S.R. Vangimalla, M. El-Sharkawy, Interoperability enhancement in health care at remote locations using thread protocol in uavs, in: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, IEEE, Washington, DC, USA, 2018, pp. 2821–2826.
[76] N. Shankar, M.K. Nallakaruppan, V. Ravindranath, M. Senthilkumar, B.P. Bhagavath, Smart IoMT framework for supporting UAV systems with AI, Electronics 12 (1) (2023) 86.
[77] S. Tanwar, J. Vora, S. Kaneriya, S. Tyagi, N. Kumar, V. Sharma, I. You, Human arthritis analysis in fog computing environment using Bayesian network classifier and thread protocol, IEEE Consum. Electron. Mag. 9 (1) (2019) 88–94.
[78] K. Hasan, K. Biswas, K. Ahmed, N.S. Nafi, M.S. Islam, A comprehensive review of wireless body area network, J. Netw. Comput. Appl. 143 (2019) 178–198.
[79] M. Umair, M.A. Cheema, O. Cheema, H. Li, H. Lu, Impact of COVID-19 on IoT adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial IoT, Sensors 21 (11) (2021) 3838.
[80] R. Dwivedi, D. Mehrotra, S. Chandra, Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review, J. Oral Biol. Craniofac. Res. 12 (2) (2022) 302–318.
[81] G. Cicirelli, R. Marani, A. Petitti, A. Milella, T. D'Orazio, Ambient assisted living: a review of technologies, methodologies and future perspectives for healthy aging of population, Sensors 21 (10) (2021) 3549.
[82] D.C. Yacchirema, C.E. Palau, M. Esteve, Enable IoT interoperability in ambient assisted living: Active and healthy aging scenarios, in: 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, Las Vegas, NV, USA, 2017, pp. 53–58.
[83] G. Aloi, G. Caliciuri, G. Fortino, R. Gravina, P. Pace, W. Russo, C. Savaglio, Enabling IoT interoperability through opportunistic smartphone-based mobile gateways, J. Netw. Comput. Appl. 81 (2017) 74–84.
[84] H.K. Ngankam, H. Pigot, S. Giroux, OntoDomus: a semantic model for ambient assisted living system based on smart homes, Electronics 11 (7) (2022) 1143.
[85] A. Mastropietro, F. Palumbo, S. Orte, M. Girolami, F. Furfari, P. Baronti, C. Candea, C. Roecke, L. Tarro, M. Sykora, et al., A multi-domain ontology on healthy ageing for the characterization of older adults status and behaviour, J. Ambient Intell. Humaniz. Comput. 14 (2021) 8725—8743.
[86] L. Angelini, M. El Kamali, E. Mugellini, O. Abou Khaled, C. Röcke, S. Porcelli, A. Mastropietro, G. Rizzo, N. Boqué, J.M. Del Bas, et al., The NESTORE e-coach: designing a multi-domain pathway to well-being in older age, Technologies 10 (2) (2022) 50.
[87] S. Sukaridhoto, A. Prayudi, M.U.H. Al Rasyid, R.P.N. Budiarti, A survey and conceptual of Internet of Things system for remote healthcare monitoring, Bali Med. J. 12 (3) (2023) 2840–2845.
[88] S. El Jaouhari, E. Bouvet, Secure firmware Over-The-Air updates for IoT: Survey, challenges, and discussions, Internet Things 18 (2022) 100508.
[89] M. Loos, Security analysis of the matter protocol, 2023.
[90] M. Langheinrich, Standing on the platforms of giants, IEEE Pervasive Comput. 21 (3) (2022) 4–6.