IoT

MDPI

Review

A Holistic Overview of the Internet of Things Ecosystem

Gaetanino Paolone [1,†], Danilo Iachetti [2,†], Romolo Paesani [3,†], Francesco Pilotti [3,†], Martina Marinelli [3,†] and Paolino Di Felice [4,*]

[1] B2B S.r.l., 64100 Teramo, Italy
[2] Meccatronica S.r.l., 64100 Teramo, Italy
[3] Gruppo SI S.c.a.r.l., 64100 Teramo, Italy
[4] Department of Industrial and Information Engineering and Economics, University of L'Aquila, 67100 L'Aquila, Italy
* Correspondence: paolino.difelice@univaq.it; Tel.: +39-3204232540
† These authors contributed equally to this work.

Abstract: The Internet of Things (IoT) is a complex ecosystem of connected devices that exchange data over a wired or wireless network and whose final aim is to provide services either to humans or machines. The IoT has seen rapid development over the past decade. The total number of installed connected devices is expected to grow exponentially in the near future, since more and more domains are looking for IoT solutions. As a consequence, an increasing number of developers are approaching IoT technology for the first time. Unfortunately, the number of IoT-related studies published every year is becoming huge, with the obvious consequence that it would be impossible for anyone to predict the time that could be necessary to find a paper talking about a given problem at hand. This is the reason why IoT-related discussions have become predominant in various practitioners' forums, which moderate thousands of posts each month. The present paper's contribution is twofold. First, it aims at providing a holistic overview of the heterogeneous IoT world by taking into account a technology perspective and a business perspective. For each topic taken into account, a tutorial introduction (deliberately devoid of technical content to make this document within the reach of non-technical readers as well) is provided. Then, a table of very recent review papers is given for each topic, as the result of a systematic mapping study.

Keywords: Internet of Things; IoT conceptual model; IoT security; IoT privacy; IoT blockchain; IoT communication; IoT fog computing; IoT edge computing; IoT cloud computing; IoT servitization; IoT business models; IoT taxonomies; IoT architectures; middleware; IoT digital twins; IoT software architecture; IoT application domains; IoT ecosystem

Citation: Paolone, G.; Iachetti, D.; Paesani, R.; Pilotti, F.; Marinelli, M.; Di Felice, P. A Holistic Overview of the Internet of Things Ecosystem. *IoT* **2022**, *3*, 398–434. https://doi.org/10.3390/iot3040022

Academic Editor: Javier Berrocal

Received: 29 July 2022
Accepted: 3 October 2022
Published: 26 October 2022

1. Introduction

Figure 1 depicts the transformation phases of the Internet up to the Internet of Things (IoT). The IoT is an ecosystem of physical objects (the "things") that connect to the Internet and to other things. These physical objects could be any device tagged with sensors (e.g., smartphones, smart electric appliances, smart office equipment, cars, and so on). The number of IoT devices worldwide is forecast to almost triple from 8.74 billion in 2020 to more than 25.4 billion IoT devices in 2030 (https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed on 5 July 2022)). Data generated by the devices are then shared (over a wired or wireless network) with servers located in cloud or on-premise, where it is processed to gain insights that help in making decisions. The IoT ecosystem can be established not only within small areas such as, for example, a building, but also over larger areas like cities. The IoT is redefining the way we interact, communicate, and go about our daily work. From homes to maintenance to cities, the IoT ecosystem is making our world smarter and more efficient.

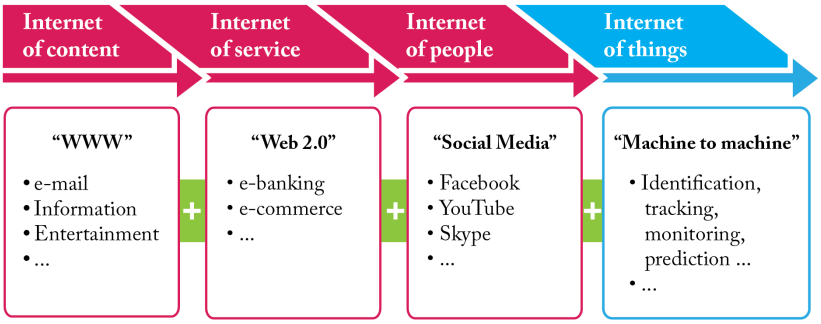

Figure 1. The evolution of the Internet.

Wang et al. in [1] conducted a bibliometric study of 3523 IoT-related articles published in 2000–2019. According to that study, the development of the IoT has gone through three stages. During the first stage, from 2002 to 2009, just nine papers were published. The second stage spans from 2009 to 2015. In those years, many countries issued action plans on the IoT. *"Internet of Things—An action plan for Europe"* is an example [2]. The third stage spans from 2015 to 2019, when 2999 publications were published in Web of Science, with an annual increase in publications of about 85%.

This huge knowledge asset has generated a fragmented picture and a lack of consensus about IoT systems, their basic constituents, their qualities, and in some cases even inconsistent terminologies and definitions. A long list of surveys (i.e., articles that in [3] are called secondary studies) have been written with the aim of overcoming this issue. Despite the relevance and soundness of most of these studies, they suffer two severe drawbacks: (a) their scope does not cover all the aspects connected with the IoT domain; (b) they are structured according to a limited number of research questions. Such a common structure of articles does not fit the needs of practitioners looking for suitable answers to overcome the daily challenges they face. That is the reason why IoT-related discussions have become predominant in various domains' forums, which moderate thousands of posts each month from practitioners with a heterogeneous background and skill.

In 2021, [4] reported on a study that investigated the questions asked by IoT practitioners on one of the relevant domains of the Internet of Things ecosystem, namely "IoT/Industry 4.0". In such a study, authors mined 176819 publicly available posts (on IoT/Industry 4.0-related questions) retrieved from Stack Exchange (the largest—it has millions of active users—and the most trusted online community of developers). The results of the analysis pointed out that the IoT-related questions concerned 100 topics, which the authors grouped into five general categories: software development, platform development (including debugging and analytics), hardware management (including monitoring and testing), network management (including automation and security), and system management (including debugging and security).

These findings tell us that to develop successful projects within a single IoT domain, IoT practitioners need to acquire knowledge about several topics, usually treated in distinct surveys. The situation becomes more tricky when the IoT practitioner aspires to capture a global picture of the composite IoT ecosystem. In fact, in that case, he has to read independent studies and then harmonize the treated concepts into a unifying frame. This accomplishment is hard to reach, especially by practitioners without an adequate background and technical expertise.

Relative to the existing literature on IoT, the present paper's contribution is twofold. First, it aims at providing a holistic overview of the heterogeneous IoT world by taking into account a technology perspective and a business perspective. For each topic taken into account, a tutorial introduction (deliberately devoid of technical content to make this document within the reach of non-technical readers as well) is provided. Then, a table of pertinent review papers (published between 2019 and April 2022) is given for each topic.

We restricted the attention to a short time interval because, as we will see later, the number of review papers is very high.

According to [3], the present paper is a systematic mapping study dealing with topics concerning the IoT ecosystem. As pointed out above, such a domain is extraordinarily broad and, moreover, a very long list of systematic reviews are already available; therefore "a systematic mapping study is more appropriate than a systematic review", [3] (p. 5). "Systematic mapping studies (. . .) are designed to provide a wide overview of a research area" [3] (p. 44), this paper aims to coherently act as the table of contents does in handbooks; indeed, by reading it, a developer can find recently published relevant studies on the concepts underlying the IoT ecosystem (usually the subject of distinct and distant reviews) which he wants to learn about. In light of what has been said above, it follows that this work is not a systematic review; thus, it does not overlap with any of the 119 review studies it cites and to which the reader is referred.

The remaining part of the paper is structured as follows. Section 2 introduces the background necessary to understand the other sections. Specifically, the following topics are introduced: an IoT conceptual model; an IoT reference model; fog computing and edge computing models; middleware; and blockchain. Section 3 describes the articulation of the research process and then the bibliographic search we have carried out. A total of 119 reviews were selected from 62 distinct Scopus-indexed journals. Section 4 reports on the way the 18 topics extracted from the 119 reviews were classified. A brief introduction to each of those topics is also part of the section. Section 5 introduces a definition of the IoT ecosystem that merges a technology perspective and a business perspective. Section 6 introduces the notion of IoT taxonomy and recalls a few recent studies which have made their own proposal. Section 7 ends the paper. Three appendices are an integral part of the paper. They collect a map of the 119 review papers that appeared from 2019 to April 2022.

2. Background

This section collects the following topics: an IoT conceptual model; an IoT reference model; IoT computing models (specifically, fog computing and edge computing); middleware, and blockchain. Given the objectives of the paper, each topic is briefly introduced in a dedicated sub-section without entering into technicalities that interested readers can find in the linked references.

The first step in understanding the IoT ecosystem is to study its architecture [5]. The (keyword thematic evolution and the keyword co-occurrence network) numerical results given in [1] confirm that the IoT architecture is a first-class research topic. Unfortunately, today, there is no one reference architecture model that is universally used. This wealth represents an obstacle for practitioners approaching the IoT ecosystem for the first time. To smooth out these difficulties, it is necessary to introduce first the basic concepts of IoT systems. We refer to the approved International Standard ISO/IEC 30141 [6]. Such a document has four merits: (a) it collects advices for the IoT architect; (b) it is technology-neutral; (c) it gives a clear picture of IoT systems to the involved stakeholders (namely, device manufacturers, application developers, users, and so on); (d) it facilitates the communication between them. Ref. [6] begins by listing the basic characteristics of IoT systems; then it abstracts them into an IoT conceptual model (CM) describing the key concepts of IoT systems; hence, a high-level reference model (RM) is derived. Overall, the ISO/IEC 30141 document serves as a base from which context-specific IoT architectures, and hence actual systems, can be defined.

2.1. IoT Conceptual Model

The IoT CM in [6] is generic, abstract and simple. It introduces a minimum vocabulary about IoT systems, contains the basic concepts to be known about, and describes how they relate to each other logically. The CM is presented by means of a certain number of UML class diagrams where two different types of relationships between classes are used: generalization (the "is-a" relationship) and association (the association names are verbs).

To keep the diagrams readable, classes have no attributes, and the cardinality constraints on association ends are omitted.

Figure 2 collects the four fundamental entities of the IoT CM: the digital entity, the physical entity, the IoT user, and the communication network. These four entities are a specialization of (the class) entity. Entities have an identity provided by a unique identifier. Each entity participates in at least a domain and is said to be contained by that domain. The notion of domain allows one to decompose complex IoT systems into smaller sub-systems.

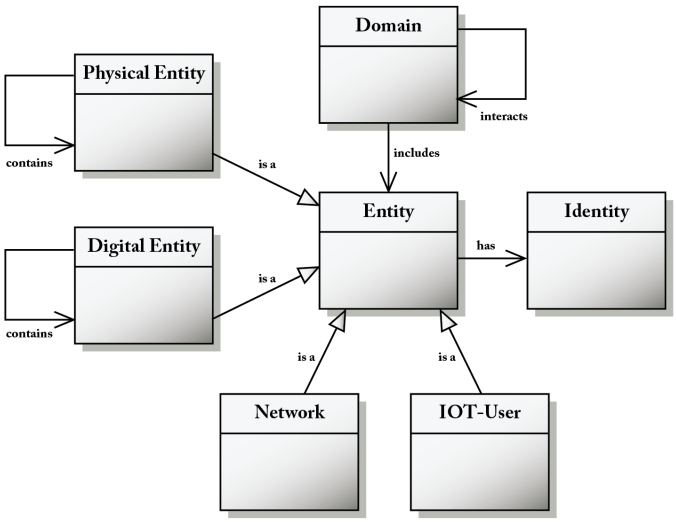

Figure 2. Entities of the IoT CM.

A digital entity is a computational or data element of an IoT system (applications, services, data stores, IoT devices, and IoT gateways are examples of digital entities), while a physical entity (a real-world "thing") is a discrete, identifiable and observable part of the physical environment (humans, animals, cars, buildings, and open spaces are physical entities).

An IoT user may be human or digital; both use applications that, in turn, use a service (Figure 3). An application is a software designed to help IoT users to carry out specific tasks. Service is an abstract concept that is usually implemented as software.

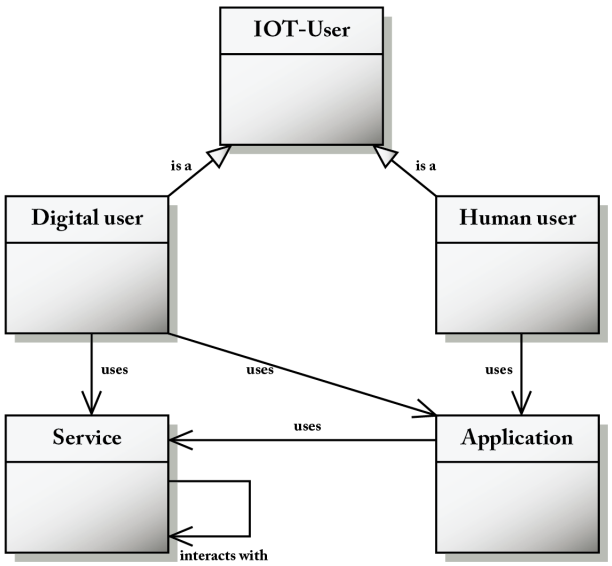

Figure 3. The IoT user class diagram.

Figure 4 shows the relationship between services and IoT devices through IoT gateways that form a bridge between the networks that connect them. A service exposes at least an endpoint by which it can be invoked. An endpoint has one or more network interfaces. An interface is a set of operations and associated parameters. Data associated with services, IoT devices and IoT gateways are archived in data stores that several entities can access. An IoT device interacts with at least a network in order to communicate with other entities in the same IoT system; moreover, it exposes at least an endpoint, can have computational capabilities and can use local data stores.

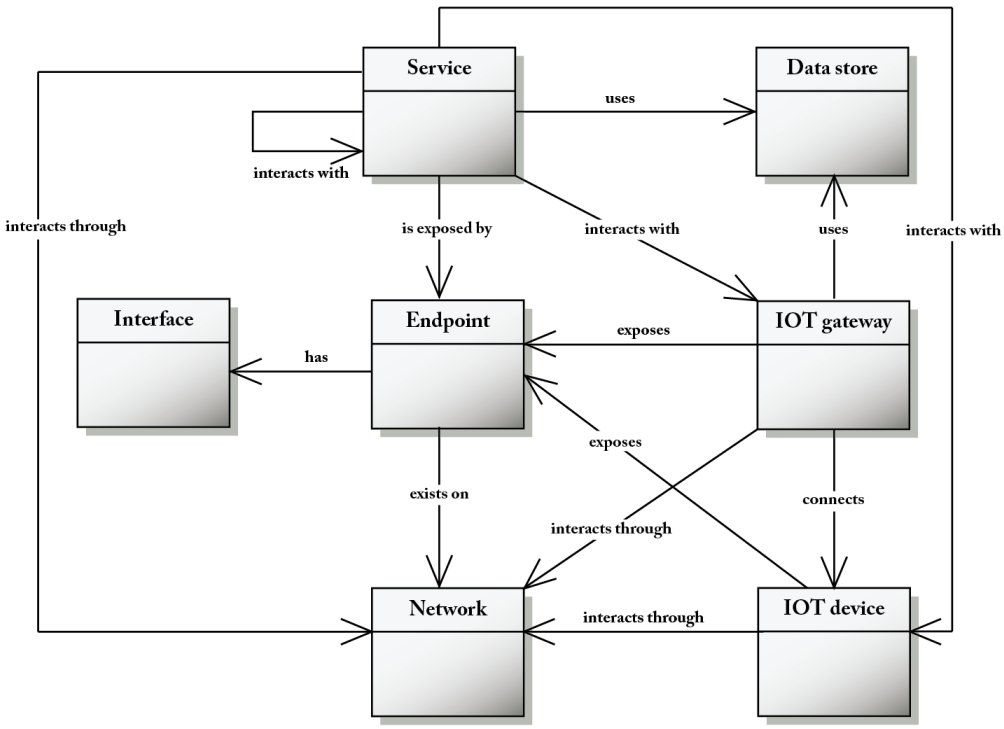

Figure 4. The service, network, IoT device and IoT gateway concepts of the CM.

Figure 5 shows the relationship between a virtual entity, a physical entity and an IoT device. Actuators and sensors are IoT devices that have a direct contact with a physical entity, or they interact with it indirectly through the associated tag. A sensor is a device that measures some property of a physical entity and outputs digital data representing the measurement that can be transmitted over a network. An actuator is a device that accepts digital inputs and, on the basis of those inputs, changes one or more properties of a physical entity. A physical entity can have one or more tags attached to it, and sensors can monitor the tag rather than the physical entity itself. A tag is a physical entity that is attached to another physical entity in order to assist in identifying and tracking that physical entity. Barcodes and RFID are common tags. A virtual entity is a digital representation of a physical entity; it is contained in a service.

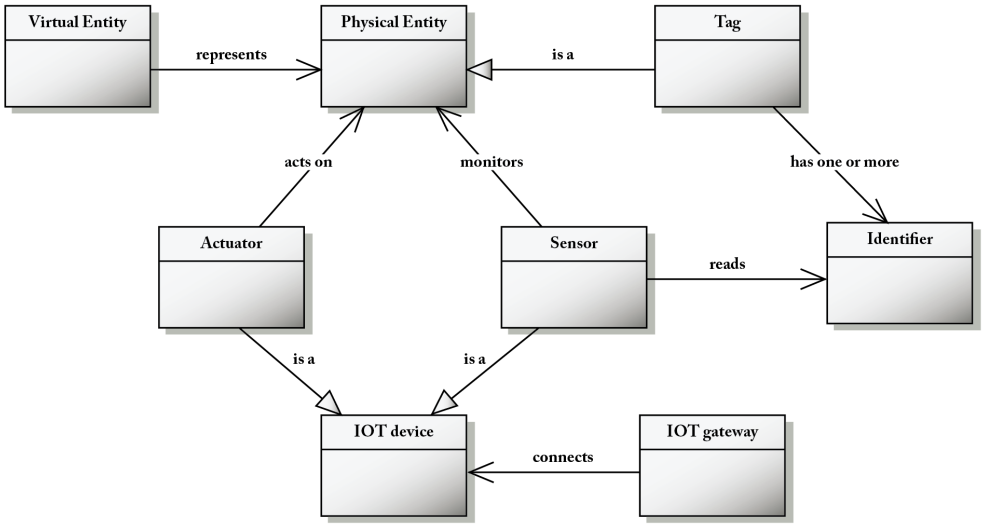

Figure 5. Virtual entity, physical entity, and IoT device concepts of the CM.

2.2. IoT Reference Model (RM)

This sub-section recalls the structure of the IoT RM introduced in [6]. Two complementary perspectives are taken into account in sequence: the first (perspective) is entity-based (Figure 6), while the second is domain-based (Figure 7).

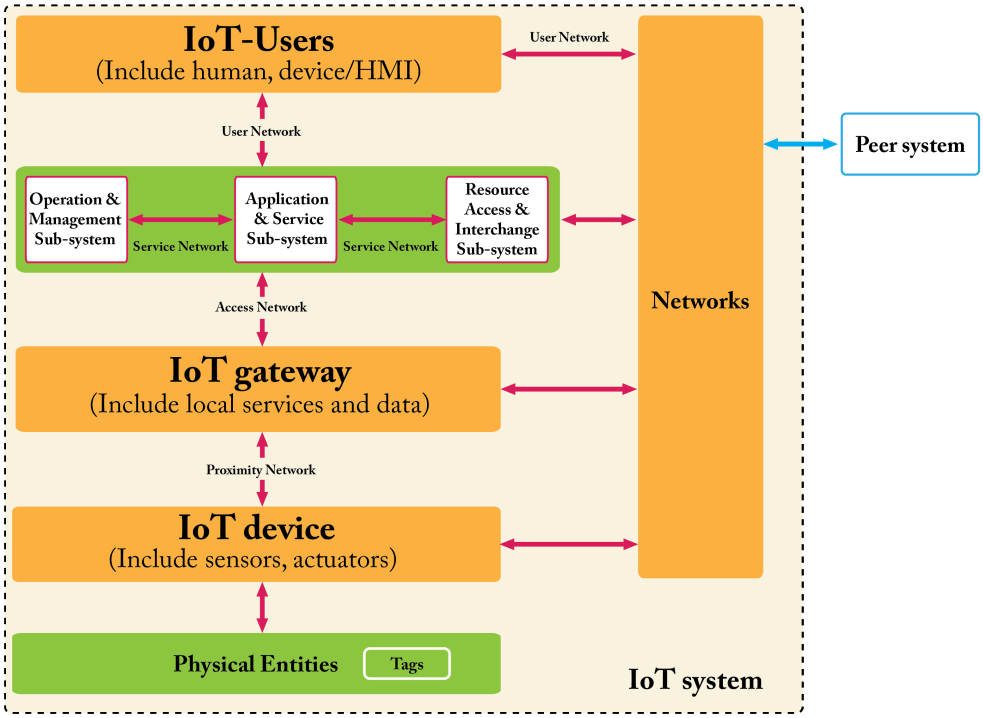

Figure 6. The entity-based IoT RM.

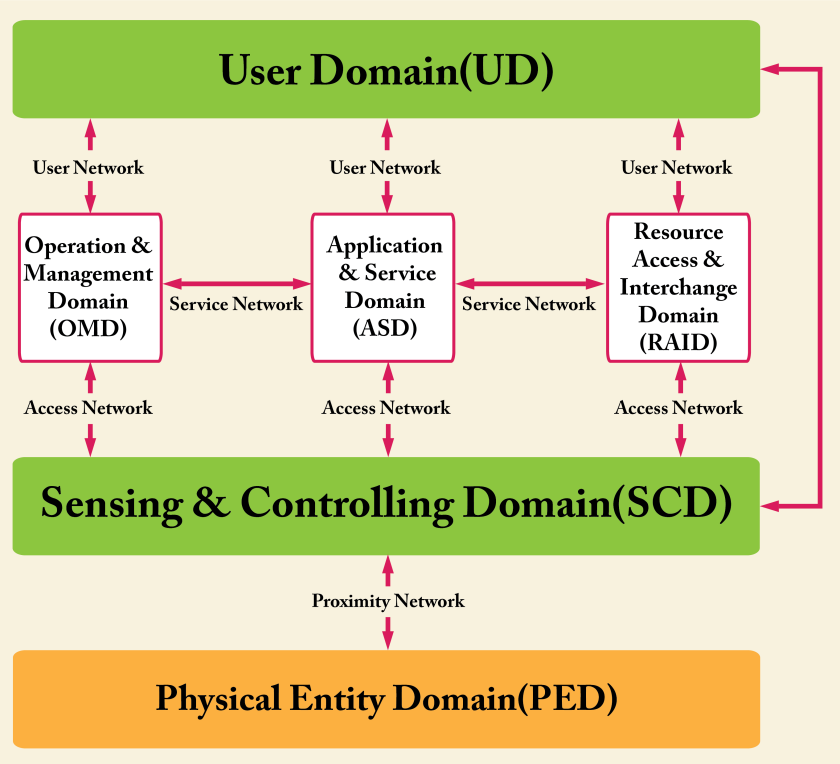

Figure 7. The domain-based IoT RM.

2.2.1. Entity-Based RM

Most of the entities in Figure 6 have been already introduced in Section 2.1, so hereafter, we limit the presentation to the three sub-systems and the (physical) connections. A much more detailed description is given in [6].

IoT devices communicate with the other entities (e.g., IoT users) taking part to IoT systems via the networks. Forward, it will be said that in IoT systems, there are the following four kinds of networks: proximity network, access network, services network, and user network (Figure 6).

The operation and management sub-system includes the device registry database and an associated device identity service, which provides lookup capabilities for applications and services. Various kinds of applications and service sub-systems exist in most IoT systems, with associated data stores. The resource access and interchange sub-system exhibits the interfaces through which both users and peer systems can access the (service/administration/business) capabilities of the IoT system.

Human users typically interact with the IoT system using smartphones, personal computers, etc. Digital users interact with IoT systems by means of APIs. Peer systems interact with the IoT system through the Internet.

2.2.2. Domain-Based RM

This representation focuses on the tasks that have to be performed. The domain-based RM identifies six mutually exclusive domains (Figure 7). Their meaning is intuitive at this point of the summary of the ISO/ICE:2018 document [6], so we say nothing more about them.

The domains of the IoT RM (and hence the entities inside them) interact by means of four different communication networks (Figures 6 and 7). They are briefly described in the following. The key role played by those networks is to support communication and data exchange activities and interactions between pairs of entities, pairs of domains, or pairs of IoT systems.

Proximity network —The role of this network is to connect sensors and actuators (belonging to the SCD) to the gateways of the IoT system. Proximity networks are necessary because of power and processing limitations of sensors and actuators. As a consequence, their scope is limited to the sensing & controlling domain. IPv6 is an example of a proximity network.

Access network— This network connects IoT gateways (and hence sensors and actuators) to the OMD and the ASD. Such a connection enables the transfer of sensor/actuator data (frequently called "edge data") to operations logic (from OMD) or to application logic (from ASD). Either wired connections (e.g., broadband, ADSL, Fibre) or wireless connections (e.g., LANs, mobile networks, etc.) are common technologies used in access networks.

Service network— It connects the applications and services in the OMD, the ASD and the RAID.

User network— It connects the user domain with the OMD and ASD; it also connects peer IoT systems and non-IoT systems with the RAID. This network is typically based on the Internet.

Figure 8 shows that the two representations of the RM are consistent.

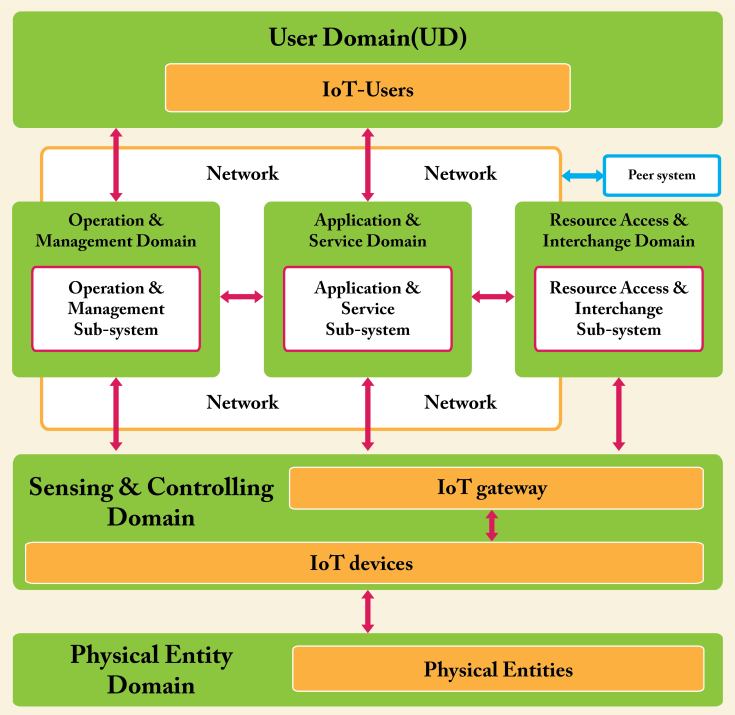

Figure 8. Entity-based RM vs. domain-based RM.

2.3. IoT Computing Models

Up until recently, the mandatory deployment model of IoT systems has been the cloud, which offers powerful services, unlimited storage, and computing capacity on-demand; unfortunately, connecting smart devices to the cloud poses severe issues. First of all, connected devices create large volumes of data, which will inevitably result in performance and network congestion challenges. Secondly, there are performance, security, bandwidth, and reliability concerns that make the cloud-only solution not suitable for all the potential real-world applications. The fog-edge computing paradigms have been introduced to bridge the gap between the cloud and IoT devices [5,7,8].

In [5,9], it is stressed that fog and edge computing are often used interchangeably, but both studies agree that these two concepts should be kept distinct. In this paper, we adopt the same point of view. According to [5], fog computing (FC) is a concept that envisions pushing computing power and storage capabilities down to the local network up to reach the gateway level, while EC brings cloud intelligence and storage capabilities at the device level.

2.3.1. Fog Computing

An example can clarify this approach. Let us refer to a high-speed train embedded with hundreds of sensors controlling its journey (besides all the internal parameters). All the sensor readings can be sent to the cloud (for instance, by using expensive satellite links), where the readings will be processed to detect abnormal conditions and send commands back to the train. There are several problems with this scenario: the bandwidth to transport the sensor and actuator data to and from the cloud is expensive; the connections could be susceptible to hackers; it may take several hundred milliseconds to react to an abnormal sensor reading; and if the connection to the cloud is down, or the cloud is overloaded, the control of the train is lost. As an alternative scenario, let us consider placing a hierarchy of local "fog nodes" inside the train. Those nodes can connect to sensors and actuators with inexpensive local networking facilities. Moreover, the fog nodes can be highly secure. Fog nodes can react to abnormal conditions in milliseconds. Moving most of the decision-making functions of this control system to the fog and only contacting the cloud occasionally to report status or receive commands creates a superior control system.

To overcome the mentioned issues, the OpenFog Consortium (www.openfogconsortium.org) delivered an architecture which offers the so-called SCALE (security, cognition, agility, latency, and efficiency) advantages over the cloud-only model [10]. The IEEE Standards Association has approved the OpenFog proposal as the official standard for FC and called it "IEEE 1934 in August 2018". This standard is introduced with the following words (https://standards.ieee.org/ieee/1934/7137/ (accessed on 5 July 2022).): "OpenFog Reference Architecture is a structural and functional prescription of an open, interoperable, horizontal system architecture for distributing computing, storage, control and networking functions closer to the users along a cloud-to-thing continuum of communicating, computing, sensing and actuating entities."

We can add that cloud and fog computing are on a mutually beneficial, inter-dependent continuum, where certain functions are more advantageous to carry out in fog nodes, while others are better suited to the cloud. The segmentation of what tasks go to fog nodes and what goes to the cloud is application-dependent.

FC architectures are commonly abstracted as a three-layer infrastructure (Figure 9) composed of: (a) IoT devices (e.g., sensors, actuators, smart devices, etc., which represent the front end of whole IoT system and, at the same time, the bottom layer of the architecture. The main purpose of this layer is to sense and capture data. The data are then usually offloaded to the higher layer for the necessary computation); (b) the fog layer (the middle tier); and (c) the cloud layer. The fog layer, in turn, is a network structured as an N-level hierarchy of fog nodes (Figure 10).

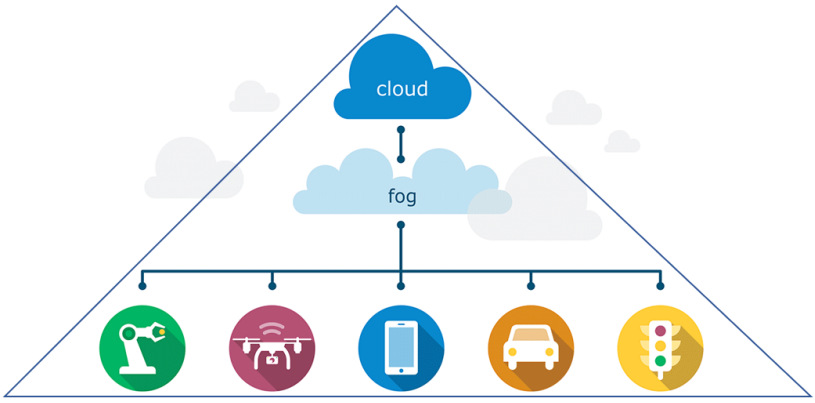

Figure 9. The FC architecture.

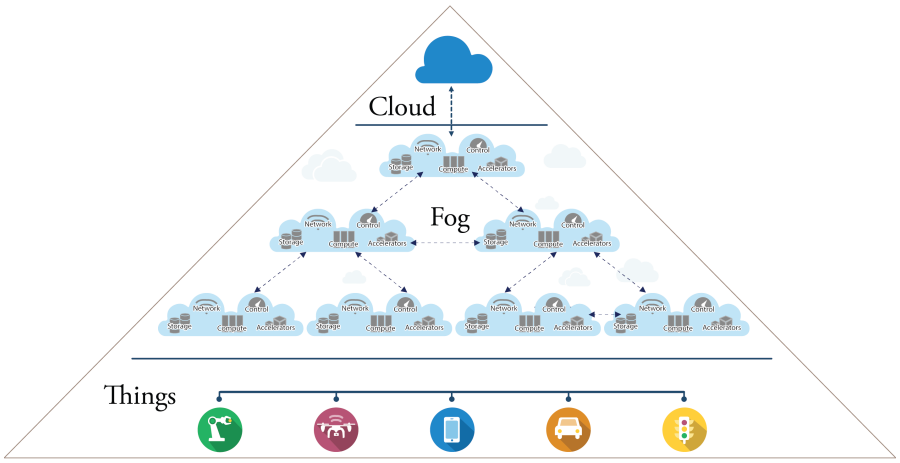

Figure 10. Details regarding the fog layer.

The number of tiers composing the fog layer depends on many factors, including: (a) the number of sensors involved; (b) the capabilities of the fog nodes at each tier; (c) the amount and type of work required by each tier; (d) the latency constraints to be satisfied.

In IoT systems so organized, each node contributes somehow to the overall service, but its role largely depends on its position in the pyramid. In general, each level of the hierarchy examines and extracts relevant data to create more intelligence while moving towards the root. The mode of communication between the things and the fog devices is wireless in nature, while the fog can communicate with the cloud using both wired and wireless means of communication. Notice that fog nodes communicate with each other both vertically and horizontally according to the load of the IoT system and the requirements of the application.

As stressed by OpenFog [10], the nodes of fog computing networks (a) satisfy requirements for security (security is essential to the overall security of the system. This includes protection for interfaces and computation); (b) supports the management of interfaces; (c) are able to communicate through the network; (d) can store data; (e) utilize accelerators (e.g., FPGA, GPGPU, . . .) to satisfy both latency and power constraints; (f) have general-purpose computing capabilities. Moreover, standard/open-source software runs on them, which is a precondition of interoperability between fog nodes.

2.3.2. Edge Computing

According to [9,11], the architecture of modern IoT systems should consist of four layers: a things layer; an EC layer; an FC layer; and a cloud computing (CC) layer. Such an architecture is a consolidation of the FC architecture.

The things layer consists of fixed-place devices (e.g., smart fridges, smart TVs, surveillance cameras, etc.) and/or mobile devices (e.g., smart vehicles, smart wearable devices, smartphones, etc.) that relate to specific applications (e.g., traffic monitoring, healthcare, smart building, and agriculture). Those devices embed micro-controllers and sensors, so they can carry out some degree of computation. This paradigm is called mist computing. Such an augmented computing capability enables IoT devices to constitute a mesh-like network.

The EC layer is equipped with dedicated routers and switches located close to the IoT devices to act as the gateway to the fog or cloud layer. This proximity minimizes the network traffic. Such a layer can also be equipped with micro-data centers (the so-called cloudlets), able to gather the sensed data of the smart devices, filter, and only send the reduced analyzed data to the fog or cloud for the sake of bandwidth preservation. The concept of a cloudlet was the de facto birth of the mobile edge computing (MEC) paradigm as the integration of mobile computing and EC.

The EC has been widely adopted in various application domains, and Market Research Future expects that the global EC market size is likely to touch USD 168.59 billion between

2020–2030 (Market Research Future, Global edge computing market. Forecast till 2030 February 2020. URL: https://www.marketresearchfuture.com/reports/edge-computing-market-3239 (accessed on 26 May 2022)).

2.4. Middleware

Middleware is the core layer of the architecture of modern IoT systems, where it acts as a bridge between applications and smart devices. Middleware masks the heterogeneity and complexity of the devices, solving many IoT issues and, consequently, simplifying the application development. An appropriate middleware layer is a determinant factor to meet the following requirements: functional-, heterogeneous-, and network-scalability; interoperability; light-weightness; real-timeness; self-adaptability; and service reliability [12].

Ref. [12] is an up-to-date survey on middleware. In the study, the authors summarize the requirements of IoT middleware by analyzing the main features of the following five application domains: environment, healthcare, industry, social, and transportation. In the same paper, the following taxonomies of IoT middleware are proposed: the service-based approach, the event-based approach, the virtual machine-based approach, the database-based approach, and the agent-based approach. Those five approaches are presented and then compared with respect to the six requirements recalled above.

Ref. [13] provides an overview of the proprietary and open-source middleware solutions currently available. The IoT middleware platforms are classified into four types (service-oriented, cloud-based, actor-based, and event-based) and compared from different aspects. The following platforms are taken into account. Cloud-based IoT middleware includes: AWS IoT, Azure IoT Hub, IBM Watson IoT, Google Cloud IoT, Xively, and Oracle IoT. Service-based IoT middleware includes: LinkSmart (Hydra), Kaa (open-source), Global Sensor Networks (GSN), ThingSpeak IoT (open-source), and Aura. Actor-based IoT middleware includes: Calvin (open-source), Node-RED (open-source), Ptolemy Accessor Host (open-source), and Akka (open-source). Event-based IoT middleware: Hermes, Gryphon, Rebeca, and FiWare (open-source).

2.5. Blockchain

Below, we touch on this topic by taking inspiration from [14], which:

- Describes the fundamental components of blockchain technologies (i.e., transactions, digital signatures, blocks, consensus mechanisms, and blockchain types) and their pros/cons when applied in the IoT domain (including eHealth, smart home and smart vehicular networks);
- Reviews almost every recent research work about blockchain;
- Identifies research gaps and challenges in those studies and discusses possible solutions.

In IoT systems, the entire network linking things to the cloud requires protection against malicious attacks and threats that, otherwise, can obstruct IoT services as well as endanger the data security, users' privacy and confidentiality. Blockchain (invented by Nakamoto in 2008 as the underlying technology of the Bitcoin cryptocurrency) seems to be destined to become the secure- and privacy-preserving technology for IoT applications. Blockchain is a transparent, trusted, and distributed database (called a ledger) on a peer-to-peer network of participants able to provide a secure method to store and process data crossing it. The data unit on the blockchain is called a transaction; sets of transactions are grouped into blocks; confirmed blocks are stored into the (blockchain) ledger. Sequential blocks in the ledger are linked through a cryptographic hash code.

The implementation of the blockchain method implies high computing costs which, today, represent the biggest challenge to its adoption for IoT systems (typically suffering limitations in the power and storage capacities). Indeed, every node/participant keeps a copy of the ledger. Upon the confirmation of a new block, it is relayed throughout the network, and every node appends the confirmed block to its local ledger. Ref. [14] states that it has been calculated that a blockchain node would need about 730 GB of (data) storage per year if 1000 participants exchange an image of 2 MB per day in a blockchain application.

3. The Research Methodology

Our research methodology is based on the well-known guidelines defined in [3] for conducting systematic mapping studies. Those guidelines are structured in terms of three stages: planning, conducting, and reporting. The third stage is self-explanatory, while the second stage consists in the implementation of the first one. Therefore, below, we detail the conducting stage. It has been articulated in terms of three activities: (a) Definition of the study need; (b) Definition of the research question; and (c) Definition of the mapping protocol.

The study need. The need for the study is motivated by the lack of consensus about IoT systems, their basic constituents, and their qualities that have been pointed out in Section 1 as the result of the preliminary investigation we have accomplished. The study aims at providing a holistic overview of the heterogeneous IoT world by taking into account a technology perspective and a business one, that, as far as we know, so far are kept distinct since they are the topic of independent research communities. The target audience are the developers who are interested in better understanding the characteristics of IoT systems in order to take them into consideration when designing and developing IoT systems.

The Research Question (RQ). To achieve the goals of the study, we investigated the following RQ:

What are the available review studies about IoT systems?

Objective: By answering this question, we aim to download review studies about topics connected with issues pertinent to the IoT ecosystem, either from the technology perspective or from the business persepctive.

Output: A set of pertinent review studies.

The mapping protocol. This activity included the four sub-activities described below.

- Search Process. We implemented it as a manual search of articles in the Scopus repository. Scopus, created by Elsevier in 2004, is the largest curated scientific database. In these days, it has achieved 195 million references (http://www.elsevier.com/solutions/scopus/content (accessed on 5 July 2022)). All major publishers (e.g., ACM, IEEE, Springer, Whiley, Elsevier, ...) are indexed in Scopus. About 99.11% of the journals indexed in Web of Science are also indexed in Scopus [15]. That is the reason why we queried only Scopus.
- Inclusion criteria. The initial search string was the following (the Scopus engine is case sensitive):
  "Internet Of Thing" OR "Internet Of Thing (IOT)" OR "Internet Of Things" OR "Internet Of Things (IOT)" OR "Internet Of Things (IoT)" OR "Inter net Of Things (IOT)" OR IOT OR IoT.
- Exclusion Criteria. As output, we received 148,773 documents. Scopus offers several ways to refine the result of a search. We restricted the output, definitely too large to be investigated, by adding the following three filters: (a) Language: English; (b) Document type: Review; (c) Source type: Journal. The bibliographic search has been restricted to journals as they are the natural destination of review studies, unlike research papers, which very often are made public at conferences. The number of items returned by the search was 3286. Table 1 and Figure 11 show the distribution of these reviews over the years.
  Through the "Source title" item exposed by Scopus, we found that the 3286 reviews came from 160 distinct journals. A large number of them have focuses distant from the IoT, which explains why the papers published in these journals have a mild connection with the IoT ecosystem. A partial list of journals that fall into this category, and which, therefore, were excluded from the research, follows: *Advanced Engineering Materials; Advanced Functional Materials; Advanced Healthcare Materials; Advanced Materials; Advanced Materials Technologies; Advanced Optical Materials; Advances in Physics: X; Aggression and Violent Behavior; Chemical Reviews; Current Opinion in Neurology; International Journal of Epidemiology; International Materials Reviews; Journal of Advanced Research in Dynamical and Control Systems; Materials Today; Nano Energy; Nature Com-*

munications; Nature Materials; Semiconductor Science and Technology; and *Sensors and Materials.*

To overcome the aforementioned criticality, the initial search was restricted to the 62 journals listed below: *IEEE Access; Journal of Network and Computer Applications; IEEE Internet of Things Journal; IEEE Communications Surveys and Tutorials; Internet of Things Netherlands; ACM Computing Surveys; Computer Communications; Future Internet; Wireless Communications and Mobile Computing; Computer Networks; International Journal of Distributed Sensor Networks; Journal of Sensor and Actuator Networks; Security and Communication Networks; Computer Science Review; IEEE Communications Magazine; Proceedings of the IEEE; Computer; Sustainable Cities and Society; Computers in Industry; IEEE Internet Computing; Computers and Security; Journal of Medical Internet Research; Journal of Theoretical and Applied Information Technology; Computers and Electronics in Agriculture; IEEE Pervasive Computing; IEEE Wireless Communications; Journal of Industrial Information Integration; Digital Communications and Networks; IEEE Transactions on Industrial Informatics; International Journal of Environmental Research and Public Health; Journal of Management Analytics; Pervasive and Mobile Computing; Annals of Emerging Technologies in Computing; Communications of the ACM; Health and Technology; IEEE Cloud Computing; Journal of Healthcare Engineering; Smart Cities; Trends in Food Science and Technology; Applied Sciences, Array; Blockchain: Research and Applications; Computer & Security; Digital Signal Processing; Future Generation Computer Systems; Industrial Marketing Management; Information Sciences; Information Systems; Information; Intelligent Systems with Applications; International Journal of Wireless Information Networks; Journal of Ambient Intelligence and Humanized Computing; Journal of Business Research; Journal of Parallel and Distributed Computing; Journal of Retailing and Consumer Services; Journal of Retailing; Journal of Systems Architecture; Journal of Open Innovation: Technology, Market, and Complexity; Mobile Networks and Applications; Sensors; Telematics and Informatics;* and *Wireless Personal Communications.*

Five journals (namely the *Journal of Business Research; Industrial Marketing Management; Journal of Open Innovation: Technology, Market, and Complexity; Journal of Retailing and Consumer Services;* and *Journal of Retailing*), among the 62 listed above are business-oriented. They have been selected in order to complement the IoT technology perspective with the IoT business perspective.

The number of items returned by the new search was 953. This number confirms the great ferment of research about the IoT ecosystem, interest substantiated by the large number and heterogeneity of the topics with a greater or lesser connection with such a domain. Given that the first objective of this work is to offer a tutorial introduction to the IoT ecosystem (Section 1), we carried out a further filter. It consisted of limiting the attention to the reviews published between 2019 and April 2022. As a result, we retrieved 119 articles; this is a manageable number which, at the same time, is definitely significant.

- Data Collection. We downloaded (as a PDF file) the title, authors' name, keywords, abstract and DOI for each article belonging to the set of items returned by Scopus.
- Data Analysis. At this stage the title, keywords, and abstract of the 119 reviews were read by three authors of the present paper. Despite the fact that, in systematic mapping studies, the investigation is usually limited to taking into account the title and abstract of each selected item, we downloaded the PDF of the 119 reviews to give a correct answer to the RQ. The other three authors read the introduction and conclusion sections of those articles. Periodic meetings were organized among the authors to make alignments regarding the proper classification of the reviews. This approach was applied iteratively until all the reviews had been explored and mapped.

Table 1. Total number of reviews archived into Scopus.

Year	#	Year	#	Year	#	Year	#
2022	376	2017	208	2012	18	2004	2
2021	1011	2016	131	2011	6	2002	1
2020	714	2015	51	2010	1	2001	1
2019	426	2014	26	2009	1	1996	1
2018	297	2013	13	2006	1	1992	1

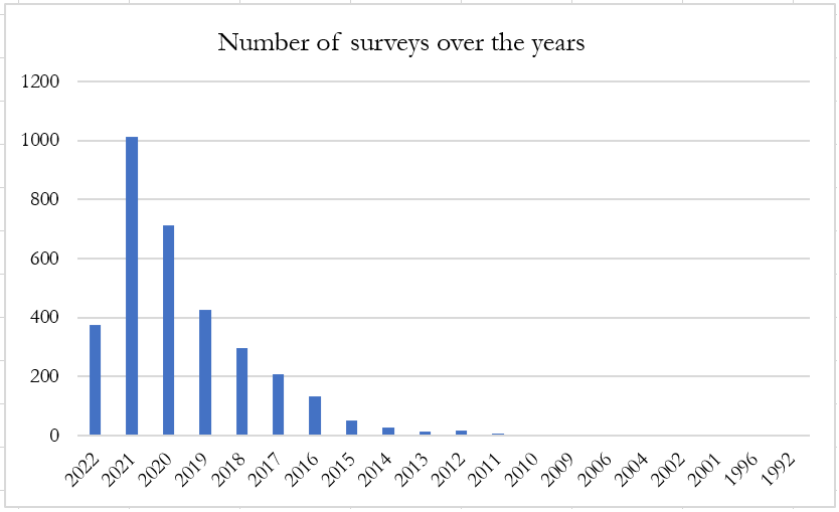

Figure 11. The graph of the reviews archived into Scopus.

4. A Map of Recent IoT Review Studies

"The data extraction process for mapping studies (. . .) can (. . .) be termed a classification (. . .) stage." [3] (p. 44); accordingly, the topics covered in the 119 review articles were grouped as three distinct dimensions (Table 2): (a) *functional blocks* (sometimes also called the constituent components) of the IoT systems (the first column), (b) their *qualities*—i.e., their non-functional characteristics (the second column), and (c) *other topics* (the third column). The six functional blocks are as in [5], the six qualities come from [16], while the six items in the last column complete those in the other two columns of the table.

Table 2. Dimensions and topics of the IoT ecosystem.

Functional Blocks	Qualities	Other Topics
Identification	Security	Application Domains
Sensing	Privacy	Business Models
Networking	Interoperability	Customers
Computation	Scalability	Servitization
Services	Latency	Digital Twins
Analytics	Reliability	Software Engineering

4.1. IoT Functional Blocks

Below, the six functional blocks in Table 2 are briefly described ([5] discusses them meticulously) and linked to the concepts introduced in Section 2. Appendix A lists the reviews (published from 2019 to April 2022) where these concepts are deepened.

- **Identification** It has been already said that IoT systems are complex systems composed of physical entities, sensors, actuators, network components, and software components. It is essential that each entity in an IoT system is distinguishable from each other in order to make it possible for the system to monitor and communicate with specific entities. The identification of the entities is done by attaching tags to them

(Section 2.1). In this way, a unique identification code is associated unambiguously to the "things". In the domain-based RM (Section 2) the identification block belongs to the SCD (Figure 7).

- **Sensing** IoT networks sense, aggregate, and broadcast data from smart objects located in a given area. IoT sensors can be deployed as individual devices (smart sensors, smart wearables, actuators) or as a network of devices (such as WSN) that execute a function collectively. A wide range of sensors are currently available on the market place and used in IoT applications [5,17,18]. In the domain-based RM (Section 2) the sensing block belongs to the SCD (Figure 7).
- **Networking** IoT networks are a combination of heterogeneous smart devices, communication technologies, and protocols that all together perform application-specific tasks. Communication protocols provide instructions on data coding, transmission and flow controls, sequencing, and error correction. There are a bulk of technologies for IoT communication [19]. Communication technologies usually used in IoT networks include near-field communication, narrowband IoT, ultra-wide bandwidth, LTE-A, WiMax, WiFi and LoRa. A comparison among largely utilized communication technologies in IoT networks may be found in [5]. As said in Section 2, there are four different kinds of networks to connect the physical components in the six domains of an IoT system: proximity networks, access networks, service networks, and user networks (Figure 7). The networking functional block also corresponds to the networks block in the entity-based RM (Figure 6).
- **Computation** Standard computation is performed by the CPU and is managed by the hardware's operating system. Unfortunately, such a paradigm is not suitable in the IoT domain where, as the number of IoT devices grows, a heterogeneous approach is required. The findings from many recent studies have shown that future IoT systems need hybrid computing capabilities ranging from low-power IoT nodes to mid-end gateways to high-computing cloud networks [20,21]. Section 2.3 has introduced the most relevant IoT computing models. Computation in IoT systems takes place at each layer of the RM (Figures 6 and 7).
- **Services** Service is an abstract concept (2) that is usually implemented as software. IoT systems can provide an increasing number of ubiquitous services with different performances and functionalities. A service in the IoT environment can be invoked by a user to perform specific tasks, such as, for instance, returning the humidity of a room [22]. Several types of services are implemented inside the operation and management sub-system, the application and service sub-systems, and the resource access and interchange sub-system (Figure 6).
- **Analytics** IoT systems sense and convey a huge volume of heterogeneous data that have to be stored and later processed by efficient algorithms to get benefit from them. Analytics services of various types are usually provided by the application and service sub-systems (Figure 6) and the ASD (Figure 7). Analytics services are also supported by the IoT gateway, typically operating on data coming from the IoT devices or from the device data store. Ref. [23] stressed the primary role that will be played by the technologies, frameworks, and platforms for big data analytics.

Ref. [5] is a rigorous systematic literature review that proposes an IoT technological stack, which has the merit of decoupling the enabling technologies, the underlying infrastructure, and vendor implementations concerning the IoT ecosystem. In the paper, the IoT functional blocks are thoroughly investigated at each layer of the stack. Table 6 in [5] associates the IoT functional blocks briefly recalled in this sub-section with the pertinent technologies.

4.2. IoT Qualities

Quality aspects are non-functional characteristics of IoT systems. As said at the beginning of Section 4, the IoT qualities we refer to come from [16]. With respect to the original taxonomy, we merged trust into security (similarly to what is done in [6]). Below,

we briefly introduce the six qualities in Table 2 and link them to the concepts introduced in Section 2. Appendix B collects the pertinent reviews.

- **Security:** Information security is a major concern of any ICT system, and IoT systems are no exception. IoT systems present particular challenges for information security because they are distributed and involve a large number of diverse components. As in [6], hereinafter, security (of an IoT system) is defined as the combination of availability, confidentiality, and integrity. Availability means that the IoT system is accessible and usable on demand by an authorized entity; the latter includes both human users and service components. Availability is a characteristic of devices, data and services. Confidentiality means that information is not disclosed to unauthorized individuals, entities, or processes. Integrity means that the data to be used for decision-making processes are accurate and complete. Therefore, integrity ensures that the data have not been altered by faulty or unauthorized devices, by malicious actors, or by environmental causes. An increasing number of scholars are investigating the security improvements that can be achieved in IoT systems using a blockchain-based approach (Section 2.5) (e.g., [24,25]). The security issue spans the four different categories of IoT networks of Figure 6.
- **Privacy:** privacy characterizes aspects related to the protection of the data of an IoT system. The privacy requirement spans all layers of IoT systems from the bottom to the top, that is, from the sensing of data, to its storage, to the processing (Figure 6). Security functions in IoT systems assure the authenticity, availability, confidentiality, and integrity of information travelling the networks. The concept of privacy overlaps the concept of protection of personally identifiable information (PII). If PII is stolen or is misused, the people identified by the information may be harmed somehow. ISO/IEC 29100 details the principles to protect PII. Task offloading is one of the key enabling ECs, (which, as has been mentioned in Section 2.3.2, continues to grow at a steep pace). Because of the vulnerability of edge servers and the wireless transmission features, serious privacy concerns come along with offloading. Ref. [26] is a comprehensive survey that systematically reviews recent studies about privacy-preserving offloading methods.
- **Interoperability:** interoperability (called heterogeneity in [6]) is the ability of IoT systems to seamlessly communicate and use each other's services. The IoT is typically cross-system, cross-product and cross-domain. Realizing the full potential of IoT requires interoperability between heterogeneous components and systems. A certain number of temperature sensors from different manufacturers and with different specifications integrated into a single IoT system is a simple, and at the same time common, example of heterogeneity. Middleware is the core component of the IoT systems devoted to enhance the interoperability (Section 2.4).
- **Scalability:** Let us refer to a smart city IoT system where the number of the attached sensors increase constantly over a time. The growth will determine an increase in the volume of sensor data flowing in the system, in the volume of data being stored in the database, in the number of devices handled by the management system, and in the number of temperature readings processed by services and applications. It is important that the IoT system continues to function effectively despite its growth. Ref. [12] distinguishes among functional scalability, heterogeneous scalability, and network scalability. Functional scalability means that a functionality can be added to, modified from, or removed from the IoT system without affecting existing activities. Heterogeneous scalability denotes the ability to add heterogeneous components and resources. Lastly, network scalability is the ability to add or remove network nodes without the need to restart the whole system. Middleware is the core component of the IoT systems devoted to enhancing the scalability (Section 2.4).
- **Latency.** Latency concerns the time an IoT system needs before responding to an external stimulus (e.g., a user request via a smartphone). Obviously, transferring large volumes of data from the environment to the cloud (the most common architecture

thus far) increases energy consumption, resource consumption, and network latency, which is not suitable for time-critical applications. To address this issue, the edge and fog computing paradigms have been proposed. They allow data storage and processing at network edges rather than on a distant cloud data center (Section 2.3).

- **Reliability:** reliability is a property of consistent, intended behavior and results [6]. Reliability is relevant with respect to communications, data, and computing. Reliability of data is of great importance for the decision-making processes of many IoT systems, while reliability of communication networks is important for ensuring the availability and correct operation of IoT systems. Health-related applications, industrial manufacturing operations and time-critical applications are examples of applications that pose stringent requirements on the reliability. Edge-fog computing and middleware enhance the reliability of IoT systems (Sections 2.3 and 2.4).

In light of the above discussion about the qualities of IoT systems, it is possible to notice that there exists an overlapping between the computation functional block and the security, privacy, reliability, and latency quality attributes (Figure 12).

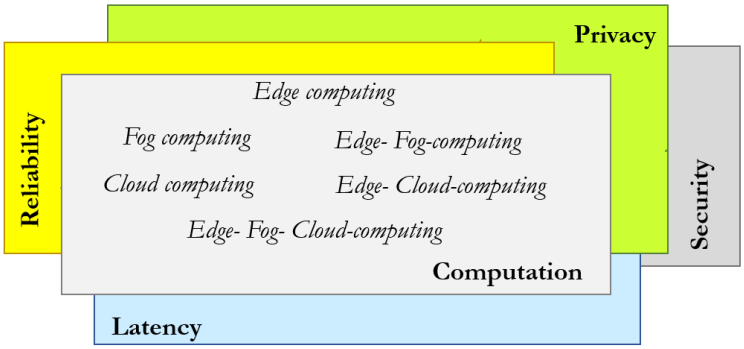

Figure 12. Overlapping of the computation functional block and four qualities of IoT systems.

4.3. Other Topics

The third column of Table 2 lists the following six items: application domains, business models, customers, servitization, digital twins, and software engineering. These arguments complement those in the first and second column of the same table.

The larger the domain of the IoT applications becomes, the more relevant the topics become concerning business models, customers, and servitization.

The digital twin (DT) is an emerging approach that promotes the softwarization of physical things into logical ones. At present, DT promises to change the way products and systems are made and used.

From the software engineering perspective, IoT applications are distributed over heterogeneous devices, operate in dynamic and uncertain environments, and, in the worst case, they can stop providing their services abruptly. It follows that to be able to provide IoT users (either humans or machines—Section 2) with robust IoT applications is a serious challenge.

Below, we introduce these five topics. Appendix C collects the pertinent reviews where the interested reader may find a suitable deepening.

4.3.1. Application Domains

IoT is becoming popular due to its wide range of applications in healthcare, retail, smart parking, transportation, agriculture, public safety, smart lighting, smart homes, smart buildings, manufacturing, logistics, and disaster management, just to mention a few (Figure 13). The list of industries and businesses using IoT is incredibly long, and the COVID-19 pandemic has forced rapid adoption because it holds the promise of enabling businesses to sail safe in the new normal.

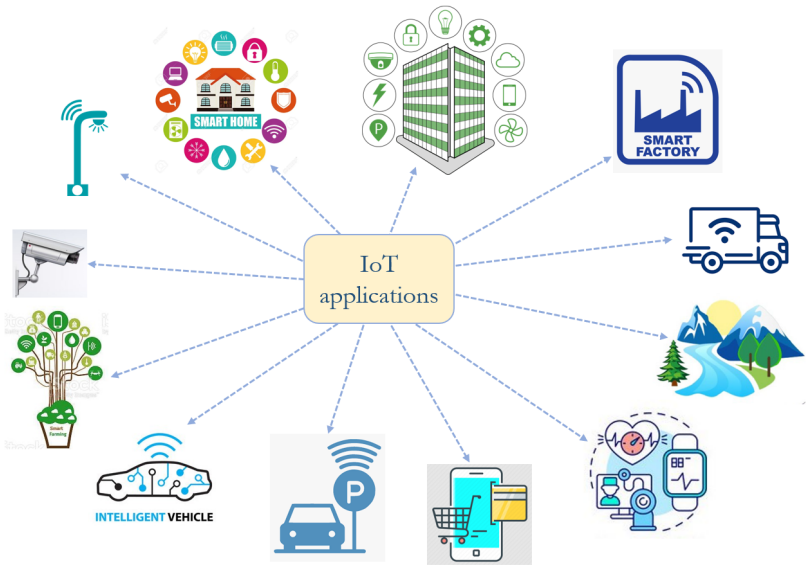

Figure 13. Examples of IoT application domains.

Ref. [27] summarizes the structure and the methodology of sustainable IoT applications; reviews the most important IoT applications; discusses the major challenges of the sustainable growth of IoT applications; highlights open research directions in the field of IoT; and proposes directives for new business opportunities.

4.3.2. Business Models

Business models are conceptual tools that explain the logic of an organization, the way it operates, and hence, how it creates value. In the meantime, while issues such as security, privacy, reliability, and network instability are solved (Section 2), currnetly, important questions are under investigation about how businesses should innovate their business models in order to create and capture added value thanks to the adoption of the IoT technology. Indeed, the IoT revolution can reshape industries, modify work processes, create new economic benefits, save time, money and ultimately improve the quality of our life. At present, "a practical and effective IoT business model is yet to emerge" [28]. The reviews collected in Appendix C provide insight into the phenomenon of IoT in order to help organizations understand the potential of such a technology and, hence, how value could be created by implementing it. For example, the literature review reported in [29] identifies four groups of articles: the first one contains studies examining the innovation of business models that takes place thanks to the digital/IoT technologies; the second collects studies dealing with the interconnection between business models and strategies in the general context of digitalization; the third group contains studies that focus on digital platforms and how they are shaping business models; eventually, the fourth group collects studies that analyze the relationship between digital/IoT technologies and business models in a servitization perspective.

4.3.3. Customers

IoT innovation impacts the customers' life in two opposite directions, as is pointed out below. It was not too long time ago when industries and retailers claimed that the key to attract and maintain customers was determined by the quality of the products they sell and their price. Now, things have changed dramatically, as explained by Batat [30], which says that: "today consumers increasingly buy experiences rather than goods or services". Given that nowadays, customers are tech-savvy, the adoption of IoT technology is becoming mandatory for industries and retailers to meet this goal; indeed, the IoT has the potential to provide personalized services to customers (since IoT is able to bridge the gap between the digital world and the real world).

The other side of the coin concerns the protection of customer identity and personal data. Indeed, the growth of IoT-enabled devices and the developments in artificial intelligence and 5G are intensifying the pressure on privacy. In a very recent review about the state-of-the-art of people-centered distributed ledger technology (DLT) [31], Pinto, da Silva, and Moro conclude that DLT-IoT architectures and the protection of individuals' interests in the data economy is in an embryonic state. In the same study, those authors conjecture that in the near future, there will be an acceleration in the proposal of reliable people-centered IoT solutions based on DLT.

Ref. [31] gives a picture of people-centered data control milestones starting from the 1960s. Here, we only mention the more recent and relevant initiatives. In 2016, the European Union published the General Data Protection Regulation; in the same year, the Self-Sovereign Identity (SSI) concept emerged. With SSI, people have the opportunity of controlling their personal data, share it or even sell it. In 2018, the MyData Global was created with the objective of empowering individuals by "improving their right to self-determination regarding their personal data", and California released the California Consumer Privacy Act.

4.3.4. Servitization

Moving from product to service is called servitization. There are a number of reasons why manufacturers and retailers should implement the servitization paradigm:

- *Revenue growth and profitability:* By adding services to their offering, companies increase their number of revenue streams, and those become recurring. Complimenting the product portfolio with ongoing services to the customers allows their income to become more predictable and secure, which in turn helps insulate the company from unpredictable market conditions.
- *Improved customer outcomes:* Focusing on solutions instead of products allows companies to think in terms of their customers' needs, which means companies can adapt products and services to help customers achieve those outcomes; furthermore, this helps companies to respond faster to issues and challenges that may arise. The resulting increase in customer satisfaction builds a stronger relationship and increased loyalty.
- *Higher entry barriers:* The more established a relationship with customers is, the more difficult it is for someone to come in and steal market share. Servitization means that customers benefit from support and knowledge in real terms, every day.

In the present time, with digitalization advancing rapidly, more and more companies are understanding the benefits of making the final step, that is, implementing the so-called digital servitization [32]. Digitalization and servitization are distinct business model innovations. In fact, manufacturing industries and retailers can invest in digitalization without providing services; vice versa, they can offer services without the support of digital technologies. However, it is worth notice that digitalization is an important enabler of servitization. Specifically, embedding IoT-enabled sensors and devices into physical products makes them intelligent and connected, so it becomes feasible for industries and retailers to achieve closer and better proximity to their customers and, at the same time, reorganize their value chains by expanding the scope of their product–service offerings.

The digital servitization paradigm addresses three relevant requirements of modern industries, that is: agility, connectivity, and decentralization. Additionally, one more point in favor of IoT-based digital servitization derives from the useful insights that can be gained by analyzing the performance of a product and using this information for continuous improvement.

All said, digital servitization can be defined as the process by which a company transforms its product-centered business model to a service-centered business model with the support of IoT/digital technologies, allowing the reorganization of its business processes, capabilities, products, and services to enhance the value for customers and

simultaneously increase the company's performance, [32], p.109. Such a definition gathers technical (i.e., offering and technology) and business perspectives.

The notion of digital servitization coincides with the notion of smart services adopted in [33]: "Smart service is a service whose value and efficiency extends beyond classic, digital service and is delivered through a smart product."

4.3.5. Digital Twins (DTs)

A severe challenge posed by IoT systems composed of thousands of "things" (such as, for instance, smart cities) concerns how to manage efficiently, and often in real-time, the big data that they produce. To become truly smart/intelligent, IoT systems have to possess, in addition, the following three core characteristics: awareness, response, and prediction. Real-time awareness (of IoT systems) is fundamental in order to keep rapidly changing parameters under constant control (for instance, the pollution level in the downtown of a city). By referring, once again, to the city domain, awareness coupled with quick response time can enhance the quality of life of citizens and, sometimes, even save lives. The ability (of IoT systems) to predict is the precondition for them to proactively respond to events. There is increasing convergence over the DT paradigm as the solution of this problem.

Many definitions of the notion of DTs have been proposed. For instance, [34] lists eight independent definitions coming from as many articles. Three alternative DT definitions, taken from [35], follow. DT refers to the ability to clone a physical object into a software counterpart. The softwarized object (the DT) reflects all the important properties and characteristics of the original object (the twin) within a specific application domain.

A DT is composed of three parts: (a) the physical object in the real space; (b) the virtual object in the virtual space; and (c) connected data that ties the physical and virtual together [36].

A DT of an IoT system consists of (a) a set of models of the system; (b) a set of contextual data traces and/or their aggregation/abstraction collected from the system; and (c) a set of services that allow using the data/models from/of the original system [37].

IoT sensors continuously collect the data necessary for companies to derive value from physical things. This feed of real-time data is what ensures that a DT maintains an actual live copy of an asset, process, or ecosystem. The marriage between the virtual and physical world allows the analysis of data and the monitoring of the IoT system to foresee problems before they occur, prevent downtime, develop new opportunities and even elaborate plans for the future by carrying out simulations.

The DT notion impacts the business model, customer (experience), and (quality of) servitization topics (discussed previously) (the point of view held by Thomas Kaiser, SAP Senior Vice President of IoT, in 2017 explains this statement: "Digital twins are becoming a business imperative, covering the entire lifecycle of an asset or process and forming the foundation for connected products and services. Companies that fail to respond will be left behind." (https://www.forbes.com/sites/bernardmarr/2017/03/06/what-is-digital-twin-technology-and-why-is-it-so-important/?sh=320198902e2a—accessed on 25 May 2022)) and software engineering (discussed next).

4.3.6. Software Engineering

From a software engineering point of view, IoT applications execute on a network consisting of hundreds to thousands of heterogeneous devices (e.g., sensors, actuators, storage, and user interface devices), operating in dynamic and uncertain environments, and they can fail to provide their services without notice. Consequently, their development differs from the development of traditional applications.

Another difference with the development of traditional software (that has to be taken into account in the development of IoT applications) resides in the multitude of involved stakeholders, namely: software designers, developers, domain experts, and technologists. It follows that, in the process of IoT application development, knowledge from multiple

concerns intersects. Moreover, those stakeholders have to address issues belonging to different life cycle phases, including development, deployment, and maintenance.

Scholars are debating whether the model-driven engineering (MDE) paradigm can mitigate the challenges posed by the development of IoT applications, but, so far, the question of whether MDE can play a key role in the future of IoT is still an unanswered research question [38]. Below, we mention two studies that adopt the MDE paradigm.

To reduce IoT development effort, Patel and Cassou [39] suggest: (a) separating this task into different concerns; (b) providing stakeholders with a set of high-level languages to specify them. In detail, their proposal consists of (a) a conceptual model; (b) a development methodology; and (c) the implementation of a development framework. Through the conceptual model, it is possible to address four major concerns for IoT application development, namely domain-specific concepts, functionality-specific concepts, deployment-specific concepts, and platform-specific concepts. In turn, the development framework supports three modeling languages: Srijan Vocabulary Language (to describe domain-specific features of the IoT application), Srijan Architecture Language (to describe application-specific functionality of the IoT application), and Srijan Deployment Language (to describe deployment-specific features consisting information about physical environment where devices have to be deployed).

MontiThings is a modeling infrastructure that facilitates the development of IoT applications by increasing abstraction, separating concerns, and their deployment to heterogeneous devices [40]. Specifically, MontiThings (a) supports the separation of error-handling from the development of business logic; (b) features a model-driven toolchain for generating executable containers; and (c) allows an efficient deployment of them even for large IoT systems. MontiThings specifies architectures of IoT systems as networks of components that exchange data with each other via black box ports. MontiThings is an extension of MontiArc (an Architectural Description Language for the MDE of IoT systems), and is implemented using MontiCore (a language workbench for the engineering of textual Domain Specific Languages) and the template engine Freemarker.

5. IoT Ecosystem

The prevalent number of definitions of the IoT-ecosystem notion comes from a technology perspective. Several scholars have proposed their own definition. Ref. [41], for example, states that an IoT ecosystem connects heterogeneous components in a handled way to build an efficient and secure system, while ref. [42] says that an IoT ecosystem comprises the following four basic components: sensors and actuators, connectivity/gateway, data processing, and the user interface.

In 2012, ref. [43] proposed a definition of the IoT business ecosystem (i.e., a definition of IoT ecosystem from the business perspective) as a metaphor adopted from biology. It is well-known that a natural life ecosystem is a biological community of interacting organisms along with their physical environment, with which they also interact. Similarly, in [43], an IoT business ecosystem is defined as being comprised of the community of interacting individuals and companies along with their socio-economic environment.

We are now able to give a definition of the IoT ecosystem which merges the technology perspective of the IoT domain with the business one. This widening of the perimeter of the definition of the IoT ecosystem is motivated by the fact that, from a commercial point of view, the IoT represents a huge opportunity for most companies to enter new markets and generate increasing revenue.

An IoT ecosystem connects resource-constrained heterogeneous devices in a handled way to build an efficient and secure system, whose final aim is to deliver services of practical utility to a community comprising a multitude of stakeholders. At a high level of abstraction, the involved stakeholders are: the industries providing the IoT technology, the developers of IoT solutions, and the customers (either individuals, companies, or machines).

6. IoT Taxonomies

The heterogeneity and complexity of the IoT ecosystem originated a huge number of classification of such a domain. Such classifications are usually called taxonomies. Classification of the IoT can be carried out in many ways, as it emerges, for example, from [16], which reports on a mapping study about 73 papers concerning IoT system taxonomies. Ref. [19], for instance, proposes an IoT taxonomy which takes into account protocols, architecture, energy efficiency, scalability, security, social networking, and interoperability, while [44] proposes taxonomies with respect to communication technologies, operating systems, gateway operating modes, architecture, middleware, platforms, storage techniques, capability and performance, entity and service life cycle, and applications. Another interesting IoT taxonomy is adopted in [41], comprising IoT devices, operating systems, communication interfaces and networks, middleware, platforms, and applications. The present paper, too, has introduced an IoT taxonomy consisting of the 18 topics listed in Table 2.

7. Conclusions

The aim of the paper was to introduce the reader to the IoT ecosystem by providing him with a broad-spectrum description of the many topics that can be traced back to it. The study of the state of the art made it possible to identify 3 distinct dimensions for a total number of 18 topics. For each topic, the link is provided to 119 very recent reviews (from 2019 to April 2022) where technical details are given, details that developers will not find in this manuscript given its introductory nature.

Author Contributions: Conceptualization , P.D.F. and G.P.; methodology, P.D.F.; data curation, R.P., F.P. and D.I.; writing—original draft preparation, F.P.; visualization, M.M.; supervision, G.P.; funding acquisition, G.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Gruppo Software Industriale, Italy.

Data Availability Statement: Not applicable

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

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
IIoT	Industry Internet of Things
IoT CM	IoT Conceptual Model
IoT RM	IoT Reference Model (RM)
PED	Physical Entity Domain
OMD	Operation and Management Domain
ASD	Application and Service Domain
RAID	Resource Access and Interchange Domain
UD	User Domain
CC	Cloud Computing
FC	Fog Computing
EC	Edge Computing
MEC	Mobile Edge Computing
SCD	Sensing and Controlling Interface
UML	Unified Modeling Language
MDE	Model-Driven Engineering
API	Application Programming Interface
PII	Personally Identifiable Information
SSI	Self-Sovereign Identity

Appendix A. Recent Review Papers about IoT Functional Blocks

This appendix is composed of six parts as per the number of topics belonging to the functional blocks dimension (Table 2). Each part collects "metadata" about reviews (published between 2019 and April 2022 and indexed in the Scopus database) which deal with the corresponding topic. The metadata describing each survey consists of four items: (a) the reference number (within this paper); (b) the keywords listed in the source file; (c) the summary of the major contributions of the study; and (d) other topics taken into account in the study (if any). The notation "0X-0Y" denotes topic 0Y belonging to dimension 0X.

Reviews about Identification

Ali, O.; Ishak, M.K.; Bhatti, M.K.L.; Khan, I.; Kim,K.I. A Comprehensive Review of Internet of Things: Technology Stack, Middlewares, and Fog/Edge Computing Interface. *Sensors*, **2022**, *22*, 995.
Keywords Internet of Things, edge computing, fog computing, stack optimization, middleware, pervasive computing, ubiquitous computing
Contribution A state-of-the-art research and open challenges of the enabling technologies and standards that build up the IoT technology stack. The study also focuses on the role of middleware platforms in IoT application development and integration. The interfacing of fog/edge networks to IoT technology stack is investigated.
(*) 01-02, 01-03, 01-04, 01-05, 01-06

Kassab, W.; Darabkh, K.A. A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, **2020**, *163*, 102663.
Keywords IoT architectures, IoT protocols, IoT applications, IoT middleware, IoT simulators, IoT challenges, Future directions, Recommendations
Contribution A discussion of the recent worldwide implementation of IoT (enabling technologies, communication protocols, and application areas). IoT stack's protocols are discussed. Middleware's definition, usages, and open research challenges are illustrated. The survey also details the simulation tools of IoT networks, IoT sensors along with application areas.
(*) 01-02, 01-03, 01-04, 01-05, 02-03, 02-04, 02-05, 03-01

Reviews about Sensing

Thakor, V.A.; Razzaque, M.A.; Khandaker,M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*, **2021**, *9*, DOI 10.1109/ACCESS.2021.3052867.
Keywords IoT, lightweight, cryptography, sensors, RFID, smart cards.
Contribution The paper compares the existing lightweight cryptography algorithms proposed to secure the communication between resource-constrained IoT devices (such as RFID tags, sensors, smart cards, etc.). The comparison is made in terms of implementation cost, hardware and software performances and attack resistance properties.
(*) 02-03

Laghari, A.A; Wu, K.; Laghari, R.A.; Ali, M.; Khan, A.A. A Review and State of Art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, **2022**, *29*, 1395–1413.
Keywords Internet of Things, fog computing, cloud computing, 6G
Contribution The paper describes the utilization of IoT in the cloud, fog, IoT technologies with applications and security. An IoT architecture for design and development with sensors in 6G is provided.
(*) 01-04, 03-01

Stavropoulos, T. G.; Papastergiou, A.; Mpaltadoros, L.; Nikolopoulos, S.; Kompatsiaris, I. IoT Wearable Sensors and Devices in Elderly Care: A Literature Review. *Sensors*, **2020**, *20*, 2826, doi:10.3390/s20102826.
Keywords IoT; wearables; sensors; devices; elders; old age; ambient assisted living (AAL); Alzheimer's; dementia
Contribution A review of IoT wearables and devices in elderly care. The study examines and categorizes the pertinent literature according to three dimensions: health focus, IoT technologies, and experimental evaluation participants' duration and outcome measures, from acceptability to accuracy.
(*) 03-01

Reviews about Networking

Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information*, **2021**, *12*, 87, https://doi.org/10.3390/info12020087.
Keywords Internet of Things; machine to machine; smart vehicle; e-health; smart building; smart home; smart city; smart agriculture; Industry 4.0
Contribution A survey on current architectures, technologies, protocols, and applications that characterize the IoT paradigm.
(*) 01-02

C.C. Sobin A Survey on Architecture, Protocols and Challenges in IoT. *Wireless Personal Communications*, **2020**, *112*, 1383–1429 https://doi.org/10.1007/s11277-020-07108-5.
Keywords Internet of Things, Architecture, Protocols, Challenges, Security
Contribution A survey of architectures and protocols for IoT systems. The paper proposes taxonomies for classification. Technical challenges (such as security and privacy, interoperability, scalability, and energy efficiency) are discussed.
(*) 02-01, 02-02, 02-03, 02-04

Raj, A.; Shetty, S.D. IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey. *Wireless Personal Communications*, **2022**, *122*, 1481–1517.

Keywords IoT architecture, Cloud computing, Machine learning, Blockchain, Edge computing, IoT security
Contribution A review of the architectures, technologies and protocols used in IoT eco-systems to deliver secure services. Moreover, the study discusses possible layer-wise attacks and new technologies (such as edge, fog, cloud, artificial intelligence, machine learning and blockchain) to be integrated into existing IoT architecture.
(*) 01-04, 02-01

Bansal, S.; Kumar, D. IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication *International Journal of Wireless Information Networks*, **2020**, *27*, 340–364.
Keywords IoT devices, OS, Middleware, Communication, Gateways, Security
Contribution The paper provides a technical overview of IoT-enabling architectures, devices, gateways, operating systems, middleware, platforms, data storage, security, communication protocols and interfaces. It also describes a relation between IoT and big data, cloud and fog computing.
(*) 01-04, 02-01, 03-01

Balaji, S.; Nathani, K.; Santhakumar, R. IoT Technology, Applications and Challenges: A Contemporary Survey. *Wireless Personal Communications*, **2019**, *108*, 363–388.
Keywords IoT, Agriculture, Industry, Life saver, Protocols, Security, Smart cities
Contribution An overview of the IoT technology and its applications in domains such as industry, smart cities, agriculture, lifesaving, etc. Existing protocols and security issues are discussed.
(*) 02-01, 03-01

Khanna, A.; Kaur, S. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. *Wireless Personal Communications*, **2020**, *114*, 1687–1762 https://doi.org/10.1007/s11277-020-07446-4.
Keywords Internet of Things, Wireless sensor networks, Radio-frequency identification, Near-field communication, Internet of Energy, Global Positioning System, Representational State Transfer, Information and Communication Technology, Service Oriented Architecture
Contribution A literature review of various aspects of IoT. Communication techniques used in IoT discussed by length. Moreover, contributions in different areas of applications are evaluated based on parameters specific to each application domain.
(*) 01-05, 03-01

Reviews about Computation

Demigha, O.; Larguet, R. Hardware-based solutions for trusted cloud computing. *Computers & Security*, **2021**, *103*, 102117.
Keywords Trusted cloud computing, Hardware-assisted security, Trusted execution environment, Intel TXT, AMD SEV, ARM TrustZone, Intel SGX.
Contribution The paper gives to cloud users and customers, application developers and security managers a comprehensive overview (analysis and comparison) of four major industrial-scale commercial hardware-based solutions (Intel TXT, ARM TrustZone, AMD SEV, and Intel SGX). The comparison is made with respect to more than twenty criteria fitting within three categories (security, functional and deployment).
(*) 02-01

Sun, P.J. Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, **2020**, *160*, 102642.
Keywords Cloud computing, Privacy security, Access control, Attribute-based encryption, Trust
Contribution The paper reviews the research progress on privacy security issues from the perspective of several privacy security protection technologies (such as access control, attribute-based encryption, trust, and search encryption) in cloud computing. It discusses privacy security risks and proposes a privacy security protection framework.
(*) 01-01, 02-01, 02-02

Jin, X.; Li, L.; Dang, F.; Chen, X.; Liu, Y. A survey on edge computing for wearable technology. *Digital Signal Processing*, **2022**, *125*, 103146, https://doi.org/10.1016/j.dsp.2021.103146.
Keywords Wearable technology, Edge computing, Computation scheduling, Energy-saving
Contribution The article investigates the drawbacks of wearable devices and explores the potential of addressing them by edge computing. A comprehensive survey on existing works from four aspects (computation scheduling, information perception, energy-saving, and security) is presented.
(*) 02-01

Zhang, T.; Li, Y.; Chen, C.L.P. Edge computing and its role in Industrial Internet: Methodologies, applications, and future directions. *Information Sciences*, **2021**, *557*, 34–65.
Keywords Edge computing, Industrial Internet, Shallow network, Broad learning system
Contribution The survey shows application scenarios in the industrial Internet that are suitable for deploying the edge computing paradigm, followed by methodologies to improve the performance of edge computing. The authors propose their concept regarding future applications of shallow network methods (broad learning systems, in particular) in edge computing. Open issues of edge computing are pointed out.
(*) 03-01

Hamdan, S.; Ayyash, M.; Almajali, S. Edge-computing architectures for Internet of things applications: A survey. *Sensors*, **2020**, *20*, 6441, doi:10.3390/s20226441, https://www.mdpi.com/1424-8220/20/22/6441.
Keywords Internet of Things; cloud computing; edge computing
Contribution The survey classifies Edge–IoT networks from four perspectives: orchestration, security, data placement, and big data.
(*) 01-03, 01-04 03-01

Rosendo, D.; Costan, A.; Valduriez, P.; Antoniu, G. Distributed Intelligence on the Edge-to-Cloud Continuum: A Systematic Literature Review. *Journal of Parallel and Distributed Computing*, **2022**, *166*, 71–94, https://doi.org/10.1016/j.jpdc.2022.04.004.
Keywords Edge computing, Distributed Intelligence, Big Data Analytics, Computing Continuum, Reproducibility
Contribution A review about state-of-the-art libraries and frameworks for machine learning and data analytics. It also describes the main learning paradigms enabling learning-based analytics on the edge-to-cloud continuum. The main

simulation, emulation, deployment systems, and testbeds for experimental research on the edge-to-cloud continuum available today are surveyed.
(*) 01-06

Yousefpour, A; Fung, C.; Nguyen, T.; Kadiyala, K.; Jalali, F.; Niakanlahiji, A.; Kong, J.; Jue, J.P. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture*, **2019**, *98*, 289–330.
Keywords Fog computing, Edge computing, Cloud computing, Internet of things, Cloudlet, Mobile edge computing, Multi-access edge computing, Mist computing
Contribution The paper provides a tutorial on fog computing and its related computing paradigms. In addition, a taxonomy of research topics in fog computing is given. The authors compile a list of challenges and future directions for research in fog computing.
(*)

Laroui, M.; Nour, B.; Moungla, H.; Cherif, M.A.; Afifi, H.; Guizani, M. Edge and fog computing for IoT: A survey on current research activities & future directions. *Computer Communications*, **2021**, *180*, 210–231.
Keywords Internet of Things, Edge computing, Cloud computing
Contribution A review about the role of cloud, fog, and edge computing in the IoT environment. The following arguments are touched upon: different IoT use cases with edge and fog computing; task scheduling in edge computing; the merger of software-defined networks and network function virtualization with edge computing; security and privacy efforts; the blockchain in edge computing.
(*) 01-01, 02-01, 02-02

Shakarami, A.; Shakarami, H.; Ghobaei-Arani, M.; Nikougoftar, E.; Faraji-Mehmandar, M. Resource provisioning in edge/fog computing: A Comprehensive and Systematic Review. *Journal of Systems Architecture*, **2022**, *122*, 102362, https://doi.org/10.1016/j.sysarc.2021.102362.
Keywords Mobile edge computing, Fog computing, machine learning, Game theory, Resource provisioning, Elasticity
Contribution A review of resource provisioning approaches in computation paradigms. A classification is proposed organized into five fields: framework-based, heuristic/meta-heuristic-based, model-based, machine learning-based, and game theoretic-based mechanisms. Such classes are compared based on performance metrics, and open issues are also discussed.
(*)

Omoniwa, B.; Hussain, R.; Javed, M.A.; Bouk, S.H.; Malik, S.A. Fog/Edge Computing-Based IoT (FECIoT): Architecture, Applications, and Research Issues. *IEEE Internet of Things Journal*, **2019**, *6*, 3.
Keywords Cyber-physical systems, enabling technologies, Fog/Edge Computing (FEC), Internet-of-Things (IoT), Service-Oriented Architecture
Contribution A survey on the IoT literature (from 2008 to 2018) on FEC-based IoTs (FECIoT). A tutorial approach is adopted that progresses from basic to advanced concepts. It is shown how FECIoT can be deployed in IoT systems, such as in smart health-care, smart homes, smart environment, smart transportation, and smart grids.
(*) 01-05, 02-01, 02-02

Nikravan, M.; Kashani, M.H. A review on trust management in fog/edge computing: Techniques, trends, and challenges. *Journal of Network and Computer Applications*, **2022**, *204*, 103402, https://doi.org/10.1016/j.jnca.2022.103402.
Keywords Fog/Edge Computing (FEC), Trust management, Privacy, Internet of things, Attack Security
Contribution A systematic review of 74 high-quality articles related to FEC trust management published from 2015 to 2021. Selected FEC trust management approaches are grouped into three categories: algorithm, architecture, and model/framework. Additionally, the study discusses and compares the FEC trust management approaches based on merits and demerits, evaluation techniques, tools and simulation environments, and important trust metrics. Open issues are pointed out.
(*) 02-01, 02-02, 02-03, 02-05, 02-06

Firouzi, F.; Farahani, B.; Marinšek, A. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *Information Systems*, **2022**, *107*, 101840, https://doi.org/10.1016/j.is.2021.101840.
Keywords Internet of Things, Cloud Computing, Fog Computing, Edge Computing, Mobile Computing, Edge-Fog-Cloud, Cloud IoT, Cloudlet, Offloading, Resource Management, Service Placement, Privacy-Preserving Machine Learning, Security and Privacy, Healthcare IoT, Case Studies
Contribution A tutorial about the main requirements, state-of-the-art reference architectures, building blocks, components, protocols, and major applications in the domain of edge–fog–cloud computing paradigms. A holistic reference architecture for edge–fog–cloud IoT is presented, and the major corresponding design and deployment considerations are discussed. The role of privacy-preserving, distributed, and collaborative analytics is discussed, as well as the interaction between edge, fog, and cloud computing.
(*) 01-06, 02-01, 02-02, 03-01

Aslanpour, M.S.; Gill, S.S.; Toosi, A.N. Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. *Internet of Things*, **2020**, *12*, 100273.
Keywords Cloud computing, Performance evaluation, Internet of things, Cloud Metrics, Fog Computing and Edge Computing
Contribution A benchmark study that presents a taxonomy of the various real-world metrics proposed to evaluate the performance of cloud, fog, and edge computing in specific application domains.
(*)

Islam, M.S.; Kumar, A.; Hu, Y.-C. Context-aware scheduling in Fog computing: A survey, taxonomy, challenges and future directions. *Journal of Network and Computer Applications*, **2021**, *180*, 103008.
Keywords Fog computing, Context-awareness, Scheduling, Resource management, Resource estimation, Resource provisioning, Contextual information
Contribution A literature analysis on context-aware scheduling in fog computing. It provides a comparison of existing scheduling approaches based on factors such as context-aware parameters, case studies, performance metrics, and evaluation tools. It also presents taxonomy, performance metrics, and context-aware parameter analysis.
(*) 01-05, 02-04, 02-06

Moura, J.; Hutchison, D. Fog computing systems: State of the art, research issues and future trends, with a focus on resilience. *Journal of Network and Computer Applications*, **2020**, *169*, 102784.
Keywords Fog computing, Internet of things, Edge computing, Cyber-physical systems, Software defined networks, Game theory, Network function virtualization, Cyber-attacks, Resilient systems, Self-awareness, Network slicing
Contribution A survey of the state of the art in the relevant fields pertaining to fog computing systems, the emerging research issues, and future trends. The authors envisage future applications with very stringent requirements (high-precision latency and synchronization between a large set of flows). Moreover, the authors propose to use game theory and the latest software/virtualization platforms to model and program fog computing systems.
(*) 01-03, 02-04, 02-05

Singh, J.; Singh, P.; Gill, S.S. Fog computing: A taxonomy, systematic review, current trends and research challenges. *Journal of Parallel and Distributed Computing*, **2021**, *157*, 56–85.
Keywords Fog computing, Frameworks, Edge computing, Applications, Internet of things
Contribution A systematic literature review of fog computing aiming at classifying recently published studies in the area. Characteristics of fog computing frameworks are discussed, as well as various issues related to architectural design, QoS metrics, implementation details, applications and communication modes. The existing fog computing research is classified into four categories: development, metrics, platforms and frameworks.
(*)

Sadri, A.A; Rahmani, A.M.; Saberikamarposhti, M.; Hosseinzadeh, M. Fog data management: A vision, challenges, and future directions. *Journal of Network and Computer Applications*, **2021**, *174*, 102882.
Keywords Fog computing, Internet of things, Data management, Data processing, Data analytics, Data storage, Data security, Systematic literature review
Contribution A systematic literature review that surveys fog data management and understands the various topics and main contexts in the domain. The paper classifies and analyzes the research on the fog data management domain (years 2014–2019). A context-based taxonomy is offered, and metrics of fog data management reference model are used to compare the grouped papers.
(*) 01-05, 01-06, 02-01

Rezapour, R.; Asghari, P.; Javadi, H.H.S.; Ghanbari, S. Security in fog computing: A systematic review on issues, challenges and solutions. *Computer Science Review*, **2021**, *41*, 100421.
Keywords Fog computing, Cloud computing, Security in fog computing
Contribution The study classifies the research related to security aspects and available solutions in fog computing (years 2014-2021). A technical taxonomy is offered for the fog security challenges and their strategies in terms of six aspects (reliability, access control, attacks, secure connection, privacy, and some special cases). Technical questions in the fog computing domain are provided; the strengths and weaknesses of each indicated fog security approach are discussed based on the questions.
(*) 01-01, 02-01, 02-06

Alli, A.A.; Alam, M.M. The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. *Internet of Things*, **2020**, *9*, 100177.
Keywords Big data analytics, Computational offloading, Content delivery network, Fogging Internet of things, IoT–Fog–Cloud ecosystems, Simulation tools, Smart city applications, Smart farm applications, Web performance
Contribution A survey on fog computing architectures, standards, tools and applications that aims at defining a foundation to solutions that involve IoT–Fog–Cloud ecosystems.
(*)

Puliafito, C.; Mingozzi, E.; Longo, F.; Puliafito, A.; Rana, O. Fog Computing for the Internet of Things: A Survey. *ACM Transactions on Internet Technology*, **2019**, *19*, 2, https://doi.org/10.1145/3301443.
Keywords Fog computing (FC), internet of things, topological proximity, cloud computing
Contribution A survey on the literature characterizing the adoption of FC to support IoT devices and services. Six IoT application domains that may benefit from the use of this paradigm are discussed. An overview of existing FC software and hardware platforms for the IoT is also given, along with the standardisation work in this area started by the OpenFog Consortium.
(*) 03-01

Zhang, J.; Mab, M.; Wang, P.; Sun, X.-D. Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions. *Journal of Systems Architecture*, **2021**, *117*, 102098.
Keywords Internet of Things, Middleware, Context-aware computing, Knowledge discovery, Self-adaptation
Contribution The survey discusses IoT middleware requirements and challenges and presents the current state of research in the domain. A technical taxonomy is presented for the IoT middleware according to the abstract and processing approach of data. Three enabling techniques to analytically present the current research trends on IoT middleware are discussed.
(*) 01-05, 02-03, 02-04, 03-01

Reviews about Services

Yousefi, S.; Karimipour, H.; Derakhshan, F. Data Aggregation Mechanisms on the Internet of Things: A Systematic Literature Review. *Internet of Things*, **2021**, *15*, 100427.
Keywords Centralized, Cluster-based aggregation, Data aggregation, Internet of Things, Mobile Agent, Tree-based aggregation
Contribution A systematic literature review about data aggregation mechanisms on IoT. Data aggregation mechanisms are divided into two main categories: client-server-based and mobile agent-based.
(*) 03-01

Achir, M.; Abdelli, A.; Mokdad, L.; Benothman, J. Service discovery and selection in IoT: A survey and a taxonomy. *Journal of Network and Computer Applications*, **2022**, *200*, 103331.
Keywords Taxonomy, Service discovery, Service selection, IoT, QoS, Quality of Experience, Classification, Architecture, Object discovery
Contribution The paper proposes a taxonomy to classify service discovery approaches in the IoT context. The approaches are evaluated according to different aspects and criteria. Gaps and advantages of each class of the taxonomy are discussed.

(*) 01-03, 01-04, 03-03

Yu, J.; Wang, M.; Liu, J.; Abnosian, K. Service management mechanisms in the internet of things: an organized and thorough study. *Journal of Ambient Intelligence and Humanized Computing*, **2022**, *13*, 75–86.
Keywords Service management, Internet of Things, Systematic literature review
Contribution The paper investigates the modern mechanisms in the IoT service management domain, categorizes them into two groups, and studies their main features. Some visions for the practitioners and scholars are presented to propose useful management mechanisms based on the features of service settings.
(*)

Dorsala, M.R.; Sastry, V.N.; Chapram, S. Blockchain-based solutions for cloud computing: A survey. *Journal of Network and Computer Applications*, **2021**, *196*, 103246.
Keywords Blockchain, Cloud computing, Cloud storage, Resource allocation, Verifiable computation, Crowdsensing
Contribution The paper surveys blockchain-based cloud services literature (years 2008–2021). The studies are classified into three categories: blockchain-based infrastructure-as-a-service; blockchain-based platform-as-a-service; and blockchain-based software-as-a-service. State-of-the-art works in blockchain-based storage-as-a-service, resource management, computation-as-a-service, data aggregation-as-a-service, microservice-as-a-service and virtual-network-functions-as-a-service are also presented.
(*) 01-05

Alberti, A.M.; Santos, M.A.S.; Souza, R.; Da Silva, H.D.L., Carneiro, J.R.; Figueiredo, V.A.C.; Rodrigues, J.J.P.C. Platforms for Smart Environments and Future Internet Design: A Survey. *IEEE Access*, **2019**, *7*, 165748–165778.
Keywords Internet of Things, middleware, platform virtualization, wireless sensor networks, clouds, information-centric networking
Contribution A review of platforms, middleware, and frameworks for building smart environments.
(*) 01-02, 01-03, 01-04, 01-06, 02-01, 02-02

Reviews about Analytics

Dutta, L.; Bharali, S. TinyML Meets IoT: A Comprehensive Survey. *Internet of Things*, **2021**, *16*, 100461.
Keywords Internet of Things, Tiny Machine Learning (TinyML), hardware-software co-design
Contribution The paper presents the key performance indicators of the TinyML framework along with its definition and overview, as well as a review of related technologies. It establishes a link between traditional ML and TinyML. The study reviews TinyML research undertaken by academia and industry research groups. It also indicates the role of 5G in TinyML research.
(*) 01-05, 02-05, 02-06

Deepa, N.; Pham, Q.V.; Nguyen, D.C.; Bhattacharya, S.; Prabadevi, B.; Gadekallu, T.R.; Maddikunta, P.K.R.; Fang, F.; Pathirana, P.N. A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Generation Computer Systems*, **2022**, *131*, 209–226.
Keywords Blockchain, Big data, Vertical applications, Smart city, Smart healthcare, Smart transportation, Security
Contribution The paper surveys blockchain services for big data. The state-of-the-art studies on the use of blockchain for big data applications in different domains (such as smart cities, smart healthcare, smart transportation, and smart grids) are reviewed. Representative blockchain-big data projects are also presented and analyzed.
(*) 01-05, 02-01, 03-01

Appendix B. Recent Review Papers about IoT Qualities

This appendix is composed of six parts as per the number of topics belonging to the qualities dimension (Table 2). Each part collects "metadata" about reviews (published between 2019 and April 2022 and indexed in the Scopus database) that deal with the corresponding topic. The metadata describing each survey consists of four items, as explained in Appendix A.

Reviews about Security

Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*, **2022**, *22*, 1094.
Keywords Blockchain, Distributed Denial of Service (DDoS) attacks, Internet of Things, Mitigation of DDoS attacks
Contribution A survey of blockchain-based solutions to mitigate DDoS attacks in IoT. The solutions are classified into four categories (distributed architecture-based solutions, access management-based solutions, traffic control-based solutions and the Ethereum platform-based solutions) and are critically analyzed.
(*) 01-05

Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in IoT: challenges and solutions. *Blockchain: Research and Applications*, **2021**, *2*, 100006.
Keywords Blockchain technology, Consensus mechanism, Blockchain cryptographic primitives, healthcare, Patient monitoring, Cloud of Things, Internet of Things, Fog of Things, Software defined network, Blockchain applications
Contribution The paper analyzes state of the art in blockchain for IoT, blockchain for Cloud IoT and blockchain for Fog IoT in various domains (such as eHealth, smart cities, and intelligent transportation). Obstacles, research gaps and potential solutions are discussed.
(*) 01-05, 02-04, 03-01

Kaur, M.; Khan, M.Z.; Gupta, S.; Alsaeedi, A. Adoption of Blockchain With 5G Networks for Industrial IoT: Recent Advances, Challenges, and Potential Solutions. *IEEE Access*, **2021**, *10*, 981–997, 10.1109/ACCESS.2021.3138754.
Keywords Blockchain, Industrial IoT (IIoT), Industry 4.0, IoT, 5G
Contribution The article examines recent achievements to highlight the major obstacles in blockchain-IIoT convergence and presents a framework for potential solutions. The literature review focuses on three primary areas: blockchain consensus algorithms in existing IoT and IIoT applications, blockchain for 5G-enabled IoT networks, and blockchain in industry.

(*) 03-01

Pal, S.; Dorri, A.; Jurdak, R. Blockchain for IoT access control: Recent trends and future research directions. *Journal of Network and Computer Applications*, **2022**, *203*, 103371, https://doi.org/10.1016/j.jnca.2022.103371.
Keywords Internet of things, blockchain, access control, identity, security
Contribution The paper reviews recent studies on blockchain-based solutions for IoT access control. Several aspects of blockchain (such as decentralised control, secure storage and sharing information in a trustless manner) are identified.
(*)

Chen, F.; Xiao, Z.; Cui, L.; Lin, Q.; Li, J.; Yu, S. Blockchain for Internet of things applications: A review and open issues. *Journal of Network and Computer Applications*, **2020**, *172*, 102839.
Keywords Blockchain, IoT, Access control, Data security, Trusted third party, Automatic payment, Usage paradigm
Contribution The paper reviews, summarizes and categorizes the most recent research advances on building IoT systems using blockchain. The research works are divided in four groups according to the blockchain role in IoT systems: an access control platform, a data security platform, a trusted third party, and an automatic payment platform.
(*) 01-05

Gadekallu, T.R.; Pham, Q.-V.; Nguyen, D.C.; Maddikunta, P.K.R.; Deepa, N.; Prabadevi, B.; Pathirana, P.N.; Zhao, J.; Hwang, W.-J. Blockchain for Edge of Things: Applications, Opportunities, and Challenges. *IEEE Internet of Things Journal*, **2022**, *9*, 964–988.
Keywords Blockchain, edge computing, Edge of Things, industrial applications, Internet of Things, security
Contribution A state-of-the-art review of recent developments in the Blockchain Edge of Things (BEoT) technology. The use of BEoT in a wide range of industrial applications is discussed, as well as security challenges in the BEoT paradigm.
(*) 03-01

Tran, N.K.; Babar, M.A.; Boan, J. Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. Journal of Network and Computer Applications, **2021**, *173*, 102844.
Keywords Blockchain, Distributed ledger, Smart contract, Web of things, Internet of Things, Systematic review
Contribution A systematic literature review of blockchain-IoT systems. The authors propose and apply a multi-perspective framework to analyse the existing systems. Ten archetypes of blockchain-IoT systems are also defined.
(*) 01-05

Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors*, **2022**, *22*, 927.
Keywords Computing, survey, security, privacy, distributed systems, computational offloading
Contribution The review identifies similarities, differences, main attacks, and countermeasures in the cloud, edge, and fog computing paradigms. Security and privacy threats are pointed out.
(*) 02-02

Lone, A.H.; Naaz, R. Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review. *Computer Science Review*, **2021**, *39*, 100360.
Keywords Blockchain, Smart contract, Security, Internet, IoT
Contribution This paper identifies and analyses the literature regarding the use of blockchain smart contracts for securing the Internet and Internet of Things in particular.
(*)

Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, **2021**, *181*, 103050.
Keywords Internet of things, Blockchain, Security, Privacy, Smart contract
Contribution An in-depth survey of the state-of-the-art in blockchain technology. The background, characteristics, classification, architecture and consensus mechanisms are discussed. The paper investigates, moreover, the integration trends of blockchain technology with IoT, as well as the security improvements achieved in IoT systems using blockchain and the related challenges. Relevant blockchain-based IoT applications are also mentioned.
(*)

Hussain, S.; Ullah, S.S.; Ali, I.; Xie, J.; Inukollu, V.N. Certificateless signature schemes in Industrial Internet of Things: A comparative survey. *Computer Communications*, **2022**, *181*, 116–131.
Keywords Industrial Internet of Things, Signature, Certificateless signature, Wireless networks
Contribution A comparative analysis of the available solutions to improve security in the Industrial Internet of Things (IIoT). The survey classifies and compares the different certificateless signature schemes of IIoT domain.
(*)

Corallo, A.; Lazoi, M.; Lezzi, M.; Luperto, A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, **2022**, *137*, 103614.
Keywords Cybersecurity awareness, Information security awareness, Industrial Internet of Things (IIoT), Industry 4.0, Cybersecurity awareness techniques
Contribution State of the art of cybersecurity awareness in the context of IIoT. The major areas of analysis are: (a) definitions of the concepts of cybersecurity awareness; (b) the techniques adopted to raise company awareness of cybersecurity; and (c) the benefits of a large-scale campaign of cybersecurity awareness. The survey analyzes the cybersecurity awareness systems, the cybersecurity awareness methods and methodologies, the cybersecurity awareness methodological frameworks, and the cybersecurity awareness models.
(*)

Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B. Landscape of IoT security. *Computer Science Review*, **2022**, *44*, 100467.
Keywords IoT, Security, Taxonomy, Attack vectors, Countermeasures, GDPR
Contribution A survey on IoT security. The study provides a list of key challenges, major security objectives, a threat taxonomy, and key countermeasures.
(*) 01-01, 01-03

Sicari, S.; Rizzardi, A.; Coen-Porisini, A. Security & privacy issues and challenges in NoSQL databases. *Computer Networks*, **2022**, *206*, 108828.
Keywords NoSQL databases, Internet of Things, Access control, Authentication, Authorization, Security, Privacy
Contribution The paper analyzes the current state of the art of security and privacy solutions tailored to NoSQL databases (i.e., Redis, Cassandra, MongoDB, and Neo4j stores).
(*) 01-05, 02-02

Chanal, P.M.; Kakkasageri, M.S. Security and Privacy in IoT: A Survey. *Wireless Personal Communications*, **2020**, *115*, 1667–1693.
Keywords Internet of things, Security, Privacy
Contribution The paper surveys several challenges for IoT (e.g., confidentiality, integrity, authentication, and availability). It also reviews IoT architecture and applications and discusses security and privacy issues.
(*) 02-02, 03-01

Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*, **2020**, *11*, 100227.
Keywords IoT, Security, Machine learning, Artificial intelligence, Blockchain technology
Contribution A survey of the IoT technology and the area of its application. Confidentially, integrity, and availability are identified as primary security issues. Machine learning, artificial intelligence, and blockchain are studied for addressing the security issue in IoT.
(*) 01-06

Karale, A. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. *Internet of Things*, **2021**, *15*, 100420.
Keywords Internet of Things, IoT Challenges, Ethical Issues, IoT Laws, Privacy Threats, Security Attacks
Contribution The paper provides an overview of the security, ethical, and privacy challenges faced by common IoT users and examines the current and emerging IoT laws and standards enacted by governments to combat the vulnerabilities of IoT. Trust and the potential challenges of smart contracts are also discussed.
(*) 02-02

Omolara, A.E.; Alabdulatif, A.; Abiodun, O.I.; Alawida, M.; Alabdulatif, A.; Alshoura, W.H.; Arshad, H. The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, **2022**, *112*, 102494.
Keywords Security and privacy challenges and solutions of the internet of things, Gaps in IoT research, Forensic in the IoT era, COVID-19 pandemic and IoTs, Future development
Contribution A systematic literature review of over 200 articles providing insights into the security of IoT and its social, economic, technical and legal implications.
(*)

Rao, P.M.; Deebak, B.D. Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, **2022**, https://doi.org/10.1007/s12652-022-03707-1.
Keywords Security, Privacy, Internet of things, Authentication, Key management, Smart cities
Contribution Numerous security threats, techniques, countermeasures, and tools are reviewed to address the key challenges of smart service intelligence within sustainable environments. The survey puts special emphasis on smart cities/industries.
(*) 01-01

Rahman, M.S.; Islam, M.A.; Uddin, M.A.; Stea, G. A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges. *Internet of Things*, **2022**, *19*, 100551, https://doi.org/10.1016/j.iot.2022.100551.
Keywords Blockchain (BC), IoT, Healthcare, Electronic health records challenge, Medical area
Contribution A survey of the state-of-the-art on BC works in healthcare. The study summarizes applications, research issues, security threats, and research challenges in the IoT-enabled healthcare system when BC is adopted for handling the privacy and storage of medical records.
(*) 02-02, 03-01

Alzoubi, Y.I.; Al-Ahmad, A.; Kahtan, H. Blockchain technology as a Fog computing security and privacy solution: An overview. *Computer Communications*, **2022**, *182*, 129–152, https://doi.org/10.1016/j.comcom.2021.11.005.
Keywords Fog computing, Cloud computing, Challenge, Security, Privacy
Contribution The survey discusses the state-of-the-art impact of the blockchain on the security and privacy of fog computing. Open challenges and future research directions are discussed.
(*) 02-02

Reviews about Privacy

Li, T.; He, X.; Jiang, S.; Liu, J. A survey of privacy-preserving offloading methods in mobile-edge computing. *Journal of Network and Computer Applications*, **2022**, *203*, 103395, https://doi.org/10.1016/j.jnca.2022.103395.
Keywords Mobile-edge computing, offloading, privacy
Contribution A review of the state-of-the-art on privacy-preserving offloading in mobile-edge computing. Privacy issues as well as related metrics and application scenarios are discussed.
(*) 01-04, 01-05, 03-01

Strous, L.; Solms, S.; Zúquete, A. Security and privacy of the Internet of Things. *Computers & security*, **2021**, *102*, 102148, https://doi.org/10.1016/j.cose.2020.102148.
Keywords IoT, security, privacy
Contribution The study mentions the roles and responsibilities of various groups of stakeholders regarding security and privacy.
(*)

Reviews about Interoperability

Alkhabbas, F.; Spalazzese, R.; Davidsson, P. Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. *Internet of Things*, **2019**, *7*, 100084.

Keywords Internet of Things, Characterization of IoT systems, Systematic Mapping Study, Taxonomies
Contribution A systematic review of existing IoT system taxonomies. A characterization of IoT systems is proposed in terms of seventeen characteristics divided into two groups: elements and quality aspects.
(*) 02-01, 02-02, 02-04, 02-05, 02-06

Reviews about Scalability

Reviews about Latency

Mwase, C.; Jin, Y.; Westerlund, T. Tenhunen, H.; Zou, Z. Communication-efficient distributed AI strategies for the IoT edge. *Future Generation Computer Systems*, **2022**, *131*, 292–308, https://doi.org/10.1016/j.future.2022.01.013.
Keywords Artificial Intelligence (AI), Machine Learning (ML) Distributed AI/ML, Communication efficient AI/ML, Fog/edge computing, Edge ML, Industry IoT (IIoT)
Contribution The study focuses on distributed ML approaches for industry-IoT applications, which face more stringent energy, latency and privacy requirements than cloud-based solutions. Then, it describes an architecture for fully edge-based solutions for IIoT. The survey characterises the cloud-to-thing continuum.
(*) 01-04, 03-01

Reviews about Reliability

Appendix C. Recent Review Papers about IoT Other Topics

This appendix is composed of six parts as per the number of topics belonging to the Other Topics dimension (Table 2). Each part collects "metadata" about reviews (published between 2019 and April 2022 and indexed in the Scopus database) which deal with the corresponding topic. The metadata describing each survey consists of four items, as explained in Appendix A.

Reviews about Application Domains

Ketu, S.; Mishra, P.K. A Contemporary Survey on IoT Based Smart Cities: Architecture, Applications, and Open Issues. *Wireless Personal Communications*, **2022**, https://doi.org/10.1007/s11277-022-09658-2.
Keywords Internet of things, Smart city, Smart devices, Smarter world, IoT-based, smart application
Contribution A survey of IoT-based smart cities (potential, current trends and developments, architecture, application area, real-world involvement, and open challenges). Key elements of various IoT-based application areas are also discussed.
(*)

Sharif, R.A.; Pokharel, S. Smart City Dimensions and Associated Risks: Review of literature. *Sustainable Cities and Society*, **2022**, *77*, 103542.
Keywords Smart cities, Smart city dimensions, Technical risks, Non-technical risks, Risk parameters, Risk assessment tools
Contribution The review investigates smart city risk assessment tools and techniques and the latest technological advancement and innovations in relation to risk assessment and management related to smart city implementation. Internet of Things, artificial intelligence, and blockchain are identified as dominant technologies.
(*)

Fahmideh, M.; Zowghi, D. An exploration of IoT platform development. *Information Systems*, **2020**, *87*, 101409.
Keywords IoT platform, Smart city, Development process lifecycle, Evaluation framework
Contribution An analysis (carried out using an evaluation framework proposed by the authors) of 63 approaches for IoT platform development and maintenance according to the information system development process lifecycle.
(*)

Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, **2020**, *61*, 102360.
Keywords Smart cities, Blockchain, Security, Privacy, Consensus protocols, Smart contract, Smart communities
Contribution State-of-the-art about the blockchain technology to solve the security issues of smart cities. Various smart communities (such as healthcare, transportation, smart grids, supply chain management, financial systems and data center networks) are surveyed.
(*) 02-01, 02-02

Ahad, M.A.; Paiva, S.; Tripathi, G.; Feroz, N. Enabling technologies and sustainable smart cities. *Sustainable Cities and Society*, **2020**, *61*, 102301.
Keywords Blockchain, IoT, Enabling technologies, WSN, Smart cities, ICT
Contribution The paper reviews and discusses the role of enabling technologies in smart cities (such as artificial intelligence, protocols, IoT, WSN, etc.). Three categories of challenges are identified (technical, socio-economic and environmental). Best practices are provided.
(*) 01-03

Javadzadeh, G.; Rahmani, A.M. Fog Computing Applications in Smart Cities: A Systematic Survey. *Wireless Networks*, **2022**, *26*, 1433–1457.
Keywords Smart cities, Fog computing, Edge computing, Fog application, Internet of Things
Contribution An overview, based on a systematic literature review, in the area of fog computing applications in smart cities. An analytical comparison of related works, the trends, and future research directions are pointed out.
(*) 01-04

Lu, M.; Fu, G.; Osman, N.B.; Konbr, U. Green energy harvesting strategies on edge-based urban computing in sustainable internet of things. *Sustainable Cities and Society*, **2021**, *75*, 103349.

Keywords Sustainable smart cities, Intelligent urban computing, Energy harvesting management, Internet of Things
Contribution A review and a taxonomy of different existing green energy harvesting strategies on the smart applications of sustainable and smart cities in edge-based intelligent urban computing. The strategies are divided into five categories: smart home management, smart cities, smart grids, smart environmental systems, and smart transportation systems. The review also classifies technical aspects of the strategies.
(*)

Almalki, F.A.; Alsamhi, S.H.; Sahal, R.; Hassan, J.; Hawbani, A.; Rajput, N.S.; Saif, A.; Morgan, J.; Breslin, J. Green IoT for Eco-Friendly and Sustainable Smart Cities: Future Directions and Opportunities. *Mobile Networks and Applications*, **2021**, https://doi.org/10.1007/s11036-021-01790-w.
Keywords Green IoT, Smart city, Sustainability, Eco-friendly, Energy efficiency, Pollution
Contribution A survey of the techniques and strategies for making cities smarter, sustainable, and eco-friendly. It focuses on IoT and its capabilities.
(*)

Khan, M.A.; Siddiqui, M.S.; Rahmani, M.K.I.; Husain, S. Investigation of Big Data Analytics for Sustainable Smart City Development: An Emerging Country. *IEEE Access*, **2022**, *10*, 16028–15036.
Keywords Decision making, sensors, big data, Internet of Things, data analysis, smart city, sustainable development, best worst method, big data analytics
Contribution The paper identifies and analyzes the barriers related to sustainable smart city development. Fourteen barriers of big data analytics are selected (using systematic literature reviews and expert input) and evaluated.
(*) 01-06

Bellini, P.; Nesi, P.; Pantaleo, G. IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. *Applied Sciences*, **2022**, *12*, 1607.
Keywords Smart cities, internet of things, big data
Contribution A review of the literature on IoT-enabled smart cities. The study classifies the most recent trends in the adoption of IoT technologies as a key driver for the efficient and sustainable development of smart cities. The main smart city approaches and frameworks are grouped in eight domains and reviewed.
(*)

Khan, A.; Aslam, S.; Aurangzeb, K.; Alhussein, M.; Javaid, N. Multiscale modeling in smart cities: A survey on applications, current trends, and challenges. *Sustainable Cities and Society*, **2022**, *78*, 103517.
Keywords Multiscale modeling, Multiscale systems, Megacities, Smart cities, Sustainable cities, Multiscale modeling applications
Contribution A review of the state-of-art on Multiscale Modelling (MM), its categories (sequential MM and concurrent MM), the need for MM in megacities and smart cities. The study also presents emerging applications of MM in smart city environments, including urban expansion modeling, atmospheric dispersion modeling, social systems modeling, disease and virus modeling, energy forecasting, and traffic control modeling.
(*)

Hasan, R.; Hasan, R. Pedestrian safety using the Internet of Things and sensors: Issues, challenges, and open problems. *Future Generation Computer Systems*, **2022**, *134*, 187–203 (https://doi.org/10.1016/j.future.2022.03.036).
Keywords Pedestrian Safety, Smartphone Zombies, Internet of Things, Obstacle Detection, Bystanders Privacy
Contribution A survey of the most recent research about pedestrian safety. The authors identify a range of safety systems for pedestrians, discussing their efficiency and usability. A competitive analysis of existing obstacle detection and collision alert systems is also provided.
(*)

Puliafito, A.; Tricomi, G.; Zafeiropoulos, A.; Papavassiliou, S. Smart Cities of the Future as Cyber Physical Systems: Challenges and Enabling Technologies. *Sensors*, **2021**, *21*, 3349, https://doi.org/10.3390/s21103349.
Keywords Cloud; IoT; smart cities; embedded systems; wireless systems; cyber physical systems; online social networks; software-defined networks
Contribution The survey discusses the challenges, the state-of-the-art, and the solutions to a set of open key issues in the domain of cyber physical systems and smart cities.
(*)

Biyik, C.; Allam, Z.; Pieri, G.; Moroni, D.; O'Fraifer, M.; O'Connell, E.; Olariu, S.; Khalid, M. Smart Parking Systems: Reviewing the Literature, Architecture and Ways Forward. *Smart Cities*, **2021**, *4*, 623–642.
Keywords Smart parking systems, architecture, layers, IoT, smart cities
Contribution A holistic survey of the current state of smart parking systems. The analysis is carried out from a technical perspective (systems and sensors available in the literature).
(*)

Barriga, J.J.; Sulca, J.; León, J.L.; Ulloa, A.; Portero, D.; Andrade, R.; Yoo, S.G. Smart Parking: A Literature Review from the Technological Perspective. *Applied Sciences*, **2019**, *9*, 4569.
Keywords Smart parking, sensors, LPWAN, networking, smart cities
Contribution The review identifies the most-used types of smart parking architecture components (sensors, communication protocols, software solutions) and highlights usage trends. In addition, the paper provides a guide of complementary features from the type of components to be considered when implementing a smart parking solution.
(*)

Yang, C.; Liang, P.; Fu, L.; Cui, G.; Huang, F.; Teng, F.; Bangash, Y.A. Using 5G in smart cities: A systematic mapping study. *Intelligent Systems with Applications*, **2022**, *14*, 200065.
Keywords 5G, Smart city, Scenario, Architecture, Technology, Systematic mapping study
Contribution A systematic mapping study on the literature (32 articles from January 2012 to December 2019) regarding using 5G in smart cities. Scenarios, architecture, technologies, challenges, and lessons learned are summarized and analyzed.
(*)

Zhang, G.; Navimipour, N.J. A comprehensive and systematic review of the IoT-based medical management systems: Applications, techniques, trends and open issues. *Sustainable Cities and Society*, **2022**, *82*, 103914, https://doi.org/10.1016/j.scs.2022.103914.
Keywords Intelligent Devices, Modern Cities, Smart Networks, Medical Management Systems, Systematic Literature Reviews
Contribution The survey investigates the role of IoT in medical management systems and discusses the involved major issues. The selected papers have been classified into four groups: (a) receiving, sharing, and storing patient information; (b) medical equipment failure management; (c) remote monitoring; and (d) security frameworks.
(*)

Kashani, M.H.; Madanipour, M.; Nikravan, M.; Asghari, P.; Mahdipour, E. A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications*, **2021**, *192*, 103164.
Keywords Internet of things, Healthcare, e-health, Systematic review
Contribution The paper identifies, compares, and classifies the existing research (146 articles between 2015 and 2020) in the healthcare IoT systems. Five categories of approaches are identified: sensor-based, resource-based, communication-based, application-based, and security-based.
(*)

Aledhari, M.; Razzak, R.; Qolomany, B.; Al-Fuqaha, A.; Saeed, F. Biomedical IoT: Enabling Technologies, Architectural Elements, Challenges, and Future Directions. *IEEE Access*, **2022**, *10*, 31306–31339.
Keywords Internet of Things, biomedical IoT, healthcare, wearable technology, biomedical implantations, constrained application protocol, implantable biosensors
Contribution The paper provides a summary of the most relevant protocols, technologies, and challenges for medical IoT. The survey provides detailed use cases to illustrate how medical IoT is applied in various medical scenarios and how different protocols presented in the paper fit together to achieve desired goals. The paper also discusses several proposed frameworks and use cases of medical IoT in hospital settings.
(*)

Adere, E.M. Blockchain in healthcare and IoT: A systematic literature review. *Array*, **2022**, *14*, 100139.
Keywords Integrating blockchain and IoT, Data management in blockchain, Blockchain and healthcare, Blockchain and IoT, Blockchain and smart city and drug supply chain management
Contribution A systematic literature review devoted to analyzing trends and highlighting the benefits of blockchain deployment in IoT and healthcare. The focus is on data security and privacy and blockchain-IoT integration.
(*) 02-01, 02-02

Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences*, **2022**, *12*, 1927.
Keywords Internet of Healthcare Things (IoHT), data privacy, healthcare systems, security and privacy, healthcare regulations
Contribution This article discusses different components of IoHT and categorizes healthcare devices based on their functionality and deployment. It also highlights possible points and reasons for data leakage. Compliance problems of IoHT devices concerning healthcare data privacy and protection regulations are analyzed.
(*) 02-01, 02-02

Ketu, S.; Mishra, P.K. Internet of Healthcare Things: A contemporary survey. *Journal of Network and Computer Applications*, **2022**, *192*, 103179.
Keywords Internet of Healthcare Things (IoHT), Internet of things, Healthcare system, Sensors, Issues and challenges, Security, Services and applications, Smart healthcare, Wireless sensor network, Industry trends and status
Contribution A review on the advances in the IoHT technologies (such as topologies, platforms/architectures, taxonomies, services and applications, industry trends, and the status of IoHT-based solutions). Privacy and security issues are discussed. This paper also addresses IoT-based health policies and regulations worldwide.
(*) 02-01, 02-02

Bhuiyan, M.N.; Rahman, M.M.; Billah, M.M.; Saha, D. Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities. *IEEE Internet of Things Journal*, **2021**, *8*, 10474–10498.
Keywords Architectures, healthcare, Internet of Things, networks, security
Contribution A survey on advances in IoT-based healthcare methods and technologies. This paper classifies an existing IoT-based healthcare network and provides a summary of all perspective networks. It also surveys IoT healthcare applications and services. Insights into IoT healthcare security (requirements, challenges, and privacy issues) are provided. An IoT-based security architectural model is proposed to mitigate security problems.
(*) 01-03, 02-01, 02-02

Krishnamoorthy, S.; Dua, A.; Gupta, S. Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions. *Journal of Ambient Intelligence and Humanized Computing*, **2021**, https://doi.org/10.1007/s12652-021-03302-w.
Keywords Healthcare 4.0, Wireless body area networks, Blockchain, Machine learning, Edge computing, Fog computing, Big data analytics, Software-defined networks
Contribution The survey identifies the research gaps and presents the state-of-the-art of healthcare systems, introducing the healthcare IoT application and service stacks. The paper also discusses the paradigm of wireless body area networks. A comparative study of different architectural implementations is carried out.
(*) 01-03, 01-04, 01-06, 02-01, 02-02

Rasool, R.; Ahmad, H.F.; Rafique, W.; Qayyum, A.; Qadir, J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ML. *Journal of Network and Computer Applications*, **2022**, *201*, 103332.
Keywords Internet of things, Edge computing, Healthcare, Internet of medical things (IoMT), Security, Privacy
Contribution The review classifies security and privacy challenges against different IoMT variants based on their usage in the healthcare domain. A comprehensive attack taxonomy on the overall IoMT infrastructure is provided. Security and privacy requirements for the development of security solutions are outlined.

(*) 01-04, 02-01, 02-02

Sworna, N.S.; Islam, A.K.M.M.; Shatabda, S.; Islam, S Towards development of IoT-ML driven healthcare systems: A survey. *Journal of Network and Computer Applications*, **2021**, *196*, 103244.
Keywords Healthcare applications, Machine learning (ML), IoT, Cloud computing, Communication, Taxonomy
Contribution A survey of the existing literature covering IoT and ML strategies from a healthcare perspective. Insights into different types of network storage and computing strategies used for health-based applications are provided. A taxonomy from an IoT-ML-based healthcare perspective is provided.
(*) 01-02, 01-04, 01-06

Raj, M.; Gupta, S.; Chamola, V.; Elhence, A.; Garg, T.; Atiquzzaman, M.; Niyato, D. A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0. *Journal of Network and Computer Applications*, **2021**, *187*, 103107.
Keywords Agriculture 4.0, Precision agriculture, Internet of Things, Smart farming, UAV, Internet of Underground Things (IoUT), Data analytics, Machine learning, Deep learning
Contribution The survey focuses on how technologies such as IoT, UAVs, IoUT, big data analytics, deep learning techniques, and machine learning methods can be used to manage various farm-related operations.
(*) 01-06

Rahimi, M.; Songhorabadi, M.; Kashani, M.H. Fog-based smart homes: A systematic review. *Journal of Network and Computer Applications*, **2020**, *153*, 102531.
Keywords Fog computing, Smart homes, Smart buildings, Systematic review, Internet of things
Contribution A systematic literature review on fog-based smart homes (2014-May 2019). A taxonomy (represented as resource management-based and service-management-based approaches) is proposed.
(*) 01-04

Malik, P.K.; Sharma, R.; Singh, R.; Gehlot, A.; Satapathy, S.C.; Alnumay, W.S.; Pelusi, D.; Ghosh, U.; Nayak, J. Industrial Internet of Things and its Applications in Industry 4.0: State of The Art. *Computer Communications*, **2021**, *166*, 125–139.
Keywords Industrial Internet of Things, Automotive Industries, Environment monitoring, Agriculture, Construction, Solar assisted system
Contribution This paper discusses the applications of the Internet of Things in automotive industries, embedded devices, environment monitoring, agriculture, construction, smart grids, health care, etc. A regressive review of the existing systems of the automotive industry, emergency response, and chain management on the industrial IoT is carried out.
(*)

Timoumi, A.; Gangwar, M.; Mantrala, M.K. Cross-channel effects of omnichannel retail marketing strategies: A review of extant data-driven research. *Journal of Retailing*, **2022**, *98*, 133–151.
Keywords Retailing, Omnichannel, Cross-channel effects
Contribution A review of 50 empirical retailing research papers appeared over the last 20 years about within-retailer cross-channel effects of omnichannel retail marketing strategies.
(*)

Shankar, V.; Kalyanam, K.; Setia, P.; Golmohammadi, A.; Tirunillai, S.; Douglass, T.; Hennessey, J.; Bull, J.S.; Waddoups, R. How Technology is Changing Retail. *Journal of Retailing*, **2021**, *97*, 13–27.
Keywords Innovation, Shopping, Customer, Supplier, Sharing economy, Smart distancing
Contribution This paper discusses how technology is transforming retail. A classification of technologies impacting retailing is provided. The authors identify and elaborate on the drivers and outcomes of technology adoption by shoppers, retailers, employees, and suppliers.
(*)
Fagerstrom, A.; Eriksson, N.; Sigurdsson, V. Investigating the impact of Internet of Things services from a smartphone app on grocery shopping. *Journal of Retailing and Consumer Services*, **2020**, *52*, 101927.
Keywords Retail grocery, Shopper-facing technology, Internet of Things services, Approach and avoidance, Conjoint study
Contribution A study investigating the impact of IoT services from a smartphone app in a retail grocery shopping situation. Four variables (price, expiry date, quality indicators and offers) are examined in relation to traditional information and IoT services.
(*)

Jabbar, R.; Dhib, E.; Said, A.B.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review. *IEEE Access*, **2022**, *10*, 20995–21031.
Keywords Blockchain, automotive communication, Internet of Vehicles (IoV), intelligent transport system, Bitcoin, Ethereum, smart contract, Internet of Things, security
Contribution This survey provides a systematic review of blockchain's applications to intelligent transportation systems and the IoV. The evolution of clockchain is presented. The state of the art of clockchain-based IoV solutions is also explored.
(*) 02-01

Reviews about Business Models

Haaker, T.; Ly, P.T.M.; Nguyen-Thanh, N.; Nguyen, H.T.H. Business model innovation through the application of the Internet-of-Things: A comparative analysis. *Journal of Business Research*, **2021**, *126*, 126–136.
Keywords Business model innovation, IoT, Internet-of-Things, Digital transformation, Morphological analysis, Entrepreneurship
Contribution The survey focuses on business model design to explain emerging IoT business models in Vietnam. Case studies and their characteristics are used to perform a morphological analysis and define a general IoT business model.
(*)

Grabowska, S.; Saniuk, S. Business Models in the Industry 4.0 Environment – Results of Web of Science Bibliometric Analysis. *Journal of Open Innovation: Technology, Market, and Complexity*, **2022**, *8*, 19, https://doi.org/10.3390/joitm.
Keywords Business model; open business model; Industry 4.0; Fourth Industrial Revolution; Pillars of the business model; open innovations
Contribution This survey identifies the pillars for building business models of the enterprises in the era of Industry 4.0.

(*)

Cranmer, E.E.; Papalexi, M.; tom Dieck, M.C.; Bamford, D. Internet of Things: Aspiration, implementation and contribution. *Journal of Business Research*, **2022**, *139*, 69–80.
Keywords Internet of Things, Business models, Value, Innovation
Contribution This study focuses on the IoT business model domain. It classifies the factors influencing and hindering the ability to implement IoT; then, it proposes the development of the aspiration, implementation and contribution (AIC) business model framework, which gives guidelines to organizations for adopting IoT in order to create value.
(*)

Palmaccio, M.; Dicuonzo, G.; Belyaeva, Z.S. The internet of things and corporate business models: A systematic literature review. *Journal of Business Research*, **2021**, *131*, 610–618.
Keywords Internet of things, Business models, Systematic literature review
Contribution This survey investigates twenty years of research on the connection of Internet of Things and business models.
(*)

Suppatvech, C.; Godsell, J.; Day, S. The roles of internet of things technology in enabling servitized business models: A systematic literature review. *Industrial Marketing Management*, **2019**, *82*, 70–86.
Keywords Internet of things, servitization, business model, systematic literature review
Contribution A survey about the state-of-the-art on the emerging concept of IoT and servitized business models.
(*) 03-04

Reviews about Customers

Pinto, F.; Ferreira da Silva, C.; Moro, S. People-centered distributed ledger technology-IoT architectures: A systematic literature review. *Telematics and Informatics*, **2022**, *70*, 101812.
Keywords Internet of Things (IoT), Distributed Ledger Technology (DLT), People-centered Data economy
Contribution This review tested 39 DLT implementations to understand how such a technology enables people-centered IoT solutions.
(*)

Herhausen, D.; Miocevic, D.; Morgan, R.E.; Kleijnen, M.H.P. The digital marketing capabilities gap. *Industrial Marketing Management*, **2020**, *90*, 276–290.
Keywords Digital marketing, Resource-based theory, Digital capabilities, Digital resources, Future research agenda
Contribution A systematic review of 129 articles to identify different digital marketing capabilities in the industry. Four topics are identified (channels, social media, digital relationships, and digital technologies) and tested through an online survey.
(*)

Reviews about Servitization

Pirola, F.; Boucher, X.; Wiesner, S.; Pezzotta, G. Digital technologies in product-service systems: a literature review and a research agenda. *Computers in Industry*, **2020**, *123*, 103301.
Keywords Smart Product-Service System (PSS), Digital Servitization, Digitalization, Industry 4.0, Modeling of Research Topics, Literature Review
Contribution The concept of Smart PSS is analyzed through a semi-systematic literature review. Five research topics are identified: PSS design, digital servitization, assessing tools for PSS decisions, knowledge management along the lifecycle, and sustainability business models.
(*) 03-01

Favoretto, C.; Mendes, G.H.S.; Oliveira, M.G. Paulo A. Cauchick-Miguel, Wim Coreynen From servitization to digital servitization: How digitalization transforms companies' transition towards services. *Industrial Marketing Management*, **2022**, *102*, 104–121.
Keywords Servitization, Digitalization, Digital Servitization, Product companies, Systematic literature review
Contribution A systematic literature review of 180 articles (years 2005–2020) on how digitalization transforms product companies in their transition towards services. This study proposes a new unified definition of digital servitization and discusses nine servitization dimensions.
(*)

Rabetino, R.; Kohtamäki, M.; Brax, S.A.; Sihvonen, J. The tribes in the field of servitization: Discovering latent streams across 30 years of research. *Industrial Marketing Management*, **2021**, *95*, 70–84.
Keywords Servitization, Topic modeling, Narratives, Literature review
Contribution This survey analyzes 550 papers to explain how servitization has emerged and developed over the past three decades.
(*)

Reviews about Digital Twins

Fuller, A.; Fan, Z.; Day, C.; Barlow, C. Digital Twin: Enabling Technologies, Challenges and Open Research. *IEEE Access*, **2022**, DOI 10.1109/ACCESS.2020.2998358
Keywords Digital twins, applications, enabling technologies, Internet of Things (IoT), Industrial IoT (IIoT), machine learning, deep learning, literature review.
Contribution This review has categorised recent publications about digital twins into three research areas: healthcare, manufacturing, and smart cities. An assessment of the enabling technologies, challenges and open research is provided.
(*)

Mylonas, G.; Kalogeras, A.; Kalogeras, G.; Anagnostopoulos, C.; Alexakos, C.; Muñoz, L. Digital Twins From Smart Manufacturing to Smart Cities: A Survey. *IEEE Access*, **2021**, 10.1109/ACCESS.2020.2998358
Keywords Digital twin (DT), smart cities, Industry 4.0, society 5.0, IoT, smart manufacturing, cyber-physical systems, open challenges

Contribution A review of the recent research on DTs in the field of smart cities. Parallels with the application of DTs in Industry 4.0 are drawn, and the open challenges are highlighted. The authors argue that DTs in smart cities should be treated as cyber-physical "systems of systems" due to their requirements, complexity, and vastly different system size in comparison to other recent applications of DTs.
(*)

Suhail, S.; et al., Blockchain-based Digital Twins: Research Trends, Issues, and Future Challenges. *ACM Computing Surveys*, **2022**, *54*, 1–34, https://doi.org/10.1145/3517189.
Keywords Distributed systems security, Artificial Intelligence (AI), Blockchain, Cyber-Physical Systems (CPSs), Digital Twins (DTs), Industrial Control Systems (ICSs), Internet of Things (IoT), Industry 4.0
Contribution A comprehensive review of the current literature for blockchain-based DTs. Based on the research trends, the authors discuss a trustworthy blockchain-based DT framework. Moreover, they highlight the role of AI in blockchain-based DTs.
(*)

Semeraro, C.; Lezoche, M.; Panetto, H.; Dassisti; M. Digital twin paradigm: A systematic literature review. *Computers in Industry*, **2021**, *130*, 103469, https://doi.org/10.1016/j.compind.2021.103469.
Keywords Digital twin, Industry 4.0, Cyber-physical systems, Predictive manufacturing
Contribution This review provides an up-to date picture of DTs' components and their characteristics. The ongoing research and technical challenges in building DTs for different application domains and related technologies are sketched as well.
(*)

Qian, C.; Liu, X.; Ripley, C.; Qian, M.; Liang, F.; Yu, W. Digital Twin – Cyber Replica of Physical Things: Architecture, Applications and Future Research Directions. *Future Internet*, **2022**, *14*, 64, https://doi.org/10.3390/fi14020064.
Keywords Digital Twin (DT); Internet of Things (IoT); cyber-physical systems; smart-world applications
Contribution A review of the architectures of DTs, data representation, and communication protocols. Existing efforts on applying DTs into IoT data-driven smart systems (including smart transportation, smart manufacturing, and smart cities) are summarized. Further, the existing challenges from CPS, data science, optimization, and security and privacy perspectives are pointed out. Finally, future research directions from the perspectives of performance, new DT-driven services, models and learning, and security and privacy are outlined.
(*)

Reviews about Software Engineering

Alreshidi, A.; Ahmad, A. Architecting Software for the Internet of Thing Based Systems. *Future Internet*, **2019**, 11, 153.
Keywords Internet of Things, software architecture, mobile cloud computing, evidence based software engineering, systematic mapping study
Contribution The evidence-based software engineering method is used to conduct a mapping study of the existing IoT solutions (88 selected papers). The paper identifies the following research themes: software-defined networking, autonomous and adaptive software- and agent-based systems, and cloud-based software ecosystems.
(*) 01-04

Dias, J.P.; Restivo, A.; Ferreir, H.S. Designing and constructing internet-of-Things systems: An overview of the ecosystem. *Internet of Things*, **2022**, *19*, 100529, https://doi.org/10.1016/j.iot.2022.100529.
Keywords Internet-of-Things, Software engineering, Embedded systems Large-scale systems, System design, System development
Contribution A survey of the state of the art in designing and constructing IoT systems from the software engineering perspective.
(*) 01-03, 02-03

Magaia, N.; Gomes, P.; Silva, L.; Sousa, B.; Mavromoustakis, C.X.; Mastorakis, G. Development of Mobile IoT Solutions: Approaches, Architectures, and Methodologies. *IEEE Internet of Things Journal*, **2021**, *8*, 16452–16472.
Keywords Architecture, Internet of Things (IoT), methodology, mobile development
Contribution The article presents approaches, architectures, and methodologies relevant to the development of mobile IoT solutions.
(*)

Fahmideh, M.; et al. Engineering Blockchain Based Software Systems: Foundations, Survey, and Future Directions. *ACM Computing Surveys* (in press)
Keywords Software engineering, Systems development methods, Blockchain, Smart contracts, Blockchain based software systems, Software development process management
Contribution A systematic literature review of the state-of-the-art in blockchain-based software (BBS) engineering research from the software engineering perspective. The relevant research is classified based on four aspects: theoretical foundations, processes, models, and roles. Based on these aspects, a rich repertoire of models, design principles, development tasks, roles, challenges, and resolution techniques is presented. The survey gives to software developers a solid body of knowledge on current BBS development.
(*)

Gavrilovic, N.; Mishra, A. Software architecture of the internet of things (IoT) for smart city, healthcare and agriculture: analysis and improvement directions. *Journal of Ambient Intelligence and Humanized Computing*, **2021**, *12*, 1315–1336.
Keywords Internet of things, Software architecture, Smart city, Healthcare, Agriculture, Architectural paradigms
Contribution An analysis of known software architectures for IoT systems in the domains of healthcare, smart cities, and agriculture. This survey proposes solutions and improvements of different software architecture types (such as layered, service-oriented and cloud-based types) and interactions between identified software architecture elements.
(*) 03-01

Fernandez, E.B.; Washizaki, H.; Yoshioka, N.; Okubo, T. The design of secure IoT applications using patterns: State of the art and directions for research. *Internet of Things*, **2021**, *15*, 100408.
Keywords IoT applications, IoT systems design, Internet of Things, Security patterns, Misuse patterns, Privacy patterns, Reference architectures, Secure systems development, Microservices, IoT survey

Contribution This survey classifies existing IoT security patterns. The authors conclude that the number of available patterns is insufficient for a working catalog; moreover, most of them are incomplete or use different descriptions. The need for a unified catalog is pointed out.
(*) 02-01, 02-02

Reggio, G.; Leotta, M.; Cerioli, M., Spalazzese, R.; Alkhabbas, F. What are IoT systems for real? An experts' survey on software engineering aspects *Internet of Things*, **2020**, *12*, 100313.
Keywords Internet of Things, Personal Opinion Survey, Software Engineering, Empirical Study, Researchers, Practitioners
Contribution A survey (433 developers answered from 53 countries) to understand the basic features of IoT systems in order to improve the software engineering support for their development.
(*)

References

1. Wang,J.; Lim,M.K.; Wang,C.; Tseng, M.L. The evolution of the Internet of Things (IoT) over the past 20 years. *Comput. Ind. Eng.* **2021**, *155*, 107174. [CrossRef]
2. Internet of Things. An Action Plan for Europe. An-Europe. 2009, Volume 278, pp. 1–15. Available online: https://www.eesc.europa.eu/en/ourwork/opinions-information-reports/opinions/internet-things-action-pl (accessed on 5 July 2022).
3. Kitchenham, B.; Charters, S. Guidelines for Performing Systematic Literature Reviews in Software Engineering. *EBSE Technical Report EBSE-2007-01*. 2007. Available online: https://www.525444systematicreviewsguide.pdf (accessed on 5 July 2022).
4. Aly, M.; Khomh, F.; Yacout, S. What Do Practitioners Discuss about IoT and Industry 4.0 Related Technologies? Characterization and Identification of IoT and Industry 4.0 Categories in Stack Overflow Discussions. *Internet Things* **2021**, *14*, 100364. [CrossRef]
5. Ali, O.; Ishak, M.K.; Bhatti, M.K.L.; Khan, I.; Kim, K.-I. A Comprehensive Review of Internet of Things: Technology Stack, Middlewares, and Fog/Edge Computing Interface. *Sensors* **2022**, *22*, 995. [CrossRef] [PubMed]
6. ISO/IEC 30141:2018, Internet of Things (IoT)—Reference Architecture Available online: https://standards.iso.org/ittf/PubliclyAvailableStandards/c065695_ISO_IEC_30141_2018(E).zip (accessed on 25 May 2022).
7. Alli, A.A.; Alam, M.M. The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. *Internet Things* **2020**, *9*, 100177. [CrossRef]
8. Firouzi, F.; Farahani, B.; Marinšek, A. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). *Inf. Syst.* 2022 *in press*.
9. Aslanpour, M.S.; Gill, S.S.; Toosi, A.N. Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research *Internet Things* **2020**, *12*, 100273. [CrossRef]
10. OpenFog: Reference Architecture for Fog Computing. 2017. Available online: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf (accessed on 27 March 2022).
11. Gill, S.S. A Manifesto for Modern Fog and Edge Computing: Vision, New Paradigms, Opportunities, and Future Directions. In *Operationalizing Multi-Cloud Environments*; Nagarajan, R., Raj, P., Thirunavukarasu, R., Eds.; EAI/Springer Innovations in Communication and Computing; Springer: Cham, Switzerland, 2022. [CrossRef]
12. Zhang, J.; Ma, M.; Wang, P.; Sun, X.-D. Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions. *J. Syst. Archit.* **2021**, *117*, 102098 doi: 10.1016/j.sysarc.2021.102098. [CrossRef]
13. Kassab, W.; Darabkh, K.A. A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *J. Netw. Comput. Appl.* **2020**, *163*, 102663. [CrossRef]
14. Uddin, M.A; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in IoT: Challenges and solutions *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
15. Singh, V.K.; Singh, P.; Karmakar, M.; Leta, J.; Mayr, P. The journal coverage of Web of Science, Scopus and Dimensions: A comparative analysis. *Scientometrics* **2021**, *126*, 5113–5142. [CrossRef]
16. Alkhabbas, F.; Spalazzese, R.; Davidsson, P. Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. *Internet Things* **2019**, *7*, 100084. [CrossRef]
17. Stavropoulos, T. G.; Papastergiou, A.; Mpaltadoros, L.; Nikolopoulos, S.; Kompatsiaris, I. IoT Wearable Sensors and Devices in Elderly Care: A Literature Review. *Sensors*, **2020**, *20*, 2826. [CrossRef]
18. Laghari, A.A.; Wu, K.; Laghari, R.A.; Ali, M.; Khan, A.A. A Review and State of Art of Internet of Things (IoT). *Arch. Comput. Methods Eng.* **2022**, *29*, 1395–1413. [CrossRef]
19. Sobin, C.C. A Survey on Architecture, Protocols and Challenges in IoT *Wirel. Pers. Commun.* **2020**, *112*, 1383–1429. [CrossRef]
20. Jin, X.; Lib, L.; Dang, F.; Chen, X.; Liu, Y. A survey on edge computing for wearable technology. *Digit. Signal Process.* 2022, *in press*. [CrossRef]
21. Rosendo, D.; Costan, A.; Valduriez, P.; Antoniu, G. Distributed Intelligence on the Edge-to-Cloud Continuum:A Systematic Literature Review. *J. Parallel Distrib. Comput.* 2022, *in press*.
22. Achir, M.; Abdelli, A.; Mokdad, L.; Benothman, J. Service discovery and selection in IoT: A survey and a taxonomy *J. Netw. Comput. Appl.* **2022**, *200*, 103331. [CrossRef]
23. Khan, M.A.; Siddiqui, M.S.; Rahmani, M.K.I.; Husain, S. Investigation of Big Data Analytics for Sustainable Smart City Development: An Emerging Country, *IEEE Access* **2022**, *10*, 16028–16036. [CrossRef]
24. Saxena, S.; Bhushan, B.; Ahad, M.A. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *181*, 103050. [CrossRef]

25. Kaur, M.; Khan, M.Z.; Gupta, S.; Alsaeedi, A. Adoption of Blockchain With 5G Networks for Industrial IoT: Recent Advances, Challenges, and Potential Solutions *IEEE Access* **2022**, *10*, 3138754. [CrossRef]
26. Li, T.; He, X.; Jiang, S.; Liu, J. A survey of privacy-preserving offloading methods in mobile-edge computing. *J. Netw. Comput. Appl.* **2022**, *203*, 103395. [CrossRef]
27. Ali, Z.H.; Ali, H.A. Towards sustainable smart IoT applications architectural elements and design: opportunities, challenges, and open directions *J. Supercomput.* **2021**, *77*, 5668–5725. [CrossRef]
28. Cranmer, E.E.; Papalexi, M.; tom Dieck, M.C.; Bamford, D. Internet of Things: Aspiration, implementation and contribution *J. Bus. Res.* **2022**, *139*, 69–80. [CrossRef]
29. Agostini, L.; Nosella, A. Industry 4.0 and business models: A bibliometric literature review. *Bus. Process. Manag. J.* **2021**, *7*, 1633–1655. [CrossRef]
30. Batat, W. *Experiential Marketing: Consumer Behavior, Customer Experience and the 7Es*; Routeledge, Taylor & Francis Group: London, UK, New York, NY, USA; 2019.
31. Pinto, F.; da Silva, C.F.; Moro, S. People-centered distributed ledger technology-IoT architectures: A systematic literature review *Telemat. Inform.* **2022**, *70*, 101812. [CrossRef]
32. Favoretto, C.; Mendes, G.H.S. Oliveira, M.G.; Cauchick-Miguel, P.-A.; Coreynen, W. From servitization to digital servitization: How digitalization transforms companies' transition towards services. *Ind. Mark. Manag.* **2022**, *102*, 104–121. [CrossRef]
33. Fischer, M; Heim, D.; Hofmann, A. Christian Janiesch, Christoph Klima, Axel Winkelmann. A taxonomy and archetypes of smart services for smart living. *Electron. Mark.* **2020**, *30*, 131–149. [CrossRef]
34. Lim, K.Y.H; Zheng, P.; Chen, C.-H. A state-of-the-art survey of Digital Twin: techniques, engineering product lifecycle management and business innovation perspectives *J. Intell. Manuf.* **2020**, *31*, 1313–1337. [CrossRef]
35. Ante, L.; Fischer, C.; Strehle, E. A bibliometric review of research on digital identity: Research streams, influential works and future research paths. *J. Manuf. Syst.* **2022**, *62*, 523–538. [CrossRef]
36. Grieves, M. *Product Lifecycle Management: Driving the Next Generation of Lean Thinking*; McGraw-Hill: New York, NY, USA, 2006.
37. Kirchhof, J.C.; Michael, J.; Rumpe, B.; Varga, S.; Wortmann, A. Model-driven Digital Twin Construction: Synthesizing the Integration of Cyber-Physical Systems with Their Information Systems. In Proceedings of the ACM/IEEE 23rd Inter. Conference on Model Driven Engineering Languages and Systems (MODELS '20), Virtual Event, 18–23 October 2020; ACM: New York, NY, USA, 2020. [CrossRef]
38. Bucchiarone, A.; Cabot, J.; Paige, R.F.; Pierantonio, A. Grand challenges in model-driven engineering: an analysis of the state of the research. *Softw. Syst. Modeling* **2020**, *19*, 5–13. [CrossRef]
39. Patel, P.; Cassou, D. Enabling high-level application development for the Internet of Things. *J. Syst. Softw.* **2015**, *103*, 62–84. [CrossRef]
40. Kirchhof, J.C; Rumpe, B.; Schmalzing, D.; Wortmann, A. MontiThings: Model-Driven Development and Deployment of Reliable IoT Applications. *J. Syst. Softw.* **2022**, *183*, 111087. [CrossRef]
41. Bansal, S.; Kumar, D. IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 340–364. [CrossRef]
42. Raj, A.; Shetty, S.D. IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey *Wirel. Pers. Commun.* **2022**, *122*, 1481–1517. [CrossRef]
43. Mazhelis, O.; Luoma, E.; Warma, H. Defining an Internet-of-Things Ecosystem. In *Internet of Things, Smart Spaces, and Next Generation Networking*; Andreev, S., Balandin, S., Koucheryavy, Y., Eds.; ruSMART NEW2AN 2012. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7469, pp. 1–14. [CrossRef]
44. Sivagami. P.; Illavarason, P.; Harikrishnan, R.; Reddy, G.V.S.R. IoT Ecosystem. A survey on Classification of IoT. In Proceedings of the First International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISET, Chennai, India, 16–17 May 2020. [CrossRef]