buildings

MDPI

Article

IoT Middleware Platforms for Smart Energy Systems: An Empirical Expert Survey

Qamar Alfalouji [1], Thomas Schranz [1], Alexander Kümpel [2], Markus Schraven [2], Thomas Storek [2,3], Stephan Gross [4], Antonello Monti [4,5], Dirk Müller [2,3] and Gerald Schweiger [1,*]

1 Institute of Software Technology, Graz University of Technology, 8010 Graz, Austria; qamar.alfalouji@tugraz.at (Q.A.); thomas.schranz@tugraz.at (T.S.)
2 Institute for Energy Efficient Buildings and Indoor Climate, E.ON Energy Research Center, RWTH Aachen University, 52074 Aachen, Germany; akuempel@eonerc.rwth-aachen.de (A.K.); mschraven@eonerc.rwth-aachen.de (M.S.); tstorek@eonerc.rwth-aachen.de (T.S.); dmueller@eonerc.rwth-aachen.de (D.M.)
3 IEK-10, Forschungszentrum Jülich, 52428 Jülich, Germany
4 Center for Digital Energy Aachen, Fraunhofer FIT, 52074 Aachen, Germany; stephan.gross@fit.fraunhofer.de (S.G.); amonti@eonerc.rwth-aachen.de (A.M.)
5 Institute for Automation of Complex Power Systems, E.ON Energy Research Center, RWTH Aachen University, 52074 Aachen, Germany
* Correspondence: gerald.schweiger@tugraz.at

Abstract: Middleware platforms are key technology in any Internet of Things (IoT) system, considering their role in managing the intermediary communications between devices and applications. In the energy sector, it has been shown that IoT devices enable the integration of all network assets to one large distributed system. This comes with significant benefits, such as improving energy efficiency, boosting the generation of renewable energy, reducing maintenance costs and increasing comfort. Various existing IoT middlware solutions encounter several problems that limit their performance, such as vendor locks. Hence, this paper presents a literature review and an expert survey on IoT middleware platforms in energy systems, in order to provide a set of tools and functionalities to be supported by any future efficient, flexible and interoperable IoT middleware considering the market needs. The analysis of the results shows that experts currently use the IoT middleware mainly to deploy services such as visualization, monitoring and benchmarking of energy consumption, and energy optimization is considered as a future application to target. Likewise, non-functional requirements, such as security and privacy, play vital roles in the IoT platforms' performances.

Keywords: Internet of Things (IoT); IoT middleware platforms; energy systems; cyber-physical systems

Citation: Alfalouji, Q.; Schranz, T.; Kümpel, A.; Schraven, M.; Storek, T.; Gross, S.; Monti, A.; Müller, D.; Schweiger, G. IoT Middleware Platforms for Smart Energy Systems: An Empirical Expert Survey. *Buildings* **2022**, *12*, 526. https://doi.org/10.3390/buildings12050526

Academic Editors: Rui Castro and Hugo Morais

Received: 22 March 2022
Accepted: 18 April 2022
Published: 21 April 2022

1. Introduction

The Internet of Things (IoT) is understood as a ubiquitous, complex network of networkable, heterogeneous entities or "things" [1]. It collects environmental data; interacts with the physical world; communicates through internet standards; and provides applications, data transfer and data analysis [2] with minimal human interaction [3]. Developments in web and communication technology and the wide availability of microchips have accelerated the integration of computing machinery into all aspects of day-to-day life.

The application of IoT technology to the urban and building sector provides opportunities, especially within the context of sustainability [4,5]. Socioeconomic changes, such as the trend towards larger homes, the automation of household chores and the advent of energy-consuming entertainment devices, have caused the buildings sector to become the largest contributor to global energy demand [6], accounting for 40% of the energy consumption in the European Union (EU) [7] and 78% of greenhouse gas emissions in the EU and Iceland [8]. The integration of renewable energy technologies into the existing energy systems and the resulting decentralization and introduction of environmentally-friendly

energy technologies are promising use cases for IoT. Services such as monitoring, maintenance and predictive control can be used to manage distributed generation and storage technologies [9] and improve operational efficiency and reliability in the energy supply system [10]. The broad availability of operational sensor data stimulates the development of data-driven services, such as energy forecasting [11], automatic fault detection [12], demand-side management and predictive control [13]. Real-time data collection allows municipal, district and building operators to streamline monitoring and maintenance through automation. In the literature, there are many works describing the application of these technologies in practice [14–19].

Communication between networkable, heterogeneous computational components, i.e., machine to machine (M2M) communication, is a key requirement in any cyber system. However, state-of-the-art devices from different vendors often employ incompatible protocols and data formats, which inhibits interoperability. There are two approaches to mitigate this issue: (i) the introduction of universal standards and (ii) the use of translation layers, so-called middleware platforms, between the components. The introduction and even more importantly, the enforcement of standards, has proven non-trivial in many instances. Consider, for example, electric socket types in Europe, or controversies around different charger standards for small electronic devices [3]. Besides, the cost of retrofitting existing systems with components that adhere to novel universal standards can be prohibitive, so backward-compatibly has to be considered as well. Consequently, practitioners typically use middleware solutions in their IoT systems.

Due to the diverse set of requirements and applications, IoT platforms need to cover a wide range of functionalities, non-functional requirements and scales [20]. To match the growing demand, there exists a considerable number of commercial and non-commercial IoT solutions. However, only a few commercial competitors include the energy sector in their portfolios. Possible reasons include the severity of security risks in what is considered to be critical infrastructure and a lack of global, universal standards [3,14,21].

Main Contribution

The digitalization of the energy sector greatly contributes to the transition towards environmentally friendly, low emission energy systems [22]. Several initiatives, such as "Digitalising the energy sector" [23] and "GAIA-X" [24], aim to provide digital infrastructure and energy services by developing trustworthy intelligent solutions for power generation, energy storage, power transmission and consumption monitoring. The IoT is the backbone of such an intelligent system [25]. Since no standards for IoT middleware or IoT energy platforms exist [26], the requirements of such platforms are unknown, and providers will often start their business based on few available components which might not be sufficient for practitioners' needs. Hence, our study contributes to this digital transformation by gathering the opinions of experts on requirements, promising technologies, limitations, etc., of IoT middleware platforms for smart energy systems. Expert surveys are a powerful research method allowing the systematic study of hard-to-measure phenomena through the aggregation of specialized expert knowledge [27]. Based on expert interviews, we define requirements for IoT middleware platforms; these include topics such as vendor locks, security, data models and communication technologies. In addition, we analyze promising applications, such as control services and demand-side management. To the best of our knowledge, there are no expert surveys on IoT middleware platforms for smart energy systems. To assess the state-of-the-art and the requirements and challenges for IoT middleware in smart energy systems, we devised a two-stage research plan, comprising a literature review and a quantitative expert survey that included (i) city officials who were responsible for smart city projects, (ii) experts in energy and energy technology companies and (iii) experts who were planning and/or operating buildings and districts. The literature review stage included reviewing IoT platform architectures, functional and non-functional requirements and the most common technologies and protocols in order to formulate survey questions that represent the real market needs of the people who operate these

services in the energy sector. During the survey process, the experts were asked to list the tools they use/plan to use as IoT platforms, and their current and future applications; and to assess the importance of certain technologies, protocols and features in the IoT middleware frameworks.

The rest of the paper is organized as follows: In Section 2, we discuss recurring building blocks, concepts, protocols and functionalities found throughout the catalog of IoT middleware solutions for smart energy systems and identify the requirements and challenges in the development and roll-out of middleware platforms. In Section 3, we identify and analyze a set of commercial and non-commercial IoT middleware solutions used in the context of smart energy systems in terms of their functionalities, their non-functional characteristics and their protocols. In the subsequent sections, we present and discuss the results of the survey among building and smart city experts.

2. Background

There is a myriad of IoT devices offered by a considerable number of vendors, many of which ship with their own firmware that employs proprietary semantic models and communication protocols. While the choice of communication protocols has converged to a select few de facto standard protocols, such as Message Queuing Telemetry Transport (MQTT), Hypertext Transfer Protocol (HTTP), LoRaWAN and Bluetooth Low Energy (BLE), the problem of incompatible semantic models remains largely unsolved [28]. Consequently, most devices are incompatible with any software stack other than the one distributed by the vendor of the device. Therefore, operators often prefer integrated, proprietary solutions, even when these solutions do not fully address all their requirements [3].

Semantic models associating unambiguous, universal meaning to metadata are a key research interest. Sections 2.1–2.3 provide a brief background on the semantic interoperability and data models, main IoT architectures and definitions and the non-functional requirements most commonly considered important in smart energy systems.

2.1. Semantic Interoperability and Data Models

Semantic interoperability problems typically arise from ambiguities caused by missing standardization in the metadata schemata employed by the components of a heterogeneous system. The schemata most commonly found in the context of building automation are:

eXtensible Markup Language (XML) [29]: which is a hierarchically structured data model, where comparison with a XML Schema Definition (XSD) is used to verify its structure. Information about things (concepts) discussed by the data model is generally fully contained within a single XML document.

Semantic Web Technologies [28]: The Resource Description Framework (RDF) and RDF schema (RDFS) constitute a graph-structured data model that is designed as a distributed knowledge-based system. RDF uses shared resource identifiers, which allows for expanding knowledge by defining entities that are linked to each other. The Web Ontology Language (OWL) RDF extends the RDF capability to organize concepts in a more object-oriented fashion and a more formalized description logic (cardinality and allowable relationships—OWL).

JavaScript Object Notation (JSON) [30]: is a lightweight, data-interchange, language independent format which uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl and Python. JSON is built on two structures: a collection of name/value pairs, such as objects, structs and associative arrays in usual programming languages; and an ordered list of values similar to arrays, vectors and lists.

Significant effort has been devoted to introducing universal standards for a metadata schema in building automation by several non-commercial initiatives, such as Project Haystack [31], the Brick Schema [32], the IPSO smart object data model [33], the oneM2M specifications [34] and the Smart Appliance REFerence ontology (SAREF) [35], developed

by the European Telecommunications Standards Institute (ETSI). The three most popular projects are:

Project Haystack is a suite of open-source technologies. The main concept in Haystack is the use of "tags," which are pieces of information that document the attributes of any entity. Haystack defines data types (an extended version of JSON, to facilitate data exchange), file types (text format definitions to exchange the Haystack data types), an HTTP API protocol (for data exchange between servers and devices), an ontology (with a specific focus on buildings and districts) and so called "Defs" that can be used to define an extend the Haystack's ontology. Practitioners can use each of these definitions on their own or as a complete stack. The technologies and semantic data models provided by Project Haystack can be used in a wide variety of applications, including automation and control in energy, HVAC and lighting systems.

The *Brick Schema* provides an extensible open-source dictionary with terms, concepts and relationships needed for modeling buildings and districts. Flexible data models are designed to seamlessly integrate with existing systems. Brick applies a tagging system similar to Project Haystack; However, Brick provides formal semantic rules to ensure consistency and modeling support for spacial information, control relationships and operational relationships [36].

The *SAREF* ontology explicitly specifies core concepts in the smart applications domain, the main relationships between these concepts and axioms to constrain the usage of these concepts and relationships. The basic concept in SAREF is a device, which is defined as any tangible object that provides functions in a building. Functions are associated with commands and devices can change states. Devices can offer their functions as services to other devices via network. SAREF provides building blocks for each of these concepts and allows practitioners to separate and recombine the ontology based on individual needs. SAREF models can be seamlessly integrated with the Brick Schema.

A related concept was developed by OMA SpecWorks [37] in the form of the Next Generation Service Interfaces (NGSI) information model [38,39]. NGSI consists of an information model and an API to publish, query and subscribe to context information through well-defined operations. NGSI has been extended into the NGSI Linked Data (NGSI-LD) meta model and defines fundamental concepts of linked data models: entities, properties, relationships and metadata concepts: values and types. The FIWARE foundation [40] has developed an HTTP-based RESTful API for the revised NGSIv2 [41] interface.

2.2. IoT Platform Definition and Architecture

In the community, there is an ongoing discussion about the fundamental building blocks, layers and concepts in architecture of the IoT [26]. For instance, Farahzadi et al. [42] and da Cruz et al. [3] identify the three most relevant layers in IoT architecture as: users or applications; IoT platform; and devices and infrastructure. Jia et al. [43] and Domingo [44] define them as: perception, network and service. Keyur K. Patel [45] presents the IoT as four layers: smart device/sensor, gateways and networks, management service and application. According to the International Telecommunication Union, each IoT architecture should be divided into five layers: sensing, accessing, networking, middleware and application [46]. Another five-layer model, proposed by Antão et al. [47] consists of business, application, middleware, network and perception layers. Figure 1 illustrates the three architectures (three-layer, four-layer and five-layer architectures), their layers and their services. More advanced models, such as cloud and fog-based architectures [48] or the communication-centric IoT reference model [49], and various six- or seven-layer models, can also be found in the literature.

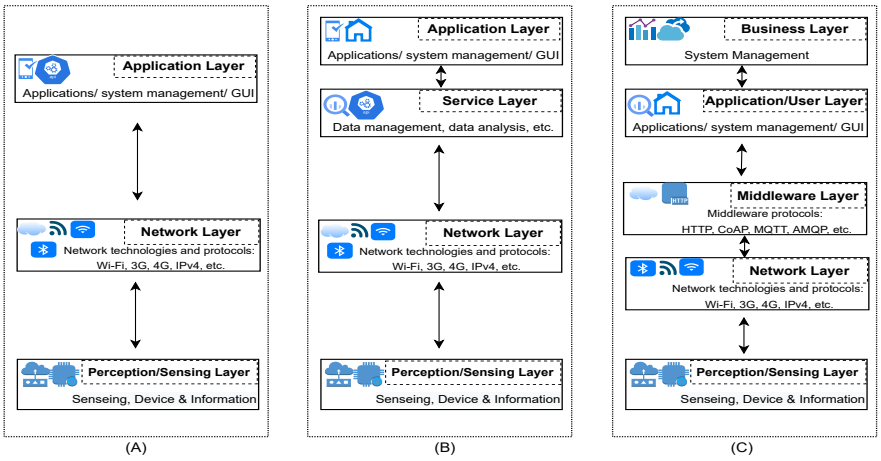

Figure 1. (**A**) Three-layer architecture [43,44], (**B**) four-layer architecture [45], (**C**) five-layer architecture [47].

In this paper, we use a five-layer approach, derived from the model in [47]. It proposes a simple separation of layers based on their functionalities and can be described as follows:

1. *Business Layer*: It offers a management and control of the IoT platform functions, including data analysis, (e.g., using Apache Spark [50] in case of dealing with big data) to help in the process of the decision-making by the responsible people.
2. *User/Application Layer*: It is responsible for delivering and presenting the application-specific service to the end user. It defines a wide range of applications where the IoT platforms can be used, such as smart services applications.
3. *Middleware Layer*: The concept of linking billions of individual devices and getting them to communicate with each other means that IoT systems are already inherently characterized by a high degree of heterogeneity [3]. The large number of different communication protocols, interfaces and platforms lead to heterogeneous IoT networks, which complicate the interaction.
   The task of middleware here is to function as a mediator between the devices by integrating the received data from the physical environment to the IoT-connected devices, networks and servers. This integration process also includes all the necessary operations, such as storing, analyzing and processing the data, allowing the connectivity between different and complex programs, which were not originally designed to provide this feature. Various protocols are used to provide the communication and services to the application in this layer. These protocols correspond to the application layer protocols in OSI model [51], such as:
   - The Hypertext Transfer Protocol (HTTP) [52]: This has been the foundation for data communication for the World Wide Web (i.e., Internet) since 1990 [53]. HTTP is a Transmission Control Protocol (TCP)/Internet Protocol (IP)-based, application-level protocol for distributed, collaborative hypermedia information systems. It is used to deliver data (HTML files, image files, query results, etc.) on the Internet, supporting both request/response and client/server interaction modes.
   - The Constrained Application Protocol (CoAP) [54]: An upgraded version of HTTP, designed for the resource constrained applications such as IoT, wireless sensor networks (WSNs) and machine to machine (M2M) communication. One reason for the CoAP's reduced complexity is the use of User Diagram Protocol (UDP) instead of TCP in HTTP, with acknowledgment messages in order to introduce a reliable communication based on a request/response interaction.
   - Message Queuing Telemetry Transport (MQTT) [55]: A protocol that enables a publish/subscribe messaging communication mode in a lightweight way. It is useful for connections with remote locations, where the bandwidth is limited.

It was originally designed for TCP/IP network, but other extensions such as MQTT-SN support UDP, ZigBee, etc.

- OPC Unified Architecture (OPC UA) [56]: It is a service-oriented, technology-independent and platform-independent approach. It has created new and easy possibilities for communicating with Linux/Unix systems or embedded controls on other platforms and for implementing OPC connections over the Internet supporting both TCP and UDP. The fundamental element in OPC UA is the use of information modeling framework that turns data into information based on rules and building blocks necessary to expose an information model, and this imposed the different data models, which are described in Section 2.1. The communication in OPC UA uses the client/server and publish/subscribe (PubSub) schemes.
- Extensible Messaging and Presence Protocol (XMPP) [57]: An open XML technology for real-time communication, which powers a wide range of applications, including instant messaging, presence and collaboration using the point/point interaction over TCP transport. The name of this protocol presents its main features and functionalities as: X (eXtensible): defines that the technology is designed to be extensible and an open system; M (Messaging): describes the exchanged instant messages (IM) between clients, and which happens in real-time using a push mechanism to avoid increasing unnecessary network loads; P (Presence): determines the state of an XMPP entity as online, offline, busy, etc.; P (Protocol): expresses it as a set of standards that allows systems to talk to each other.
- Advanced Message Queuing Protocol (AMQP): An open standard for passing business messages between applications or organizations using TCP. It connects systems, feeds business processes with the information they need and reliably transmits onward the instructions that achieve their goals using the point/point and publish/subscribe interaction modes [58]. It was designed to achieve main goals of: message orientation; queuing; routing; security; reliability; interoperability.
- Data Distribution Service (DDS) [59]: A middleware, M2M, Object Management Group (OMG) protocol and API standard for data-centric connectivity. It integrates the components of a system, providing low-latency data connectivity, high reliability and high scalability in publish/subscribe and request/response patterns over TCP and UDP.

4. Network Layer: It is also known as the *transport layer*; it is responsible for transporting the data provided by the perception layer to the application layer. It uses an enormous number of standards and protocols to enable this connection, such as:

- IP version 6 (IPv6) [60]: This has been designed to be an evolutionary step from IP version 4 (IPv4). The changes from IPv4 to IPv6 fall into the these main categories: expanded addressing capabilities; header format simplification; improved support for extensions and options; flow labeling capability; authentication and privacy capabilities.
- ZigBee [61]: A low data rate, low-power-consumption, low cost, wireless networking protocol, to target automation and remote control applications. ZigBee's best quality is its low-power-consumption that can allow batteries in devices using ZigBee to last for several years. The main advantages of ZigBee over Z-Wave are the higher data rate and the ability to connect an unlimited number of nodes together.
- Z-Wave [62,63]: A wireless protocol evolved by Zensys and confirmed by the Z-Wave Alliance for automation devices for homes and commercial environments. It enables reliable transmission of short messages from the control unit to one or more devices in the network with the minimum noise, low-power-consumption (less than ZigBee) and long battery life. It also operates at a low frequency range (800–900 MHz), which means a less congested band and covers a larger range

of data transmission. On the other hand, in comparison with ZigBee, Z-Wave allows connecting a limited number of nodes, with lower data rates.

- Bluetooth [64]: A wireless technology standard that is used for exchanging data between fixed and mobile devices over short distances using Ultra High Frequency (UHF) radio waves and building personal area networks (PANs) instead of wire connections. In the most widely used mode, transmission power is limited to 2.5 milliwatts, giving it a very short range of up to 10 m (30 feet).
- WiFi [65]: It (also called 802.11) was released in 1997. It is a wireless technology that transmits data using high frequencies over short ranges (100 m/300 feet outdoors and 50 m/150 feet indoors). WiFi has different types based on the chosen frequency and transmission rate, such as 802.11a, 802.11b, 802.11g and 802.11n. The main limitations of WiFi include its susceptibility to interference from devices that use the same frequency band such as Bluetooth devices, in addition to the impact of obstructions on its signal path, which may lock the signal in some cases.
- 4G/Long Term Evolution (LTE) [66]: Telecommunication networks are classified into generations based on speed, connectivity and reliability standards set by the International Telecommunications Union-Radio communications sector (ITU-R). 4G is the 4th generation of communication services. It was developed in 2009 after the two older generations 2G and 3G. It has slowly replaced 3G, since it is about 10 times faster than 3G. It also provides more capacity than older generations, and thus larger bandwidth. LTE is the technology behind 4G, and it was designed at the same time as some other standards, such as the UMB (Ultra Mobile Broadband) and the Worldwide Interoperability for Microwave Access (WiMax). LTE is the global standard technology for cellular communications. It is an open, interoperable standard used by virtually all carriers. It provides mobile and broadband data, telephone service with high speed and supports public safety functions as well.
- 5G [67]: The 5th generation mobile network is a wireless standard which was designed after 4G networks. 5G networks connects virtually everyone and everything, including machines, objects and devices. The main advantage of the 5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra low latency, more reliability, higher network capacity and more availability than any previous mobile network technologies.
- LoRAWAN: One of the low-power wide area networking (LPWAN) technologies. It is a wireless networking protocol which uses the LoRa radio modulation technique layer. It features low-power operation (around 10 years of battery lifetime), a low data rate and a long communication range. It was developed by Cycleo, a French company acquired by Semtech [68].
- Low-Power Personal Wireless Area Networks (6LoWPAN): A developing standard from the Internet Engineering Task Force (IETF) 6LoWPAN Working Group. It was designed from the start to be used in small/pico sensor networks [69]. This type of wireless sensor network sends data as packets using IPv6—and here is where the name comes from—over Low-Power Personal Wireless Area Networks.
- Long-term evolution machine (LTE-M) [70]: An LPWAN technology (also called LTE-MTC or LTE Cat M) which allows the reuse of an LTE installed base with extended coverage. LTE M, which stands for LTE-Machine Type Communication (MTC), is also a LPWAN technology developed by 3GPP to enable devices and services specifically for IoT applications.
- Narrow Band Iot (NB-IoT) [70]: An LPWAN radio technology deployed over mobile networks which is especially suited for indoor coverage, low cost, long battery life and a large number of devices.

5. Perception layer: Physical/device layer, which includes all the passive, semi-passive and active hardware needed for gathering information from the environment, or taking actions in the physical system, such as sensors, actuators and other physical devices.

2.3. Non-Functional Requirements and Challenges of IoT Platforms

Non-Functional Requirements (NFRs) can be defined as the system attributes, which are not directly related to the offered functionalities, but are related to the emerging properties of the system. The importance of NRFs of the IoT middleware platform changes based on the perspective, the system domain and the end-users, and they provide a number of restrictions and challenges that the platform needs to address. Hence, when considering the smart cities and smart buildings domain, NFRs define the following challenges:

- *Interoperability*: Different components of the IoT system must be able to connect and contact to each other. Historically, the building automation domain has always had interoperability issues, especially due to the segmented building process, leading to contractors offering trade-specific devices which are often incapable of communicating with devices from other trades. According to the economic research, up to 60% of the value that IoT systems might reveal is now locked by a lack of interoperability. Considering this, the IoT offers a great chance to actually improve interoperability by integrating and standardizing different components within the IoT platform [71].
  The interoperability challenge combines three elements:
  1. Device and connectivity: the starting point of the IoT architecture, which includes device capabilities and protocols.
  2. Data: several problems may arise when trying to combine data from different sources for different needs.
  3. Services/applications: these problems occur in the case of using data generated by a specific IoT device, in another application.
- *Scalability*: Device scalability defines its ability to adapt to the new changes in the environment, which is an essential feature for the growing IoT systems. Reliable IoT middleware needs to provide similar functionalities and similar quality of service (QoS) in small-scale and in large-scale environments [72].
- *Flexibility and Openness* [73]: Any IoT system needs to be flexible enough to support future technologies. Manufacturers typically create specialized hardware which gives optimal performance, while on the other hand, limiting the hardware's ability to track new updates and features. This introduces one of the most challenging problems for the IoT frameworks: vendor locking. Hence, a balance between software features and specialized hardware capabilities is one approach that must be considered in order to achieve the necessary flexibility of the system. The need for hardware-independence introduces the need for open IoT platforms, open standards, open APIs and open data. In particular, openness in smart cities and buildings services is critical, since such systems usually include humans, which in turn increases the importance of having a flexible, resilient and open platforms, which allows all possible users actions such as the data exchange.
- *Energy Efficiency* [74]: Energy conservation and consumption is one of the major challenges to be addressed by IoT systems, especially in smart cities where the devices are used everywhere in the environment and closely to the nature and to the humans. Accordingly, the energy challenge of the IoT platforms includes: battery lifetime and power consumption of the sensors and devices which depend on the sensing time; bandwidth/data range/throughput/latency; and the application range. Possible solutions include using the suitable communication technologies that are convenient for the needed covered range by the IoT application, such as using the Low-Power Local Networks for the short-range solutions and the Low-Power Wide Area Networks for communications that exceed 1000 m.
- *Security* [73,75]: Since a large number of "things" are connected together in one heterogeneous system, the security feature is fundamental in any system and includes all the

different components. Thus, the system must be robust enough to deal with any of the possible security attacks by: firstly being able to detect the attack; then diagnosing the attack; and eventually deploying countermeasures and repairs. Considering an open, flexible, low power, lightweight platform makes providing the needed heavyweight security computations critical for future researches.

- *Privacy [73]*: Human interaction, data exchange and wireless communication through the middleware platforms provide good functionalities, but also create a high possibility of violating privacy. Privacy solutions have been addressed by many works, offering secured authorization and authentication mechanisms for the users to access the data sources, e.g., the sensors and the data, in addition to encrypting the transmitted data during the communication.

3. Literature Review

A comprehensive analysis of IoT middleware platforms can be found in [3,76,77]; an application-domain-specific survey of cloud-based IoT platforms can be found in [21], which shows that application development and monitoring management are the mostly served domains by the current IoT clouds. An extensive state of the art review of cloud-based IoT middleware is presented in [78]. da Cruz et al. [79] provides a performance evaluation of 11 open-source middleware solutions based on qualitative metrics, in addition to a quantitative assessment of five of them (InatelPlat, Konker, Linksmart, Orion + STH and Sitewhere). The study concludes that Sitewhere outperforms all the other studied tools for the considered scenario. Ngu et al. [80] identifies and compares middleware platforms of different architectural types. They derive four key challenges in developing IoT middleware: a light-weight middleware platform that operates on power-constrained devices; an application-independent composition engine; a security mechanism that works in all resource-constrained environments; a semantic-based IoT device/service. The architectural designs and features of 16 cloud-based IoT platforms are analyzed in [20] in order to identify the gaps in the state-of-art IoT platforms and the theoretical foundations and vision of IoT. It also provides a set of principles for developing a model-driven IoT platform based on survey results, including providing Applications As a Service, using Capabilities Ontology to define the device's capabilities to sense and/or actuate and using RDF as a transport protocol. Hossein Motlagh et al. [81] presents a literature review on the applications of IoT technology in the energy sector with a focus on smart grids. It provides a summary of the challenges of using IoT in smart energy services, such as providing a reliable end-to-end connection, the integration of IoT with subsystems, standardization, providing efficient energy consumption, security-related issues and maintaining user privacy, along with possible solutions. Bedi et al. [82] analyzes the roles and impacts of smart IoT technology in digitizing electric power and energy systems, concentrating on the role of IoT sensors by providing an assessment of sensors' technical parameters. Martín-Lopo et al. [83] presents a comparative analysis of energy platforms for end users; analyzes recurrent hierarchical building blocks, main design options and strategies; and provides a set of IoT levels to evaluate the implementations of IoT technologies. The green quadrant report published by Verdantix [84] and Gartner's 2021 MQ [85] provide detailed comparisons of the most recent Industrial IoT (IIoT) solutions. In the next Section 3, we exclusively review the IoT tools and platforms that have been mentioned by the experts who were involved in the survey.

Middleware Platforms in Smart Energy Systems

Apache Kafka [86] is an open-source, distributed publish-subscribe messaging system. It focuses on collecting data from high-throughput streams into persistent storage. Apache Kafka clients and clusters communicate via binary TCP connections. These connections are comparatively complex to establish and maintain. In a setting where large numbers of IoT devices communicate through unstable, unreliable networks, the overhead might be prohibitive. It is, however, possible to extend Apache Kafka with MQTT connectivity, circumventing this issue. On the other end of a stream, Kafka can interface with a number

of platforms, such as Java, .NET, PHP, Ruby and Python; and visualization services such as Grafana.

Aidon Gateware [87] provides a service package for Advanced Metering Infrastructure (AMI) management and assessment, including Aidon Gateware Head-End System (HES) which manages the head–end systems communications. The IoT communication in Geteware is provided using three parts: Aidon Linkware for interfaces integration to the Distribution System Operators (DSO)'s information systems; Aidon Gateware for management and execution of various AMM tasks based on scheduling using a graphical user interface; and Aidon Meteringware for data collection and storage from the smart devices.

Amazon Web Services (AWS) [88] is a suite of commercial, cloud-based, on-demand computing platforms. AWS IoT is a middleware solution that connects IoT devices with each other and to cloud services offered by AWS. It supports four communication protocols: MQTT, MQTT over secure web sockets, HTTP and LoRaWAN. AWS SDKs provide language-specific wrappers for the HTTP/HTTPs API to connect with custom applications on various platforms and with various languages, including Android, iOS, Python, Java, JavaScript and C++. Amazon provides seamless integration between device software, connection and management software (control services) and data analysis services.

Cisco Kinetic [89] offers a wide portfolio of commercial end-to-end IoT solutions ranging from network connectivity to cyber security. The Cisco Kinetic IoT platform consists of three modules, gateway management, edge and fog computing and data control. IoT devices can be connected via AMQP or MQTT. Application can be developed from pre-built functions in a proprietary SDK. The platform components can be used on a subscription-based license with optional visualization service components.

CO4 Cloud [90] is an energy management tool which provides an overview of the important energy, room and system data to the user. The provided features include energy monitoring and data visualization, data aggregation from the individual room to the portfolio, energy management, optimization and automation functions, energy accounting and billing, meter integration, virtual meters and data points, reports and data export, notifications, alerts and a ticket system.

EDP Remote Energy Dynamics (Re:dy) [91] is an IoT service developed by EDP commercial. Re:dy connects and integrates the energy sources at home to be managed by the user. This platform needs a set of hardware devices in order to operate, which includes: Re:dy Box, Re:dy Plug, Re:dy Meter, Re:dy Switch and Re:dy plug A/C—an application in the EDP servers where the service is configured and a set of mobile applications for remote access.

Element IoT [92] is an IoT platform developed by ZENNER IoT Solutions GmbH in Hamburg. Element IoT includes a LoRaWAN network server, device and gateway management, and a number of data management functions. It provides solutions to improve the flexibility, interoperability and security of the system by supporting various communication protocols, such as LoRaWAN, NB-IoT, MQTT, HTTP, Sigfox, MS Azure and AWS; and supporting different integration technologies, such as REST, Websockets, MS Azure and AWS.

Siemens [93,94] is a global leader in power and utilities management. One of the services Siemens provides is the EnergyIP meter data management (MDM) application, which is currently enabling more than 200 electricity, gas and water utility companies to manage more than 90 million meters. In 2020, a cloud-hosted MDM started to be used, with the support of Amazon Web Services (AWS). The IoT-platform EnergyIP offers a set of tools and features, which address traditional and emerging use cases, such as billing. Additionally, it uses a unified data model and unified information technology (IT) and operational technology (OT) integration, which allow connecting smart meters from different vendors, with secured connectivity via wireless, radio, LAN and power line communication.

Enerbrain S.R.L. [95] is a company that provides solutions for optimizing energy consumption for air conditioning, improving environmental comfort and reducing CO_2

emissions and one's carbon footprint. The Enerbrain IoT solution offers remote control of heating, ventilation and air conditioning (HVAC) systems by connecting them to the cloud. The provided solutions include a set of sensors, actuators, controllers, meters, etc., such as eSense, eNode, ePLC and eMeter. The main IoT solution is eGateway, which connects the Enerbrain devices to WiFi or Ethernet (ETH) supporting WiFi-GSM-ETH communications in three different operating modes (from GSM to WiFi, from GSM to ETH, from ETH to WiFi).

FIWARE [96] provides a curated framework of building blocks for IoT middleware solutions, building upon the standards, ontologies and reference models described by the SAREF ontology and the NGSI specifications suite. The Orion context broker acts as the central entity in the middleware platform and supports communication via HTTP. Data persistence is handled by a MongoDB. These two components constitute the minimal setup required to deploy the platform. The FIWARE framework proposes various well-established open-source software components from other developers for additional functionality. For instance, to connect to IoT devices via other protocols than HTTP, the platform can use a separate module, the IoT agent. The IoT agent supports LightweightM2M over CoAP qne JSON or UltraLight over HTTP/MQTT, OPC-UA, Sigfix and LoRaWAN. To capture spatial-temporal time-series data about the system state, FIWARE proposes the QuantumLeap services in conjunction with a time-series database such as CrateDB or TimescaleDB. The FIWARE project has received a lot of attention in the research community, and there are many examples in the literature of IoT platforms developed within the FIWARE framework, such as [14–16,97].

Microsoft Azure IoT Central [98] is a commercial cloud-based application platform specifically aimed at enterprise-grade IoT solutions. It provides a webUI to connect, manage and monitor devices and connect them to line-of-business applications. IoT devices' communications are possible via MQTT, MQTT over WebSockets, AMQP, AMQP over WebSockets and HTTPS. High-level services such as visualization, data analysis and data monitoring can be implemented by using pre-defined application templates [99], such as smart meter analytics and solar panel monitoring, or by building custom applications from scratch.

Niota Cross IoT Platform [100,101] is an IoT platform for developing and deploying vertical IoT solutions across multiple industries. It combines data from various sources, such as sigfox, NB-IoT, LoRaWAN, M2M and NFC. Niota's IoT platform allows one to integrate new and old features and business models of Industrial Internet of Things (IIoT), within the current IT ecosystem. Additionally, it offers number of advantages, such as supporting different communication technologies; inbound and outbound interfaces; providing a visual IoT service builder; focusing on the integration, interoperability, flexibility and the security of sensitive data.

OdinS [102] offers smart solutions for infrastructure management of different applications, including industry, agriculture, environmental projects, intelligent buildings, smart cities, mobility and transportation. In the field of intelligent buildings and smart cities, OdinS provides solutions for improving energy efficiency in buildings and living spaces according to the facilities that are included, in addition to the integrated management in building and infrastructure networks and the cloud-based solutions with simultaneous and multi-user management. For the application designing, OdinS platform uses smart cities platforms such as FIWARE.

Telegraf/Influx/Chronograf/Kapacitor (TICK-Stack) consists of a set of modular services built around the time-series database InfluxDB [103]. The database is offered as an open-source version to be run on the user's infrastructure, as a cloud service or as an enterprise-grade production-ready cluster. InfluxData Inc. (San Francisco, CA, USA) provides their time-series database as an application for cloud-based platforms AWS IoT and Microsoft Azure. InfluxDB handles data persistence only; data collection happens through the open-source server agent plug-in Telegraf [104]. Telegraf allows users to connect IoT devices, other systems and databases to the InfluxDB. It supports push and pull operations

via MQTT, HTTP and third-party APIs; Apache Kafka services; AWS cloudwatch; MongoDB; or visualization services, such as Grafana or Influxdata's web-based dashboard and real-time visualization plugin Chronograf [105]. On top of collecting (Telegraf), storing (InfluxDB) and visualizing (Chronograf), TICK-Stack provides the processing framework Kapacitor [106], which can be used for data analysis purposes, such as anomaly detection.

4. Method

In order to analyze IoT middleware platforms in smart energy systems, we pursued a two-stage research plan, consisting of a literature review and a quantitative expert survey. First, we conducted literature analysis in order to identify technologies, requirements and challenges that are relevant in the development and roll-out of IoT middleware platforms and to form a set of survey questions that would assess the experts' needs. Based on the results, we developed an online questionnaire that was made accessible to 47 experts from Europe: (i) 13% were city officials responsible for smart city projects and smart platforms; (ii) 50% were experts in energy and energy technology companies, including data analysts, IoT experts and researchers; and (iii) 37% were experts who planned and/or operated buildings and districts, such as experts in electricity markets, flexibility management, digitalization of district heating and energy in buildings. The experts were selected based on their involvement and interest in the development and operation of middleware platforms. Out of the 47 experts, 28 provided us with a complete set of answers, which corresponds to a response rate of 60%. Qualitative statements about IoT platforms tools, technologies, requirements and business cases were the core of the survey. Experts were asked to report their agreement with certain statements through simple yes/no answers or Likert answers. The survey took place between September and December 2020. The questionnaire and expert responses are openly available at GitHub: https://github.com/tug-cps/iot-survey (accessed on 21 March 2021).

4.1. Presentation of the Results

Hallowell and Gambatese [107] argue that the median value is more appropriate for analyzing results of a survey than the mean, as it is less dependent on outliers and extreme values introduced by biased responses.

Sachs [108] argues that the interpolated median, as given by (1), is even more appropriate than the median, as it provides a metric within the lower and upper bounds of the median, in the direction that the data is more heavily weighted.

$$IM = \begin{cases} M & \text{if } n_2 = 0, \\ M - 0.5 + \frac{0.5 \cdot N - n_1}{n_2} & \text{if } n_2 \neq 0 \end{cases} \quad (1)$$

where M is the standard median of the responses, N is the number of answers to a specific question, n_1 is the number of answers strictly less than M and n_2 is the number of answers equal to M.

To maximize the transparency of the results, they are presented in bar charts, as means, medians and interpolated medians.

4.2. Threats to Validity and Limitations of the Study

There is no universal criterion that allows for an unbiased assessment of what it means to be an expert in a certain field. Academic experts are often identified based on their numbers of publications and citations. However, there is no general criterion that allows an unbiased comparison of the impact of a researcher's work. This applies, in particular, to the comparison between disciplines. For experts in industry, there is no metric such as number of citations that would allow classification as an expert, since most experts in industry do not publish their work in (peer-reviewed) journals. In this study, experts from industry were selected based on their involvement and interest in the development and operation of

middleware platforms. We are aware that this is a threat to validity. However, we claim that this is the most transparent selection procedure.

5. Results

In this section, we present the results of the quantitative expert survey divided into the following categories: business layer and end-users; NFRs and challenges; applications; middleware communications protocols; network communications protocols.

5.1. Business Layer and End-Users

Figure 2 shows that while most practitioners consider the development of uniform semantic models important, only a minority already use unified models in their systems. It can be seen in Figure 3 that most experts would share data models and schemata freely, and a majority would be willing to sign a service contract for a IoT platform. Besides, responses show that about for half of the experts, IoT middleware platforms are a core aspect in their business model. Additionally, we asked the experts about whether they operate their current/future IoT solutions on private or public clouds, or they prefer cooperating with a service partner. The answers for this question indicate that 40% of the users prefer to host IoT solutions on their private systems, and similarly 40% reported that they choose collaborations with service partners. On the other hand, Only 20% of the experts were interested in using the public clouds for operating such services.

Figure 4 shows how much each of the participants categories considers using IoT solutions for monitoring and operation of buildings/districts/cities as important. To assess how much is it important to have an open-source platform, participants were asked to answer some related questions as shown in Table 1.

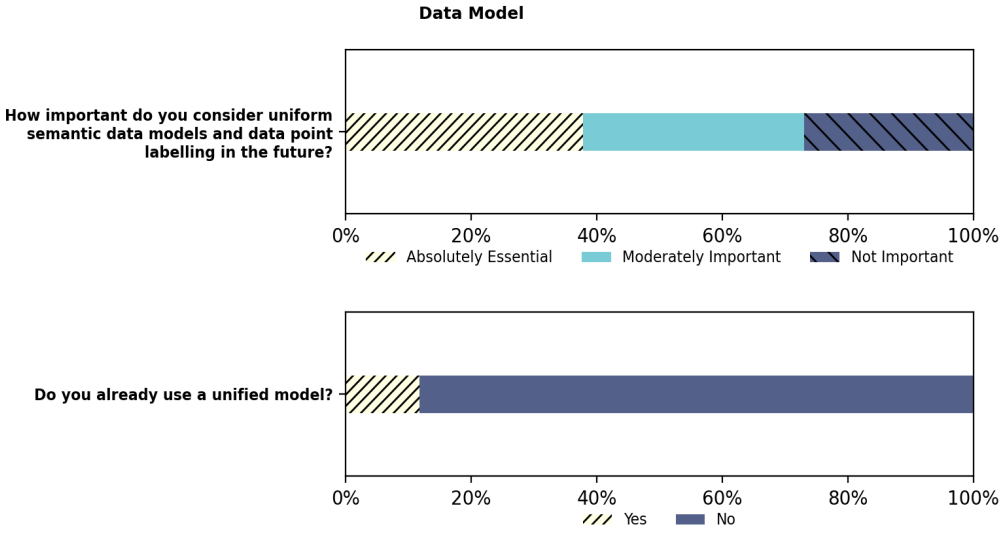

Figure 2. Responses to a survey questions to assess the importance of data models.

5.2. NFRs and Challenges

The pie chart in Figure 5 shows that only 15.6% of the participants planned to use or used IoT platforms for one building, while the remaining answers were evenly distributed between considering a scope of multiple buildings, districts, entire cities or other larger scales.

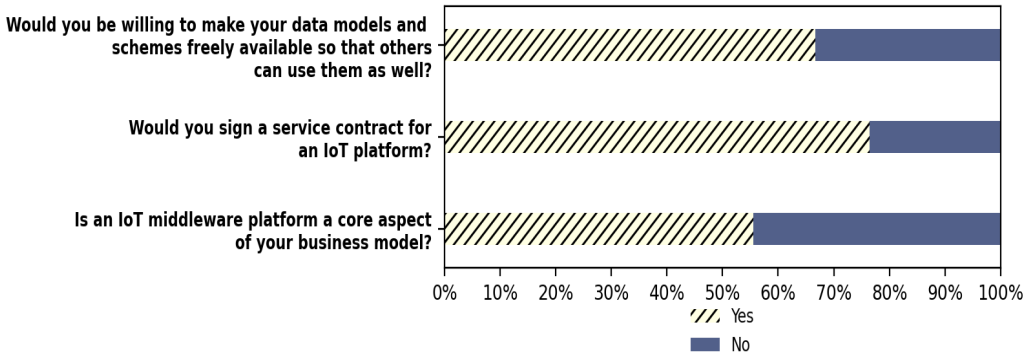

Figure 3. Responses to general survey questions to business owners and end users.

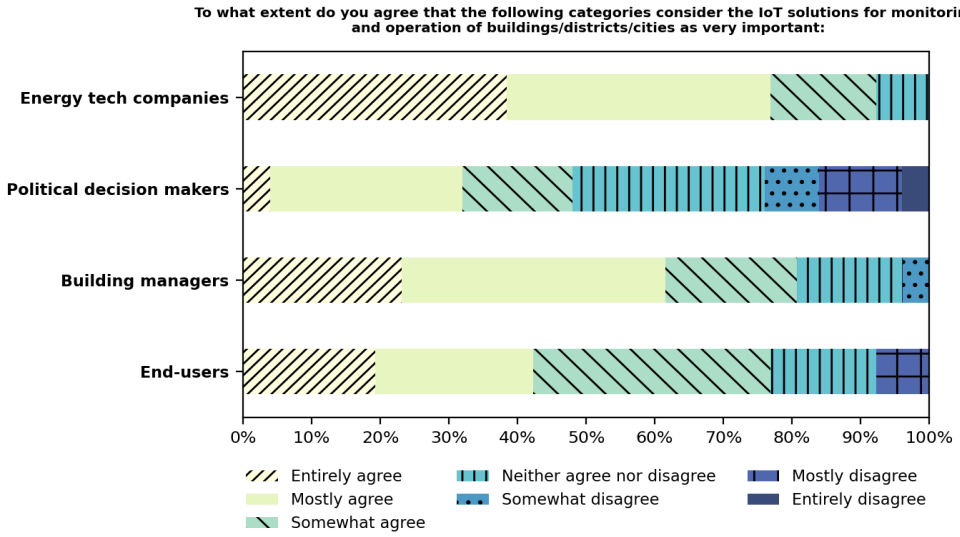

Figure 4. Responses to survey questions show how important are the IoT platforms for different categories of users.

Table 1. Means, medians and interpolated medians of answers to questions prefaced by: To what extent do you agree with the following statement?

	Mean	Median	IM
It is important for us to use open source IoT Middleware Platforms	5.3	6.0	5.9
We would participate in the development of an open source IoT Middleware Platform	5.4	5.0	5.0
We would rather pay for a full service than administrating on our own	4.7	4.0	4.3

This imposes crucial security and sacalability requirements on the middleware platform, as data exchange needs to be secure regardless of the scale.

This observation is highlighted by the responses visualized in Figure 6, where more than 95% classified security as either extremely or very important. Furthermore, Figure 6 and Table 2 emphasize that other non-functional requirements, such as openness, availability, reliability and avoiding vendor locks need to be considered as well.

Table 2. Means, medians and interpolated medians of answers to questions prefaced by: How important is the following property for you when you operate an IoT platform?

	Mean	Median	IM
Avoid vendor locks	5.7	6.0	6.2
Open source	5.3	6.0	5.9
Providing a GUI	5.7	6.0	5.8
Standardized API	6.4	7.0	6.7
Performance	6.1	6.0	6.2
Availability	6.5	7.0	6.6
Reliability	6.5	7.0	6.6
Security	6.7	7.0	6.9

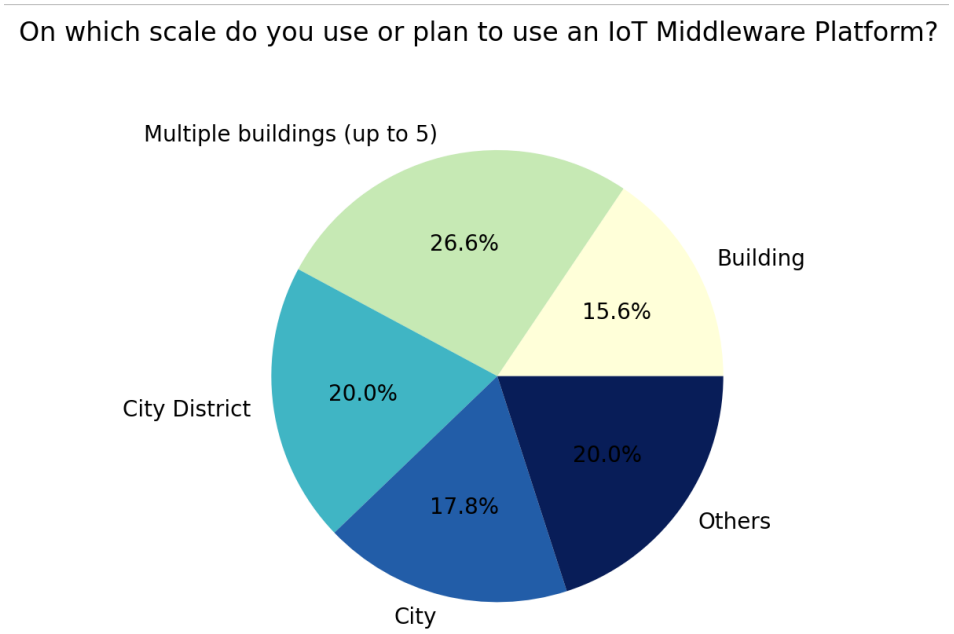

Figure 5. Responses to a survey question show the scalability of the application in which the IoT platform is used/planned to be used.

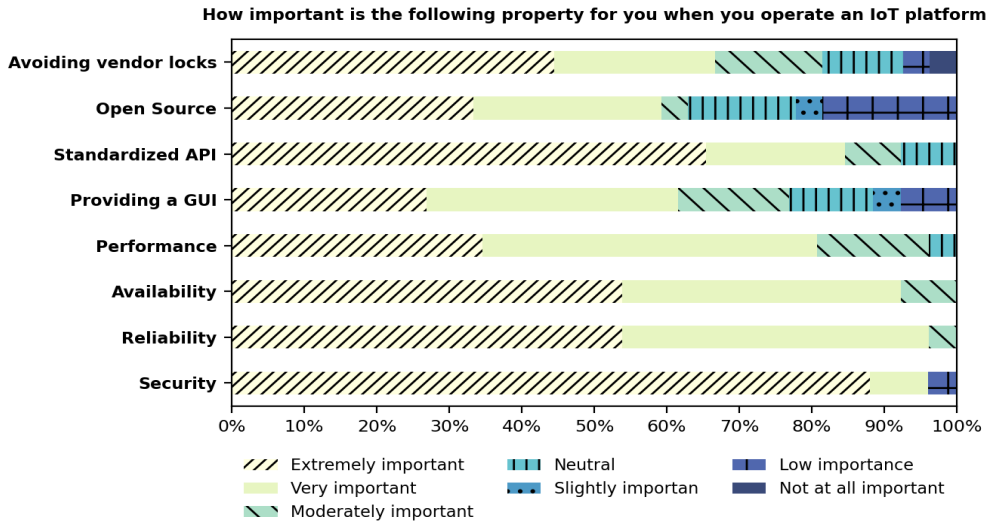

Figure 6. Responses to survey question list the eight most important features that should be offered by the IoT platforms.

5.3. Applications

The main goal of the IoT is to connect sensors, devices and networks in one aggregated system, providing a basis for a wide range of applications, including data-analysis and visualization. Figure 7 shows a list of applications that the survey participants are either already using or planning to use IoT middleware for.

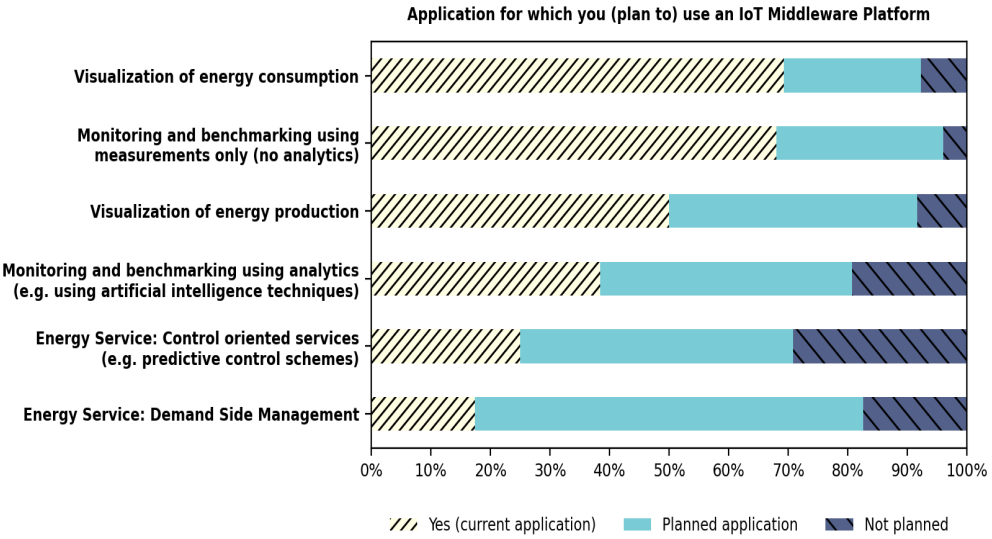

Figure 7. Responses to survey question list the applications in which the IoT middleware is used/planned to be used.

5.4. Middleware Communication Protocols

An IoT platform needs to support various communication protocols to be able to connect with a wide variety of devices, networks and external systems. Accordingly, in our survey we asked experts to identify the most important communication protocols for IoT technology. Figure 8 shows that MQTT and HTTP are considered fundamental protocols by the survey participants.

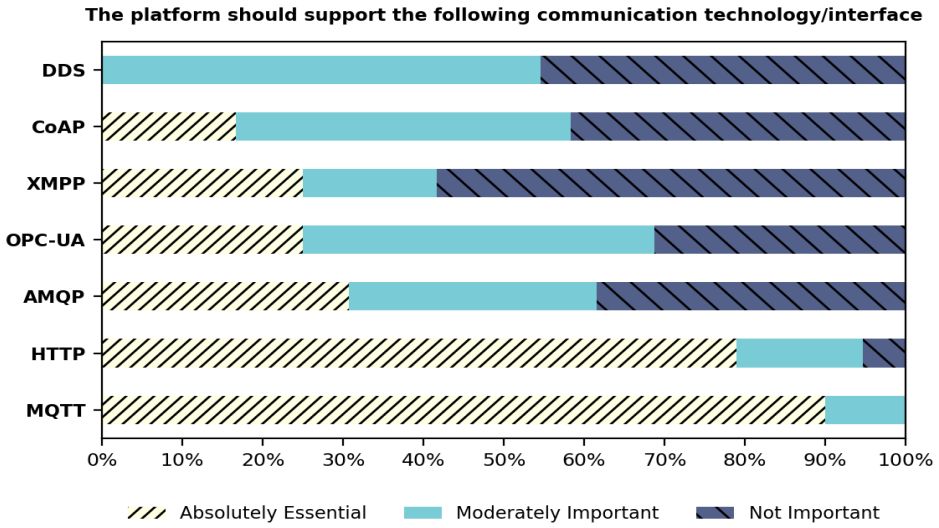

Figure 8. Responses to a survey question about the communication protocols that need to be supported by the IoT middleware platforms.

5.5. Network Communication Standards

Similarly to the protocol requirements, IoT middleware solutions have to be able to support communication through a variety of network communication standards in order to provide maximum flexibility.

Figure 9 depicts how the survey participants rate the importance of the most common network protocols in IoT middleware. Results show that LoRaWAN and are considered the most important technologies by the experts.

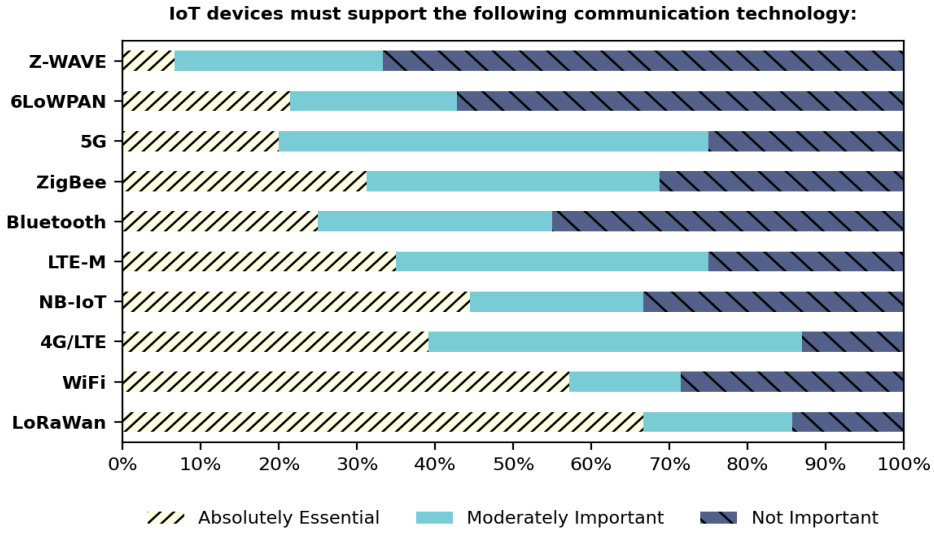

Figure 9. Responses to a survey question about the communication technologies that need to be supported by the IoT middleware platforms.

6. Discussion

Monitoring and operation through IoT solutions is seen as a key interest for energy technology companies, building managers and end users. This highlights that scalability and modularity are key requirements for IoT solutions. IoT platforms have to support a wide range of functionalities, as the use cases for energy technology companies are fundamentally different from the use cases of the other end users. Based on the expert survey, around 70% of the respondents found that visualization of energy production and consumption remains the central use for IoT infrastructure, and the potential of data analysis services and control automation are not yet exploited. However, there seems to be rising interest in energy optimization, including benchmarking, automation and control, and demand side management. Many commercial platforms provide services, service templates and SDKs for seamless integration with their platforms.

Regarding the IoT architecture model, in our research, we found that a five-layer approach offers the most practical solution by distinguishing layers based on their functionalities, while keeping it as simple as possible. The most relevant application layer protocols used by most of the middleware platforms in research are HTTP, CoAP, MQTT, OPC UA, XMPP, AMPQ and DDS. On a network communication level, IPv6, ZigBee, Z-Wave, Bluetooth, 4G/LTE, 5G, LoRAWAN, 6LoWPAN, LTE-M and NB-IoT are the predominant technologies. The survey results highlight that MQTT is considered to be even more important than HTTP by the respondents of the survey; however, especially in the matter of scalability and real-time control, CoAP, XMPP or DDS might find more relevance in future applications. Regarding the communication technology, LoRaWAN got the spot of the most relevant technology in the survey at roughly 65%, followed by WiFi, at slightly more than 55%. Offering more technologies could also help in drawing the attention to some alternatives that solve the drawbacks of the used technologies, such as using HTTP instead of MQTT to improve the scalability. To improve the portability of energy services between different platforms and to avoid vendor locks, it will be necessary to be able to

use uniform semantic data models and data point labels in the future (see Figure 3). In addition, to allow the integration of a wide variety of third-party services, devices and (legacy) systems, it is critical to standardize APIs.

Extending the scales in which the IoT middleware platforms are used imposes the need of sharing and handling large amounts of real-time data in a scalable, controlled and secured way. Indeed, at least 64% of the participants claimed to use IoT middleware for multiple buildings.

Security is particularly important considering the severity of security breaches in the context of privacy and confidentiality and the risks for the operation of buildings, districts and grids. Figure 6 demonstrates how important security is for the users, by being considered as the most important non-functional requirement with approximately 90% of the votes.

With more services and functionalities being automated, it is imperative to ensure the reliability of the middleware platform. Although openness is seen as the least important property provided by middleware platforms among the NFRs, Figure 3 shows that while there is a general willingness to participate in the development of open-source IoT platforms by practitioners in energy technology companies, building operators and municipality officials, many users would still prefer to outsource operation and maintenance of platforms to third-parties. The same opinion applies for the management of these platforms: the majority of users would prefer to pay for the administration of the middleware platforms, rather than administrating their own. At the same time, some users are still undecided and have a wait-and-see attitude. Hence, we promote extensive research in this area.

7. Conclusions

Developments in Internet and communication technology and in the availability of microchips have accelerated the integration of computing machinery into all aspects of day-to-day life. Smart energy applications are prominent examples, where IoT solutions provide the opportunity to improve energy efficiency, reduce costs and increase comfort. Predictive control, monitoring, automatic fault detection and demand-sided management are examples of new energy services. The rapid development and wide availability of IoT devices with proprietary firmware confront practitioners with compatibility issues. IoT middleware platforms are a promising solution to mitigate these issues and provide integration of devices, data persistence and energy services. IoT middleware is an emerging market, with a wide range of commercial and non-commercial alternatives. While the introduction of universal standards in IoT remains a pious hope for the future, there are recurrent building services, concepts, protocols and functionalities that are found in both commercial and non-commercial platforms. This paper presented an expert assessment of requirements, limitations and challenges for large-scale deployment of IoT middleware in smart energy systems. The results corroborate findings in the literature, such as the need to standardize semantic data models, data point labels and APIs to improve portability and interoperability between devices and services from different vendors, More than 50% of the participants considered unified data models important; at the same time, only 15% of the experts currently used a unified data model, marking this as an important area for future research. Results show that the application layer protocols used by most of the middleware platforms are MQTT and HTTP, whereas on the network communication level, LoRAWAN, WiFi and 4G/LTE are the prevalent technologies. In the literature, the most important non-functional requirements were identified as: interoperability, scalability, flexibility and openness, energy efficiency, security and privacy. Results of the survey show that experts consider security a crucial feature in any middleware platform, in addition to showing a big interest in developing open solutions. The fact that about 30% of the survey participants were not willing to make their data models freely available shows that further research should be devoted to highlighting the importance and the commercial and non-commercial benefits of using open-source solutions and contributing to open-source projects. Development of unified data models, data representations and naming schemes by

considering the collaborations between academic researchers and practitioners should also be considered; this data model's harmonization helps in enabling a seamless interaction between digital sub-systems. This is strongly required for any kind of smart energy system that relies on sector coupling or enforces any kind of demand-side management or continuous adaptation of simulation models, such as fault detection and predictive control. Moreover, in this paper we discussed different protocols and technologies, but more research is required on assessing the suitability of these technologies and protocols for certain applications under real conditions.

Author Contributions: Conceptualization, Q.A., T.S. (Thomas Schranz), G.S., A.K., T.S. (Thomas Storek), M.S., A.M. and S.G.; methodology, G.S.; formal analysis, Q.A., T.S. (Thomas Schranz) and G.S.; writing—original draft preparation, G.S.; writing—review and editing, Q.A., T.S. (Thomas Schranz), G.S., A.K., T.S. (Thomas Storek), S.G. and M.S.; visualization, Q.A.; supervision, G.S., A.M. and D.M.; project administration, G.S.; funding acquisition, G.S. All authors have read and agreed to the published version of the manuscript.

Funding: This project (GA numbers 879315 and 880792) is funded by the Austrian Climate and Energy Fund and the BMK within the programs "ERA-NET" and "Vorzeigeregion". It is a;sp supported by TU Graz Open Access Publishing Fund. Furthermore, this research is supported by Bundesministerium für Wirtschaft und Energie (BMWi) under grant agreement number 03EI6051A.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Publicly available questionnaire and expert responses are openly available at GitHub. This data can be found here: https://github.com/tug-cps/iot-survey (accessed on 21 March 2021).

Acknowledgments: Open Access Funding by the Graz University of Technology.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lee, G.M.; Crespi, N.; Choi, J.K.; Boussard, M. Internet of Things. In *Evolution of Telecommunication Services: The Convergence of Telecom and Internet: Technologies and Ecosystems*; Bertin, E., Crespi, N., Magedanz, T., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; pp. 257–282. [CrossRef]
2. Jin, J.; Gubbi, J.; Marusic, S.; Palaniswami, M. An Information Framework for Creating a Smart City Through Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 112–121. [CrossRef]
3. da Cruz, M.A.A.; Rodrigues, J.J.P.C.; Al-Muhtadi, J.; Korotaev, V.V.; de Albuquerque, V.H.C. A Reference Model for Internet of Things Middleware. *IEEE Internet Things J.* **2018**, *5*, 871–883. [CrossRef]
4. Ahmad, T.; Zhang, D. Using the internet of things in smart energy systems and networks. *Sustain. Cities Soc.* **2021**, *68*, 102783. [CrossRef]
5. Schweiger, G.; Eckerstorfer, L.V.; Hafner, I.; Fleischhacker, A.; Radl, J.; Glock, B.; Wastian, M.; Rößler, M.; Lettner, G.; Popper, N.; et al. Active consumer participation in smart energy systems. *Energy Build.* **2020**, *227*, 110359. [CrossRef]
6. Allouhi, A.; El Fouih, Y.; Kousksou, T.; Jamil, A.; Zeraouli, Y.; Mourad, Y. Energy consumption and efficiency in buildings: Current status and future trends. *J. Clean. Prod.* **2015**, *109*, 118–130. [CrossRef]
7. European Commission. Proposal for a Directive of the European Parliament and of the Council Amending Directive 2010/31/EU on the Energy Performance of Buildings. COM(2016) 765 Final 2016. Available online: https://ec.europa.eu/info/news/focus-energy-efficiency-buildings-2020-lut-17_en. (accessed on 21 March 2021).
8. European Environmental Agency. Annual European Union Greenhouse Gas Inventory 1990–2018 and Inventory Report 2020: Submission under the United Nations Framework Convention on Climate Change and the Kyoto Protocol. Technical Report, European Commission, DG Climate Action European Environment Agency. 2020. Available online: https://www.eea.europa.eu/publications/european-union-greenhouse-gas-inventory-2020/download (accessed on 21 March 2021)
9. Ipakchi, A.; Albuyeh, F. Grid of the future. *IEEE Power Energy Mag.* **2009**, *7*, 52–62. [CrossRef]
10. Mariano-Hernández, D.; Hernández-Callejo, L.; Zorita-Lamadrid, A.; Duque-Pérez, O.; Santos García, F. A review of strategies for building energy management system: Model predictive control, demand side management, optimization, and fault detect & diagnosis. *J. Build. Eng.* **2021**, *33*, 101692. [CrossRef]
11. Sun, Y.; Haghighat, F.; Fung, B.C.M. A Review of The-State-of-the-Art in Data-Driven Approaches for Building Energy Prediction. *Energy Build.* **2020**, *221*, 110022. [CrossRef]

12. Bode, G.; Thul, S.; Baranski, M.; Müller, D. Real-World Application of Machine-Learning-Based Fault Detection Trained with Experimental Data. *Energy* **2020**, *198*, 117323. [CrossRef]
13. Rätz, M.; Javadi, A.P.; Baranski, M.; Finkbeiner, K.; Müller, D. Automated data-driven modeling of building energy systems via machine learning algorithms. *Energy Build.* **2019**, *202*, 109384. [CrossRef]
14. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
15. Terroso-Saenz, F.; González-Vidal, A.; Ramallo-González, A.P.; Skarmeta, A.F. An Open IoT Platform for the Management and Analysis of Energy Data. *Future Gener. Comput. Syst.* **2019**, *92*, 1066–1079. [CrossRef]
16. Storek, T.; Lohmöller, J.; Kümpel, A.; Baranski, M.; Müller, D. Application of the Open-Source Cloud Platform FIWARE for Future Building Energy Management Systems. *J. Phys. Conf. Ser.* **2019**, *1343*, 012063. [CrossRef]
17. Patti, E.; Acquaviva, A. IoT Platform for Smart Cities: Requirements and Implementation Case Studies. In Proceedings of the 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow (RTSI), Lausanne, Switzerland, 7–9 September 2019; IEEE: Bologna, Italy, 2016; pp. 1–6. [CrossRef]
18. Moura, P.; Moreno, J.I.; López López, G.; Alvarez-Campana, M. IoT Platform for Energy Sustainability in University Campuses. *Sensors* **2021**, *21*, 357. [CrossRef] [PubMed]
19. Bakhouya, M.; NaitMalek, Y.; Elmouatamid, A.; Lachhab, F.; Berouine, A.; Boulmrharj, S.; Ouladsine, R.; Felix, V.; Zinedine, K.; Khaidar, M.; et al. Towards a Context-Driven Platform Using IoT and Big Data Technologies for Energy Efficient Buildings. In Proceedings of the 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, Morocco, 24–26 October 2017; IEEE: Rabat, Morocco, 2017; pp. 1–5. [CrossRef]
20. Zdravković, M.; Trajanović, M.; Sarraipa, J.; Jardim-Gonçalves, R.; Lezoche, M.; Aubry, A.; Panetto, H. Survey of Internet-of-Things platforms. In Proceedings of the 6th International Conference on Information Society and Techology, ICIST 2016, Barcelona , Spain, 18–20 March 2016; Volume 1, pp. 216–220.
21. Ray, P.P. A Survey of IoT Cloud Platforms. *Future Comput. Inform. J.* **2016**, *1*, 35–46. [CrossRef]
22. Światowiec Szczepańska, J.; Stępień, B. Drivers of Digitalization in the Energy Sector; The Managerial Perspective from the Catching Up Economy. *Energies* **2022**, *15*, 1437. [CrossRef]
23. European Commission Initiatives and Action Plans. 2021. Available online: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13141-Digitalising-the-energy-sector-EU-action-plan_en (accessed on 21 March 2021).
24. Gaia-X European Association for Data and Cloud AISBL. 2021. Available online: https://www.gaia-x.eu/ (accessed on 21 March 2021).
25. Awan, N.; Khan, S.; Rahmani, M.K.I.; Tahir, M.; Md, N.A.; Alturki, R.; Ullah, I. Machine Learning-Enabled Power Scheduling in IoT-Based Smart Cities. *Comput. Mater. Contin.* **2021**, *67*, 2449–2462. [CrossRef]
26. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
27. Steinert, C.V.; Ruggeri, A. Who are Our Experts? Predictors of Participation in Expert Surveys. *Peace Econ. Peace Sci. Public Policy* **2020**, *26*, 20200007. [CrossRef]
28. Bergmann, H.; Mosiman, C.; Saha, A.; Haile, S.; Livingwood, W.; Bushby, S.; Fierro, G.; Bender, J.; Poplawski, M.; Granderson, J.; et al. Semantic Interoperability to Enable Smart, Grid-Interactive Efficient Buildings. 2020.
29. Bray, T.; Paoli, J.; Sperberg-McQueen, C.M.; Maler, E.; Yergeau, F.; Cowan, J. Extensible Markup Language (XML) 1.0. 2000. Available online: https://www.w3.org/TR/xml/ (accessed on 21 March 2021).
30. Douglas Crockford. Introducing JSON. 2009. Available online: https://www.json.org/json-en.html (accessed on 31 December 2021).
31. Project Haystack. 2021. Available online: https://project-haystack.org/ (accessed on 7 December 2021).
32. Balaji, B.; Bhattacharya, A.; Fierro, G.; Gao, J.; Gluck, J.; Hong, D.; Johansen, A.; Koh, J.; Ploennigs, J.; Agarwal, Y.; et al. Brick: Towards a Unified Metadata Schema For Buildings. In Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments, Palo Alto, CA, USA, 16–17 November 2016; ACM: Palo Alto, CA, USA, 2016; pp. 41–50. [CrossRef]
33. Jimenez, J.; Koster, M.; Tschofenig, H. IPSO Smart Objects. Position Paper for the IOT Semantic Interoperability Workshop. 2016. Available online: https://omaspecworks.org/wp-content/uploads/2018/03/ipso-paper.pdf (accessed on 21 March 2021).
34. oneM2M. oneM2M Technical Specifications. 2021. Available online: https://www.onem2m.org/technical (accessed on 17 November 2021).
35. Daniele, L.; den Hartog, F.; Roes, J. Created in Close Interaction with the Industry: The Smart Appliances REFerence (SAREF) Ontology. In *Formal Ontologies Meet Industry*; Cuel, R., Young, R., Eds.; Lecture Notes in Business Information Processing; Springer International Publishing: Cham, Switzerland, 2015; pp. 100–112. [CrossRef]
36. Brick Consortium, Inc. Brick Ontology Documentation. 2021. Available online: https://docs.brickschema.org (accessed on 8 December 2021).
37. OMA SpecWorks. 2021. Available online: https://omaspecworks.org (accessed on 23 November 2021).
38. Context Information Management (CIM) ETSI Industry Specification Group (ISG). Context Information Management (CIM); NGSI-LD API. 2021. Available online: https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.04.01_60/gs_cim009v010401p.pdf (accessed on 31 December 2021).

39. FIWARE Foundation. FIWARE-NGSI LD. 2021. Available online: https://ngsi-ld-tutorials.readthedocs.io/en/latest/ (accessed on 9 December 2021).
40. FIWARE Foundation. The FIWARE Foundation. 2021. Available online: https://www.fiware.org/foundation (accessed on 29 November 2021).
41. FIWARE Foundation. FIWARE-NGSI v2 Specification. 2021. Available online: https://fiware.github.io/specifications/ngsiv2/stable (accessed on 4 November 2021).
42. Farahzadi, A.; Shams, P.; Rezazadeh, J.; Farahbakhsh, R. Middleware Technologies for Cloud of Things: A Survey. *Digit. Commun. Netw.* **2018**, *4*, 176–188. [CrossRef]
43. Jia, X.; Feng, Q.; Fan, T.; Lei, Q. RFID technology and its applications in Internet of Things (IoT). In Proceedings of the 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, China, 21–23 April 2012; pp. 1282–1285.
44. Domingo, M.C. An overview of the Internet of Things for people with disabilities. *J. Netw. Comput. Appl.* **2012**, *35*, 584–596. [CrossRef]
45. Keyur, K.; Patel, S.M.P. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. 2016. Available online: http://tarjomefa.com/wp-content/uploads/2018/07/9256-English-TarjomeFa.pdf (accessed on 21 March 2021).
46. Xu, L.D.; He, W.; Li, S. Internet of Things in Industries: A Survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
47. Antão, L.; Pinto, R.; Reis, J.; Gonçalves, G. *Requirements for Testing and Validating the Industrial Internet of Things*; ICST Workshops; IEEE Computer Society: Washington, DC, USA, 2018; pp. 110–115.
48. Kumar, N.M.; Mallick, P.K. The Internet of Things: Insights into the Building Blocks, Component Interactions, and Architecture Layers. *Procedia Comput. Sci.* **2018**, *132*, 109–117. [CrossRef]
49. Al-Masri, E.; Kalyanam, K.R.; Batts, J.; Kim, J.; Singh, S.; Vo, T.; Yan, C. Investigating Messaging Protocols for the Internet of Things (IoT). *IEEE Access* **2020**, *8*, 94880–94911. [CrossRef]
50. Apache Spark. Apache Spark. 2018. Available online: https://spark.apache.org/ (accessed on 20 December 2021).
51. Day, J.; Zimmermann, H. The OSI reference model. *Proc. IEEE* **1983**, *71*, 1334–1340. [CrossRef]
52. Bormann, C.; Castellani, A.P.; Shelby, Z. CoAP: An Application Protocol for Billions of Tiny Internet Nodes. *IEEE Internet Comput.* **2012**, *16*, 62–67. [CrossRef]
53. Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Lee, B. Hypertext Transfer Protocol—HTTP/1.1 1999. Available online: https://www.w3.org/Protocols/rfc2616/rfc2616.html (accessed on 21 March 2021).
54. CoAP Technology. CoAP, RFC 7252 Constrained Application Protocol. 2021. Available online: https://coap.technology/ (accessed on 20 December 2021).
55. Egli, P.R. MQTT—Message Queueing Telemetry Transport Introduction to MQTT, a Protocol for M2M and IoT Applications. 2017. Available online: https://www.researchgate.net/publication/320126053_MQTT_-_Message_Queueing_Telemetry_Transport_Introduction_to_MQTT_a_protocol_for_M2M_and_IoT_applications (accessed on 21 March 2021).
56. OPC Foundation. OPC Unified Architecture Specification. 2021. Available online: https://opcfoundation.org (accessed on 17 October 2021).
57. XMPP Standards Foundation. Extensible Messaging and Presence Protocol. 2021. Available online: https://xmpp.org (accessed on 26 November 2021).
58. OASIS Open. AMQP is the Internet Protocol for Business Messaging. 2021. Available online: https://www.amqp.org (accessed on 30 November 2021).
59. Pardo-Castellote, G. OMG Data-Distribution Service: Architectural overview. In Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, Providence, RI, USA, 19–22 May 2003; pp. 200–206. [CrossRef]
60. Deering, S.; Hinden, R. *RFC 2460 Internet Protocol, Version 6 (IPv6) Specification*; Internet Engineering Task Force: Fremont, CA, USA, 1998.
61. Ergen, S.C. ZigBee/IEEE 802.15.4 Summary. 2004. Available online: https://www.semanticscholar.org/paper/ZigBee%2FIEEE-802.15.4-Summary-Ergen/5776ea5847cb475bd543ac4028e7cfe78be2732b (accessed on 21 March 2021).
62. Z-Wave. *An Introductory Guide to Z-Wave Technology*; 2013. Available online: https://www.homekit.ae/post/introductory-guide-to-z-wave-technology (accessed on 21 March 2021).
63. Z-Wave. *Z-Wave Technical Basics*; 2011. Available online: https://stevessmarthomeguide.com/z-wave-basics/ (accessed on 21 March 2021).
64. Bisdikian, C. An Overview of the Bluetooth Wireless Technology. *IEEE Commun. Mag.* **2001**, *39*, 86–94. [CrossRef]
65. Ferro, E.; Potorti, F. Bluetooth and Wi-Fi wireless protocols: A survey and a comparison. *IEEE Wirel. Commun.* **2005**, *12*, 12–26. [CrossRef]
66. Huang, J.; Qian, F.; Gerber, A.; Mao, Z.M.; Sen, S.; Spatscheck, O. A Close Examination of Performance and Power Characteristics of 4G LTE Networks. In Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services-MobiSys '12, Ambleside, UK, 25–29 June 2012; ACM Press: Low Wood Bay, UK, 2012; p. 225. [CrossRef]
67. Shafi, M.; Molisch, A.F.; Smith, P.J.; Haustein, T.; Zhu, P.; De Silva, P.; Tufvesson, F.; Benjebbour, A.; Wunder, G. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 1201–1221. [CrossRef]

68. Adelantado, F.; Vilajosana, X.; Tuset-Peiro, P.; Martinez, B.; Melia-Segui, J.; Watteyne, T. Understanding the Limits of LoRaWAN. *IEEE Commun. Mag.* **2017**, *55*, 34–40. [CrossRef]
69. Ma, X.; Luo, W. The Analysis of 6LowPAN Technology. In Proceedings of the 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Wuhan, China, 19–20 December 2008; Volume 1, pp. 963–966. [CrossRef]
70. Telenor Connexion. LTE-M vs. NB-IoT—A Guide Exploring the Differences between LTE-M and NB-IoT. 2020. Available online: https://www.telenorconnexion.com/iot-insights/lte-m-vs-nb-iot-guide-differences (accessed on 23 November 2021).
71. Manyika, J.; Chui, M.; Bisson, P.; Woetzel, J.; Dobbs, R.; Bughin, J.; Aharon, D. Unlocking the potential of the Internet of Things. Report, McKinsey Global Institute. 2015. Available online: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. (accessed on 21 March 2021).
72. Chaqfeh, M.A.; Mohamed, N. Challenges in middleware solutions for the internet of things. In Proceedings of the 2012 International Conference on Collaboration Technologies and Systems (CTS), Denver, CO, USA, 21–25 May 2012; pp. 21–26. [CrossRef]
73. Stankovic, J.A. Research Directions for the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 3–9. [CrossRef]
74. Perkovic, T.; Damjanovic, S.; Solic, P.; Patrono, L.; Rodrigues, J.J.P.C. *Meeting Challenges in IoT: Sensing, Energy Efficiency, and the Implementation*; ICICT (1); Yang, X.S., Sherratt, R.S., Dey, N., Joshi, A., Eds.; Advances in Intelligent Systems and Computing; Springer: Berlin/Heidelberg, Germany, 2019; Volume 1041, pp. 419–430.
75. Zhang, Z.K.; Cho, M.C.Y.; Wang, C.W.; Hsu, C.W.; Chen, C.K.; Shieh, S. *IoT Security: Ongoing Challenges and Research Opportunities*; SOCA; IEEE Computer Society: Washington, DC, USA, 2014; pp. 230–234.
76. Razzaque, M.A.; Milojevic-Jevric, M.; Palade, A.; Clarke, S. Middleware for Internet of Things: A Survey. *IEEE Internet Things J.* **2016**, *3*, 70–95. [CrossRef]
77. Mineraud, J.; Mazhelis, O.; Su, X.; Tarkoma, S. A gap analysis of Internet-of-Things platforms. *Comput. Commun.* **2016**, *89-90*, 5–16. [CrossRef]
78. Botta, A.; de Donato, W.; Persico, V.; Pescapé, A. Integration of Cloud Computing and Internet of Things: A Survey. *Future Gener. Comput. Syst.* **2016**, *56*, 684–700. [CrossRef]
79. da Cruz, M.A.; Rodrigues, J.J.; Sangaiah, A.K.; Al-Muhtadi, J.; Korotaev, V. Performance Evaluation of IoT Middleware. *J. Netw. Comput. Appl.* **2018**, *109*, 53–65. [CrossRef]
80. Ngu, A.H.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, M.Z. IoT Middleware: A Survey on Issues and Enabling Technologies. *IEEE Internet Things J.* **2016**, *4*, 1–20. [CrossRef]
81. Hossein Motlagh, N.; Mohammadrezaei, M.; Hunt, J.; Zakeri, B. Internet of Things (IoT) and the Energy Sector. *Energies* **2020**, *13*, 494. [CrossRef]
82. Bedi, G.; Venayagamoorthy, G.K.; Singh, R.; Brooks, R.R.; Wang, K.C. Review of Internet of Things (IoT) in Electric Power and Energy Systems. *IEEE Internet Things J.* **2018**, *5*, 847–870. [CrossRef]
83. Martín-Lopo, M.M.; Boal, J.; Sánchez-Miralles, Á. A Literature Review of IoT Energy Platforms Aimed at End Users. *Comput. Netw.* **2020**, *171*, 107101. [CrossRef]
84. Callaghan, D. Green Quadrant IoT Platforms For Smart Buildings. 2019. Available online: https://research.verdantix.com/report/green-quadrant-iot-platforms-for-smart-buildings-2019 (accessed on 21 March 2021).
85. Velosa, A.; Friedman, T.; Thielemann, K.; Berthelsen, E.; Peter Havart-Simkin, E.G.; Flatley, M.; Jones, L.; Quinn, K. Magic Quadrant for Industrial IoT Platforms. 2021. Available online: https://www.gartner.com/doc/reprints?id=1-27IESWUW&ct=210922&st=sb (accessed on 21 March 2021).
86. Garg, N. *Apache Kafka*; Packt Publishing: Birmingham, UK, 2013.
87. Aidon . Aidon Head-End System. 2021. Available online: https://www.aidon.com/our-solutions/#head-end-system (accessed on 2 December 2021).
88. Amazon Web Services, Inc. What Is AWS IoT? 2021. Available online: https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html (accessed on 30 November 2021).
89. Cisco. Cisco Kinetic IoT Platform. 2021. Available online: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-kinetic.html (accessed on 21 November 2021).
90. CO4-Energy & CO_2 Comfort and Cost. 2021. Available online: https://co4.cloud/ (accessed on 1 December 2021).
91. EDP Commercial. Re:dy-innovation at EDP. 2018. Available online: https://www.edp.com/en/innovation/redy (accessed on 1 December 2021).
92. ZENNER International GmbH. Element IoT. 2021. Available online: https://zenner.de/iot-services-software/softwareloesungen/element-iot (accessed on 1 December 2021).
93. SIEMENS. EnergyIP®—The Powerful IoT Platform and Application Suite for the Future. 2021. Available online: https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/energyip-meter-data-management/energyip.html (accessed on 1 December 2021).
94. Amazon. Siemens AG Launches Industry-Leading EnergyIP MDM Application on AWS. 2020. Available online: https://aws.amazon.com/solutions/case-studies/siemens-energyip/ (accessed on 1 December 2021).
95. Enerbrain, S.L.R. Enerbrain—For an Intelligent Use of Energy . 2021. Available online: https://www.enerbrain.com/en (accessed on 1 December 2021).

96. Cirillo, F.; Solmaz, G.; Berz, E.L.; Bauer, M.; Cheng, B.; Kovacs, E. A Standard-Based Open Source IoT Platform: FIWARE. *IEEE Internet Things Mag.* **2019**, *2*, 12–18. [CrossRef]
97. Joint Research Centre (European Commission). *A JRC FIWARE Testbed for SMART Building and Infrastructures: Implementation of the FIWARE Platform for Performance Testing and Heterogeneous Sensor Nodes*; European Union Publications Office: Luxembourg, 2020. [CrossRef]
98. Microsoft. Architectural Concepts in Azure IoT Central. 2021. Available online: https://docs.microsoft.com/en-us/azure/iot-central/core/concepts-architecture (accessed on 28 November 2021).
99. Microsoft. What are Application Templates in Azure IoT Central. 2021. Available online: https://docs.microsoft.com/en-us/azure/iot-central/core/concepts-app-templates (accessed on 28 November 2021).
100. DIGIMONDO GmbH. DIGIMONDO's Software Solution Niota 2.0. 2021. Available online: https://www.digimondo.com/en/solutions/iot-platform-niota/ (accessed on 1 December 2021).
101. DIGIMONDO GmbH. Niota Manual. 2020. Available online: https://docs.niota.io/ (accessed on 1 December 2021).
102. Odin Solutions S.L.R. Odin Solutions. 2021. Available online: www.odins.es/ (accessed on 1 December 2021).
103. InfluxData Inc. InfluxDB Time Series Platform. 2021. Available online: https://www.influxdata.com/products/influxdb (accessed on 30 November 2021).
104. InfluxData Inc. Telegraf Open Source Server Agent. 2021. Available online: https://www.influxdata.com/time-series-platform/telegraf (accessed on 30 November 2021).
105. InfluxData Inc. Chronograf: Complete Dashboard Solution for InfluxDB. 2021. Available online: https://www.influxdata.com/time-series-platform/chronograf (accessed on 30 November 2021).
106. InfluxData Inc. Kapacitor & Real-Time Stream Processing. 2021. Available online: https://www.influxdata.com/time-series-platform/kapacitor (accessed on 30 November 2021).
107. Hallowell, M.R.; Gambatese, J.A. Qualitative Research: Application of the Delphi Method to CEM Research. *J. Constr. Eng. Manag.* **2010**, *136*, 99–107. [CrossRef]
108. Sachs, L. *Angewandte Statistik*; Springer: Berlin/Heidelberg, Germany, 1997.