 doi:10.20944/preprints202111.0214.v2

Article

IoT: Communication Protocols and Security Threats

Apostolos Gerodimos[1], Leandros Maglaras [2], Ioanna Kantzavelou[3] and Nick Ayres[4]

1 School of Computer Science and Informatics, University of Thessaly, Lamia, Greece
2 School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK; leandros.maglaras@dmu.ac.uk
3 School of Engineering, Dept.of Informatics and Computer Engineering, University of West Attica, Athens, Greece; ikantz@uniwa.gr
4 School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK; nick.ayres@dmu.ac.uk
* Correspondence: leandros.maglaras@dmu.ac.uk; ikantz@uniwa.gr

Abstract: The IoT is recognized as one of the most important areas of future technology and is gaining vast attention from a wide range of industries. Although, after 20 years from the first published literature (2002) the technology (as a whole) is not yet mature. In this study we will review the fundamentals of IoT with a general approach, by addressing the problems of a standard architecture, vulnerabilities and use cases of this promising technology. Moreover, we will review some of the communication protocols that have invented especially for IoT technology, security threats and general implementation challenges. Discussion over the findings of this review reveals and specifies the next steps required to expand and support IoT systems in a protected framework.

Keywords: IoT; Security; Protocols; Threats

1. Introduction

Few decades earlier, the Internet revolutionized our world by connecting users across the globe simultaneously in real time. Today, the Internet of Things, which is also known as the Internet of Everything or sometimes referred to as the Industrial Internet, is a paradigm of technology envisaged as a network, connecting machines and devices globally and making them capable of interacting both with each other and the physical world autonomously within the existing Internet infrastructure.

By the term The Internet of Things, abbreviated to IoT, we refer to the innumerable tangible devices around the globe that can be connected to the internet. All of these devices collect and share data with each other while, simultaneously, eliminating the need for human-to-human or even human-to-computer communication. Thanks to the advent of computer chips at a remarkably low cost, the fact that wireless networks seem to be ubiquitous, and in addition, the advance of numerous technologies like machine – learning, big data analysis, smart sensors and especially 5G, it has become plausible to convert anything, regardless of its size, to a part of the IoT, since the technology can be applied to anything, as minuscule as a pill, or even as huge as a tanker ship. [1].

Although plenty of devices can connect to the Internet, we define IoT devices those that would not normally be supposed to have an Internet access, such as home appliances, health-monitoring devices or any kind of equipment and that, at the same time, have the ability to interact with each other without human involvement. Subsequently, neither a laptop nor a smartphone are considered as IoT devices, regardless of the fact that both carry sensors and communicate over the Internet. However, wearables, like smartwatches or fitness trackers could be regarded as ones. Nevertheless, it is possible for a PC or a smartphone to interact to an IoT network [2,3].

Connecting all these different objects, which are uniquely identifiable, and attaching sensors, transforms them to digitally intelligent devices, an attribute they would otherwise not possess. As a result, they are capable of communicating data in real time, subsequently

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2022 doi:10.20944/preprints202111.0214.v2

improving their efficiency, accuracy and making the environment surrounding us more clever and quick-to-respond, accomplishing the fusion of the digital and the physical world. [4].

This notion has multiplied the areas where it could be applied, which in turn, can improve the common welfare by making use of the means already available in ways never thought before and it is considered to be one of the most crucial fields of future technology that is becoming popular with an extensive number of industries [5]. Except from efficiency and accuracy, the interconnection of IoT devices opens a number of security threats to the users that can be connected to critical systems [6]. The authors in [7] have identified the major attacks on fog-based Internet of Things (IoT) applications.

The IoT technology forecast of connected devices is expected to increase by about 300% from 8.7 billion devices in 2020 to more than 25 billion IoT devices in 2030. In 2020, China was leading the IoT applications race with more than 3 billion devices in operation. The prevailing IoT devices are present in each industrial field and retail market. In particular, the retail market comprises around 60 percent of the total number of IoT devices in 2020. This allocation is predicted to remain unaltered in the next ten years. [8].

The contributions and novelty of this article are:

- Examines and describes a generic IoT architecture;
- Presents communication protocols;
- Identifies and describes current security threats in IoT;
- Examines present challenges and proposes efficient solutions.

The rest of this paper is organized as follows: In Section 2 we present the generic architecture of IoT and in Section 3 we give an overview of communication protocols used. Section 4 discusses security issues and concerns and gives a thorough understanding of IoT security threats. In Section 5 we present the main IoT applications. In Section 6 we discuss open security issues and challenges. Finally, Section 7 collects and discusses all the conclusions we draw from the presented research work.

2. A Generic IoT Architecture

In theory, the term IoT is commonly used to describe the design and implementation of a network that is successfully handling information data within the devices included in it. In practice though, since this network is the Internet, this is something challenging because all of the devices (Smart Sensors, Data Centers etc.) that are participating must be able to communicate seamlessly with each other, either directly or indirectly (i.e. Gateways), in a secure way. As a result, making all the devices of the Internet compatible is something that requires specific protocols for communication, standard structure, application compatibility, advanced Data Processing capabilities and many more. Despite their complexity in certain implementations, their elementary operation is quite simple [9].

A smart object transmits data collected by its sensors (physical world) to a data center, (either local or cloud-based), or even another smart object through an intermediate (gateway). The use of the gateway is not mandatory as the smart object can potentially work as a gateway too. Then, the data received "on the other side" are handled and multiple actions can be initiated. These actions are the ones that add complexity to the implementation because more interoperability is required to control or monitor an autonomous car, as to turn on the heater in certain degrees.

Although the IoT technology applies to a vastly major number of fields and is not standardized in any way, we will address a simple approach by reviewing the basic architecture and the most common protocols invented for this technology [10].

To define a reference architecture that supports current features and future extensions scalability, interoperability, data distribution, computing power and off course security, some fundamental factors must be considered regarding the architectural standardization, since several model architectures are described in the literature [11].

For example, in a systematic review about the Internet of Things architecture, examining more than 145 studies and their underlined architectures, we noticed that architectures

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2022 doi:10.20944/preprints202111.0214.v2

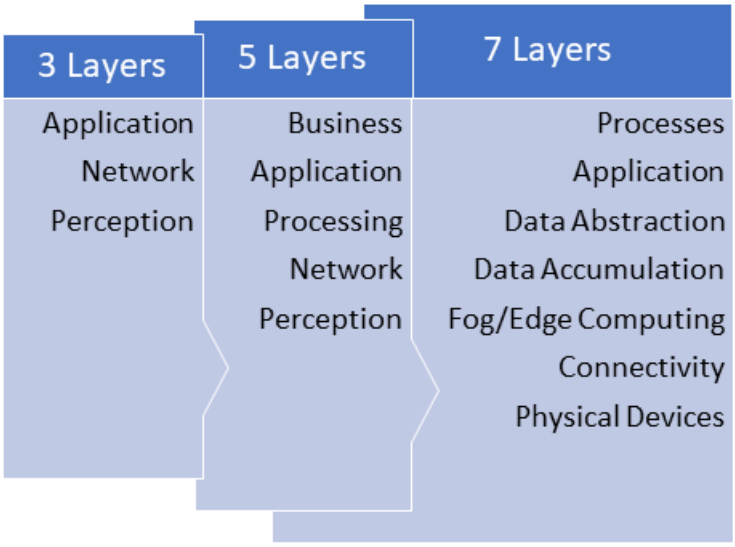

Figure 1. Elementary IoT Structure

in reference were mainly three-layer, four-layer or five-layer models, while in another survey the layer classification was applied in three-, four-, five-, six- or seven-layer models [12] (See Figure 1).

To make things more complicated, international organizations and big tech companies, like the International Telecommunication Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), Cisco, Google, Amazon and the European Telecommunications Standards Institute (ETSI), have presented different IoT frameworks based on application requirements, network topology, protocols, business and service models, as it encompasses a variety of technologies. [13].

Since there's still no single standard reference architecture for IoT and not an easy blueprint that can be followed for all possible implementations, in our approach we chose the 3-layer model that consists of the Perception, Network/Transmission and Application Layer, in which the layers in any case cannot be considered as sub-layers and can fully describe the elementary operations of an IoT implementation [14].

2.1. Perception Layer

The Perception or Physical Layer consists of the physical devices, which are the cornerstone of IoT technology, whose purpose is to collect information, transform them into digital data and pass them to another layer, so that actions can be done based on that information. Acting as a medium between the digital and real world, these physical devices can be Sensors (Temperature, Humidity, Light etc.), Actuators (Electric, Mechanical, Hydraulic etc.), RFID (RFID tags), [15], Video Trackers (IP camera) or anything that can use data to interact with different devices through a network.

The difference between the traditional sensors and the smart sensors used in IoT however is that smart sensors include an integrated microprocessor (DMP), that can process the digitized data captured by the sensor. These data can be normalized, noise filtered, or transformed for the sake of signal conditioning before being forwarded to other devices throughout the network.

2.2. Transmission Layer

The Transmission Layer that can also be found in the literature as Transportation or Network Layer, is located between the perception and the application layer. In this layer the data collected by smart sensors are transformed and forwarded to the Application Layer using the suitable communication channels and protocols for further processing,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2022 doi:10.20944/preprints202111.0214.v2

like analysis, data mining, data aggregation, and data encoding, while providing network management functionality and not only a basic packet routing as the network layer of the ISO/OSI model does.

In IoT implementations, wireless protocols are more commonly used compared to wired ones, since wireless sensors can be installed even in places that lack the main requisites for wired sensors like power, communication cabling etc. Moreover, in a wireless sensor network, it is easier for nodes to be added, removed or relocated without reconsidering the structure of the entire network. The selection of protocols to be used, can be based in several factors like hardware heterogeneity, power consumption, the transmission speed, and the transmission distance needed in each application and many others.

In other implementations however, a wired sensor network is preferred since these networks are more reliable, more secure and offer higher transmission data speeds. For example, IoT implementations in a hospital, where reliability and speed are major factors for saving a patient's life, wired sensors are preferable and the requisites for their installation can be planned during hospital's initial design (wiring, power delivery cables etc.).

In general, smart sensors must be able to communicate with each other through Internet to handle information and interact with the physical world, while being uniquely identified to prevent data conflicts. Depending on the specific applications, smart objects can be directly reachable without the need of an intermediary gateway, implement a UI making user interaction possible and many more.

2.3. Application layer

The Application Layer is present just above the Transmission Layer, it is based on the implementation, and can be organized in different ways. This layer, depending on the implementation, is responsible for analyzing and processing the information data that came from the below Layers (Perception and Transmission). More specific, it handles these data to applications in order to be used for the desired actions (i.e., control actuators), acting like a bridge to transform and forward it to other nodes or hand it over to another application for further processing.

Moreover, this is the layer where the user interface is placed (if any), giving the choice for users to interact with the IoT system and perform various actions (for example if a technical equipment needs servicing, the IoT will inform the technician through an interface that "structurally" is operating on the Application layer.

The Application layer, in contrast with Transmission and Perception Layer, can vary a lot based on the implementation. Since it is designed with a desired application in mind, this layer is formed by its functionalities. For example, real-time monitoring and decision-making applications are in charge of taking actions based on the data collected from the perception layer, information digitization is responsible for collecting and transforming analog data into digital, analytics are used to process collected data and create an evaluation model, while hardware control for transforming data into physical actions [16].

3. Communication Protocols

Many protocols contribute to an IoT implementation, but communication protocols are mandatory for IoT networks. To choose the best IoT protocol means accurately weighing the criteria of desired application range, power consumption threshold, information bandwidth and latency, Quality of Service, all viewed through the prism of security. As mentioned earlier, IoT devices use network standards and protocols to enable communication between physical objects connected through cloud. Network protocols and standards are policies that comprise certain rules that define the communication language between different network devices.

Every device generally is connected to the internet by using the Internet protocol (IP) but can also be connected locally via Bluetooth, NFC (near-field communication) and others. Some of the differences between both types of connections are power, range, and CPU power used. IP connections are complex and require increased power and memory,

 doi:10.20944/preprints202111.0214.v2

but there are no range limitations. Bluetooth connections, on the other hand, are simple and require less power and memory, but the range is limited.

Single devices like smartphones and personal computers use network protocols for communication, however general protocols used by these devices might not meet specific requirements like bandwidth, latency, and cover distance of IoT-based solutions. Although IoT devices are easy to deploy, their communication protocols are the ones that must bridge the lack of processing power, range, and reliability with existing internet infrastructure. Since the existing protocols are not meeting the criteria for IoT implementation (Wi-Fi 802.11 a/b/g/n/ac, etc.), we will review some new IoT protocols created for IoT application requirements.

For the reason that power consumption is an important factor when designing IoT networks, low power wireless network technologies are preferable. These technologies generally fall into two groups:

- Low Power Wide Area Networking (LPWAN) that provide extended range up to several kilometers, but with limited data rates for most (e.g., 6LoWPAN, LoRaWAN, Sigfox, NB-IoT, Wi-Fi HaLowTM);
- Wireless Personal Area Networking (WPAN) technologies, with range up to 100 meters and data rates up to 250 kbps for Zigbee and up to 3 Mbit/s for Bluetooth Low Energy.

3.1. LPWAN

LPWANs (Low Power Wide Area Networks) are a category of protocols developed for short range communications. Although "traditional" cellular networks are capable in supporting wide-area communication networks, their drawbacks, like complex infrastructure (Antennas, Amplifiers, etc.) and high-power consumption requirements, are making them a less favored solution when considering IoT applications. On the other hand, LPWAN protocols are to be used by simple, low-power, low CPU capabilities, allowing the deployment of sensors without investing in gateways, which are based on inexpensive batteries that last, making it a more favorable option in contrast to cellular networks.

With a low requirement hardware capability in mind, LPWAN technology can operate in more than 10 km distance depending on the surrounding and obstacles and data transfer rates from 0.3 kbit/s to 50 kbit/s per channel. Moreover, while power consumption and data rate are big challenges for LPWANs, Quality of Service (QoS) and scalability are important factors when selecting an LPWAN protocol. The 6LoWPAN protocol is an LPWAN protocol example, that combines IPv6 and LoWPAN technologies, and has many advantages, like exceptional connectivity, compatibility with earlier architectures, low-energy consumption, and ad-hoc self-organization.

3.2. WPAN

WPAN is a local mesh network of devices organized in a mesh topology, in which, every device is connected directly (without a gateway) with the other devices of the network and transfers data between each other, until it reaches the final recipient inside this network. This structure promotes network resilience, is simple to implement and costs less to set it up than other networks, particularly over large areas due to the absence of extra equipment (i.e., gateways).

ZigBee is considered the most popular mesh protocols used in IoT. It has a short-range but consumes minimal power, which can extend communication over several IoT devices. In comparison with LPWAN protocols, ZigBee can deliver high data transfer rates at a single instance, but with more power efficiency due to its mesh topology. However, due to their short physical range, ZigBee and every other mesh protocol are best suited for small to medium-range implementations, like smart home networks [17].

4. Security Issues and Concerns

Since IoT technology is designed to apply in many sectors that are crucial, especially for national security and economy with different industry standards and specifications,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2022 doi:10.20944/preprints202111.0214.v2

security issues require primary attention to minimize the attack surface and prevent security issues. For example, in 29 of April 2021, Microsoft's IoT security research group, discovered critical memory allocation vulnerabilities in IoT devices that could potentially be used to bypass security controls and execute malicious code or cause a system crash [18].

Beside cyber-attacks, the development of large-scale heterogeneous networks of constrained nodes engaging in real-time, should be based on an architecture that is resilient to manage factors arisen from Reliability, QoS, Modularity, Semantic Interoperability, Privacy Management, Hardware and Software Compatibility. Based on the 3-layer protocol, we will discuss in the following issues and concerns that address the security threats of each layer.

4.1. Perception Layer

The most important threats that endanger the Perception Layer have been selected and described in the sequel.

- Eavesdropping: IoT Devices are vulnerable to Eavesdropping Attacks because they lack the processing power for encryption techniques, in contrast to non IoT network devices. Additionally, if the devices are operating in a remote location with minimum or no physical monitoring, eavesdropping attacks are easier to implement more difficult to expose [19];
- Node Capture: Since there is a huge number of devices that can participate in an IoT network, network's attack surface increases exponentially. An attacker can potentially gain control over a network's key node, such as a gateway, which in turn gives him access to all the information exchanged through the network;
- Malicious Fake Node: The IoT's advantage to easily create a network can become a weakness. An adversary can always install a node to the network that inputs false data, an action could drain resources from the legitimate nodes, undermining the whole network's operation;
- Replay Attack: In the Replay Attack, an intruder eavesdrops authentic information transferred over the communication line between the sender and a receiver and captures it. Then, he sends the same authenticated information to the victim that had already been received in his communication, by showing proof of her identity and authenticity. Since the message is encrypted, the receiver may treat it as a legitimate request and respond accordingly to the intruder;
- Timing Attack: Timing Attack is more effective in devices with minimal computing capabilities. This attack enables an adversary to expose vulnerabilities and extract information maintained in the security of a system by timing how long it takes the system to respond to different queries, inputs, cryptographic algorithms and other.

4.2. Network Layer

The Network Layer is highly sensitive to attacks with security problems mainly to the integrity and availability of information exchanged throughout a network. Selected security threats of the Network Layer are summarized next.

- Denial of Service (DoS) Attacks: With a DoS attack, users are prevented from accessing devices or other network resources. This action is accomplished by flooding targeted devices or network resources with superfluous requests making it impossible or difficult for other users to communicate;
- IP Fragmentation Attacks: It is a DoS category attack where the adversary exploits a network's Maximum transmission Unit (MTU). When IP packets are reassembled after transmission, their size is larger than the maximum transmission unit the network can service, and therefore it collapses;
- Man in The Middle Attacks: In a MiTM attack, the attacker, while unobserved, intercepts and alters the communication data between two parties. Since they are both unaware of the interception, the attacker can control their communication, by changing messages according to his needs. It is considered a serious threat to network's

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2022 doi:10.20944/preprints202111.0214.v2

security because the attacker can capture and manipulate information in real time, before being exposed;

- Storage Attacks: Since all data is stored on storage devices (Locally or Cloud) they can be attacked by changing legitimate data to incorrect ones or even delete them permanently. Therefore, if many groups of users have access to the storage, the more possible it is for these types of attacks;
- Exploit Attack: Exploit Attacks are attacks that take advantage of security vulnerabilities in applications, systems, or hardware. Their goal is to gain partially or fully control of a system and steal or alter the information stored. Although the system's admin can patch the security vulnerability, every single change on application or hardware can create new vulnerabilities for an attacker.

4.3. Application Layer

The Application Layer is more prone to security issues compared to the other two layers, due to its diversity. The Application Layer consists of the applications and software built for IoT implementations and since these are countless, so are the applications built for them. For example, when IoT is used for Smart Home applications, the threats and vulnerabilities may come from every application with access to the hardware used either from the inside (control center or even our mobile app) or outside (remote applications).

Some of the most common security threats of the Application Layer in IoT are:

- Cross Site Scripting: In Cross Site Scripting attacks the adversary injects malicious code scripts, such as java scripts, in a trusted domain site viewed by many other users. With this action the adversary can alter the contents of an application according to his purposes and use original information in a malicious way. [20];
- Malicious Code Attack: Every software is built with by code and so as malicious software. Either a Trojan, Virus, Worms or Backdoors are malicious code intended to cause undesired effects to system's operations. Usually, these types of attacks cannot be blocked or exposed with anti-virus software and can activate itself either when certain criteria are met or after user interaction (i.e., opening a file);
- Cinderella Attacks: These attacks can occur when a malicious user, gains access to a system, and changes the internal clock of the network. This action leads to false premature expiration of the security software (i.e., antivirus), making it useless thus increasing network's vulnerabilities;
- Big Data Handling: Large IoT networks with many devices interacting, creates massive amount of data. If the hardware used in the network cannot process the data according to present or future requirements, it can lead to network disturbance and data losses [21].

5. IoT Applications

As mentioned above, IoT systems could be deployed to support endless applications. Basically, "anything" can be turned into an IoT device that can interconnect with other devices on a network boosting productivity, safety and cost reduction. However, we will address some of the areas that IoT would reinvent, providing unimaginable capabilities never thought before.

5.1. Agricultural

IoT implementations can improve different parts in the agro-industrial industry, like soil state and environmental conditions evaluation (Oxygen, Hydration, temperature, CO2), biomass consistency and more, but also to adjust variables during production or transportation phase. Another implementation is to keep track and predict a product's inventory on shelves or even inside refrigerators, while processing valuable analytics. Moreover, it can provide reliable information to the end user about the originality and ingredients of the product and promote an informed, connected, developed and adaptable rural community. In summary, IoT in Agriculture can literally reinvent the industry in

 doi:10.20944/preprints202111.0214.v2

the years to come affecting farmers, suppliers, technicians, distributors, businessmen, consumers, and government representatives [22].

5.2. Health Care

IoT, in conjunction with real-time connected objects, can play a significant role in preventing serious illnesses and reducing healthcare cost [23]. Moreover, the implementation has a long-term impact on the health monitoring, administration, and clinical service to patient's physiological information. The basic concept consists of patients connected with sensors and the data are forwarded to the health-monitoring unit. Sometimes data are stored in the cloud, which helps to manage the amount of data with safety [24].

An IoT implementation coupled with machine learning, can be used for early detection of heart diseases [25] or arthritis. This type of implementation consists of wearable devices for collecting sensor data, a cloud center for storing the data, and a regression-based prediction model for heart diseases and arthritis.

Each year, millions of people over 65 years old fall. An IoT implementation with simple detection algorithm, can be used to detect people who fall on specific areas. These areas will contain RFID information and location identification data that can be used to provide alert to hospitals and family members thus preventing a possible life loss [26].

IoT-based healthcare system can provide ways to collect data from cancer patients and monitor them on real-time for long periods, while using a variety of sensors and communication protocols. The use of a network of sensors and suitable communication protocols allow us to have smart devices which can transmit data remotely through different servers from one end to the other. It can become quite easy for patients and the specialized medical staffs, such as oncologists, to monitor and analyze the health condition of cancer patients, especially beneficial for those with deteriorating health situation.

During a pandemic, like COVID-19, IoT can be used to monitor quarantined and high-risk patients by using the internet and a smart sensor or a mobile phone [27]. Moreover, tracking the location of medical equipment in real time can improve treatment process speed while providing procedure transparency.

5.3. Environmental Applications

As ESG (Environmental-Social-Governance) is common tool worldwide for new technology evaluation, environmental IoT applications can be considered important. Real time maps with air and water pollution, pandemic data, noise levels, temperature, and harmful radiation, can now become a reality with the use of smart sensors. Besides that, IoT is capable in collecting and storing environmental records, check the compliance of environmental variables with local policies, trigger alerts, or send recommendation messages to citizens and authorities. These data can be used by governments and organizations as inputs for predictive models to forecast environmental variables and track pollution sources over time and space, ultimately leading to faster and better decisions to ensure a safe and healthy environment for all citizens [22]

5.4. Maritime Industry

Ships and vessels are lacking many of the technologies that are used on shore, due to the open sea environment (absence of steady internet coverage, equipment more prone to defections etc.). Since many on board departments need to cooperate, real time information on board is crucial. The maintenance department could monitor shipboard equipment in real time to deal proactively with maintenance, by monitoring shipboard equipment and machinery enhanced with IoT technology, to discover issues and prevent potential failures. In addition, since fuel represent about 55 percent of total ship operating costs, smart sensors and monitoring equipment on-board can track ship's performance and report back to the headquarters on shore, which in turn can support the ship master and chief engineer with guidance when planning the most fuel-efficient route. Finally, identifying optimal speed,

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2022 doi:10.20944/preprints202111.0214.v2

current and upcoming weather conditions and engine configuration will potentially save significant amounts of fuel, while minimizing CO2 emissions [28].

5.5. Military

The capabilities of an IoT system besides wealth creation, productivity and security can also be used in Military. Many Countries worldwide are already trying to promote Military and Defense Applications through IoT implementations in order to overcome various warfare and battlefield challenges. In this case we have the "Internet of Military Things" (IoMT) which is a class of IoT applications for Intelligent warfare and modern combat operations. By creating a miniature ecosystem of smart technology capable of distilling sensory information and autonomously governing multiple tasks at once, the IoMT is conceptually designed to offload much of the physical and mental burden that war fighters encounter in a field combat. Use cases like real-time Health monitoring, Augmented reality training, superior Fleet management, Target recognition and Battlefield awareness are only a few of the capabilities provided by an IoT implementation.

5.6. Smart Cities

IoT applications in a city are unimaginable, and include everything from energy management, smart lighting, intelligent traffic management to water treatment and wastewater management or evacuation guidelines in case of an emergency. In a machine-to-human approach, data from sensors in traffic lights can be used from the central authority to adjust traffic flow. In a machine-to-machine approach, intelligent traffic systems (i.e., smart traffic lights, traffic cameras and a cloud data center) can monitor traffic and public transportation to calculate possible upcoming congestions with the use of A.I. and prevent them by adjusting traffic flow. IoT sensors in streetlights could also adjust not only power states (ON/OFF) but also brightness depending on real light conditions (i.e., from dusk till dawn). Considering the number of streetlights that can be found in a city, these few watts from every streetlight add up, making the savings and environmental impact worthy. Moreover, those same sensors can also alert if a light needs servicing, reducing repair tickets and saving time to the service department [29].

5.7. Transportation and Logistics

Transportation and logistics are industries that already reap the benefits of IO systems from a variety of applications. However, IoT could inform, in real time, all kinds of fleets (cars, trucks, ships, trains etc.) that carry goods, to reroute based on traffic, upcoming weather conditions, vehicle or driver availability, thanks to IoT sensor data. The inventory itself could also be equipped with sensors for tracking and temperature-control monitoring, as many industries like food and beverage, flower, and pharmaceutical often carry temperature-sensitive products. In this case, alerts can be sent when temperatures change to a level that threatens the product. Furthermore, blockchain technologies can be used to ensure that the information about the transportation of the goods has not been altered. [21]

5.8. Smart Grid

Since always, energy grids were designed to deliver electricity from large power stations power by coal, nuclear etc. to a wide network of homes and businesses. Until now, the electric grid could not accept power contributions from houses and businesses that are harvesting power via renewable sources (solar panels, windmills etc.). A smart grid though, is capable in accepting power from decentralized mini power stations like a house with solar panels while coupled with wireless smart meters, can monitor how much energy a net-positive establishment is generating and reimburse them accordingly. Besides smart meters, every equipment can connect to the grid as well, enhancing its utilization. For example, data from weather stations could inform the grid that in an upcoming cloudy weather the solar panels will stop contributing power, hence the grid should adapt to this parameter. [30]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 January 2022 doi:10.20944/preprints202111.0214.v2

6. Challenges

Nowadays, numerous IoT devices are interacting through networks to provide for the user, the required information. However when addressing IoT implementations it is not that easy, as besides security, many challenges arise and in the next sessions we will briefly describe some of the key challenges [31].

6.1. Standardization

As mentioned above, a standardization is necessary because without established regulation, precise guidelines and worldwide standards, the industry will eventually face serious incompatibilities from unregulated IoT expansion which are more difficult to track and examine their impacts to different sectors. In addition, many IoT devices are handling unstructured data that are stored in various types of databases (NoSQL etc.) with different querying approach, creating incompatibilities between systems. Since the number of the end users keeps rising along with the extensive use of IoT devices in many sectors, a new attack vector arises. Similar attack methods have led to increased acceptance of the need for regulation, legislation, stronger protection measures and more strict controls for devices that authenticating on the Internet [3].

6.2. Integration

In communication networks, device integration is highly affected by the lack of the effective standards and IoT is no exception. Since "traditional" communication interoperability is challenging due to the wide range of available technologies making it hard to communicate seamlessly between multi-vendor devices, IoT communication interoperability is more difficult to implement due to different programming languages and enormous number of different components, utilized in the IoT hardware development. With these types of incompatibilities, the reliability of a network is dramatically decreased making the communication unstable. These issues have led the market to propose certain solutions like standardization of protocols, but these solutions leave behind many incompatible hardware devices.

6.3. Privacy

Since connected devices around the world are increasing exponentially, adversaries now have many more potential entry points into a network. In simple terms, for every new IoT device connected to a network the attack surface increases because an adversary now has many more devices prone to hacking thus exposing the whole network's safety. Additionally, the ability to collect and distribute data and information to another device or network autonomously is also a disadvantage since the data could be sensitive but certainly will be vulnerable. For example, there are IoT devices that require users to agree to terms and condition of service before interacting with them. These types of agreements can expose users' data making them vulnerable to attack. Therefore, strategies need to be developed to handle people's privacy options across a broad spectrum of expectations. Since ease of use and security are "enemies", the industry must figure out a solution that promotes technological innovation and services while avoiding putting sensitive private data and information in danger.

6.4. Regulation

Due to the diversity in the implementations of IoT technology and the legal scope that regulates IoT devices, there have been numerous dilemmas with reference to the regulations and laws that apply, complicating its users whether certain actions are prohibited or not in each jurisdiction [32]. Some of the legal questions that have arisen with regard to the use of IoT devices include data retention and destruction policies, legal liability for unintended uses of IoT devices, security breaches or privacy lapses, to name just a few [33]. Additionally, global regulation, for instance, rules, processes, protocols, audits, transparency and continuity, is thus far absent in the IoT sphere, as a result of the nonexistent

legislation applying in general in the IoT field. Such regulations in the industrial, national and international sphere could be remarkably beneficial in assisting organizations become more efficient and reliable as far as systems are concerned and contribute to the lessening of errors in the future [34].

7. Conclusions

With the advance of low-cost computing, cloud services, big data technologies, analytics, and mobile technologies, small size physical devices forming a network, can collect and exchange data without human intervention. In this hyperconnected environment, every node can record, monitor, and adjust each interaction between connected things. Although, this promising technology also threatens user's privacy and security in the different environments under which is deployed. For this reason, solutions to threat detection [35], intrusion, compromise or misuse in the IoT domain should be developed and generally agreed-upon standards and security regulations are necessary for the industry to thrive. Since the advantages of the technology are not questionable, governments and engineers must unite their powers and overcome the challenges to make IoT networks be viewed as the traditional networks making the term Internet of Everything valid.

Author Contributions: Conceptualization, A.G., N.A. and L.M.; Methodology, A.G., N.A., I.K. and L.M.; Software, A.G. and N.A.; Validation, N.A., L.M., and I.K.; formal analysis, A. G. and N.A.; investigation, A.G., N.A., and L.M.; resources, A.G. and N.A.; data curation, A.G., N.A., I.K. and L.M.; writing—original draft preparation, A.G., N.A. and L.M..; writing—review and editing, N.A., I.K. and L.M.; visualization, N.A., I.K. and L.M.; supervision, N.A. and L.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not applicable.

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

References

1. Rayes, A.; Salam, S. Internet of things from hype to reality. *Springer* **2017**.
2. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons* **2015**, *58*, 431–440.
3. Ferrag, M.A.; Maglaras, L.; Derhab, A. Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends. *Security and Communication Networks* **2019**, *2019*.
4. Khan, S.; Shakil, K.A.; Alam, M. *Internet of Things (IoT): Concepts and Applications*; Springer, 2020.
5. Wang, J.; Lim, M.K.; Wang, C.; Tseng, M.L. The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering* **2021**, *155*, 107174.
6. Maglaras, L.; Ferrag, M.A.; Derhab, A.; Mukherjee, M.; Janicke, H.; Rallis, S. Threats, protection and attribution of cyber attacks on critical infrastructures. *arXiv preprint arXiv:1901.03899* **2019**.
7. Mukherjee, M.; Ferrag, M.A.; Maglaras, L.; Derhab, A.; Aazam, M. Security and privacy issues and solutions for fog. *Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics* **2020**, pp. 353–374.
8. Al-Sarawi, S.; Anbar, M.; Abdullah, R.; Al Hawari, A.B. Internet of Things market analysis forecasts, 2020–2030. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE, 2020, pp. 449–453.
9. Chaudhary, A.; Peddoju, S.K.; Kadarla, K. Study of internet-of-things messaging protocols used for exchanging data with external sources. 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS). IEEE, 2017, pp. 666–671.
10. Serpanos, D.; Wolf, M. The IoT Landscape. In *Internet-of-Things (IoT) Systems*; Springer, 2018; pp. 1–6.
11. Gupta, B.B.; Quamara, M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience* **2020**, *32*, e4946.

12. Santos, M.G.d.; Ameyed, D.; Petrillo, F.; Jaafar, F.; Cheriet, M. Internet of Things Architectures: A Comparative Study. *arXiv preprint arXiv:2004.12936* **2020**.
13. Pierleoni, P.; Concetti, R.; Belli, A.; Palma, L. Amazon, Google and Microsoft solutions for IoT: architectures and a performance comparison. *IEEE access* **2019**, *8*, 5455–5470.
14. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* **2021**, *12*, 87.
15. Sparavigna, A. Labels discover physics: the development of new labelling methods as a promising research field for applied physics. *arXiv preprint arXiv:0801.2700* **2008**.
16. Setetemela, K.; Keta, K.; Nkhabu, M.; Winberg, S. Python-based FPGA implementation of AES using Migen for Internet of Things Security. 2019 IEEE 10th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT). IEEE, 2019, pp. 194–198.
17. de Almeida, I.B.F.; Mendes, L.L.; Rodrigues, J.J.; da Cruz, M.A. 5G waveforms for IoT applications. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 2554–2567.
18. Ahamed, J.; Rajan, A.V. Internet of Things (IoT): Application systems and security vulnerabilities. 2016 5th International conference on electronic devices, systems and applications (ICEDSA). IEEE, 2016, pp. 1–5.
19. Aarika, K.; Bouhlal, M.; Abdelouahid, R.A.; Elfilali, S.; Benlahmar, E. Perception layer security in the internet of things. *Procedia Computer Science* **2020**, *175*, 591–596.
20. Papaspirou, V.; Maglaras, L.; Ferrag, M.A. A Tutorial on Cross Site Scripting Attack-Defense **2020**.
21. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE access* **2020**, *8*, 32031–32053.
22. Talavera, J.M.; Tobón, L.E.; Gómez, J.A.; Culman, M.A.; Aranda, J.M.; Parra, D.T.; Quiroz, L.A.; Hoyos, A.; Garreta, L.E. Review of IoT applications in agro-industrial and environmental fields. *Computers and Electronics in Agriculture* **2017**, *142*, 283–297.
23. Rehman, O.; Farrukh, Z.; Al-Busaidi, A.M.; Cha, K.; Park, S.J.; Rahman, I.M. IoT Powered Cancer Observation System **2020**.
24. Kelli, V.; Sarigiannidis, P.; Argyriou, V.; Lagkas, T.; Vitsas, V. A Cyber Resilience Framework for NG-IoT Healthcare Using Machine Learning and Blockchain. ICC 2021-IEEE International Conference on Communications. IEEE, 2021, pp. 1–6.
25. Kumar, P.M.; Gandhi, U.D. A novel three-tier Internet of Things architecture with machine learning algorithm for early detection of heart diseases. *Computers & Electrical Engineering* **2018**, *65*, 222–235.
26. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Applied Sciences* **2020**, *2*, 1–8.
27. Umair, M.; Cheema, M.; Cheema, O.; Li, H.; Lu, H. Impact of COVID-19 on IoT Adoption in Healthcare, Smart Homes, Smart Buildings, Smart Cities, Transportation and Industrial IoT. *Sensors* **2021**.
28. Plaza-Hernández, M.; Gil-González, A.B.; Rodríguez-González, S.; Prieto-Tejedor, J.; Corchado-Rodríguez, J.M. Integration of IoT Technologies in the Maritime Industry. International Symposium on Distributed Computing and Artificial Intelligence. Springer, 2020, pp. 107–115.
29. Balandina, E.; Balandin, S.; Koucheryavy, Y.; Mouromtsev, D. IoT use cases in healthcare and tourism. 2015 IEEE 17th conference on business informatics. IEEE, 2015, Vol. 2, pp. 37–44.
30. Hassan, R.; Qamar, F.; Hasan, M.K.; Aman, A.H.M.; Ahmed, A.S. Internet of Things and its applications: A comprehensive survey. *Symmetry* **2020**, *12*, 1674.
31. Karie, N.M.; Sahri, N.M.; Haskell-Dowland, P. IoT threat detection advances, challenges and future directions. 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT). IEEE, 2020, pp. 22–29.
32. Ploennigs, J.; Cohn, J.; Stanford-Clark, A. The future of IoT. *IEEE Internet of Things Magazine* **2018**, *1*, 28–33.
33. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security. *Sensors* **2019**, *19*, 3119.
34. Hanes, D.; Salgueiro, G.; Grossetete, P.; Barton, R.; Henry, J. *IoT fundamentals: Networking technologies, protocols, and use cases for the internet of things*; Cisco Press, 2017.
35. Ferrag, M.A.; Maglaras, L.; Ahmim, A.; Derdour, M.; Janicke, H. Rdtids: Rules and decision tree-based intrusion detection system for internet-of-things networks. *Future internet* **2020**, *12*, 44.