Internet of Things (IoT)

Subjects: Engineering, Electrical & Electronic | Automation & Control Systems | Computer Science, Information Systems

Contributor: Omer Ali

The Internet of Things (IoT) is an extensive network of heterogeneous devices that provides an array of innovative applications and services. IoT networks enable the integration of data and services to seamlessly interconnect the cyber and physical systems.

Internet of Things (IoT) edge computing fog computing security optimization

1. Introduction

The Internet of Things (IoT) is widely regarded as one of the most prevailing technology revolutions of the previous two decades. IoT devices are often perceived as computing devices with sensing capabilities, onboard computational power, and an internet-enabled network to communicate with each other. It is one of the most rapidly growing areas that relies on machine-to-machine communications and utilizes an internet stack for end-to-end connectivity. In its simplest term, IoT is perceived as a network of billions of devices that can sense, actuate and relay the information to a centralized system. Nowadays, IoT devices and applications are deployed in various domains such as logistics, retail, health care, smart city network, intelligent transportation and disaster management. Despite the technological advancements in these individual domains, the heterogeneity of IoT devices and lack of standardization challenges are yet to be addressed. It is vital to examine the “Things” themselves, which operate differently depending on the implementation scenario, ranging from time-critical to mission-critical applications.

2. IoT Architectures, Platforms and Technology Stack

The modern Internet is a complex blend of Internet nodes, IoT devices, and smart objects. Internet-enabled networks require the implementation of an IP stack for communication between networks of objects. With the expansion of Internet networks, enterprises as well as research communities are investing in flexible and scalable IP networks for the future [1]. Currently, the Internet-enabled networks vary greatly both in technical implementations and in end-application needs. A conventional computing node (such as Personal Computers, Laptops, Mobiles and Tablets) implements an entire TCP/IP stack based on the Open Systems Interconnection (OSI) Model. However, due to the limited resources available on IoT devices, a lightweight IP stack is normally implemented. The on-board resource availability and energy consumption of the device primarily regulate the implementation of suitable protocols and standards in IoT devices. Therefore, it is fundamentally important to investigate the IoT architectures and platforms to understand the role and behavior at every layer of the technology stack.

The horizontal fabric is made up of “Things” and the communication stack, whereas middlewares, edge networks, and the cloud make application development simpler and thus enable vertical markets on top of this fabric [2]. A closer look at **Figure 1** reveals a three-tier architectural model for IoT systems. A subtle balance between components and processes is presented in this model, where devices or “Things” are the primary layer of the architecture. It is apparent that this layer is open for vendor-specific implementations, resulting in a myriad of distinct components, modules and operating systems.

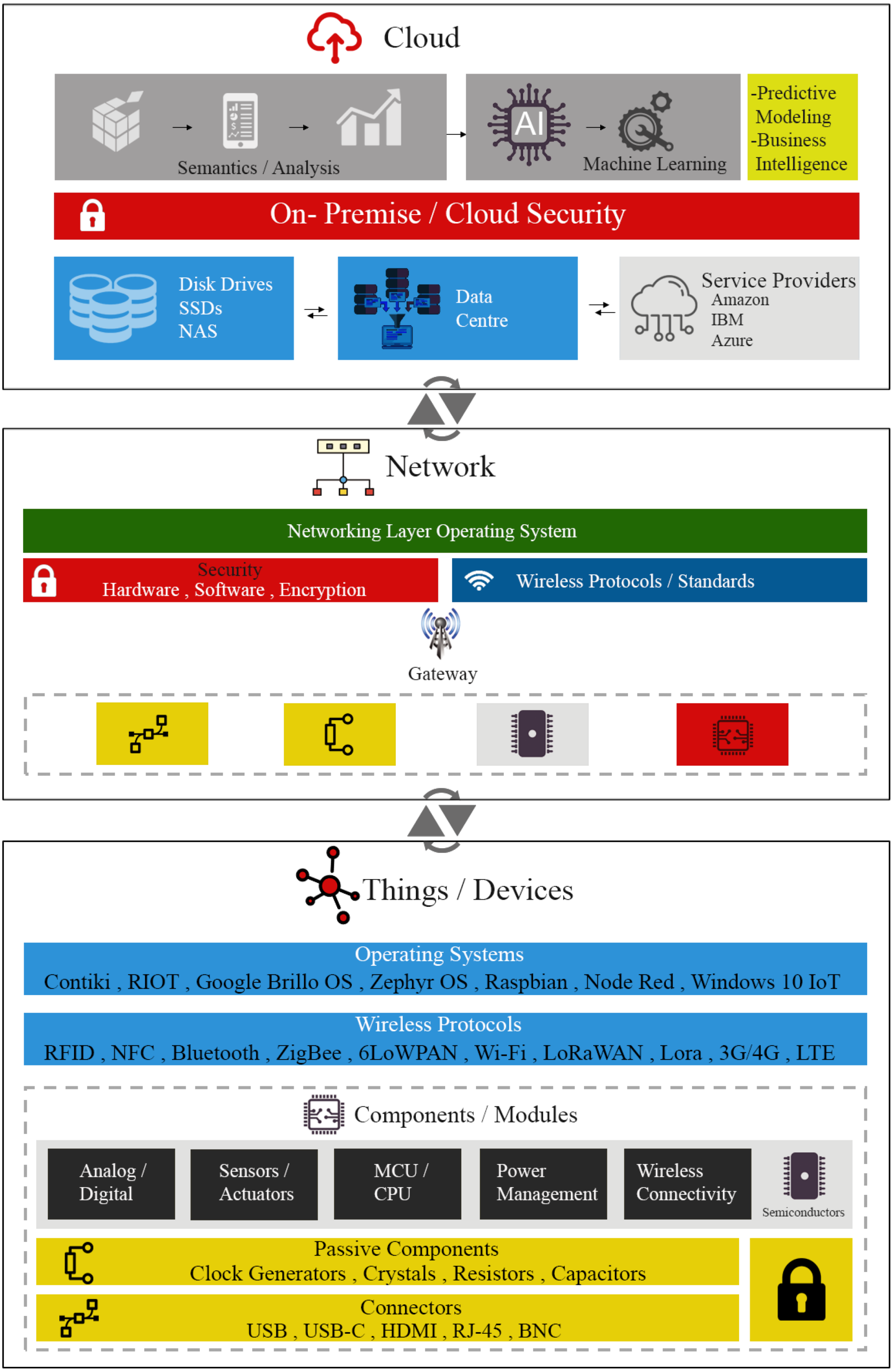

Figure 1. IoT architecture model: technology fabric from physical (PHY) to application (APP) layers.

This layer is responsible for translating and propagating the heterogeneity of the entire IoT stack. The network layer exhibits similar variation in terms of component, module, and operating system selection. Devices are connected to the cloud at this layer, either through gateway devices or through a fog/edge network interface. The cloud layer is in charge of handling raw data from billions of IoT devices. To integrate business intelligence, current cloud-driven corporate systems offer solutions based on Artificial Intelligence (AI) and Machine Learning (ML). The cloud layer is dominated mostly by enterprise solutions that offer a variety of IoT network applications. While each cloud technology is different, the heterogeneity of this layer is often defined by the efficacy of the application design.

Since the Internet of Things primarily relies on the internet to connect these devices to services, most reference models and architectures use a layered approach to understanding and defining the functions at each layer. [3]. The alignment of this reference architecture model in layers that greatly simplify overall design goals is a popular trend. However, it is important to remember that most of these reference models do not correspond to the Internet or the TCP/IP stack [4]. It is indeed worth noting that the majority of alliances and organisations contribute to the standardisation of IoT protocol and architecture stacks by proposing their own reference models. This section looks into several of these models, which range from three-layer to middleware and five-layer models, as given in the literature [5][6][7].

Most architecture models now support the inclusion of middleware as a software-based interface between IoT processes and components. Middleware enables reliable and efficient communication between elements that are mostly not supported within the native operating systems. This results in simpler and standardised communication between processes, components, and devices, thus enabling a software interface that can extend to upper layers and promote vertical market integration.

uBiuitous, secUre inTernet-of-things with Location and contExt-awaReness (BUTLER) is one of the first European consortium research projects to focus on pervasive computing and security for IoT applications in various domains. One of the project’s main objectives was to create context-aware and secure apps for a variety of deployment scenarios (such as healthcare, transportation, smart offices, and smart homes). The researchers proposed a device-centric architecture that included smartObjects, smartMobiles, and smartServers as three key components. The BUTLER project examines technology versus integration concerns using a five-layer architecture that closely resembles the internet layer model, with enabling technologies that help develop the horizontal fabric and address vertical integration problems [8] as shown in **Figure 2**.

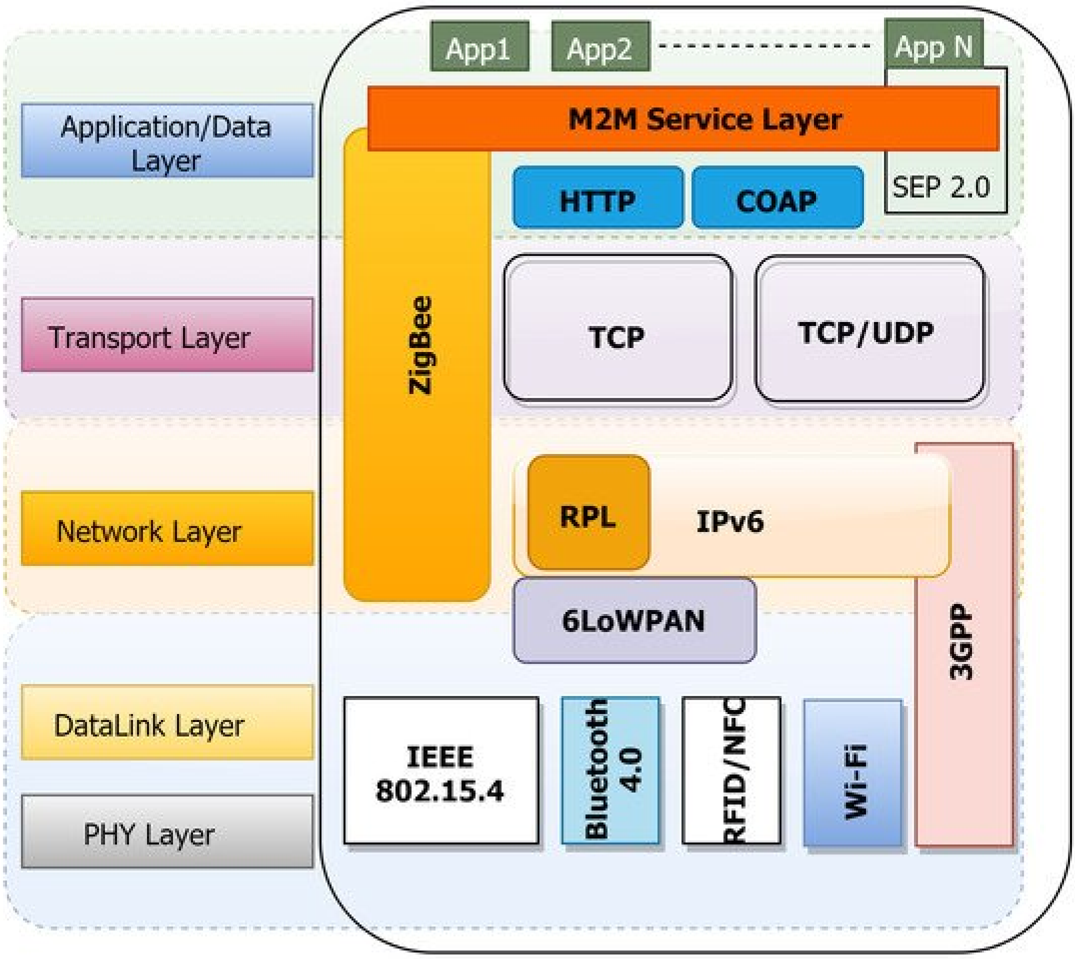

Figure 2. BUTLER EU Project—layered IoT architecture model.

Instead of incorporating middlewares into lower layers that enable vertical market integration, another architectural alternative is to add a business layer on top. The top market layer uses a service-oriented approach to provide application availability, sharing, and cross-vendor deployment as necessary [9][10]. These models are mostly service oriented in design, and they extend object extractions to middleware service management layers. Thus, the application and business layers enable intelligence and integration of the SOA-based fabric into vertical markets. Al-Fuqaha et al. [11] investigated various architecture models and presented a comparison of a few architectures based on multiple layers toward the need to design a reference architecture that provides scalability, interoperability, and easier integration.

R. Khan et al. [7] proposed a basic IoT architecture model where the three-layered approach aligns the IoT fabric close to the internet stack. The three layers, namely Perception, Network and Application, as presented in **Figure 3**, outline the technology and device-level information in the perception layer. The network layer is responsible for the transport or communication of this information to the upper layers. The application layer is a unique blend of managing the data and scaling vertical application-specific integration in multiple domains.

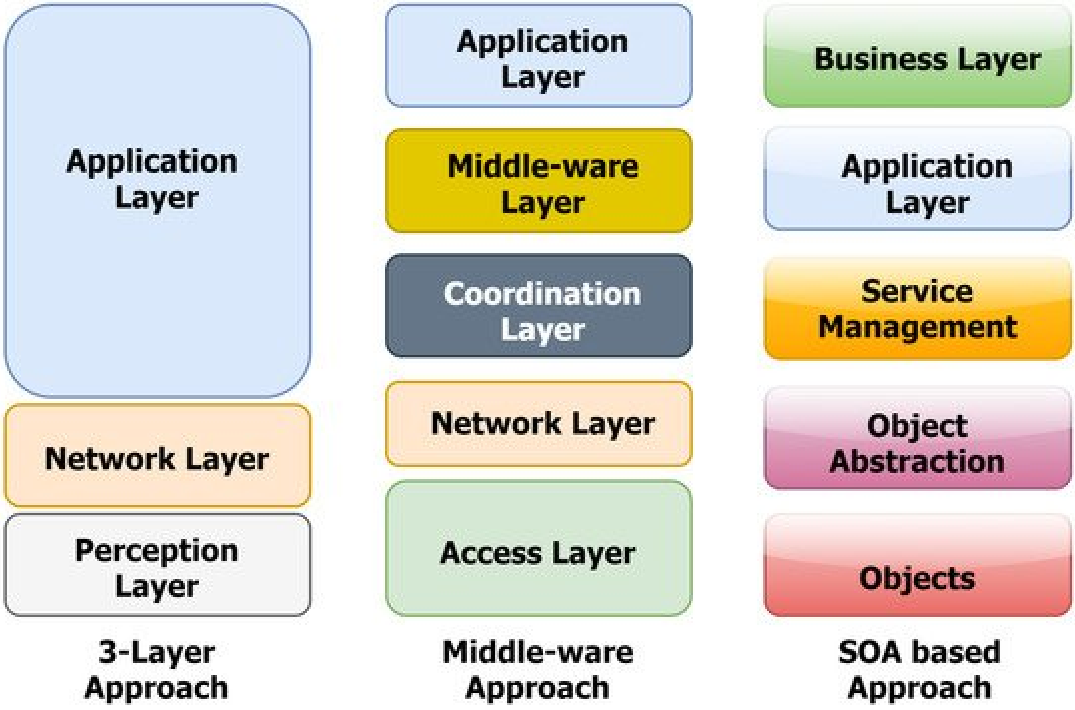

Figure 3. The IoT architecture: layered model approach.

Modern internet-based systems are made up of billions of devices with varying components, modules, operating systems, and thus standards implementation. Due to limited equipment resources and energy usage requirements, the introduction of lightweight protocols and specifications is a common trend in IoT-based systems. This deviation from the standard IP-based implementation necessitates a thorough examination of various technology layers. This section provided a reference IoT architecture model with device, network, and cloud layers, with components and processes decoupled at each layer. There are also several other reference models that support a layered architecture. Support for middlewares and enterprise business layers to enable vertical market integration is one of the most notable developments in comparison to IoT architectures. Reference IoT architectures were found to be mostly aligned with application-specific markets. In addition, the reference models proposed a layered architecture that can be mapped to the OSI layer models. However, a tradeoff in terms of complexity and scalability is on the horizon, limiting the standardisation of IoT architecture even further.

3. Understanding IoT Functional Blocks

3.1. Identification

Typically, data streams on the Internet are aggregated to monitor overall network traffic. To successfully provision network resources and security policies on an IP-based network, source identification is required. Traditional internet traffic relied on the IPv4 addressing scheme, which is gradually giving way to the IPV6 addressing scheme. The IP stack implementation in IoT devices differs from that of traditional Internet nodes. The Internet endpoint typically implements the entire TCP/IP stack, whereas IoT applications frequently use a lightweight protocol implementation. With the number of IoT devices expected to exceed 75 billion by 2025, the IPv4 addressing scheme may be insufficient. As a result, almost every IoT implementation now uses the IPv6 addressing scheme. IEEE protocols, such as 6LowPAN (IPv6 Low-power wireless Personal Area Network), provide a full-stack IPv6 protocol implementation alternative in low-power devices [12][13]. It enables encapsulation and header compression, reducing network overhead while providing unique node addresses for billions of devices.

Another important factor to consider when addressing IoT nodes is the various roles that the node may take on (such as sensing, actuation, relaying or edge-gateway). The aggregation of information based on common service roles is very popular, so nodes must be identified using their Service IDs. An IPv6 address can only identify a node in the network and cannot provide additional information about its roles or behaviours. Therefore, service tag identification is also required for IoT nodes [14]. Radio Frequency Identification (RFID) provides a typical example of service identification by assigning Electronic Product Codes (EPC) to differentiate between various objects and services [15][16].

IP-based networks are becoming very large and complex as IoT applications grow at such a rapid pace. A high volume of network traffic on a single route can degrade overall network traffic, causing congestion and bottlenecks. It is therefore critical to logically slice a larger network in order to ensure faster and more reliable network traffic routes. Traditional IP-based networks logically subnetted a large network by using a private addressing scheme and techniques like Network Address Translation (NAT). Maintaining private routing information for billions of IoT devices, on the other hand, is a challenge. IoT edge-gateway devices may be unable to maintain routing and translation tables due to limited on-board computing and networking resources.

A lot of researchers are investigating smart addressing schemes for these devices. One such interesting addressing mechanism is proposed by Moghadam et al. [17], where traditional EPC codes are mapped over the IPv6 addressing scheme to uniquely identify IoT objects. The mapping technique discussed in this research focuses on creating a unique IPv6 address for every unique EPC code assigned to an IoT node based on its functionality. However, one may argue that the proposed scheme may not scale well, as multiple addresses are required to identify the same node. Hirotsugu Seiki et al. [18] presented a unique concept of a de-centralizing blockchain-based µCode management system that can also be implemented on IoT nodes, allowing scalability and a unique addressing scheme.

3.2. Sensing

IoT networks sense, aggregate, and relay data from billions of smart objects all over the world. In cloud data warehouses, a large amount of raw data is stored and analysed. The knowledge gained from the data assists in the introduction of business intelligence in order to make informed decisions. IoT sensors can be deployed as individual devices (actuators, smart sensors, smart wearables) or as a network of devices (such as WSN) that perform a similar function collectively [19].

WSNs are commonly used in military and industrial research applications where a large number of IoT nodes sense, collect, and relay data collectively. The roles/behaviors of on-board sensors may differ depending on the application. It is also common to see IoT nodes equipped with a variety of sensors that can be triggered based on the situation. These smart sensors' operational requirements (such as degree of accuracy and/or power consumption) may also vary. **Figure 4** provides an overview of a range of sensors typically deployed in industrial applications.

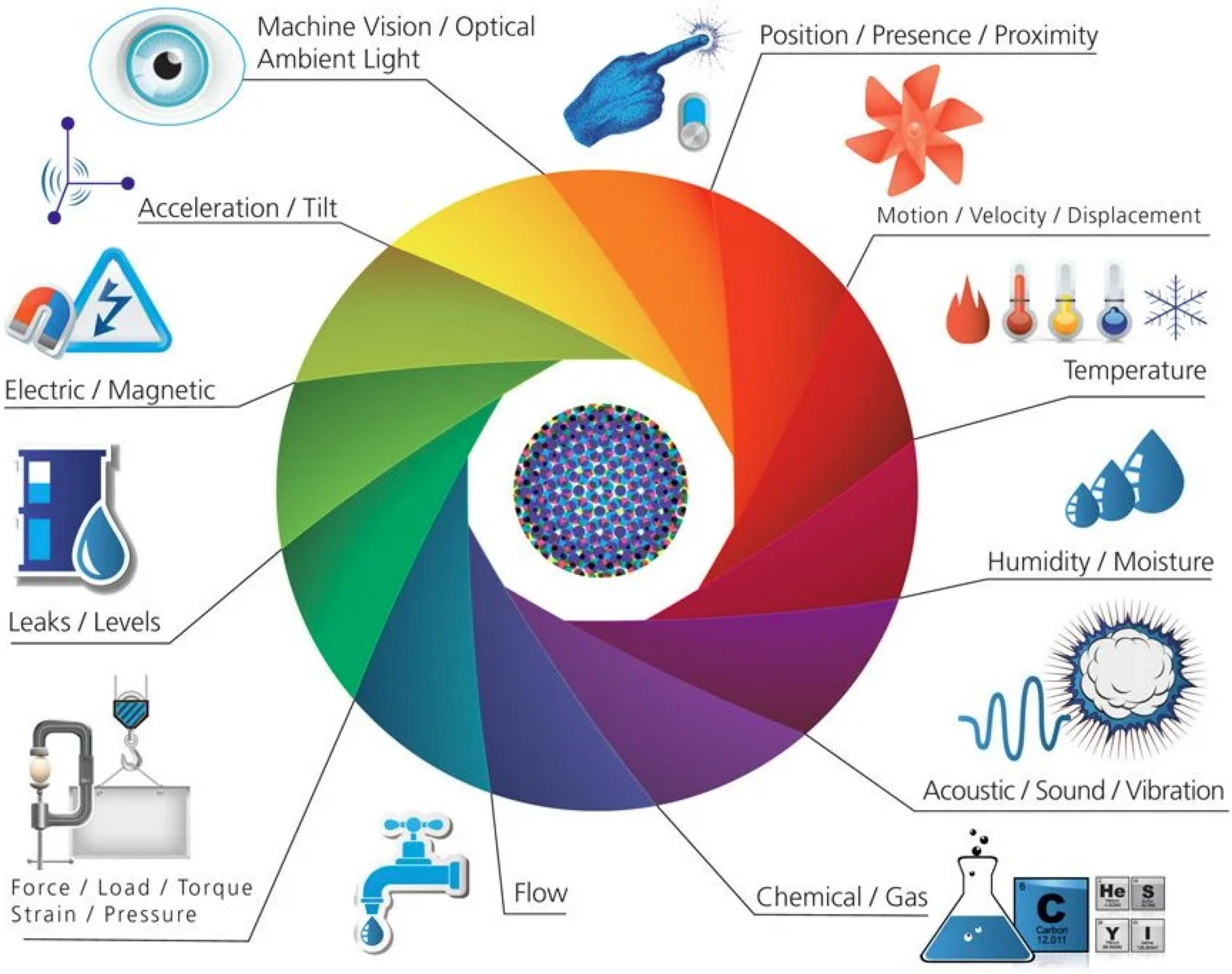

Figure 4. Sensors and actuators currently deployed in the IoT domain [20].

Most of the sensors are passive in nature and require a hardware platform to process the input. Usually a Single Board Computer (SBCs) is capable of processing the information on-board. These SBCs then use the communication tools and built-in TCP/IP stack to connect these nodes to the internet. Currently, we have several IoT-enabled plug and play platforms available that are extensively used in IoT research (e.g., Arduino, Raspberry Pi, Galileo, and BeagleBone). These devices are typically deployed as a single sensing node or in a mesh network topology as the sensing requirements grow. These nodes can be programmed to relay data within their network or to connect with a central management portal where the data is offloaded, analyzed, and then presented on custom dashboards.

IoT nodes are energy-constrained devices that require optimal use of on-board computing to conserve energy. Another consideration that regulates the use of energy-efficient sensors is the overall price of the IoT device. A typical node usually integrates passive sensing devices to reduce its cost. Therefore, smart sensing schemes [21] are required to conserve and, in some cases, harvest energy for IoT nodes [22][23]. In addition, IoT devices generate exabytes of data every day, which is relayed to data warehouses for processing. Researchers have been investigating ubiquitous energy autonomy and compressing schemes to provide smart sensing in recent years [23][24].

Energy autonomous compressing schemes aggregate the sensor data and relay the critical information to the data warehouses. Amarlingam et al. [25] presented an exciting compressed sensing technique for WSNs. The fundamental observation was based on treating the WSN network as the sensing node for IoT networks. The researchers presented the concept of dictionary learning of data over the wireless nodes that could be aggregated to save energy by choosing the minimal transmission cost path from the data to the sink. Such compressed sensing techniques can significantly help to save energy resources over large-scale deployments.

3.3. Communication

IoT networks are a combination of heterogeneous smart objects, communication technologies, and protocols that collectively perform application-specific tasks. Most of the IoT networks are built on top of the WSN that use low power wireless communications [26]. The IoT nodes must run in low power modes during their lifespan due to energy restrictions. Low power radios and the (noisy) wireless channel contribute to their architecture and working complexities. A typical communication protocol must provide instructions on data coding, transmission and flow controls, sequencing, and error correction. The hardware stack implements these protocols to develop basic applications and interfaces to transmit the data towards the target device. There are several technologies for IoT communication, which currently range from close-to-short range communications. Examples of communications technologies commonly used in IoT networks include Near Field Communication (NFC), Narrowband IoT (NB-IoT), Ultra-Wide Bandwidth (UWB), LTE-A, WiMax, WiFi and LoRaWAN [27].

RFID Technology has been extensively used in the last decade for M2M autonomous communication. Several RFID-based systems (active, passive, and hybrid) for object identification and communication have been developed in the past. RFID systems operate on a data query signal that returns locally stored object information from the reader. RFID-based systems are mostly passive, offering a low-transmission rate over a short range [28]. Logistics and warehousing is one of these industry applications [29]. Some very fascinating IoT implementations focused on RFID have now emerged, including pervasive RFID installations for real-time information systems [30].

Intelligent healthcare systems are one of the most active research subjects in electronics, bioengineering, and computer science [31][32]. The current expenditure on Intelligent Health Care is about $7 billion annually. Amendola et al. [33] presented an environment of a health care system that included the implementation of body-centric wearable RFID tags to track the patient's motion and environmental features autonomously, generating a real-time knowledge database. Wearable smart devices (smart tags, fitness trackers, smartwatches) are increasingly being deployed for health and personal activity monitoring. A wearable fitness tracker is mainly concerned with sensing personal activity and computing a fitness rating. Low cost and low power consumption are some of the common design considerations of wearable devices. Many of these devices combine identical sensors and computational algorithms; there are considerable wireless technologies available. In [34], Fan Wu et al. presented an interesting comparison in wireless technology that is suitable for wearable nodes.

LoRa is another networking technology that operates over longer transmission distances and consumes low power. The lower cost compared to cellular and WiFi systems is a significant efficiency factor for LoRa. LoRa-based IoT systems are commonly used for long-range communication where high transmission speeds are not required. One such design and evaluation environment is presented by H. Lee [35], where LoRa is chosen as the communication technology for a mesh network of IoT sensor nodes. The research also proposed an architecture for improved coverage, with fewer gateways to reduce complexity and overall deployment costs.

Cellular communication, especially 3G, 4G, LTE, and LTE-A (including the prospects of 5G technologies), is thought of as a significant communication technology for IoT applications that demand multimedia transfer or streaming capabilities [36]. Current research on 5G systems supports a design trend that enables LTE-A and beyond cellular technologies as major backbone network contenders for extended coverage, high throughput, and lower latencies [36][37]. Although, by its design, the IoT architecture is heterogeneous, it seems nearly impossible to use a single communication technology implementation for IoT applications.

3.4. Compute

Computation is the process of calculating the system workload (both arithmetic and non-arithmetic) for a set of I/O instructions. In traditional computer technology, microprocessors handle the computing load in their CPU cores. High computation and efficiency tasks necessitated the implementation of GPU in order to form computational clusters. IoT systems are primarily governed by a number of factors, including device costs, lower calculation loads, and low energy usage, necessitating the use of power and cost-effective processing units (microprocessors, microcontrollers, System on Chip (SOC), and Field Programmable Gate-Arrays (FPGAs)). The majority of IoT deployments include sensing, processing, and relaying data to the cloud for intensive calculations. These requirements necessitate a limited on-board processor and storage space, thereby reducing system costs and complexity. CPU optimization is frequently essential when the idle CPU wastes a significant amount of computing power. An under-provisioned CPU, on the other hand, will quickly reach its processing peak, necessitating more resources and potentially causing processing bottlenecks. As a result, workload optimization is critical and is taken into account during the initial design stages.

Traditionally, workload optimization is performed by the CPU and is typically managed by the device's operating system. However, as the number of IoT devices grows year after year, it is clear that a heterogeneous approach is required, with edge computing playing a significant role. In comparison to low-processing, node-level IoT devices, such a solution necessitates heavy computing devices. Processing platforms such as (Arduino, Raspberry Pi, Intel IoT Development Boards, BeagleBone, and ARM Corstone) provide a range of processing capabilities from low-power to full application-specific SoC platforms. In terms of programming, the hardware is only as good as the operating system (OS) that it runs. IoT OS enables devices and applications to communicate with one another as well as other devices such as cloud networks and utilities. The IoT OS also handles the computing power and other services required to collect, transfer, and store data, essentially acting as the device's central nervous system.

The cloud infrastructure model for IoT devices has matured in recent years. Market leaders such as Amazon IoT, Google Cloud Server, ThingWorx, and IBM Watson are attempting to turn their IoT platform (PaaS) into a service. Cloud systems, as opposed to traditional IoT networks, have greater computational, storage, redundancy, and analysis capabilities. Many exciting solutions (augmented by the cloud computing model) for real-world challenges, such as traffic management in the Internet of Vehicles, are proposed (IoV) [38][39]. It is one of the fastest growing areas of research that relies entirely on high-speed cloud computing. The Open Automotive Alliance (OAA) is investing a great deal of technical resources to realise an IoV-based Intelligent Transportation System (ITS) [40][41]. It is worth mentioning that future IoT systems need hybrid computing capabilities ranging from low-power IoT nodes to mid-end gateways to high-compute cloud networks.

3.5. Services

The Internet of Things (IoT) is a vast network of heterogenous devices, infrastructure, protocols, and applications. In the previous section, we looked at several IoT architectures that provide a variety of services for vertical market integration. SOAs (Service Oriented Architectures) provide an abstraction layer that connects objects to application layers. The underlying device complexities in the technology stack are greatly simplified by an abstraction layer, allowing for easier vertical market integration. However, the addition of an abstraction layer alters the system architecture at both the OS and Middleware levels. A few researchers also proposed simplifying the architecture by integrating web services directly into IoT sensors [42][43]. This strategy not only eliminates the need for abstraction, but it also ensures rapid production and deployment.

Although several service models are available, the long-term objective is to incorporate scalability, interoperability, and easier market integration. However, the categorization will distinguish between different IoT service industries and service models in terms of their services. Mathew Gigli et al. [44] presented an IoT service model based on four categories, including, identity-related services, information aggregation services, collaborative-aware services, and ubiquitous services. These categories use processes that integrate components into various layers of the technology stack. The object identification service helps to sense and identify the virtual object, which is passed on to the information aggregation layer for data aggregation. Collaborative-awareness is achieved by aggregation of information gathered from similar service profile end devices. The omnipresence of IoT intelligence is the desired end goal that can be accomplished by creating collaborative-conscious services that are intelligent enough to make automated decisions. Applications that require user-related data (such as in banking, health care, smart homes) may contain confidential information that can enable user-tailored ubiquitous services. However, the actual implementation of ubiquitous services still seems complicated and challenging.

A category-specific application analysis is used to highlight the scope of these Services in the following context. The goal is to link the literature to application scenarios in which different services stack up to achieve ubiquitous computing. Intelligent automation and orchestration are expected to be features of future ubiquitous IoT environments. RFID-based technologies are frequently used by early adopters of WSN and IoT-based technologies, including application domains such as logistics, digital storage, and fleet management. M2M systems, which include mobile, GPS, and internet technology, have been used in recent years to automate logistics operations and track goods in real time [45][46]. These examples classify applications on the basis of identity-related classes in the service model. Some of the top developments in the logistics industry, where identity-related information is mainly used, are location management systems and inventory and tracking systems [47][48]. Intel reports that almost 30% of perishable produce from farms never make it to the markets [49]. Object and inventory tracking can help track products such as farm produce, pharmaceuticals, and industrial chemicals in real-time, thus saving a fortune annually.

Logistics 4.0 enables to monitor the shipment quality and object tracking in real-time. Real-time logistics tracking systems are commonly used in the transportation of pharmaceuticals, industrial hazardous chemicals, and life-saving drugs [50][51]. On-board sensors transmit information on shipping in real-time, which lets companies not only monitor items but also ensure the optimal consistency of handling procedures. Next, ITS systems are known to be a core component of the information aggregation class. These networks include a range of subsystems, such as smart parking, smart roads, traffic management, and control systems. The sensor information from these subsystems is aggregated to ensure a consistent and safe transport experience. The aggregated information is then passed to the upper collaborative-aware services model in order to thoroughly investigate the data and make smart decisions [46]. Connected vehicles utilize this concept to leverage a collaborative-aware service model, to make real-time collaborative decisions. Driver-less cars use this service model to adapt to road and weather conditions, avoid highway congestion, and book parking spaces in advance [38][52].

Connected vehicles or smart vehicles use this concept to leverage information gathered from all of the modules mentioned above and present it to the cloud via a Collaborative-aware service mode, where real-time decisions are made, allowing for the driverless self-driving vision of cars to become a reality. Google is widely regarded as a pioneer in the development and deployment of self-driving vehicles. It creates a collaborative-aware experience for driverless cars by combining user-generated data and cloud-based machine learning models [53]. The technology has advanced so much that autonomous cars have reportedly already driven more than 4 million miles [54]. Scientific standardisation is constantly updating its blueprint to keep up with such fast-paced research and deployments. IEEE 802.11p included amendments to support short-range communication vehicles.

Wireless Access for Vehicular Environments (WAVE) [55] is an approved standard for ITS systems. The National Highway Traffic Safety Administration, USA (NHTSA) has been working closely with research organizations, standards bodies, and academic institutions to advance the goal of Vehicle-to-Vehicle (V2V) communications [56].

Researchers investigated the self-configuration capabilities of future IoV systems that support the standardized technologies and protocols [57]. In a recent report on the readiness of V2V Technology, NHSTA reported a decline in the annual deployment costs of V2V technology. The study further proposed that cross-industry standardization not only decreases the cost of development but also assures a quick rollout. Standardization also helps eliminate loopholes in the area of transportation which can be crucial, and in some cases, life-saving. The report also stated that if V2V safety applications are adopted, it could prevent 25,000 to 592,000 car crashes annually [58]. This report provides vital statistics regarding technological advancement and the standardization efforts towards the internet of connected vehicles.

Another important IoT area that is rapidly expanding is the Industrial Internet of Things (IIoT). In most cases, IIoT systems are associated with high-volume, high-speed data streams. A typical IIoT system is ideally a low-power, small-form-factor sensor or actuator node with internet connectivity that can relay sensed data to the cloud. The cloud-based ML models are then required to automate the industrial systems in near real-time.

Many industrial IIoT architectures and their integration with existing automation platforms require a layer of abstraction. Siemens, one of the world's most prominent industrial automation leaders, proposed the addition of a connectivity layer to the present automation products and technologies. This concept is integrated into its cloud-based industrial automation solution, the MindSphere [59]. Lastly, smart cities can be observed as an application of the ubiquitous services class [60][61][62]. It is a system of numerous smaller subsystems, including smart homes, smart grids, ITS and environmental response systems, that form a completely pervasive system focused on collaborative awareness [63][64][65][66].

3.6. Semantics and Analytics

Intelligence and autonomy at the device level are needed in order to achieve ubiquitous computing where devices can self-configure and adapt to their environment [67][68]. The autonomy of future IoT networks is projected to minimize working loads by accurately, efficiently, and smartly collecting, processing, and modelling the information [69]. A semantics framework is needed that provides granularity to distinguish between a multitude of objects and their attributes in the IoT networks [69][70][71]. Such a system helps to define and understand the correct object, and can demand the appropriate resource for the desired feature or behavior, thus acting as the central intelligence or brain of the overall operation [72].

Resource Description Framework (RDF) and its variants have been widely deployed to map attributes to the data. The semantic frameworks are used at various levels in the architecture to make the overall data trustworthy. A semantic framework for translating between different technologies and protocols may be used at the lower layers as a gateway, whereas at the higher layers it can be used for data collection. Word Wide Web Consortium (W3C) Semantic Sensor Network (SSN) ontology and annotation framework is one such example [73]. Effective XML Interchange (EXI), a lightweight representation of Extensible Markup Language (XML), is often commonly utilized for constrained devices [74].

The researchers investigated RDF frameworks to efficiently store and retrieve data from IoT devices. Rahman et al. [75] proposed a lightweight, dynamic ontology-based IoT scheme. The proposed scheme develops dynamic feature-based clusters using ML models. This abstraction of the ML-based SSN ontology scheme reduces query response latency as well as memory footprints. Padiya et al. [76] used the RDF model to analyze vast amounts of IoT-based sensor data management. They used various RDF storage mechanisms to store and retrieve data efficiently. The study also compares vertical portioning and hybrid data-aware methodology, concluding that the latter technique yields a 12% increase in results. Although the reviewers have analyzed a comprehensive data collection using various data storage and retrieval models, it is still unclear how it compares with the other EXI or JSON-LD techniques. It is also uncertain if the solution can be adequate to ensure the interoperability between various layers and systems. In general, the research model and the test bed will serve as excellent starting points for a detailed analysis of data management in IoT systems.

Hasemann et al. [77] presented a rather fascinating use-case focused on asymmetric data transfer by IoT devices. Their approach is based on IoT networks that publish a large amount of data, but receive relatively few updates. They incorporated serialization for RDF documents and opted for streaming Header-Dictionary-Triples (HDT) serialization to encrypt sensor data, resulting in a reduced data lookup table size that enables the re-use of searching entities to further save resources. Along the same lines, lightweight serialization based on RDF documentation seems to be a promising approach, since it reduces the size of data collection and can be conveniently integrated. WiseLib is one of the most common lightweight serialization frameworks for constrained heterogeneous devices. The serialization maps various device role and behaviors to the data by encoding at the device level. On the one hand, reduced table sizes can help to store and retrieve data efficiently. On the other hand, the devices use additional computational power for the encoding of information. This also opens up debates about a major study gap in the benchmarks for IoT-related energy saving schemes.

Maarala et al. [78] presented an evaluation model to test various sizes of IoT networks and corresponding semantics reasoning data. Maintaining performance, scalability, and interoperability as their primary goals, researchers calculated latencies imposed by various semantic models. During the assessment of semantic models, the researchers suggested data aggregation strategies suitable for the heterogeneous IoT network. The experimental results claim that distributed reasoning with Entity Notation (EN) formats outperforms other techniques. The results also summarized the possibility of having multiple reasoning nodes with a short EN format as the best case. The researchers also proposed that time-based aggregation produces a more stable output as compared to other strategies. Many researchers also focus on content caching schemes that reduce the energy consumption footprint for IoT networks [79].

The research provided a rigorous model for analysing emerging semantic technologies and determining the best supply cases. The effects of data formats on centralised structures, on the other hand, have not been reported. Another notable trend in their research is the similarity and uniformity in latencies as system resources or overall throughput increase, whereas this may not be the case in real-world heterogeneous IoT systems.

References

1. Stankovic, J.A. Research Directions for the Internet of Things. IEEE Internet Things J. 2014, 1, 3–9.
2. Kiljander, J.; D'Elia, A.; Morandi, F.; Hyttinen, P.; Takalo-Mattila, J.; Ylisaukko-Oja, A.; Soininen, J.P.; Cinotti, T.S. Semantic Interoperability Architecture for Pervasive Computing and Internet of Things. IEEE Access 2014, 2, 856–873.
3. Singh, D.; Tripathi, G.; Jara, A. Secure layers based architecture for Internet of Things. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 321–326.
4. Alsubaei, F.A.A.; Shiva, S. An Overview of Enabling Technologies for the Internet of Things. In Internet of Things A to Z; Book Section 3; John Wiley & Sons, Inc., Wiley Online Library: Hoboken, NJ, USA, 2018.
5. ITU. An Overview of Internet of Things. 2012. Available online: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items (accessed on 26 November 2021).
6. Krčo, S.; Pokrić, B.; Carrez, F. Designing IoT architecture(s): A European perspective. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 79–84.
7. Khan, R.; Khan, S.U.; Zaheer, R.; Khan, S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 2012 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17–19 December 2012; pp. 257–260.
8. ITU. The BUTLER Project Overview. 2012. Available online: https://www.slideshare.net/legallf/butler-project-overview (accessed on 3 November 2021).
9. Zhihong, Y.; Yingzhao, Y.; Yu, Y.; Yufeng, P.; Xiaobo, W.; Wenji, L. Study and application on the architecture and key technologies for IOT. In Proceedings of the 2011 International Conference on Multimedia Technology, Hangzhou, China, 26–28 July 2011; pp. 747–751.
10. Patel, Z.D. A Review on Service Oriented Architectures for Internet of Things (IoT). In Proceedings of the 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–12 May 2018; pp. 466–470.
11. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.

12. IETF. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). 2007. Available online: https://tools.ietf.org/pdf/rfc4919.pdf (accessed on 3 November 2021).
13. Korte, K.D.; Tumar, I.; Schönwälder, J. Evaluation of IPv6 over low-power wireless personal area networks implementations. In Proceedings of the 2009 IEEE 34th Conference on Local Computer Networks, Zurich, Switzerland, 20–23 October 2009; pp. 881–888.
14. Aftab, H.; Gilani, K.; Lee, J.; Nkenyereye, L.; Jeong, S.; Song, J. Analysis of identifiers in IoT platforms. Digit. Commun. Netw. 2020, 6, 333–340.
15. Kamina, T.; Aoki, T.; Eto, Y.; Koshizuka, N.; Yamada, J.; Sakamura, K. Verifying Identifier-Authenticity in Ubiquitous Computing Environment. In Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), Niagara Falls, ON, Canada, 21–23 May 2007; Volume 2, pp. 403–408.
16. Koshizuka, N.; Sakamura, K. Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things. IEEE Pervasive Comput. 2010, 9, 98–101.
17. Moghadam, A.Q.; Imani, M. A new method of IPv6 addressing based on EPC-mapping in the Internet of Things. In Proceedings of the 2018 4th International Conference on Web Research (ICWR), Tehran, Iran, 25–26 April 2018; pp. 92–96.
18. Seike, H.; Hamada, T.; Sumitomo, T.; Koshizuka, N. Blockchain-Based Ubiquitous Code Ownership Management System without Hierarchical Structure. In Proceedings of the 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, China, 8–12 October 2018; pp. 271–276.
19. Bryzek, D.J. Roadmap for the Trillion Sensor Universe. 2013. Available online: https://www-bsac.eecs.berkeley.edu/scripts/show_pdf_publication.php?pdfID=1365520205 (accessed on 26 November 2021).
20. PostScape. What Exactly Is the Internet of Things. 2015. Available online: https://www.postscapes.com/what-exactly-is-the-internet-of-things-infographic/ (accessed on 26 November 2021).
21. Wai, L.; Sharma, A. Smart sensing for IoT applications. In Proceedings of the 2016 13th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT), Hangzhou, China, 25–28 October 2016; pp. 362–364.
22. Martinez, B.; Monton, M.; Vilajosana, I.; Prades, J.D. The Power of Models: Modeling Power Consumption for IoT Devices. IEEE Sens.J. 2015, 15, 5777–5789.
23. Kansal, A.; Hsu, J.; Zahedi, S.; Srivastava, M.B. Power management in energy harvesting sensor networks. ACM Trans. Embed. Comput. Syst 2007, 6, 32.

24. Belleville, M.; Fanet, H.; Fiorini, P.; Nicole, P.; Pelgrom, M.J.M.; Piguet, C.; Hahn, R.; Van Hoof, C.; Vullers, R.; Tartagni, M.; et al. Energy autonomous sensor systems: Towards a ubiquitous sensor technology. Microelectron. J. 2010, 41, 740–745.
25. Amarlingam, M.; Mishra, P.K.; Prasad, K.V.V.D.; Rajalakshmi, P. Compressed sensing for different sensors: A real scenario for WSN and IoT. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 289–294.
26. Ali, O.; Ishak, M.K.; Bhatti, M.K.L. Adaptive clear channel assessment (A-CCA): Energy efficient method to improve wireless sensor networks (WSNs) operations. AEU—Int. J. Electron. Commun. 2021, 131, 153603.
27. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols: Review. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017; pp. 685–690.
28. Want, R. An introduction to RFID technology. IEEE Pervasive Comput. 2006, 5, 25–33.
29. Lian, X.; Zhang, X.; Weng, Y.; Duan, Z. Warehouse Logistics Control and Management System Based on RFID. In Proceedings of the 2007 IEEE International Conference on Automation and Logistics, Jinan, China, 18–21 August 2007; pp. 2907–2912.
30. Welbourne, E.; Battle, L.; Cole, G.; Gould, K.; Rector, K.; Raymer, S.; Balazinska, M.; Borriello, G. Building the Internet of Things Using RFID: The RFID Ecosystem Experience. IEEE Internet Comput. 2009, 13, 48–55.
31. Aghdam, Z.N.; Rahmani, A.M.; Hosseinzadeh, M. The Role of the Internet of Things in Healthcare: Future Trends and Challenges. Comput. Methods Programs Biomed. 2021, 199, 105903.
32. Islam, S.M.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K. The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access 2015, 3, 678–708.
33. Amendola, S.; Lodato, R.; Manzari, S.; Occhiuzzi, C.; Marrocco, G. RFID Technology for IoT-Based Personal Healthcare in Smart Spaces. IEEE Internet Things J. 2014, 1, 144–152.
34. Wu, F.; Rüdiger, C.; Redouté, J.; Yuce, M.R. WE-Safe: A wearable IoT sensor node for safety applications via LoRa. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 144–148.
35. Lee, H.C.; Ke, K.H. Monitoring of Large-Area IoT Sensors Using a LoRa Wireless Mesh Network System: Design and Evaluation. IEEE Trans. Instrum. Meas. 2018, 67, 2177–2187.
36. Alsulami, M.M.; Akkari, N. The role of 5G wireless networks in the internet-of- things (IoT). In Proceedings of the 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 4–6 April 2018; pp. 1–8.

37. Ijaz, A.; Zhang, L.; Grau, M.; Mohamed, A.; Vural, S.; Quddus, A.U.; Imran, M.A.; Foh, C.H.; Tafazolli, R. Enabling Massive IoT in 5G and Beyond Systems: PHY Radio Frame Design Considerations. IEEE Access 2016, 4, 3322–3339.
38. Dandala, T.T.; Krishnamurthy, V.; Alwan, R. Internet of Vehicles (IoV) for traffic management. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017; pp. 1–4.
39. Srivastava, J.R.; Sudarshan, T.S.B. Intelligent traffic management with wireless sensor networks. In Proceedings of the 2013 ACS International Conference on Computer Systems and Applications (AICCSA), Ifrane, Morocco, 27–30 May 2013; pp. 1–4.
40. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of Internet of Vehicles. China Commun. 2014, 11, 1–15.
41. Xu, X.J. Technology Is Changing What a Premium Automotive Brand Looks Like. 2018. Available online: https://hbr.org/2018/05/technology-is-changing-what-a-premium-automotive-brand-looks-like (accessed on 27 November 2021).
42. Riedel, T.; Fantana, N.; Genaid, A.; Yordanov, D.; Schmidtke, H.R.; Beigl, M. Using web service gateways and code generation for sustainable IoT system development. In Proceedings of the 2010 Internet of Things (IOT), Tokyo, Japan, 29 November–1 December 2010; pp. 1–8.
43. Dohndorf, O.; Krüger, J.; Krumm, H.; Fiehe, C.; Litvina, A.; Lück, I.; Stewing, F. Towards the Web of Things: Using DPWS to bridge isolated OSGi platforms. In Proceedings of the 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Mannheim, Germany, 29 March–2 April 2010; pp. 720–725.
44. Gigli, M.; Koo, S. Internet of Things: Services and Applications Categorization. Adv. Internet Things 2011, 01, 27–31.
45. Yongfu, L.; Dihua, S.; Weining, L.; Xuebo, Z. A service-oriented architecture for the transportation Cyber-Physical Systems. In Proceedings of the 31st Chinese Control Conference, Hefei, China, 25–27 July 2012; pp. 7674–7678.
46. Leng, Y.; Zhao, L. Novel design of intelligent internet-of-vehicles management system based on cloud-computing and Internet-of-Things. In Proceedings of the 2011 International Conference on Electronic & Mechanical Engineering and Information Technology, Harbin, China, 12–14 August 2011; Volume 6, pp. 3190–3193.
47. Di, H. Logistics management inventory model based on 5G Network and Internet of Things system. Microprocess. Microsys. 2020, 103429.
48. Maguire, E.; Moreno, K.W.; Moreno, H.S.; Gagnon, R. IoT Marches into the Enterprise, Transformation Follows Quickly. 2018. Available online: https://www.iotjournaal.nl/wp-content/uploads/2018/12/1-REPORT-FINAL-WEB.pdf (accessed on 27 November 2021).

49. Hullum, C. How Rogue Ales Makes a Great Beer from Wet Hops, Clean Water and Innovation. 2018. Available online: https://blogs.intel.com/iot/2018/02/06/how-rogue-ales-makes-a-great-beer-from-wet-hops-clean-water-and-innovation/#gs.hpkby6 (accessed on 27 November 2021).
50. Yang, G.; Xie, L.; Mantysalo, M.; Zhou, X.; Pang, Z.; Xu, L.D.; Kao-Walter, S.; Chen, Q.; Zheng, L.R. A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box. IEEE Trans. Ind. Inform. 2014, 10, 2180–2191.
51. Jara, A.J.; Alcolea, A.F.; Zamora, M.A.; Skarmeta, A.F.G.; Alsaedy, M. Drugs interaction checker based on IoT. In Proceedings of the 2010 Internet of Things (IOT), Tokyo, Japan, 29 November–1 December 2010; pp. 1–8.
52. Gerla, M.; Lee, E.; Pau, G.; Lee, U. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In Proceedings of the 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, Korea, 6–8 March 2014; pp. 241–246.
53. Stewart, J. Google Is to Start Building Its Own Self-Driving Cars. 2014. Available online: https://www.bbc.com/news/technology-27587558 (accessed on 27 November 2021).
54. Lumb, D. Waymo’s Autonomous Cars Have Driven 4 Million Miles. 2017. Available online: https://www.engadget.com/2017/11/27/waymo-autonomous-cars-drove-4-million-miles/ (accessed on 27 November 2021).
55. Uzcategui, R.A.; Sucre, A.J.D.; Acosta-Marum, G. Wave: A tutorial. IEEE Commun. Mag. 2009, 47, 126–133.
56. U.S. Department of Transportation. Factsheet: Improving Safety and Mobility through Vehicle-to-Vehicle Communication Technology. 2014. Available online: https://www.its.dot.gov/factsheets/pdf/safetypilot_nhtsa_factsheet.pdf (accessed on 1 November 2021).
57. Zhang, H.; Lu, X. Vehicle communication network in intelligent transportation system based on Internet of Things. Comput. Commun. 2020, 160, 799–806.
58. Transportation. Vehicle-to-Vehicle Communications: Readniess of V2V Technology for Applications. 2014. Available online: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf (accessed on 27 November 2021).
59. MindSphere, S. MindSphere: Enabling the World’s Industries to Drive Their Digital Transformations. 2017. Available online: https://www.plm.automation.siemens.com/media/global/en/Siemens-MindSphere-Whitepaper-69993_tcm27-29087.pdf (accessed on 27 November 2021).
60. Gea, T.; Paradells, J.; Lamarca, M.; Roldán, D. Smart Cities as an Application of Internet of Things: Experiences and Lessons Learnt in Barcelona. In Proceedings of the 2013 Seventh

International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Taichung, Taiwan, 3–5 July 2013; pp. 552–557.

61. Jin, J.; Gubbi, J.; Marusic, S.; Palaniswami, M. An Information Framework for Creating a Smart City Through Internet of Things. IEEE Internet Things J. 2014, 1, 112–121.
62. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. IEEE Internet Things J. 2014, 1, 22–32.
63. Pan, J.; Jain, R.; Paul, S.; Vu, T.; Saifullah, A.; Sha, M. An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments. IEEE Internet Things J. 2015, 2, 527–537.
64. Mohanty, S.P.; Choppali, U.; Kougianos, E. Everything you wanted to know about smart cities: The Internet of things is the backbone. IEEE Consum. Electron. Mag. 2016, 5, 60–70.
65. Acampora, G.; Cook, D.J.; Rashidi, P.; Vasilakos, A.V. A Survey on Ambient Intelligence in Health Care. Proc. IEEE Inst. Electr. Electron. Eng. 2013, 101, 2470–2494.
66. Wu, J.; Chou, D.; Jiang, J. The Virtual Environment of Things (VEoT): A Framework for Integrating Smart Things into Networked Virtual Environments. In Proceedings of the 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), Taipei, Taiwan, 1–3 September 2014; pp. 456–459.
67. Hall, M.W.; Gil, Y.; Lucas, R.F. Self-Configuring Applications for Heterogeneous Systems: Program Composition and Optimization Using Cognitive Techniques. Proc. IEEE 2008, 96, 849–862.
68. Matsuda, M.; Hase, T. Self-configuring and auto-executing audio-visual system for consumer use. IEEE Trans. Consum. Electron. 2003, 49, 642–646.
69. Sheth, A. Internet of Things to Smart IoT Through Semantic, Cognitive, and Perceptual Computing. IEEE Intell. Syst. 2016, 31, 108–112.
70. Datta, S.K.; Bonnet, C. Describing things in the Internet of Things: From CoRE link format to semantic based descriptions. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Nantou, Taiwan, 27–29 May 2016; pp. 1–2.
71. Yu, J.; Kwon, S.; Kang, H.; Kim, S.; Bae, J.; Pyo, C. A Framework on Semantic Thing Retrieval Method in IoT and IoE Environment. In Proceedings of the 2018 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 29–31 January 2018; pp. 1–6.
72. Barnaghi, P.; Wang, W.; Henson, C.; Taylor, K. Semantics for the Internet of Things. Int. J. Semant. Web Inf. Syst. 2012, 8, 1–21.

73. Compton, M.; Barnaghi, P.; Bermudez, L.; García-Castro, R.; Corcho, O.; Cox, S.; Graybeal, J.; Hauswirth, M.; Henson, C.; Herzog, A.; et al. The SSN ontology of the W3C semantic sensor network incubator group. J. Web Semant. 2012, 17, 25–32.

74. Consortium, W.W.W. Efficient XML Interchange (EXI) Format 1.0 (Second Edition). 2014. Available online: https://www.w3.org/TR/exi/ (accessed on 27 November 2021).

75. Rahman, H.; Hussain, M.I. A light-weight dynamic ontology for Internet of Things using machine learning technique. ICT Express 2021, 7, 355–360.

76. Padiya, T.; Bhise, M.; Rajkotiya, P. Data Management for Internet of Things. In Proceedings of the 2015 IEEE Region 10 Symposium, Macao, China, 1–4 November 2015; pp. 62–65.

77. Hasemann, H.; Kröller, A.; Pagel, M. RDF provisioning for the Internet of Things. In Proceedings of the 2012 3rd IEEE International Conference on the Internet of Things, Wuxi, China, 24–26 October 2012; pp. 143–150.

78. Maarala, A.I.; Su, X.; Riekki, J. Semantic Reasoning for Context-Aware Internet of Things Applications. IEEE Internet Things J. 2017, 4, 461–473.

79. Xu, C.; Wang, X. Transient content caching and updating with modified harmony search for Internet of Things. Digit. Commun. Netw. 2019, 5, 24–33.