Scientific Research Publishing

Advances in Internet of Things, 2022, 12, 35-64
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

Internet of Things: Towards a Solid Ecosystem of Interconnected Things

Mohamad Chakroun[1], Jinane Sayah[2], Chadi Kallab[3], Samir Haddad[3*]

[1]Faculty of Computer Science and Electrical Engineering, Universität Rostock, Rostock, Germany
[2]Issam Fares Faculty of Technology, Department of Telecom and Network, University of Balamand, Koura, Lebanon
[3]Faculty of Arts and Sciences, Department of Computer Science, University of Balamand, Koura, Lebanon
Email: mohamad.chakroun@gmail.com, *samir.haddad@balamand.edu.lb

How to cite this paper: Chakroun, M., Sayah, J., Kallab, C. and Haddad, S. (2022) Internet of Things: Towards a Solid Ecosystem of Interconnected Things. *Advances in Internet of Things*, **12**, 35-64.
https://doi.org/10.4236/ait.2022.123004

Received: April 20, 2022
Accepted: July 5, 2022
Published: July 8, 2022

Abstract

The Internet of Things (IoT) is a technological revolution that has changed everything we do and given us a new perspective on our daily lives, but despite the fact that numerous publications have focused on characterizing the many edges and technologies that make up an IoT system, the IoT ecosystem is still seen as too complex to be recognized as a stand-alone environment due to its significant diversity; hence, the objective of this research is to address such a complex environment in a way that highlights its components and distinguishes them both individually and in relation to their broader context. Therefore, the definition of IoT and its emergence were discussed and organized around the timeline of Internet development phases demonstrating that IoT has been a need that has accompanied the presence of the Internet since its early stages, and then its growth and impact were discussed and highlighted with estimates and numbers. On the technical side, each of the following groups, IoT components, protocols, and architectures, was defined, discussed, and grouped in such a way that their intergroup organization, as well as their placement and contribution to the overall ecosystem, was highlighted. This, in addition to the various examples mentioned throughout the discussion, will provide the reader with a better understanding of the Internet of Things and how deeply it has become entwined in our daily lives and routines as a result of its numerous applications.

Keywords

Internet of Things, IoT Components, IoT Architectures, IoT Economic Impact, IoT Growth, Networking Protocols, TCP/IP, IoT Protocols, IoT Challenges, IoT Attacks

1. Introduction

The internet of things, or IoT, is a network of computational and sensor-equipped devices that are ready to be connected and work in an internet-connected workplace, and where web-based software has provided the software development industry more flexibility by allowing a software/database running on a server to respond to client requests from a variety of different operating systems, the Internet of Things has added even more diversity, since an IoT project necessitates the usage of diverse devices, systems, and databases that can be hosted on various platforms and operated from various locations [1]-[7]. A shipping company, for example, could have a cloud-based system on which employees from various branch offices can submit orders, as well as another cloud-based system that tracks the activity of its drivers who collect items from company clients using a Global Positioning System (GPS), and a local server at the main branch of the company that uses sensors and other devices and analytical capacities to keep track of some stocks and send out alerts if the stock of a certain material has gone low [8] [9] [10] [11] [12].

In addition to the technological diversity shown in the preceding example, IoT systems are often made up of smart systems, which add to the system's complexity, Because each network item is strengthened by the IoT System in such systems, which enables it to perform even more efficiently by going beyond its basic functions and benefiting from the System's layers, consequently, having such a network expands the organization's prospects while simultaneously raising the obstacles it faces and the system's success, because even a small sensor's activities can be analyzed by software on the Cloud dedicated to tracking its activities and filtering the data submitted from it based on some algorithms to determine whether the captured data is contributing to the project's mission or not, and whether the data is accurate or noisy [4] [9] [10] [11] [13] [14] [15]. As an example, having a watch dedicated to tracking a patient's pulse may entail doing numerous tasks, each of which necessitates accuracy, pattern recognition, and a quick response time, where the system may instruct the watch not to measure the patient's pulse if the patient is roaming outside on a sunny day with a temperature above 30 degrees Celsius because the system has learned from previous data submitted by other patients that the sun affects human blood pressure under these conditions, and thus the sensor will be sending data that does not serve the purpose for which the system was designed [9] [10] [12] [16] [17].

Therefore, from a system-wide perspective, end-users, particularly non-technical users, believe that IoT provides relatively smooth and practical services because it packages a mix of data, devices, and a variety of processes in the form of an email that the user receives in case of extreme climate events, for example, or in the form of a short message on a cell phone (SMS) that the parents of a patient receive in case their relative with a weak heart is exposed to any crisis, thanks to an application on the patient's watch measuring the patient's vital signs [9] [10] [16].

Meanwhile, from another perspective, a closer look will reveal the convergence between the individual's integration into society and the interaction among all edges of such technical systems. They both expressed their different edges' need to interact, exchange, and develop themselves in a healthy and orderly environment, despite the fact that collisions, whose effects can be resounding, are difficult to avoid [5].

The complexity of such an environment stems from the fact that it utilizes a variety of platforms and technologies that have revolutionized every aspect of our lives, including networking, databases, software engineering concepts, cloud computing, and machine learning, as well as other factors such as design concepts and user interface, and such diversification appears complicated enough to appear as a mash-up of assimilated technologies, devices, and applications with no pre-determined boundaries or operating constraints.

As a result, if there hadn't been a science working behind the scenes to provide the necessary visions, practices, frameworks, and architectures to smartly boost this transformation from the age of traditionally connected devices to the era of smart connected things, which can interpret, decide, and lead in some scenarios, this transformation would not have happened [2] [4] [13] [15] [18], and the purpose of this paper is to identify the elements that makeup such an ecosystem and their responsibilities, as well as how they are organized within such a complex environment, what data transfer methods they use, and what architectures were proposed to guide the development of such systems, as well as to address other aspects of IoT such as defining it, highlighting its potentials, growth, impact, challenges and attacks.

This paper's sections will be organized as follows, Section 2 will examine several definitions from various angles, Section 3 will revise the rise of IoT and its economic impact, Section 4 will monitor the causes for IoT's widespread success, and Section 5 will describe the essential components required for any IoT system, then Section 6 will show the scope of the components, Section 7 will explain the networking concepts that will be used in the following Section 8 while discussing and grouping the most well-known IoT protocols, Section 9 will focus on showing how various architectures may be conceptually separated and briefly explain the important components of each of them. Before the conclusion, Section 10 will review challenges and attacks.

2. Definition

There are too many definitions of IoT in the literature, starting with Kevin Ashton, who was the first to define the term "Internet of Things" in 1999. "The internet of things has the potential to change the world, just as the internet did. Maybe even more so", says Ashton. With this definition, Ashton not only described the IoT, but also gave us a way to imagine the size that this science might take up in our future lives, which we'll talk about in the next section while comparing it to the evolution of the internet [11] [19] [20] [21].

To demonstrate even more the hopes that were placed in IoT, another definition has been added, this time from the standpoint of a corporation. According to the Cisco Internet Business Solutions Group, "IoT is simply the point in time when more things or objects were connected to the Internet than people", Cisco dates the advent of this technology around 2008-2009; based on this definition, it's possible to gain a sense of how far machine dependency will progress in the future [22].

Aside from the numerous definitions for the Internet of Things, there was a lot of bet on this new technology, and the importance of IoT was widely anticipated, as evidenced by the following preface of the United Nations International Telecommunications Union Report from 2005, which serves as a definition and detailed explanation for the future of IoT: "Technological advances in 'always on' communications promise a world of networked and interconnected devices that will provide relevant content and information to users, wherever they may be located. Machine-to-machine communications and person-to-computer communications will be extended to things, from everyday household objects to sensors monitoring the movement of the Golden Gate Bridge or detecting earth tremors. Everything from Tyres to toothbrushes will fall within communications range, heralding the dawn of a new era, one in which today's internet (of data and people) gives way to tomorrow's Internet of Things" [23].

3. Growth of IoT

Many studies have been done to demonstrate how successfully and efficiently the Internet of Things (IoT) can manage with heterogeneous edges when looking back at the phases that the IoT has gone through, especially in the last ten years [1] [5] [8].

Furthermore, the Internet of Things has proved that it is one of the few sciences that will take use of emerging technologies while reserving the right to innovate and update both the global environment in which it functions and the other parties it comprises [8], or else this entire methodology would have failed at the first hurdle, but not with IoT, which prompted the development of new architectures in a variety of disciplines, such as [16] from 2009, which introduced a fully integrated biomedical programmable sensor chip, or [2], which was able to capitalize on the momentum of a well-known and consistent phenomenon in the tech world, namely the Blockchain that underpins Bitcoins and many other cryptocurrencies [24] [25] [26].

Because Ashton's definition connects the potential capabilities of IoT to the actual capabilities of the internet, and because IoT arose from the growing need for more devices to connect to the internet, and for a better understanding of how these needs began to be translated into actual devices, this section will be divided into the following sections. Looking at the internet's growth phases, then see how much faith was placed in IoT, whether it performed as expected until 2020, and how much the IoT has the potential to impact an economy based on the number of connected devices [27].

3.1. Internet Development Phases

Given that Bernes-Lee launched the first website on the Internet in 1991, which had come to be considered the date when the Internet became publicly accessible, that day, however, is divisive because it masks years of growth, which some experts split into three parts [22] [28] [29] [30] [31].

- 1960-1985: The principles for partitioning data into packets that can be delivered across a network appeared, the appearance of wide-area networks, connecting computers with a telephone line, the appearance of local area networks, the appearance of the electronic mail system, and the invention of the TCP/IP protocol.
- 1985-1995: Increase in the number of personal computers (PCs) and local area networks (LANs) in use. The World Wide Web was born, and with it came the appearance of internet browsers, online stores, and other connected items.
- 1995-present: The number of websites on the internet is growing, making online shopping a popular trend. Web banks, online marketing, and internet music have all followed suit, as has the development of internet calls and videos, and eventually social media.

3.2. IoT Growth

Knowing that the term "Internet of Things" was coined by Ashton in 1999, but the concepts of "Internet of Things" had already permeated our daily lives, the first device connected to the internet was invented in 1982, when students from Carnegie Mellon university equipped a Cola fridge with micro switches to count the number of bottles and detect when the fridge was empty, after 1990, the number of connected devices began to increase dramatically, so don't be surprised if you come across an article from a 1998 newsletter with the title "Internet ovens and fridges are looming on the horizon" [8] [22] [32] [33].

The Internet of Things gained popularity quickly, and many organizations, industries, and government agencies embraced it. According to some cautious estimates, the number of linked devices in 2020 is predicted to be in the 30 billion, but some optimistic sources predicted over 40 billion by 2020, or even more, as in the case of Cisco, which predicted approximately 50 billion by 2020 (**Figure 1**) [10] [22] [31] [33] [34] [35] [36].

Have the expectations, on the other hand, been met? According to research, the forecasted device connectivity was more or less achieved; on average, the number of linked devices was approximately 40 billion in 2020, with 75 billion expected in 2025 [4] [31] [34] [35].

The increase in connection numbers might also be interpreted economically. A 10% growth in machine to machine (M2M) connections in the United States and Germany over the next 15 years (2018-2032) would result in an increase in the gross domestic product (GDP) of $370 billion in Germany and $2.26 trillion in the United States (**Figure 2**) [2] [37] [38].

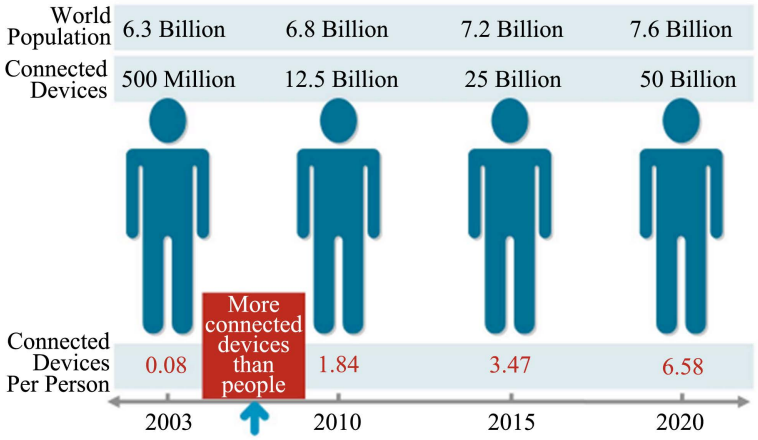

Figure 1. 2011 Cisco's IoT forecasts to 2020.

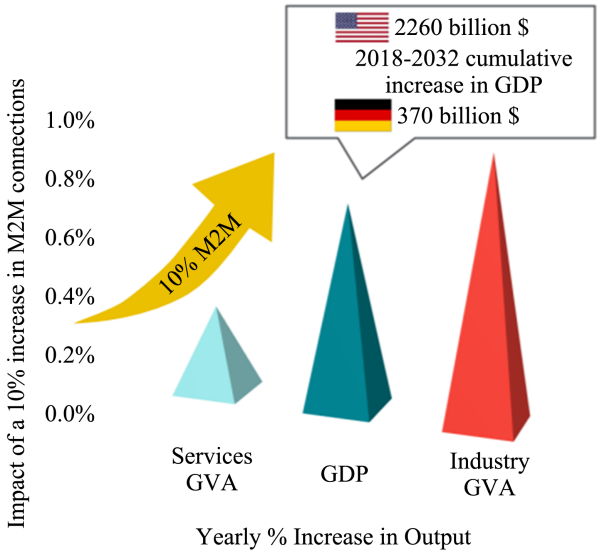

Figure 2. Impact of a 10% increase in M2M connections.

Furthermore, the advantages of IoT have become more tangible than ever before, not just on a local but also on a global scale. The entire universe recognizes the importance of data sharing in combating the modern chokepoint "Corona virus." To accurately characterize the current state of IoT (2020-2021), one must consider what life would be like without IoT, which leads to a series of further questions. What were the alternatives for the educational industry, which has changed to a digital-based operation in most areas of the world [39]? How would the health sector manage this pandemic if it didn't have all of the tools it needed to function super-efficiently, to the point that the systems in place to track the statistics around the world resembled a portfolio management system [40] [41]?

4. The Reasons behind IoT's Rapid Adoption

The success of IoT originated from the necessity for an efficient system that could get the most out of the diversity amongst linked items. We'll go through

some of the key aspects that contributed to IoT becoming a viable option [8] [27].

4.1. Positioning and Localisation Diversification

While many GPS-based projects were limited to outdoor use, IoT expanded such projects to include inside and underground locations where GPS reception was unavailable, which was critical for many industries like manufacturing and mining [9] [10] [42] [43].

4.2. Developing in Cloud Computing Abilities

One of the primary factors that have propelled IoT to where it is now is the advancement in networking capabilities, as well as the massive advancement in cloud computing [4] [8] [10] [11] [13].

4.3. Getting the Most Out of the Collected Data

IoT appears to utilize data more efficiently than any other science; the massive amounts of data pouring from sensors and cameras allow for greater pattern recognition and prediction of changes in consumer behavior, it enables businesses to prepare for any impending crisis [10] [37].

4.4. Entrusting Great Activities to a Slew of Sensors

The Internet of Things (IoT) has infiltrated every aspect of our lives, regardless of who benefits, whether it is an institution or a person, IoT has greatly contributed to both improving their lifestyles by sharing data and automating a significant portion of their daily routines, as well as by simplifying and shortening a series of processes, which leads to [3] [10] [18]:

- Reduced efforts/expenses: For example, the job of viewing a company's building, which traditionally required a surveillance team, might be shifted to a set of sensors and cameras, which can respond and take action much faster than humans because the sensor's response time is significantly faster [10] [44] [45] [46].
- Eliminating some costs: The user is now able to deal more closely with complicated things that they previously could not deal with because they were strictly close to technicians. For example, the user does not need to know how to fix a car, fridge or oven, but he will be able to replace a specific part of such Things as long as this Thing becomes smart and tells the user to do so, and it redirects the user to where the replaceable item can be purchased and how to replace it. As a result, some maintenance costs will be eliminated [3] [10] [11] [37].
- Eliminating some activities: Users will no longer have to worry about some things that are being automated by IoT, such as a coffee maker that orders coffee capsules automatically when the quantity of remaining capsules reaches a certain threshold [10] [14].

4.5. Great Efficiency and Precision

This growing reliance on IoT solutions is bolstered by the high levels of precision attained by machines, as in [47] which compared the human versus machines accuracy on visual scenes and objects to conclude the lack of evidence that human pattern matching techniques should take precedence over ordinary machine learning algorithms [11] [13] [14] [48] [49].

As a result, it's reasonable to conclude that this rapid adoption of the IoT, as well as the associated benefits, stem from the fact that individuals and entities are able to have more control over their daily routines because they finally found who granted them the ability to control these routines in an automated and flexible manner, allowing them to focus more on "business logic" rather than getting lost in their procedural activities [14] [50].

5. IoT's Main Components

The following are the essential components that make up an internet of things ecosystem.

5.1. The Thing

In the Internet of Things, there is no concrete limit to the term Things. This term could be applied to a wide range of objects: "Things were defined as anything and everything stretching from appliances to buildings to cars to people to animals, to trees, to plants, etc." [14] [34].

The fundamental role of devices and sensors is to collect data, which is the first layer of any IoT design, generally known as the Perception layer. Sensors were not introduced by IoT, industries had been dealing with sensors for some time, but IoT bolstered their use by simplifying their installation process and arranging communication among the many devices [6] [13].

Temperature sensors, motion and sound detecting sensors, light-detecting sensors, pressure sensors, proximity sensors, moisture sensors, gas and other chemical substance sensors, smoke sensors, and infrared sensors are among the many types of sensors available [14].

Furthermore, the device's job is not limited to detecting and receiving data from the environment in which it is positioned, but also to allowing things to move or go from working to sleep mode or the other way around in response to system orders, and this what is essentially done by an Actuator, which we deal with on a daily basis, for example, an actuator opens the store doors for us when motion sensors detect our presence, or it is what allows a water pump to turn on and off based on water level [51] [52].

Actuators differ in the type of motion they generate, which can be linear or rotational, as well as the source of energy they use to generate the mechanical motion. For example, an electric actuator converts electrical energy into mechanical motion, whereas other actuators use other sources of energy, such as hydraulic actuators, which convert hydraulic energy into motion [14].

5.2. Gateway

An IoT Gateway allows different devices to communicate with each other using different protocols. A greater understanding of a Gateway can be gained by thinking of it as a network router, as it not only provides bidirectional data transfer across multiple networks, but also performs additional functions such as basic data processing and providing security functions to identify any unauthorized access and prevent some attacks from impacting the system in addition to allowing different devices to communicate with each other or with the IoT platform using multiple protocols [1] [12] [14] [51] [53] [54].

5.3. Cloud Computing

Processing the data acquired by billions of devices, users and applications, as well as assessing the accuracy and competence of the data collected, is another critical part of IoT success. Cloud computing refers to the addition of computing capabilities to a system through the use of cloud services. It assists businesses by converting all acquired data into visions and paths that guide a company's future insights through analytics in order to improve their products and services [4] [18] [49].

Cloud computing ensures that a company's systems and services are always available, allowing it to get up and running faster than if it had to dedicate a room for its own server, which is usually accompanied by a variety of services and maintenance activities, including routers, switches, firewalls, database servers, and mail servers, among other things, all of which incur additional costs and time investments and expose the company to a variety of risks [2]. This may be avoided by using a cloud computing system like Google, which already has experts on staff who can ensure you have highly available, dependable, cost-effective, and secure cloud computing [33] [50] [51] [53].

5.4. Analytics

Analytics is a collection of managed services that make performing advanced analytics on massive amounts of IoT data simple and effective. It allows a firm to deduce crucial patterns and trends, as well as a better understanding of its consumers, from vast amounts of data. This results, for instance, in a company's sales and marketing operations being strengthened, as well as being much more sensitive to changes in their customers' needs [9] [18] [53] [55].

IoT systems are backed up by analytics, which serves as the key unit for making critical decisions. Analytics' importance is highlighted more in some industries that must respond in real-time to any recognized trend, such as fraud in banking or criminal acts that can be spotted by cameras [9] [10] [27] [49].

5.5. User Interface

End customers are more interested in how user-friendly the device is and how much it facilitates connecting to other devices they already own (such as a watch

or wireless music box) than in what types of complicated backend services are running or from which geographical location the services are responding to their requests. As a result, and because the user interface is a tangible aspect of the IoT system for customers, it will become a criterion for them to choose one device over another [9] [10] [18] [19] [27].

6. IoT's Components from a Wider Perspective

Because an IoT system is made up of various interconnected items, different connection scenarios can be observed in any IoT system. For example, a sensor may only need to interact with an actuator without sending data to the internet, as in the case of a sensor that detects motion and triggers an alarm, or this sensor may also need to send data to the internet so the user can receive an SMS on his phone while also triggering an alarm [18] [55].

Choosing which connectivity scenario should be provided to each device is based on the system preferences, but other factors such as overall security and privileges of users and devices should also be considered. Hence, to highlight where components are placed within the system's network based on their core purpose, this is how interconnected items in an IoT system might appear in **Figure 3** [13] [56].

A Thing at the network's edge can establish bi-directional connections with [4] [9] [13] [34] [42] [48] [53]:

- Another Thing (Sensor/Actuator) is to take rapid action without having to exchange data with an IoT platform.
- IoT platform, if the Thing creates IP-based data and has a SIM card or other means of connecting to the internet (WIFI, Ethernet), it can communicate directly with the IoT platform.
- A gateway If the Thing is unable to generate IP-based data, the gateway will convert the data the device exchanges with the IoT platform into IP-based data.

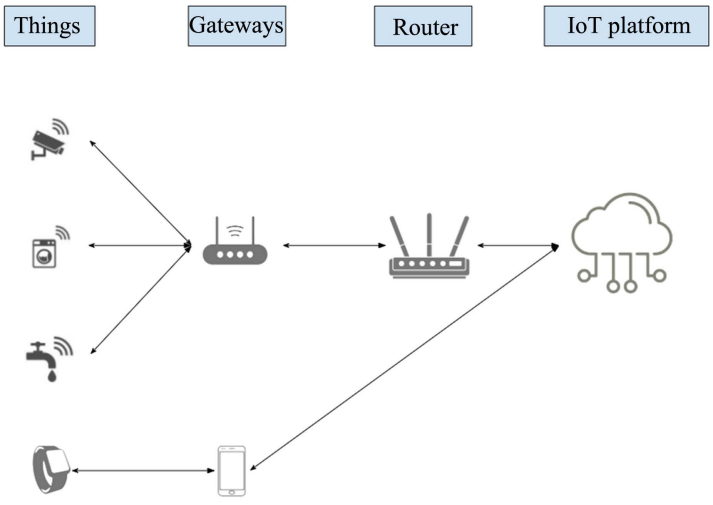

Figure 3. a broader view of IoT components.

- A router, if the device already generates IP-based data, it can be transferred to the IoT platform via a router.
- A smartphone, where an application is in charge of receiving data and sending it to the IoT platform.

A Gateway is in charge of bi-directional connections between Things and a router; it's capable of translating data from different protocols such as Z-Wave or ZigBee into IP-based data that can be exchanged with the IoT platform over the internet via the router. Therefore, even the Smartphone is also considered a Gateway because it can allow data to flow between a Thing and the IoT platform [4] [18] [31] [50] [53] [54].

7. Networking Fundamentals

This section will go over some of the networking fundamentals that will be needed in the next section, which will review and classify the various IoT protocols.

7.1. Network Topologies

The most often used IoT network topologies are [12] [27] [34] [37] [50] [53] [57] [58]:

- Peer-to-Peer: it only links two devices.
- Star: all edges in this network are connected to a central point that serves as a link between them; data sent from one edge to another will be routed through the central point.
- Mesh: The nodes in this network can connect directly to each other, and Mesh networks can be divided into two types: full mesh, which connects each node to the others, and partial mesh, in which some nodes are not connected to the rest of the nodes, requiring data to be routed through an intermediate node(s) [2].

7.2. TCP/IP Communication

TCP/IP is a set of communication protocols that govern how devices are connected via a network. TCP and IP stand for Transmission Control Protocol and Internet Protocol, respectively, and they are the two fundamental protocols in this set. IP is a necessary protocol for establishing a connection, but it has significant limitations due to its inability to track packets and detect problems. This is where TCP comes in, providing extra functions like error detection and packet tracking [13] [29] [31] [56] [59].

The TCP/IP Protocol Stack is divided into four layers: application, transport, internet, and network [31] [59] [60] [61] [62].

- The application layer represents the software with which the end-user normally interacts, such as a web browser.
- The TCP will take charge of the transport layer, the Data at this level is called "Segment", and communication between the TCP and the application layer is

done in terms of Port, so the TCP will know from what port the Segment is coming from. TCP, on the other hand, does not send a "Segment" all at once. Instead, it divides it into packets and attaches the necessary information as a header to each packet. The header will contain useful information about packet order so that TCP on the other machine knows how to order the packet, as well as error tracking information to let the other machine know whether a packet was properly received.

- After TCP has done its mission, the IP layer in the Internet layer will attach the sender and receiver IP addresses to each packet before passing it to the network layer.
- The Network layer will convert the packet (known at this level as "Frame") into a physical form and transfer it depending on the medium used to send the data.

7.3. Classification Based on TCP/IP Stacks

Because devices like a Hub, Switch and Router are more suitable for the networking type just described, this section will explain which layer of the TCP/IP model each piece of hardware belongs to, as the same categorization will be used to classify IoT protocols later [48].

Assume that five computers are connected to a Hub via network cables (Ethernet cables), which is a piece of hardware that resends any packets received to all devices connected to it. So, any packets received from any of the connected computers will be resent to the remaining four machines by the Hub. This means that the packet will be transmitted to machines other than the intended recipient, which creates security problems. However, the important thing here is that the Hub job is confined to resending the packet without revealing its contents or the IP addresses it includes. As a result, a Hub job is limited to the physical level of the TCP/IP model when comparing this work to the TCP/IP model's layers [17] [50] [59] [60] [62].

If a Switch is used in place of the Hub, which is likewise a hardware device, but unlike the Hub, the Switch will only deliver packets to the destination computer based on the packet's physical address, and when compared to the TCP/IP architecture, one may conclude that the job of a Switch is also limited to the physical level (network layer) [2].

Performing a job that corresponds to a layer above the Physical layer of the TCP/IP paradigm entails leaving a local area network, where a Hub or switch is usually used, and sending data over a larger network, which is the Internet, and this needs the use of a Router, which is also a hardware device that can read the IP connected to a packet, allowing it to determine where the packet should be routed next, hence, when compared to the TCP/IP model, the job of a router reaches the second level [48] [60].

8. IoT Protocols

This section will list the most popular IoT protocols, which will be organized

according to the TCP/IP model layers that were just covered in the previous section, and then Table 1 will compare some essential protocol elements at the end of this section.

8.1. Network Layer IoT Protocols

8.1.1. WI-FI

A simple example of a LAN would be a computer connected to the router via a cable, and on the same network, there might be a smartphone connected wirelessly to the router's access point (routers usually have a built-in access point), thus this part of the network is known as a wireless network or WLAN, and this is accomplished thanks to the Wi-Fi [9] [18] [37].

Wi-Fi is a wireless technology that uses radio waves (2.4 GHz and 5 GHz bands) to allow wireless devices to communicate with an access point. Wi-Fi has several advantages, including mobility, which ensures device connectivity while moving around. It also has a much quicker installation process, but data encryption is required to prevent unauthorized users from accessing the network and stealing your data [2] [57] [58].

8.1.2. Ethernet

Ethernet is one of the most common protocols for connecting devices that was created in the early 1980s to carry data between the edges of a local area network (LAN). Ethernet began with coaxial wire, and as time went on, new types of cables, such as twisted-pair copper cables and fiber optic cables, were added to the mix. Ethernet is known for being dependable and low-cost, but its speed is dependent on network traffic, and resolving connection issues is difficult [49] [63].

Table 1. IoT network and internet layers protocols specs.

Protocol	Range	Max Data Rate	efficient battery consumption
Wi-Fi 6	~100 meters	9.6 Gbps	No
ETHERNET	<100 meters	10,000 Mbps	-
BLUETOOTH	~100 meters	3 Mbps	yes
Wi-Fi DIRECT	~100 meters	250 Mbps	yes
NFC	~20 cm	424 Kbps	yes
BLE	~50 meters	3 Mbps	yes
ZIGBEE	10 - 100 meters	250 Kbps	yes
Z-WAVE	15 - 150 meters	40 Kbps	yes
6LOWPAN	~100 meters	250 Kbps	yes
LORAWAN	>15 km	50 kbps	extended (>10 yrs)
SIGFOX	3 - 50 km	1 Kbps	extended (>10 yrs)
NB-IOT	1 - 10 km	1 Mbps	extended (>10 yrs)
LTE-M	~50 km	1 Mbps	yes

8.1.3. NFC

First, RFID must be defined; RFID (Radio Frequency Identification) is a technology used, for example, in hotels to open doors using a card. It's a read-only technology that consists of a transmitter, which is the card, and a receiver, which is scanning the card, with data being transferred in one direction from the card to the reader [46] [64].

NFC (Near-Field Communication) is similar to RFID, but it allows two-way communication over a considerably shorter distance. NFC has a shorter range (maximum 4 cm) than Wi-Fi and Bluetooth, and unlike those technologies, it does not require a battery because it is based on the exchange of electromagnetic fields between two coils. An NFC connection is established when two devices are taped together. Contactless payment and smartphone cordless charging are two of the most prevalent applications for NFC [10] [12] [14] [17] [46] [57].

8.1.4. Bluetooth

This is a short-range communication protocol that is widely supported by most smartphones and PCs, and is the most well-known among wearable devices. It uses far less power than Wi-Fi [16] [18] [37].

8.1.5. Bluetooth Low-Energy (BLE)

BLE consumes a lot less power than regular Bluetooth and is designed for applications that need to function for a month or more on batteries. It's also used to send and receive small amounts of data in both directions. So, to illustrate the differences between the two technologies, a device that only supports conventional Bluetooth, such as wireless headphones, will not be able to communicate with a device that only supports BLE, such as a smart watch. As a result, BLE was introduced as a new technology aimed at Internet of Things (IoT) applications. BLE is mostly used in wearables, medical devices, and trackers [9] [16] [17] [18] [36] [49] [54].

8.1.6. Cellular IoT

Both (NB-IoT/LTE-M) are known as Cellular IoT and are considered the safest alternative for IoT connectivity because they operate in licensed spectrum. Furthermore, the SIM card allows secure connections due to the unique properties of LTE networks in terms of authenticating and encrypting data in transit [24] [36] [37] [43] [54].

- NB-IOT: Narrowband Internet of things is a low-power wide-area network (LPWAN); it is a protocol for cellular communication tailored for the purposes of IoT. It's usually used to convey data from a stationary site like in the case of smart metering. NB-IoT may handle both IP and non-IP communication modes, removing the need for a gateway and allowing devices to communicate with central servers directly [1] [36] [49].
- LTE-M: LTE-M is based on LTE (Long Term Evolution), often known as the 4G LTE, which provides the fastest 4G mobile internet connectivity. It provides significantly more capacity than NB-IoT for low-bandwidth data

communications. LTE-M differs from NB-IoT in that it supports mobility, including voice, and it's better for sending large messages, whereas NB-IoT is better for sending fewer data. This makes LTE-M much preferable for industrial controls and transportation tracking where there's no nearby coverage, such as Wi-Fi or Ethernet, and only small amounts of data need to be sent, such as reporting generator status. LTE-M, like NB-IoT, supports Non-IP Data Delivery (NIDD), which allows data to be transferred without the need for an IP address [1] [37] [49] [56] [58].

8.1.7. ZigBee

This is an additional wireless technology designed to transfer small amounts of data over short distances while using low power, but unlike Wi-Fi and Bluetooth, it was introduced specifically for control and sensor networks, which defines its main functions, which are to monitor and control devices. ZigBee is most widely utilized in IoT applications, and it's frequently used in home automation to interact with smart devices in order to collect data like temperature and execute control activities like turning on and off lights [9] [12] [17] [18] [37] [43] [53] [57] [61].

8.1.8. Z-Wave

It's a wireless smart home communication system that employs lower frequency bands around 1 GHz instead of the 2.4 GHz band used by Wi-Fi, Bluetooth, BLE, and ZigBee.

Furthermore, because it is mostly utilized in home automation, the 1 GHz band is thought to be less busy, reducing the possibility of interference with other devices. Z-Wave is simple to set up and use, although it transmits data at a slower rate than BLE [12] [17] [18] [49] [57] [61].

8.1.9. LoRaWAN

LoRaWAN is a low-power, wide-area wireless communication protocol in which devices are connected to The LoRaWAN gateway, which is responsible for transferring messages from connected devices to the internet, rather than to the internet directly. LoRaWAN is becoming more popular in Smart cities and industrial applications because it is a low-cost long-range bi-directional communication protocol with very low power consumption. Using the LoRaWAN protocol to connect street lights to a LoRa gateway is an example of smart street lighting [6] [9] [37] [56] [57].

8.1.10. WI-FI Direct

Wi-Fi Direct is a peer-to-peer communication protocol that links devices without the necessity of an intermediary access point. It operates at the same frequency and speed as Wi-Fi, allowing two devices to create a direct Wi-Fi connection without the need for an internet connection. Wi-Fi Direct is significantly faster than Bluetooth and consumes significantly more power and is supported by the majority of smartphones and tablets [2] [57].

8.2. Internet Layer Iot Protocols

6LoWPAN

IPv6 over Low Power Wireless Personal Area Network was created with the goal of making the Internet Protocol accessible to small devices [1]. As a result, 6LoWPAN is an IP-based network similar to Wi-Fi, and each device has its own IPv6 address, allowing it to connect to the internet. 6LoWPAN is a low-power wireless protocol that is widely used in home automation [12] [17] [37] [49] [54] [57].

8.3. Application Layer Iot Protocols

8.3.1. MQTT

This is a messaging protocol that, unlike typical protocols that rely on the direct connection between the device and the server, uses a different concept; it was first released in 1999 by IBM. MQTT has a sender and a receiver, referred to as the Publisher and Subscriber, respectively. In order to get specific messages to specific Subscribers, MQTT introduced the Topic concept, as well as the MQTT Broker, which is a central point to which all subscribers will be connected. A Subscriber will subscribe to a specific topic then, and the MQTT broker will filter the messages by topic, sending each message to the Subscribers who have subscribed to each Topic [12] [17] [53] [54] [56] [57].

8.3.2. XMPP

XMPP (Extensible Messaging and Presence System) is a well-known communication protocol that uses XML (Extensible Markup Language) tags to transmit and receive messages and presence status over a network in real-time, unlike MQTT, which uses a publisher-subscriber architecture, XMPP uses TCP sockets to create a client-server approach. Stanzas are snippets of XML tags that can be used to communicate between a client and a server for a variety of purposes. Message stanzas will be used to convey messages, whereas Presence Stanzas will be used to share status information and IQ Stanzas will be used to control server setup [2] [11] [17].

8.3.3. Sigfox

Sigfox is a communication technology that allows devices to communicate brief messages. Sigfox covers all TCP/IP stacks unlike the other protocols that have been examined so far, and the full Sigfox technological stack, including cloud servers and endpoint software, is owned by a French network operator (founded in 2010). Sigfox is already available in over 50 countries, with the other countries to follow soon.

Practical use of Sigfox is the monitoring of parking lots employing trackers that communicate to detect which places have been taken and which spots are still accessible. The three main components of Sigfox are objects, base stations, and the Sigfox cloud. The objects are the devices that send data to the Sigfox base station (antenna), which subsequently sends it to the Sigfox cloud, which stores and analyzes it [8] [19] [43] [49].

Sigfox utilizes less power and is effective over greater distances than other technologies like Bluetooth and Wi-Fi, which are designed for short-range and require more power [36] [37] [56].

9. Architectures

We will begin our discussion of architecture in this section by simplifying it according to the main tasks that an anticipated architecture should perform, so that the most important aspects of architecture can be highlighted and built on top of that to shed light on reference architectures that have the most clout among others.

Developers consider reference architecture to be the cornerstone of their work since it allows them to map their work to a guiding model; so, what are the key functions that architecture should provide, and who are the major players involved in a structure to make it consistent and sustainable? [50] [65]

In its most basic form, an IoT system architecture should enable the transmission of data from Things, which are essentially sensors, to the cloud over a network, as well as the transmission of commands or instructions derived from processing and analyzing the stored data to actuators, which represent the parts that allow the system to respond to its environment [8] [57].

There are four major actors in the data flow model above, in addition to the different activities that allow this flow to keep up with its mission [1] [8] [19] [53]:

- The devices are represented by sensors and actuators and which also include smart devices.
- Gateways and networks represent a means of gaining access to the world of the Internet.
- The platforms add a number of computational skills to the collected data, including the ability to store and analyze it.
- Applications that bring the user into contact with the real world.

Building on that, when moving on to discussing reference architectures, it's been noted that the key groups above have been restructured and adapted in the form of layers, all while maintaining the same essence [52].

There were numerous IoT reference architectures proposed by diverse parties, making it difficult for a system builder to pick amongst them. Domain-specific architectures, layer-specific architectures and industrial/commercial defined architectures are the three basic ways to categorize IoT architectures [52] [60] [66] [67] [68].

9.1. Layer Specific Architectures

Gubbi *et al.* introduced the 3-layers design in 2013, which is considered the most straightforward architecture among the others because it is made up of three layers and the majority of IoT architectural research starts here [57] [69].

9.1.1. The Three Layers Architecture

The components of this model are organized into three layers (**Figure 4(a)**) [13]

[42] [51] [57] [60] [69] [70]:

- The perception layer represents sensors, actuators, and other edge devices, or "things", this layer is in charge of tying the whole structure together with its surroundings.
- The Network layer sits on top of the Perception layer, allowing items to be extended by connecting them to other objects such as software, network devices, and servers.
- The Application layer sits on top of the Network layer, cloud and servers are typically found here, this layer is in charge of interacting with the user via data processing, data sharing, and services.

9.1.2. The Five Layers Architecture

The 5-layer design arose from an attempt to expand the constraints of the 3-layer paradigm by adding two additional layers, the business and processing layers (**Figure 4(b)**) [13] [30] [42] [57] [69] [71]:

- The application and perception layers are identical to those found in the 3-layer design. The application layer allows for the personalization of services and Perception layer maintains the system's contact with its surroundings.
- The network layer: send the Things data in both directions over networks (up and down).
- The Processing layer: the information received from the transport layer will be stored, analyzed, and processed by this layer.
- The Business layer: control the entire system, limiting or enabling processes, applications, and models.

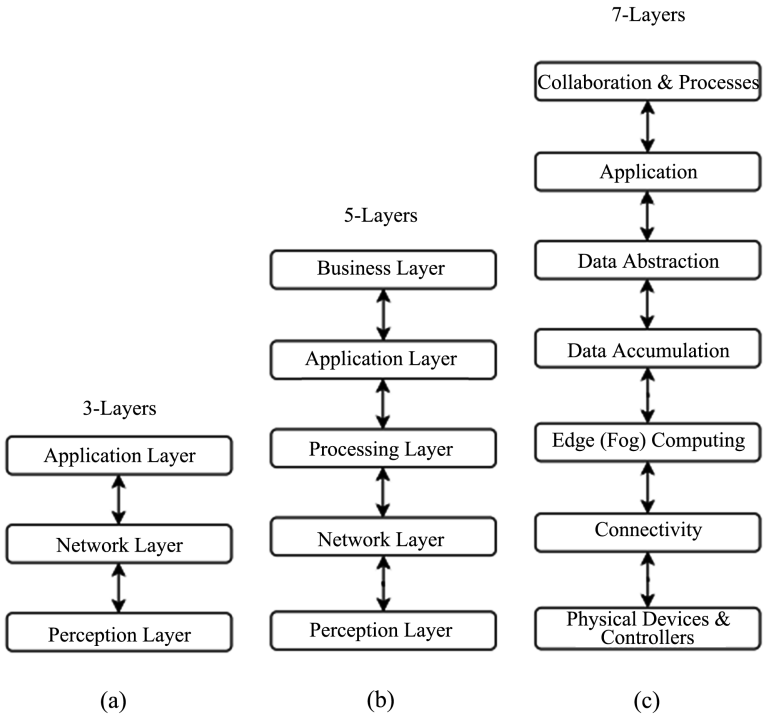

Figure 4. IoT layers architectures.

9.1.3. The Seven Layers Architecture

The 5-layers architecture is said to be more focused on data storage and processing, yet there are other critical factors such as security and privacy that the 5-layers architecture overlooks, hence, the 7-layer architecture is regarded as the complete model, the entire architecture is depicted as follows (**Figure 4(c)**) [1] [11] [13] [17] [33] [42] [57] [65] [69] [72] [73].

- Physical devices and controllers: this layer is made up of physical devices and device controllers.
- Connectivity: this layer is responsible for communication with and between level 1 devices, trustworthy network distribution, protocol translation, switching, routing, and other security issues, among other things.
- Edge computing/ Fog computing: Fog computing is having sensors and network gateways handle some of the data processing and analytics; these devices are referred to as edge computing since they are positioned at the network's edge. This entails equipping physical equipment such as cameras with smart data preprocessing capabilities.
- Data accumulation: this layer performs actions such as storage of things-data, big data, and data correctness checking in order to make the collected data meaningful and accessible to the system's applications.
- Data abstraction: data acquired from things is often known to be in many formats. Thus, the main responsibility of this layer is to identify any data format conflicts and ensure that data is delivered in a manner that can be accessed and processed by higher levels.
- Application: this level's major duties include monitoring device data, analyzing information, and reporting.
- Collaboration & processes: individuals and business processes are involved in this layer, where people use various applications and methodologies to extract the most value from IoT data in order to make the best business decisions.

9.2. Domain Specific Architectures

The layered reference designs serve as a starting point for system builders who want to place all of the previously stated components on the same network and get the most out of them. However, an IoT system for surveillance is not the same as one dedicated to the automotive industry, the nature of each project necessitates handling in different ways. For example, monitoring a line of robots requires far more sensors than monitoring a building, and the quality of the sensors is also different [3]. Furthermore, because robots work in a linked chain, task handover occurs in milliseconds or microseconds, necessitating real-time, lightning-fast reactions from the system [9] [73]. This meant that data had to be processed immediately, rather than being routed to the cloud to be analyzed before being sent back to the next robot while in a surveillance system, the system can wait for seconds to send data to the cloud, after which the data is analyzed to ensure that the detected motion is actually a robbery, the system can then take

the appropriate action, which could include reporting to a police station, sending Email, SMS, or sending back an instruction to the network to trigger an alarm [8] [10] [27].

As a result, one can see the difference between an IoT system and an industrial IoT (IIoT) system, which usually revolves around one point: IoT is more user-focused, as evidenced by the wearable products it offers or the applications on smartphones that a user uses to respond and interact with the system, whereas IIoT is more focused on improving industrial operations and preventing issues that could cost a significant amount of money [16] [64] [67] [69].

This is why industries required an adapted architecture, which led to the IIoT architecture. Similarly, other domains required an architecture that efficiently mimicked their processes, but since this is outside the scope of this paper, only the IIoT architecture is mentioned here because it covers the majority of industries [3].

9.2.1. IIoT Architecture

Industries, which include Manufacturing, Water, Energy, Telecommunications, Mining, and Agriculture [6] [74], are among the various areas addressed by IoT. The Industrial Internet of Things (IIoT) is the name given to this type of IoT application. Industries anticipate a highly qualified architecture that can meet the sector's expectations and put all of the Things that fall within the scope of IoT into action with the Industrial Software utilized by each industry [3] [13] [74].

Different variations of IOT architectures are examined in [75], which were mainly instantiated from the above x-layers architectures, and then they propose a potential Industrial IoT architecture for the manufacturing industry based on their review, which is composed of 4 layers as shown in **Figure 5**.

The first layer is Data, which is similar to the Perception layers previously discussed under the x-layers category, but with more features because data received through sensors, asset details, photos, and users will be classed with metadata before preliminary evaluations are made [3].

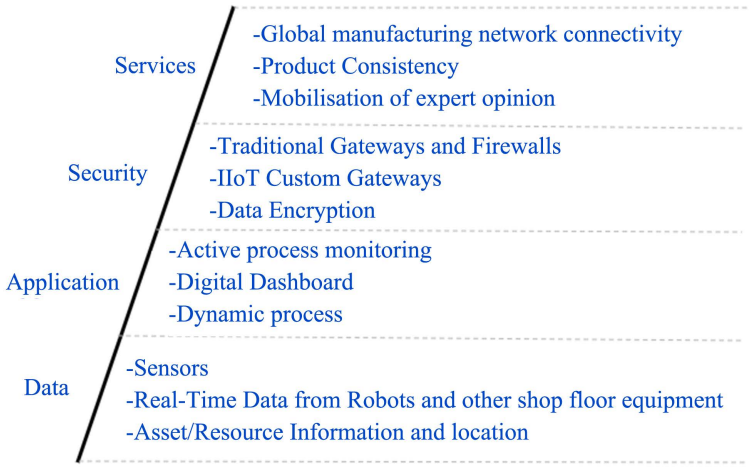

Figure 5. a proposed Industrial IoT architecture by [75].

The application layer is the next layer, where a Human Machine Interface (HMI) and a programming interface application must be built to meet the previously described requirements and to allow access to process-related data via monitoring programs that allow the workshop operator to track the development, then, on top of the application layer, a security layer was added, reflecting the need to ensure the system's safety due to the large number of edges, which typically include sensors, industrial controls, embedded systems, and other tools used for automation, and which outnumber the traditional edges considered in other environments [27] [52].

The fourth tier is the service layer, which establishes access to external devices and services. With the advent of cloud services, this layer has been extended to build links to suppliers and vendors as well as employ cloud computing services [11] [37] [75].

9.2.2. Industry-Defined Architecture

Because of the growing popularity of IoT and the rapid adoption of its various technologies, businesses are increasingly looking for a dependable IoT platform. As a result, some companies, such as Google, Cisco, Intel and IBM have developed their own designs and reference architectures, resulting in the third category of IoT architectures, known as industrial/commercial defined architectures [18] [33] [51].

Reviewing the architecture of each of these platforms is beyond the scope of this paper; we're only interested in putting everything learned together and figuring out how companies combined all of the components into one architecture, which is why one of the major industry players has been chosen, Amazon AWS IoT **Figure 6** [1] [8] [12] [18] [27] [52] [72]:

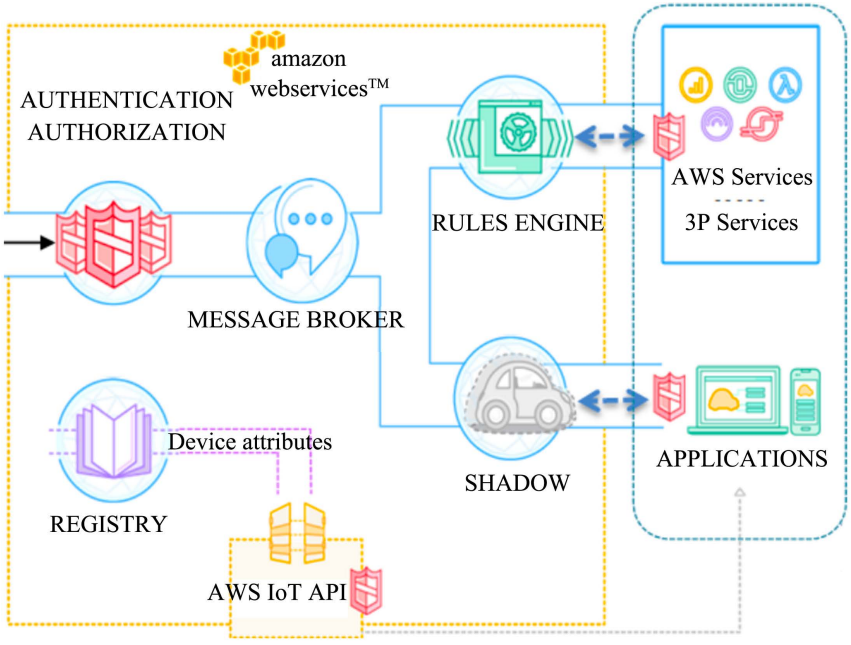

Figure 6. AWS IoT reference architecture.

- AWS IoT Core lets you manage IoT device connections to AWS services (or other devices), as well as message routing, authentication, and connectivity.
- The Device Gateway supports a variety of protocols, including MQTT, HTTP, and WebSocket, and ensures a stable and secure connection thanks to authentication and encryption, which prevents any untrusted data from going through.
- The rules engine allows the routing of messages to a device or to any AWS cloud service, such as Amazon S3, which is essentially a storage service, and it also allows you to query the messages using SQL.
- Device shadow permits dealing with active and inactive devices by preserving their statuses, allowing you to speak with them and transmit commands even when they are inactive. Synchronization will be maintained whenever the devices become active again.
- Thing Registry categorizes and organizes the resources connected with each Thing.

10. Challenges and Attacks

New challenges have emerged as a result of the new aspects and functions brought by IoT to traditional information and industrial systems, as well as the world of programmable Things in general. The challenges resulting from such a major evolution emerged at multilateral levels, as illustrated in this section [18] [64] [65] [76].

10.1. Challenges

The massive number of sensors and data sources utilized in IoT systems to collect data from the physical world and convert it into digital form for processing, transporting, or storing is becoming an increasingly essential challenge. Particularly because IoT primarily relies on Cloud computing services, which poses important problems about what data to store, where, and for how long, and by specifying such factors, not only the data management system, but the entire system performance will be impacted [13] [22] [27] [44] [45] [76].

Data collected from various Things within an IoT system does not always have the same formats, for example, a sensor that measures traffic density or light temperature does not send data in the same format as a microphone connected to a building's entrance or a camera that covers a specific area, so data heterogeneity is an important factor to consider at this level [17] [35] [54] [64] [77].

Other dimensions must be considered at this level as well, because the data collected touches almost every aspect of life, from our daily routines and activities to financial aspects and even more crucial data, bringing to the fore even more defining challenges, such as data-security, data-privacy, and data-integrity [4] [12] [18] [24] [42] [44] [56] [77].

Furthermore, a practical system would be expandable, taking into account the

increasing rate of emerging devices, which necessitates projecting the current system into the future to allow it to handle new protocols for newly connected devices while ensuring the availability of actual devices. It's worth noting that the emergence of new network devices comes with it new challenges, such as the maintainability of such devices, which originate from many manufacturers and so require a new platform to maintain [11] [12] [18] [37] [51].

10.2. Attacks

From a physical standpoint, security and privacy are a major challenge because interconnected objects may have some edges exposed outside of a building/area, making them vulnerable to piracy, especially wireless connected objects. For example, if a camera is hacked, it will be broadcasting the person(s) privacy in the wind, and not only the devices/edges are vulnerable, but rather the entire layers of an IoT system [13] [18] [44] [76] [77]. The most prevalent attacks are listed here and categorized by what they target the most.

Perception layer attacks [25] [33] [44] [56] [65] [78] [79]:

- Side-channel: the most common side-channel attacks are: Observing and studying the electromagnetic field radiation emitted by a computer monitor, Encryption key theft based on power consumption monitoring, spying on and capturing the sound of the user's keystrokes, which will be utilized to obtain user-key information.
- Tag cloning: is the process of exploiting user data obtained through a side-channel attack to gain access to confidential information or gain access to an unauthorized facility or data.
- Tampering devices: physical devices and sensors can be tampered with by attackers in order to gain control of them and modify data in various ways.
- Sensor tracking: manipulating sensors to follow and spy on user position, which is highly risky in medical IoT systems.

Network layer attacks [12] [25] [44] [49] [51] [56] [78] [79]:

- Eavesdropping: is the practice of monitoring data transmitted by sensors in order to gather information about users.
- Replay: recording and resending a network authentication request in order to gain access to a user software account or a device.
- Man in the middle: An attacker can gain access to data by exploiting a flaw in the system, allowing him to tamper with data and secretly repeat communications between authorized parties.
- Rogue access: the tracker/attacker will put up a fake wirelessly accessible gateway that the system users would believe is part of the system and they use it, allowing the attacker to execute a number of actions, such as storing the users' data [1].
- Denial of Service (DoS): is the act of flooding a device with requests, causing it to become completely paralyzed. This can then affect other interconnected services/devices, causing the entire system to become unavailable.

- Sinkhole: the attacker will start this attack by delivering better false services to real consumers and advertising them to them. Sinkhole attacks allow the attacker to carry out a variety of attacks, such as requesting user data or requesting that they download software onto their system so that they can monitor other users' actions.

Middleware attacks [1] [44] [79]:

- CSRF: Cross-site request forgery is a common occurrence in RESTful-based services, in which an attacker sends an email to a legitimate user with a link that leads to a specific request on the system, such as transferring funds or requesting an email address update. As a result, the attacker will attack the system via genuine users.
- Session hijacking, Cross-site scripting: in HTTP-based communication, when a legal user sends a request to a server, the web server, in order to identify the user in future requests and after successful authentication for the user, gives back a session-token, which is just a string. The session hijacking attack primarily focuses on stealing the session token, whereas cross-site scripting attempts to bypass the authentication procedure so that the attacker can establish a connection with the web server and conduct further requests, such as stealing the user's personal data.

Application layer attacks [6] [25] [44] [79] [80]:

- SQL injection: it entails injecting SQL queries into the server/application using the data given by the user. The attacker's main goal is to change administration restrictions/privileges, allowing him to access sensitive data or engage in other pirate activities.
- Ransomware: after executing other acts of piracy to get access to the user's machine/account, the attacker will encrypt the user's data and demand money in exchange for the password to decrypt the hard disk's content.
- Brute force: in order to obtain access to the system/device, the attacker will use an application/tool that will try all possible combinations of characters/numbers to guess a legitimate password.
- Business layer attacks [18] [44] [49] [77] [79]:
- Deception: the attacker's goal is to deceive data by using various types of attacks, such as "man-in-the-middle" or "sinkhole," which might have disastrous consequences depending on how data integrity is compromised.
- Disruption: performing DoS attacks to make the system or some services inaccessible will endanger humans' lives if the system is tied to Medical IoT.
- Information disclosure: performing some of the previously stated attacks on users' private data.

11. Conclusions

This paper covered a wide range of topics related to the Internet of Things, including defining it, explaining examples of its different applications, and pinpointing its emergence, which turned out to be a necessity that has accompanied the Internet since its inception.

Furthermore, we highlighted IoT's tremendous growth and success, where, as discussed, IoT has met at least the expectations in terms of numbers, use, and popularity, to the point where it now plays a critical role in ensuring people's safety and community security.

This paper also showed that IoT has gone beyond breaking the barrier of worry connected with data protection and privacy for many users, where the benefits have outweighed the disadvantages, and the reasons why people have embraced IoT were addressed.

Furthermore, more emphasis was placed on highlighting the complex infrastructure, including protocols and architectures, in a well-organized and thorough manner then we discussed some of the challenges and attacks that affect the IoT ecosystem.

Finally, other significant factors should be added to the findings of this paper because they will have a significant quantitative and qualitative impact on the future of IoT, such as the growth rate of IoT, which will not be the same as before cause IoT has gained widespread popularity and a solid foundation. And more importantly, the adoption of 5G technology, which is around 10 times quicker than 4G and is already being used in some countries, and how much it will accelerate IoT growth.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Pramudianto, F., Simon, J., Eisenhauer, M., Khaleel, H., Pastrone, C. and Spirito, M. (2013) Prototyping the Internet of Things for the Future Factory Using a SOA-Based Middleware and Reliable WSNs. 2013 *IEEE* 18*th Conference on Emerging Technologies & Factory Automation* (*ETFA*), Cagliari, 10-13 September 2013, 1-4. https://doi.org/10.1109/ETFA.2013.6648066

[2] Novo, O. (2018) Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, **5**, 1184-1195. https://doi.org/10.1109/JIOT.2018.2812239

[3] Oracle (2021) What is IoT? https://www.oracle.com/internet-of-things/what-is-iot/#link0

[4] Wu, F.J., Solmaz, G. and Kovacs, E. (2018) Toward the Future World of Internet of Things. *Proceedings of the* 2018 *Global Internet of Things Summit* (*GIoTS*), Bilbao, 4-7 June 2018, 1-6.

[5] Mihovska, A., Prasad, R. and Pejanovic, M. (2017) Human-Centric IoT Networks. In: Dixit, S. and Prasad, R., Eds., *Human Bond Communication*: *The Holy Grail of Holistic Communication and Immersive Experience*, John Wiley & Sons, Hoboken, 71-86. https://doi.org/10.1002/9781119341451.ch5

[6] Kovalchuk, V., Voitovich, O., Demchuk, D. and Demchuk, O. (2021) Development of Low-Cost Internet-of-Things (IoT) Networks for Field Air and Soil Monitoring within the Irrigation Control System. *International Conference on Computer Science*, *Engineering and Education Applications*, Kyiv, 21-22 January 2020, 86-96.

https://doi.org/10.1007/978-3-030-55506-1_8

[7] Gbadamosi, A.Q., Oyedele, L.O., Delgado, J.M.D., Kusimo, H., Akanbi, L., Olawale, O. and Muhammed-yakubu, N. (2020) IoT for Predictive Assets Monitoring and Maintenance: An Implementation Strategy for the UK Rail Industry. *Automation in Construction*, **122**, Article ID: 103486. https://doi.org/10.1016/j.autcon.2020.103486

[8] Celesti, A., Mulfari, D., Galletta, A., Fazio, M., Carnevale, L. and Villari, M. (2019) A Study on Container Virtualization for Guarantee Quality of Service in Cloud-of-Things. *Future Generation Computer Systems*, **99**, 356-364. https://doi.org/10.1016/j.future.2019.03.055

[9] Sadowski, S. and Spachos, P. (2018) RSSI-Based Indoor Localization with the Internet of Things. 2018 *IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference* (*IEMCON*), Vancouver, 1-3 November 2018, 24-29. https://doi.org/10.1109/IEMCON.2018.8614863

[10] Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., Castedo, L. and González-López, M. (2016) A Review on Internet of Things for Defense and Public Safety. *Sensors*, **16**, Article No. 1644. https://doi.org/10.3390/s16101644

[11] Vambe, W.T., Chang, C. and Sibanda, K. (2020) A Review of Quality of Service in Fog Computing for the Internet of Things. *International Journal of Fog Computing*, **3**, 22-40.

[12] Sobin, C.C. (2020) A Survey on Architecture, Protocols and Challenges in IoT. *Wireless Personal Communications*, **112**, 1383-1429. https://doi.org/10.1007/s11277-020-07108-5

[13] Gabr, B. and Azer, M.A. (2018) IoT Agile Framework Enhancement. 2018 1*st International Conference on Computer Applications & Information Security* (*ICCAIS*), Riyadh, 4-6 April 2018, 1-4. https://doi.org/10.1109/CAIS.2018.8441993

[14] Rayes, A. and Salam, S. (2019) The Things in IoT: Sensors and Actuators. In: Springer Nature Switzerland AG 2019, *Internet of Things from Hype to Reality*, Springer, Cham, 67-87. https://doi.org/10.1007/978-3-319-99516-8_3

[15] García-Magariño, I., Muttukrishnan, R. and Lloret, J. (2019) Human-Centric AI for Trustworthy IoT Systems with Explainable Multilayer Perceptrons. *IEEE Access*, **7**, 125562-125574. https://doi.org/10.1109/ACCESS.2019.2937521

[16] Zou, X.D., Xu, X.Y., Yao, L.B. and Lian, Y. (2009) A 1-V 450-nW Fully Integrated Programmable Biomedical Sensor Interface Chip. *IEEE Journal of Solid-State Circuits*, **44**, 1067-1077.

[17] de Moura Costa, H.J., da Costa, C.A., da Rosa Righi, R. and Antunes, R.S. (2020) Fog Computing in Health: A Systematic Literature Review. *Health and Technology*, **10**, 1025-1044. https://doi.org/10.1007/s12553-020-00431-8

[18] Ammar, M., Russello, G. and Crispo, B. (2018) Internet of Things: A Survey on the Security of IoT Frameworks. *Journal of Information Security and Applications*, **38**, 8-27. https://doi.org/10.1016/j.jisa.2017.11.002

[19] Hause, M., Hummell, J. and Grelier, F. (2018) MBSE Driven IoT for Smarter Cities. 2018 13*th Annual Conference on System of Systems Engineering* (*SoSE*), Paris, 19-22 June 2018, 365-371. https://doi.org/10.1109/SYSOSE.2018.8428705

[20] Ashton, K. (2010) That "Internet of Things" Thing. *RFID Journal*, **22**, 97-114.

[21] Avoussoukpo, C.B., Xu, C.X. and Tchenagnon, M. (2020) Polyvalent Wireless Communication System (PWCS): A Potentially Useful Technology for Opportunistic Networks. 2020 *IEEE International Conference on Artificial Intelligence and In-*

formation Systems (*ICAIIS*), Dalian, 20-22 March 2020, 762-766. https://doi.org/10.1109/ICAIIS49377.2020.9194809

[22] Evans, D. (2011) The Internet of Things, How the Next Evolution of the Internet Is Changing Everything. CISCO.

[23] International Telecommunication Union (2005) ITU Internet Reports The Internet of Things.

[24] Mistry, I., Tanwar, S., Tyagi, S. and Kumar, N. (2020) Blockchain for 5G-Enabled IoT for Industrial Automation: A Systematic Review, Solutions, and Challenges. *Mechanical Systems and Signal Processing*, **135**, Article ID: 106382. https://doi.org/10.1016/j.ymssp.2019.106382

[25] Srivastava, A., Gupta, S., Quamara, M., Chaudhary, P. and Aski, V.J. (2020) Future IoT-Enabled Threats and Vulnerabilities: State of the Art, Challenges, and Future Prospects. *International Journal of Communication Systems*, **33**, e4443. https://doi.org/10.1002/dac.4443

[26] Stute, M., Agarwal, P., Kumar, A., Asadi, A. and Hollick, M. (2020) LIDOR: A Lightweight DoS-Resilient Communication Protocol for Safety-Critical IoT Systems. *IEEE Internet of Things Journal*, **7**, 6802-6816. https://doi.org/10.1109/JIOT.2020.2985044

[27] Eclipse IoT Working Group (2016) The Three Software Stacks Required for IoT Architectures.

[28] Dimenstein, I.B. and Dimenstein, S.I. (2013) Development of a Laboratory Niche Web Site. *Annals of Diagnostic Pathology*, **17**, 448-456. https://doi.org/10.1016/j.anndiagpath.2013.05.002

[29] Mowery, D.C. and Simcoe, T. (2002) Is the Internet a US Invention? An Economic and Technological History of Computer Networking. *Research Policy*, **31**, 1369-1387. https://doi.org/10.1016/S0048-7333(02)00069-0

[30] Agarwal, A., Xu, L.D. and Whitmore, A. (2016) The Internet of Things: A Survey of Topics and Trends. *Information Systems Frontiers*, **17**, 261-274.

[31] Ma, X.B., Qu, J., Li, J.F., Lui, J.C.S., Li, Z.H. and Guan, X.H. (2020) Pinpointing Hidden IoT Devices via Spatial-Temporal Traffic Fingerprinting. *IEEE Conference on Computer Communications*, Toronto, 6-9 July 2020, 894-903.

[32] Boca Raton Newsletter (1998).

[33] CISCO (2014) The Internet of Things Reference Model.

[34] Ip, K., Asok, A., Xu, Y., Le, D., Mionis, N., Srinivasan, S. and Batoukov, R. (2020) ML-Assisted Monitoring and Characterization of IoT Sensor Networks. 2020 *IEEE Conference on Evolving and Adaptive Intelligent Systems* (*EAIS*), Bari, 27-29 May 2020, 1-8.

[35] Berhea, S., Maynardb, M. and Khomh, F. (2020) Software Release Patterns When Is It a Good Time to Update a Software Component? *Procedia Computer Science*, **170**, 618-625. https://doi.org/10.1016/j.procs.2020.03.142

[36] Sinha, R.S., Wei, Y.Q. and Hwang, S.H. (2017) A Survey on LPWA Technology: LoRa and NB-IoT. *ICT Express*, **3**, 14-21.

[37] Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M. and Guizani, S. (2017) Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. *IEEE Communications Magazine*, **55**, 16-24. https://doi.org/10.1109/MCOM.2017.1600514

[38] Rodríguez, J.M. and Stammati, L. (2018) The Economic Impact of IoT: Putting Numbers on a Revolutionary Technology. Frontier-Economics.com.

[39] Holton, K. and Sandle, P. (2020) Online Learning Rockets in Coronavirus Pandemic, Says Pearson. Reuters.

[40] Deutsche Welle (2020) Germany Gradually Warming up to COVID-19 Tracking App. https://www.dw.com/en/germany-gradually-warming-up-to-covid-19-tracking-app/av-53022217

[41] Deutsche Welle (2020) Germany Launches 'Best' Coronavirus Tracing App. https://www.dw.com/en/germany-launches-best-coronavirus-tracing-app/a-53825213

[42] De Donno, M., Tange, K. and Dragoni, N. (2019) Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog. *IEEE Access*, **7**, 150936-150948. https://doi.org/10.1109/ACCESS.2019.2947652

[43] Sotenga, P.Z., Djouani, K. and Kurien, A.M. (2020) Media Access Control in Large-Scale Internet of Things: A Review. *IEEE Access*, **8**, 55834-55859. https://doi.org/10.1109/ACCESS.2020.2982357

[44] Alsubaei, F., Shiva, S. and Abuhussein, A. (2017) Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. 2017 *IEEE* 42*nd Conference on Local Computer Networks Workshops* (*LCN Workshops*), Singapore, 9 October 2017, 112-120. https://doi.org/10.1109/LCN.Workshops.2017.72

[45] Biswas, A., Majumdar, A., Nath, S., Dutta, A. and Baishnab, K.L. (2019) LRBC: A Lightweight Block Cipher Design for Resource Constrained IoT Devices. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-01694-9

[46] Khoo, B. (2011) RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. 2011 *International Conference on Internet of Things and* 4*th International Conference on Cyber*, *Physical and Social Computing*, Dalian, 19-22 October 2011, 709-712. https://doi.org/10.1109/iThings/CPSCom.2011.83

[47] Parikh, D. and Zitnick, C.L. (2010) The Role of Features, Algorithms and Data in Visual Recognition. Toyota Technological Institute, Chicago and Microsoft Research, Redmond.

[48] El-Haddad, S., Genet, M.G., El-Hassan, B. and El-Nabbouch, D. (2008) MDSAP Simulation Using TinyOs and Hospital Application Modeling. 2008 *First International Conference on the Applications of Digital Information and Web Technologies* (*ICADIWT*), Ostrava, 4-6 August 2008, 133-138. https://doi.org/10.1109/ICADIWT.2008.4664332

[49] Merenda, M., Porcaro, C. and Iero, D. (2020) Edge Machine Learning for AI-Enabled IoT Devices: A Review. *Sensors*, **20**, Article No. 2533. https://doi.org/10.3390/s20092533

[50] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013) Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*, **29**, 1645-1660.

[51] Intel® (2015) The Intel® IoT Platform. Architecture Specification White Paper Internet of Things (IoT).

[52] Guth, J., Breitenbücher, U., Falkenthal, M., Fremantle, P., Kopp, O., Leymann, F. and Reinfurt, L. (2018) A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences. In: Di Martino, B., Li, K.C., Yang, L. and Esposito, A., Eds., *Internet of Everything*, Springer, Singapore, 81-101. https://doi.org/10.1007/978-981-10-5861-5_4

[53] Zhang, Z.Y. and Jin, Y. (2020) Design of Temperature Remote Monitoring System Based on STM32. 2020 *IEEE International Conference on Artificial Intelligence and*

Computer Applications (*ICAICA*), Dalian, 27-29 June 2020, 757-759. https://doi.org/10.1109/ICAICA50127.2020.9182397

[54] Yan, W.Y., Wang, Z.X., Wang, H., Wang, W.D., Li, J.H. and Gui, X.L. (2020) Survey on Recent Smart Gateways for Smart Home: Systems, Technologies, and Challenges. *Transactions on Emerging Telecommunications Technologies*, **33**, e4067.

[55] Nitti, M., Murroni, M., Fadda, M. and Atzori, L. (2016) Exploiting Social Internet of Things Features in Cognitive Radio. *IEEE Access*, **4**, 9204-9212. https://doi.org/10.1109/ACCESS.2016.2645979

[56] Nouraa, H., Hatouma, T., Salmanb, O., Yaacoubb, J.P. and Chehab, A. (2020) LoRaWAN Security Survey: Issues, Threats and Possible Mitigation Techniques. *Internet of Things*, **12**, Article ID: 100303.

[57] Barot, V. and Kapadia, V. (2020) Air Quality Monitoring Systems Using IoT: A Review. 2020 *International Conference on Computational Performance Evaluation* (*ComPE*), Shillong, 2-4 July 2020, 226-231. https://doi.org/10.1109/ComPE49325.2020.9200053

[58] Nour, B., Ibn-Khedher, H., Moungla, H., Afifi, H., Li, F., Sharif, K., Khelifi, H. and Guizani, M. (2019) Internet of Things Mobility over Information-Centric/Named-Data Networking. *IEEE Internet Computing*, **24**, 14-24. https://doi.org/10.1109/MIC.2019.2963187

[59] Alani, M.M. (2014) Chapter 3 TCP/IP Model. In: SpringerBriefs in Computer Science, *Guide to OSI and TCP/IP Models*, Springer, Cham, 19-50. https://doi.org/10.1007/978-3-319-05152-9

[60] Wu, M., Lu, T.L., Ling, F.Y., Sun, L. and Du, H.Y. (2010) Research on the Architecture of Internet of Things. 2010 3r*d International Conference on Advanced Computer Theory and Engineering* (*ICACTE*), Chengdu, 20-22 August 2010, V5-484-V5-487. https://doi.org/10.1109/ICACTE.2010.5579493

[61] Babun, L., Aksu, H., Ryan, L., Akkaya, K., Bentley, E.S. and Uluagac, A.S. (2020) Z-IoT: Passive Device-Class Fingerprinting of ZigBee and Z-Wave IoT Devices. 2020 *IEEE International Conference on Communications* (*ICC*), Dublin, 7-11 June 2020, 1-7. https://doi.org/10.1109/ICC40277.2020.9149285

[62] Cannon, D., O'Hara, B.T. and Keele, A. (2016) Networking Technology Basics. John Wiley & Sons, Hoboken.

[63] Zhao, L.X., Pop, P., Zheng, Z. and Li, Q. (2018) Timing Analysis of AVB Traffic in TSN Networks Using Network Calculus. 2018 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), Porto, 11-13 April 2018, 25-36. https://doi.org/10.1109/RTAS.2018.00009

[64] Jaafar, A.A., Sharif, K.H., Ghareb, M.I. and Jawawi, D.N.A. (2019) Internet of Thing and Smart City: State of the Art and Future Trends. In: Bhatia, S., Tiwari, S., Mishra, K. and Trivedi, M., Eds., *Advances in Computer Communication and Computational Sciences*, Springer, Singapore, 3-28. https://doi.org/10.1007/978-981-13-0344-9_1

[65] Sun, Y.C., Song, H.B., Jara, A.J. and Bie, R.F. (2016) Internet of Things and Big Data Analytics for Smart and Connected Communities. *IEEE Access*, **4**, 766-773.

[66] Guth, J., Breitenbücher, U., Falkenthal, M., Leymann, F. and Reinfurt, L. (2016) Comparison of IoT Platform Architectures: A Field Study Based on a Reference Architecture. 2016 *Cloudification of the Internet of Things* (*CIoT*), Paris, 23-25 November 2016, 1-6. https://doi.org/10.1109/CIOT.2016.7872918

[67] Sarkar, C., Akshay Uttama Nambi, S.N., Venkatesha Prasad, R. and Rahim, A. (2014) A Scalable Distributed Architecture towards Unifying IoT Applications. 2014

IEEE World Forum on Internet of Things (*WF-IoT*), Seoul, 6-8 March 2014, 508-513. https://doi.org/10.1109/WF-IoT.2014.6803220

[68] Kaur, H. and Kumar, R. (2020) A Survey on Internet of Things (IoT): Layer-Specific, Domain-Specific and Industry-Defined Architectures. In: Gao, X.Z., Tiwari, S., Trivedi, M. and Mishra, K., Eds., *Advances in Computational Intelligence and Communication Technology*, Springer, Singapore, 265-275.

[69] dos Santos, M.G., Ameyed, D., Petrillo, F., Jaafar, F. and Cheriet, M. (2020) Internet of Things Architectures: A Comparative Study. arXiv:2004.12936.

[70] Atmani, A., Kandrouch, I., Hmina, N. and Chaoui, H. (2019) Big Data for Internet of Things: A Survey on IoT Frameworks and Platforms. In: Ezziyyani, M., Ed., *Advanced Intelligent Systems for Sustainable Development* (*AI2SD*'2019), Springer, Cham, 59-67. https://doi.org/10.1007/978-3-030-33103-0_7

[71] Jamali, M.A.J., Bahrami, B., Heidari, A., Allahverdizadeh, P. and Norouzi, F. (2019) IoT Architecture. In: Towards the Internet of Things. EAI/Springer Innovations in Communication and Computing. *Springer, Cham*, 9-31. https://doi.org/10.1007/978-3-030-18468-1_2

[72] Atlam, H.F. and Wills, G.B. (2019) IoT Security, Privacy, Safety and Ethics. In: Farsi, M., Daneshkhah, A., Hosseinian-Far, A. and Jahankhani, H., Eds., *Digital Twin Technologies and Smart Cities*, Springer, Cham, 123-149. https://doi.org/10.1007/978-3-030-18732-3_8

[73] Wang, K., Wang, Y.H., Sun, Y.F., Guo, S. and Wu, J.S. (2016) Green Industrial Internet of Things Architecture: An Energy-Efficient Perspective. *IEEE Communications Magazine*, **54**, 48-54. https://doi.org/10.1109/MCOM.2016.1600399CM

[74] Boyes, H., Hallaq, B., Cunningham, J. and Watson, T. (2018) The Industrial Internet of Things (IIoT): An Analysis Framework. *Computers in Industry*, **101**, 1-12. https://doi.org/10.1016/j.compind.2018.04.015

[75] Caesarendra, W., Pappachan, B.K., Wijaya, T., Lee, D., Tjahjowidodo, T., Then, D. and Manyar, O.M. (2018) An AWS Machine Learning-Based Indirect Monitoring Method for Deburring in Aerospace Industries towards Industry 4.0. *Applied Sciences*, **8**, Article No. 2165. https://doi.org/10.3390/app8112165

[76] CISCO (2020) Cisco Annual Internet Report (2018-2023).

[77] Alsubaei, F., Abuhussein, A. and Shiva, S. (2018) Quantifying Security and Privacy in Internet of Things Solutions. 2018 *IEEE/IFIP Network Operations and Management Symposium*, Taipei, 23-27 April 2018, 1-6. https://doi.org/10.1109/NOMS.2018.8406318

[78] Smart, N.P. (2000) Physical Side-Channel Attacks on Cryptographic Systems. *Software Focus*, **1**, 6-13. https://doi.org/10.1002/1529-7950(200012)1:2%3C6::AID-SWF10%3E3.0.CO;2-W

[79] Owasp (2020) What Is an Attack? https://owasp.org/www-community/attacks/

[80] Rakovic, V., Karamachoski, J., Atanasovski, V. and Gavrilovska, L. (2019) Blockchain Paradigm and Internet of Things. *Wireless Personal Communications*, **106**, 219-235. https://doi.org/10.1007/s11277-019-06270-9