





Article

DNS for IoT: A Survey

Ibrahim Ayoub ^{1,2,*} , Sandoche Balakrichenan ¹ , Kinda Khawam ³  and Benoît Ampeau ¹ 

- ¹ Association française Pour le Nommage Internet en Coopération (Afnic), 1 Rue Stephenson, 78180 Montigny-le-Bretonneux, France; sandoche.balakrichenan@afnic.fr (S.B.); benoit.ampeau@afnic.fr (B.A.)
- ² École Doctorale Sciences et Technologies de l'Information et de la Communication (ED STIC), Université Paris-Saclay, 3 Rue Joliot Curie, 91190 Gif-sur-Yvette, France
- ³ Laboratoire DAVID, Université de Versailles St-Quentin, 45 Avenue des États-Unis, 78035 Versailles, France; kinda.khawam@uvsq.fr
- * Correspondence: ibrahim.ayoub@afnic.fr

Abstract: The Internet of Things (IoT) is paving the way to becoming necessary in numerous aspects of people's lives. IoT is becoming integrated in many domains, such as medical, industrial, and personal. Recent years have witnessed the creation of many IoT technologies that differ not only in their applications and use cases but also in standards. The absence of universally accepted standards and the variety of technologies are only some challenges the IoT market faces. Other challenges include the constrained nature of most IoT devices, the diverse identification schemes, the inadequate security mechanisms, and the lack of interoperability between different technologies. The Domain Name System (DNS) persisted throughout the years as the Internet's naming service and accumulated more trust from users with the introduction of its security extensions. DNS could be utilized to address some of the challenges the IoT market faces. However, using DNS for IoT applications might jeopardize DNS infrastructure. In this survey, we study the coexistence of DNS and IoT. We define IoT, present its architecture and discuss its main challenges. We then introduce DNS and its function; we discuss its security and privacy drawbacks and the extensions standardized to address them. We further discuss the uses of DNS in IoT environments to address some of IoT's challenges and the impact these uses might have on DNS.

Keywords: DNS; DNS security; IoT; IoT challenges



Citation: Ayoub, I.; Balakrichenan, S.; Khawam, K.; Ampeau, B. DNS for IoT: A Survey. *Sensors* **2023**, *23*, 4473. <https://doi.org/10.3390/s23094473>

Academic Editor: Claudio Savaglio

Received: 19 March 2023

Revised: 29 April 2023

Accepted: 25 April 2023

Published: 4 May 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Like other breakthrough technologies, the Internet of Things (IoT) shapes our world and how we perceive it. If the average user were asked 20 years ago about her first thought when hearing the term *connected device*, the answer, if any, would probably be the personal computer. Cars, refrigerators, pets, and other daily-use objects were never thought to one day need a network connection. Even phones were only known as voice-call devices and had limited functionality besides that. Currently, however, the definition of connected devices has vastly changed. Personal computers are no longer the only ones with network connectivity; they have become only one of many categories of connected devices. One of the catalysts for this change was the introduction of smartphones, the devices that redefined our relationship with the Internet. Smartphone users are no longer required to be seated at a desk to access the Internet. Pocket-size mobile phones became the primary interface with the network, and users could hardly imagine being disconnected as many services became available online. After that, the appreciation of connected devices increased, and the IoT industry boomed. The number of connected devices and their functions and underlying standards increased. Currently, with the deployment of 5G, IoT technologies are expected to benefit immensely. 5G offers faster data rates, lower latency, and greater network capacity. Sensor networks are already reaping huge benefits from the reliability of 5G [1,2]. Consequently, many regular devices typically considered isolated are now connected.

The average number of devices connected per household in the United States rose from 11 in 2019 to 25 in 2021 [3]. The predictions about the global number of IoT devices in the future vary anywhere between 25 billion [4] and 125 billion devices [5] in 2030, with total revenue of USD 1 trillion [6] to 1.5 trillion [7]. These predictions illustrate the significance of IoT, which will be increasingly palpable with time. Nevertheless, despite their omnipresence, IoT technologies face some challenges. Figure 1 presents the taxonomy of challenges facing IoT technologies.

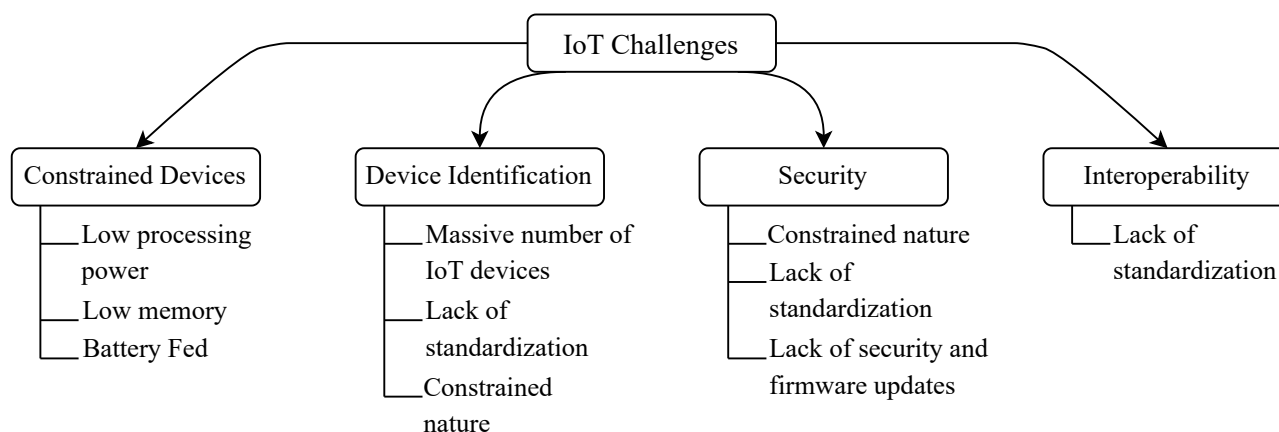


Figure 1. Taxonomy of challenges Facing IoT.

The **first challenge** is that most IoT devices are constrained. Devices of this kind are designed to perform specific jobs, such as measuring temperature or detecting motion. These tasks do not require significant resources, and manufacturers of such devices aim to mass-produce while keeping the prices low. Therefore, constrained devices of this kind have limited memory and processing power and are usually battery-powered. The constrained nature of IoT devices complicates their management. Mechanisms commonly used on the Internet today for regular, more powerful devices cannot be directly used with constrained IoT devices. These mechanisms, for example, include encryption and decryption of data and receiving software updates or security patches. Such mechanisms, therefore, must be redeveloped to suit the less powerful IoT devices.

The **second challenge** lies in the identification of these devices. IoT or not, any device connected to a network needs an identifier. The most commonly used identifier on the Internet is the IP address. Identifiers serve at least one primary purpose: the data sender uses them to specify the exact recipient. On the other hand, the recipient can use them to verify the source of the data or to determine whether the data are intended for them. Identifiers must be unique in the scope they are used in to identify each device uniquely. The massive number of IoT devices, lack of standardization, and constrained nature impede finding a global identification scheme similar to IP addresses. The lack of global identification schemes, or at least large-scale ones, makes it challenging to manage and track the large number of IoT devices, leading to potential security vulnerabilities and interoperability issues.

The **third challenge** is security. Security of exchanged data is vital in any communication, and IoT communications are no exception. However, contrary to regular Internet communications, where security and privacy mechanisms are generally standardized and trustworthy, IoT technologies suffer from security drawbacks. These devices have a relatively large attack surface, making them vulnerable to several cyber attacks. IoT devices, for example, are the primary target of attackers who aim to launch Denial of Service (DoS) attacks, as these devices are easily compromised. The constrained nature of IoT devices prevents them from using up-to-date security mechanisms as they require more memory and processing power resources than these devices have. In addition, the lack of standardization also impairs security since every manufacturer uses a proprietary

security mechanism that is predominantly incompatible with other manufacturers. Lastly, these devices are usually not adequately maintained regarding software updates, especially security patches.

Lastly, the **fourth challenge** we identify is the lack of interoperability between IoT manufacturers. The lack of global standards provokes heterogeneity between different IoT technologies. For example, a motion sensor from one manufacturer would not be able to communicate with a motion sensor from a different manufacturer or with the backend server of that sensor, even if they belong to the same network. Moreover, devices from one network would be unable to communicate with devices from different networks if these networks are based on different IoT technologies. Heterogeneity arises in identification, data formatting, and security mechanisms used, among other things. This causes the IoT environment to become vertically divided into separate silos where different technologies cannot communicate. This lack of interoperability disperses research and development efforts since a breakthrough in one technology is, with high probability, not useful to others. Interoperability between different IoT technologies is necessary for globally standardized IoT.

Given the spread of IoT technologies today and the projections of further large-scale deployments of its technologies, identifying and addressing its challenges is a must. Of course, having one remedy for all IoT drawbacks is not attainable, but it is possible today, with tools already available to ameliorate IoT environments and their user experience. So, instead of developing new ones, it would be meaningful and efficient to consider tools and standards we currently use on the Internet and adapt them to constrained IoT to address its challenges.

A service that stood the test of time as one of the cornerstones of the Internet is the Domain Name System (DNS). The DNS is the Internet's naming service that has been essential for the Internet since its inception in 1987 [8]. The job the DNS does, along with its efficiency and robustness, rendered it an essential service. Drawbacks of the DNS, which mostly revolve around its not so security-oriented original design [9], are being addressed by many initiatives, which resulted in several protocol evolutions to make DNS more secure. For the billions of connected devices forming the IoT, DNS is also a necessary tool. Even the simplest IoT devices, such as thermometers or motion sensors, might need to use DNS to contact their backend servers [10]. IoT technologies could also utilize the DNS in other manners. For example, the functions of DNS and its distributed nature make it an ideal candidate for IoT naming and identification. Some proprietary IoT naming schemes are already using it [11]. Moreover, its recent security extensions help make IoT communications more secure if adapted to constrained devices.

However, having discussed the former points about DNS and IoT and how DNS could be useful, the possible repercussions for DNS should be noticed. According to the projections discussed earlier, billions of IoT devices will be added yearly. This raises questions regarding the scalability and security of DNS. There have already been some worrisome impacts on DNS due to IoT, such as the infamous Mirai attack [12,13].

In this work, we explore and examine the challenges IoT environments face. We primarily focus on challenges due to the constrained nature of IoT devices and challenges related to the identification of these devices, security of IoT communications, and interoperability between different IoT technologies. We elaborate on each challenge and investigate how DNS is being used to address some of these challenges. We then illustrate the effects this usage might have on the DNS infrastructure. Overall, this study aims to understand better IoT challenges and the benefits DNS might have to address these challenges. This work can provide valuable insights for IoT researchers, manufacturers, and policymakers of IoT technologies to create a safer, more reliable IoT ecosystem.

2. Related Work

Upon conducting our literature review, we noticed a lack of comprehensive surveys that address IoT challenges and how DNS could be used to address them. Even though

several surveys touched on the subject by studying some uses of DNS with IoT, they were not comprehensive regarding the addressed challenges. Instead, most of these surveys dealt with one of the IoT challenges, mainly the security challenge, and studied how DNS could address that. Other surveys discuss IoT's impact on the DNS infrastructure without a detailed discussion of the benefits IoT might receive from using DNS. Our survey, on the other hand, is more comprehensive. It introduces the concept of IoT, details IoT's challenges, and then explains the functions of DNS and how DNS can be used to address these challenges. The survey ends with a discussion about the impact of IoT on the DNS infrastructure. In this section, we discuss the most notable surveys we found. We highlight their contribution and what they lack compared to our work.

The survey in [14] discusses how DNS is to be used, by IoT devices or intermediary devices such as gateways, to communicate with backend servers. The survey discusses the possible advantages IoT might gain from using DNS. These advantages include the security gains from DNS security extensions and device transparency gains from monitoring DNS-using IoT devices. However, rather than moving on to more IoT challenges that DNS solves, the work in [14] studies the risks to the DNS caused by using it in IoT applications. The main risk lies in the large number of IoT devices that could generate DDoS attacks against DNS either intentionally due to malware or unintentionally due to coding errors that could be encountered at the IoT scale. The work in [15] is also a survey regarding the uses of DNS in IoT environments. The effects of IoT on DNS are also discussed. The authors, however, did not explore the full potential of DNS as a tool to address DNS challenges. Other surveys discuss the challenges encountered in IoT environments. The work in [16] is a comprehensive survey about the possible security threats on IoT. The authors adopted a three-layer model and detailed the possible security threats on each layer. The two surveys in [17,18] are also about IoT security threats and possible solutions. However, [16–18] only discuss the security aspect of IoT challenges. Some works explored IoT when deployed in specific domains. The survey in [19] is about consumer IoT device classification using different Machine Learning-based methods. The study provides recommendations for creating the best possible home IoT environment. The survey in [20] discusses the uses of IoT in the maritime industry, while [21] is a literature review about IoT healthcare applications and the security and privacy requirements of IoT when used in healthcare. The surveys in [19–21], however, are only concerned with IoT implementations in specific domains and deal only with security challenges of such implementations. The work in [22] studies industrial IoT's possible identity resolution systems. The paper presents a general framework for reviewing identity resolution systems. In [23], the authors studied the IoT identification techniques and the Manufacturer Usage Description (MUD) standard used to reduce the IoT attack surface. The paper studies the security of infrastructure instead of the security of IoT data. The authors in [24] presented three methods to detect IoT devices on the Internet, namely an IP-based method that detects servers that IoT devices contact from Internet flows, a DNS-based method that detects the names of such servers from DNS queries, and a certificate-based method that detects HTTPS-accessible IoT devices by inspecting their TLS certificates.

3. Survey Overview and Significance

IoT is expected to touch many aspects of daily life. Many objects connected today, like pets, cars, and home appliances, were never thought to one day need a network connection. This tells us that many objects we see today as isolated and needing no network connectivity will also be connected in the future. This is likely as IoT predictions are predominantly optimistic, and larger-scale future deployments are expected. These optimistic predictions demand a closer look at the present state of IoT to ensure that IoT growth will be safe and beneficial to all stakeholders. Having more connected devices means, on the one hand, more load on network infrastructure and, on the other hand, more personal data entrusted to these devices. Hence, it is pivotal to study the IoT environment's current challenges and elaborate on possible solutions. Addressing these challenges will allow a larger adoption of

IoT technologies. It is important to highlight these challenges, study their effect on limiting IoT today, and study possible solutions. When thinking about solutions for IoT technologies, it is essential to find solutions that do not themselves create further challenges. For example, focusing on name resolution for a single IoT technology that is not interoperable with other technologies is counterproductive since IoT as a technological concept will not benefit from that solution, only that specific technology for which the solution was designed. Hence, considering solutions encompassing as many IoT technologies as possible is of great benefit and importance. DNS could play a significant role in addressing current IoT networks' challenges. DNS, the domain name system that converts domain names to IP addresses, could benefit IoT by resolving the domain names of IoT devices or their backend servers. Moreover, DNS's security extension could play a role in securing IoT DNS traffic. However, using DNS in IoT environments could be rewarding for IoT but could simultaneously negatively impact the DNS infrastructure. The work in this survey aims to explore this coupling between IoT and DNS. The research questions we aim to answer are the following:

1. What are the main challenges facing the implementation and adoption of IoT on larger scales?
2. How can the Domain Name System be used to address these challenges to facilitate the growth of IoT safely and cooperatively?
3. What impact could the large-scale implementation of IoT have on DNS?

Upon researching the topic, we noticed an increased interest in IoT and DNS, specifically in articles mentioning the two terms. Figure 2 is a visualization of this interest, and it shows the number of hits on Google Scholar for articles mentioning IoT and DNS between the years 2000 and 2022. The figure shows an upward trend in results mentioning IoT and DNS. This is merely an inconclusive indicator but shows that an association between the two terms is getting stronger. We aim to form a solid starting point for research that tackles the different IoT challenges by using DNS as a significant contributor to alleviate these challenges while minding IoT's impact on its infrastructure.

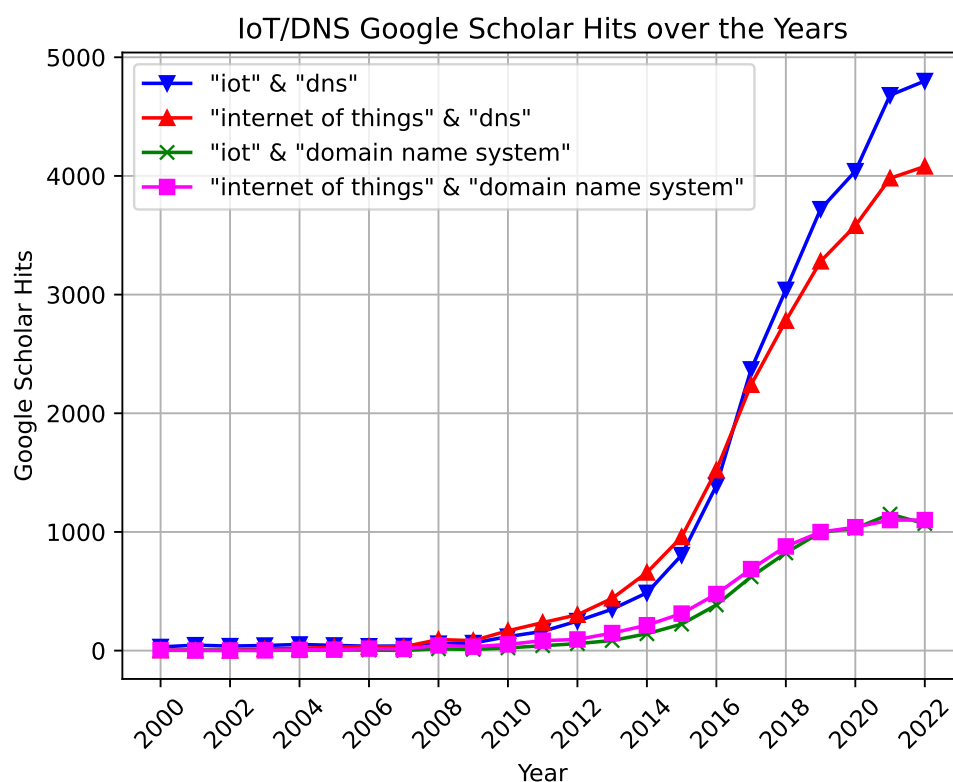


Figure 2. IoT/DNS Google Scholar hits between the years 2000 and 2022.

Our contributions in this work:

- We introduce IoT, its applications, and its main challenges.
- We explain the function of DNS, its security drawbacks, and the most important DNS security protocols and extensions.
- We perform a comprehensive literature review to investigate utilizing DNS to address the various challenges of IoT environments. To the best of our knowledge, a comprehensive survey of this nature has not been previously carried out. Hence, we perform a literature review about DNS usage in IoT environments to address the various challenges.

4. Method

Our survey covers three main topics. Firstly, it introduces IoT, its applications, and its challenges. Secondly, it introduces DNS, its security drawbacks, and the relevant security extensions and protocols. Finally, it studies how DNS is used in the literature to serve IoT environments and examines how IoT might affect the DNS infrastructure.

We searched for relevant articles in various databases, including IEEE Xplore, Google Scholar, ACM Digital Library, SpringerLink, and ScienceDirect, to investigate these topics. We included articles published after 2018 to ensure that our work is up-to-date. However, we also included a few articles published before 2018 if they had a significant contribution and reinforced our understanding of the topics. We included scientific conference papers, research papers, surveys, and technical reports. We also studied and cited several IETF Requests for Comments (RFCs), as these documents are the standards in the industry. We considered relevant RFCs regardless of their publication date. The keywords we used include: DNS Security, DNS and IoT, DNS IoT Survey, IoT Challenges, and IoT Security.

We screened the collected papers based on their titles, abstracts, introductions, and conclusions. We included articles that covered one of our three main topics: DNS and DNS security, IoT and IoT challenges, and the coexistence of DNS and IoT. In addition, we added relevant articles from the reference lists of the included articles and from articles that cite them. We excluded articles not written in English or that diverted greatly from our survey's main topics.

We finally studied in detail the articles we obtained from the initial screening. The articles that were eventually included in our survey had to discuss explicitly at least one of the following topics:

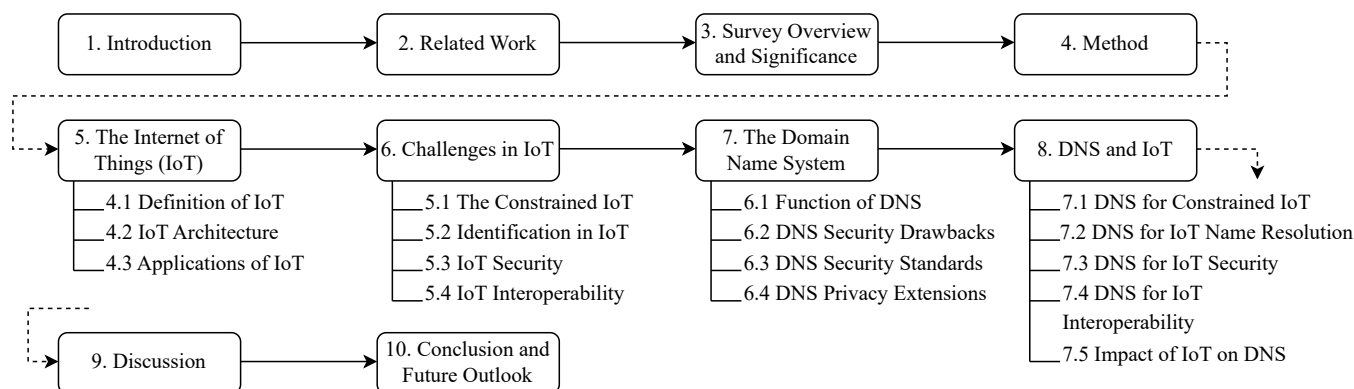
- The concepts of IoT, its architecture, and applications.
- IoT's challenges, including the constrained nature of IoT devices, IoT identification, interoperability between IoT technologies, and IoT security.
- DNS function, security and privacy drawbacks, and security and privacy extensions and protocols.
- The use of DNS in IoT environments to address at least one of the IoT challenges mentioned above.
- The effect IoT might have on DNS. Here we considered negative effects.

The list of abbreviations used in this paper is presented in Table 1.

The work is divided as follows. Section 5 introduces IoT and its applications. Section 6 lists IoT challenges. Section 7 introduces DNS, its functions, and its security drawbacks. Furthermore, we explain DNS's most common security extensions, which could serve both regular and IoT-connected devices. The literature is not rich with surveys about using DNS in IoT environments, even though we found numerous articles where DNS is purposefully used to address IoT challenges. Accordingly, Section 8 is a literature review of DNS-related IoT applications. The impact IoT might have on DNS is studied as well. In Section 9, we discuss our findings. We finalize with a conclusion in Section 10. The contents of the survey are detailed in Figure 3.

Table 1. List of abbreviations.

Abbreviation	Definition	Abbreviation	Definition
IoT	Internet of Things	DNS	Domain Name System
IP	Internet Protocol	TCP	Transmission Control Protocol
RFID	Radio-Frequency Identification	IoMT	Internet of Medical Things
IIoT	Industrial Internet of Things	RFC	Request for Comments
CoAP	Constrained Application Protocol	UDP	User Datagram Protocol
DOI	Digital Object Identifier	EPC	Electronic Product Code
URL	Uniform Resource Locator	URI	Universal Resource Identifier
ONS	Object Name Service	URN	Uniform Resource Names
MAC	Media Access Control	OID	Object Identifier
IETF	Internet Engineering Task Force	ORS	OID Resolution System
TLD	Top Level Domain	RR	Resource Record
DANE	DNS-Based Authentication of Named Entities	QNAME	Query Name
DDoS	Distributed Denial of Service	DNSSEC	DNS Security Extensions
DoH	DNS-over-HTTPS	DoT	DNS-over-TLS

**Figure 3.** Contents of the Survey.

5. The Internet of Things (IoT)

Even though the Internet of Things (IoT) has been around for a while (the term Internet of Things was coined in 1999 by Kevin Ashton [25]), it is not until recently that it became an appealing topic in industry and research. Recent years have witnessed a rapidly growing IoT integration in many industries and research domains. Unlike Internet devices which are predominantly IP-based and use the TCP/IP protocol suite, IoT is not a single technology and is not governed by a single organization. It is a general term encompassing different technologies with high diversity in terms of communication protocols, data representation, and transmission technologies. The technologies are numerous and include, but are not limited to, Narrowband IoT (NB-IoT) [26,27], Bluetooth Low Energy (BLE) [28], Sigfox [29], Zigbee [30], and LoRaWAN [31].

5.1. Definition of IoT

A standard definition of IoT has yet to be agreed upon, but we can infer a definition from its applications. It is the network created by connecting physical or virtual objects to the Internet, including many objects that were not traditionally considered to require Internet connectivity. The ITU Telecommunication Standardization Sector (ITU-T) defines IoT in Y4000: Overview of the Internet of things [32] as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT)”.

The devices in an IoT network, again, according to [32], could be:

- **Data carriers:** These are usually static, such as barcodes, and attached to physical things.
- **Data-carrying devices:** These devices might have the information stored in them altered by a data-capturing device, e.g., Radio-frequency identification (RFID).
- **Data-capturing devices:** These devices can read from or write to a physical thing. The physical thing could be a data carrier or a data-carrying device.
- **Sensing and actuating devices:** This category includes sensors that can interact with their environment, gather data and measurements, and send them over the network for processing. This category also includes actuators that can perform operations in their environment based on information received over the network or their measurement of the environment around them.
- **General devices:** These include industrial machinery, home appliances, personal computers, and mobile phones that have embedded processing and wired or wireless communication capabilities.

5.2. IoT Architecture

As with its definition, IoT has many standard architectures. The most notable are the three-layer [33,34], four-layer [35], also referred to as Service-Oriented Architecture (SOA), and five-layer [34] architectures. See Figure 4.

5.2.1. Three-Layer Architecture

- **Perception Layer:** This layer contains devices like sensors, actuators, barcodes, and RFID tags. It is mainly the layer that interacts with the environment to collect data to be sent to the upper layers.
- **Network Layer:** This layer receives data from the perception layer. It includes the network infrastructure that transfers data between the Perception and Application layers.
- **Application Layer:** This layer processes and analyzes data passed through the network layer.

5.2.2. Four-Layer (SOA) Architecture

- **Sensing Layer:** This layer is similar to the perception layer in the three-layer model. It contains sensing tools to perform the measurements in these devices' environments.
- **Network Layer:** This layer is the network infrastructure (wired or wireless) that ensures connectivity between things among themselves and between things and their backend.
- **Service Layer:** This layer stores and processes information. Services required by users are created and managed here.
- **Interface Layer:** This layer defines interaction rules between users and devices. It also attempts to solve compatibility issues between devices from different vendors that follow different standards.

5.2.3. Five-Layer Architecture

- **Perception Layer:** This layer is similar to the Perception Layer in the three-layer architecture.

- **Transport Layer:** Also referred to as the network layer. This layer receives data from the perception layer and passes them to the processing layer.
- **Processing Layer:** This layer processes and analyzes data passed through the network layer.
- **Application Layer:** Data from the processing layer are used here for IoT applications.
- **Business Layer:** This layer contains the management of the IoT system.

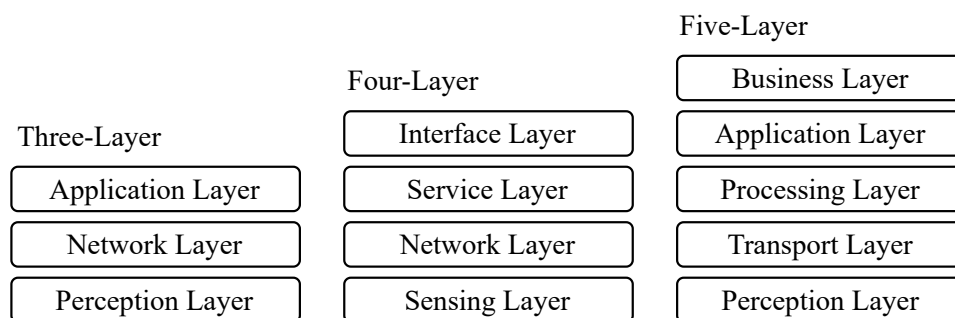


Figure 4. IoT architectures.

5.3. Applications of IoT

Applications of IoT are numerous and diverse. Smart cities use IoT devices to monitor traffic conditions [36], predict pollution levels [37], and provide smart parking [38]. Furthermore, cities deploy IoT networks for security purposes such as asset monitoring [39] and identification [40]. The agriculture industry benefits from IoT for produce distribution [41], supply chain management [42], and overall smart agriculture [43]. IoT plays a significant role in the health sector and is commonly known as the Internet of Medical Things (IoMT). IoMT helps improve the quality of life while decreasing the pressure on the medical system by allowing patients to self-diagnose when possible or to obtain a healthcare professional's recommendation from a distance [44,45]. Care for the elderly [44], monitoring the state of mind [46], physical activity [47], and even eating habits [48] are a few examples of what IoMT has to offer in terms of ameliorating the healthcare system. The digital transformation also found its way to different industries, leading to what is referred to as the fourth industrial revolution (Industry 4.0) with the Industrial Internet of Things (IIoT) [49]. In addition, IoT proved to be helpful in emergencies where communication with the individuals at risk is of utmost importance [50–53]. Finally, in light of the COVID-19 pandemic, IoT has been used to help trace, detect, and consequently mitigate the spread of the virus [54,55].

The predictions that IoT will grow significantly are already starting to materialize. The diverse domains discussed above that are driven forward by incorporating IoT in their functioning corroborate these predictions. Therefore, it is evident that IoT technologies have to be in their best form to connect everything securely. This highlights the importance of pinpointing the shortcomings of IoT and the challenges its various technologies face. Accordingly, we explore today's IoT challenges in Section 6.

6. Challenges in IoT

The challenges facing IoT could be divided into the following: the constrained nature of IoT devices, their identification, security, and the interoperability between different IoT technologies. We introduce these challenges in the following subsections.

6.1. The Constrained IoT

A considerable fraction of IoT devices is constrained. According to RFC 7228 [56], titled 'Terminology for Constrained-Node Networks', constrained devices are those that have:

- Limited ROM\Flash, leading to limitations on the maximum code complexity;
- Limited RAM, leading to constraints on the buffer sizes;
- Limited processing power;
- Batteries as sources of power;

- Constraints on user interface and accessibility in deployment.

Table 2 shows the classes of constrained devices according to their data and code sizes. Class 0 devices are ultra-constrained and need intermediary devices to communicate with designated servers. Class 1, on the other hand, could use protocols explicitly designed for constrained devices, such as Constrained Application Protocol (CoAP) over UDP [57]. Finally, Class 2 devices, which are more powerful, could use protocols used by regular devices on the Internet and benefit from lightweight specifically-designed protocols.

Table 2. Classes of constrained devices (KiB = 1024 bytes) [56].

Name	Data Size (e.g., RAM)	Code Size (e.g., Flash)
Class 0, C0	≪10 KiB	≪100 KiB
Class 1, C1	~10 KiB	~100 KiB
Class 2, C2	~50 KiB	~250 KiB

Such devices usually engage in gathering data from the real world. The data collected by these devices are generally sent to one or more servers on the network for processing. Due to the constraints mentioned above, designers of such devices are limited in choosing their operating systems or security mechanisms. The low processing power and low memory force the designers to abandon today's well-maintained popular operating systems running on personal computers and servers. Instead, they go for operating systems that comply with the stringent constraints of IoT devices but need a better reputation regarding performance and code complexity, leading to a bad reputation in security. In addition, these devices' power sources, mainly batteries that are expected to last for years, add further constraints. Consequently, such devices are only active for a short time, mostly use low bit rates, and usually lack user interfaces, making them harder to maintain and monitor.

6.2. Identification in IoT

Whenever an entity needs to connect to a network, it will need identification. People use these identifiers daily, but it may have become second nature that they overlook them. The mobile phone number is one of the most widespread identification methods for devices connected to networks. It provides a unique global identifier for every user. Thanks to its uniqueness, a user can initiate calls and receive calls from any other mobile phone number. This uniqueness guarantees that only the intended user is contacted and not any other user on the network. Regardless of the context where the identifier is used, its construction must follow an identification scheme. Identification schemes formulate the rules to be followed when creating and using an identifier. For example, domain names are identifiers used in the context of the Internet to identify resources. However, creating a domain name is not random but abides by rules and regulations, i.e., by the identification scheme mentioned in RFC 1035 [58].

The need for identification also applies to IoT devices. However, identification in IoT is not straightforward, and the hurdles stem from the interoperability challenge mentioned earlier. Different technologies use different identification schemes which are not interoperable. This further vertically divides the IoT environment since globally comprehensible identifiers are necessary for fixing interoperability problems.

The heterogeneity between IoT technologies and the lack of global standardization complicates discussing how identifiers should be, what properties they should have, or what requirements they should abide by. However, several vendor-neutral initiatives have tried to create a framework for IoT identifiers. These initiatives helped set up a taxonomy and requirements for IoT identifiers.

6.2.1. Taxonomy of IoT Identifiers

The *EU–China Joint White Paper on Internet-of-Things Identification* issued by the EU–China IoT Advisory Group [59] and the *Identifiers in IoT* report issued by The Alliance for

Internet of Things Innovation (AIoTI) [60] define a taxonomy for IoT identifiers. Table 3 presents this taxonomy with the function and use cases for each category.

Table 3. Taxonomy of IoT identifiers.

Identifier Category	Function	Use Case
Objects/Things Identifiers [59,60]	Used to identify the entity of interest, which could be physical or virtual	Sensors, machines, humans, merchandise (physical). Data, files, metadata (virtual)
Communication Identifiers [59,60]	Used to identify Things in the scope of communicating with other devices, including Internet-based communications.	IP address, MAC address, E.164
Application and Service Identifiers [59,60]	Used to identify applications/services used in the scope of IoT applications.	URL, URI, identifiers for different services on a single platform
User Identifier [60]	Used to identify physical or virtual objects that interact with IoT devices on the Internet.	ID for humans/animals (physical). ID for software applications interacting with IoT devices (virtual)
Data Identifier [60]	Used to identify data instances and datatypes	Digital Twin, stored sensor measurements
Location Identifier [60]	Used to specify a location within a geographical region	Coordinates, postal codes
Protocol Identifier [60]	Used to identify protocols so that, for example, layers within a communication stack can identify what protocols are being used by other layers	Ethertype

6.2.2. Requirements for IoT Identifiers

Table 4 lists the most common requirements for IoT identifiers suggested by AIoTI [60] and the ITU-T [61].

Table 4. Requirements of IoT Identifiers.

Requirement	Definition
Identify anything physical or virtual [61]	The identifier should be able to identify any physical or virtual thing as it is required that any physical or virtual thing can be connected to network infrastructure, which implies the necessity of having an identifier.
Communication between things [61]	Connection between things using identifiers, regardless if a particular thing needs to communicate or not, should be guaranteed.
Networking technology independence [61]	Identifiers should be independent of the underlying network technology used by the thing they identify.
Uniqueness [60]	Uniqueness is required within the specific application context. If a larger scope is needed where identifiers are no longer unique, a replacement or an extension of the identification scheme is always necessary to guarantee the identifier's uniqueness.
Security and Privacy [60]	Identifiers used should be privacy- and personal-information-preserving. Ideally, identifiers should not leak information about the entity they define. The identifier by itself should not reveal, based on its structure, information about the identified thing.
Scalability [60]	The identification scheme should be able to accommodate the increasing number of identification-needing things in the future.
Interoperability [60]	Even if a single identification scheme does not exist, the existing and any newly proposed ones should account for interoperability between different schemes.

6.2.3. IoT Identification Schemes

The identification schemes in IoT are diverse. Unlike machines using the TCP/IP protocol suite identified by unique IP addresses, IoT devices are defined by whichever identifier their manufacturer decides to use. We introduce some of the most known IoT identification schemes today in the following. We mainly focus on ones that are widely used in practice. We start with IP, which has been used as an identifier in 6LoWPAN. We follow that with the Digital Object Identifier, Electronic Product Code, and Object Identifier.

- **IP Addresses:** We start with the most common identifier, the Internet Protocol (IP) address. In the context of IoT, IP typically means IPv6 since the 32-bit IPv4 is already exhausted. On the other hand, the 128-bit IPv6 has a massive address space (2^{128} addresses) and could theoretically accommodate existing and future IoT devices. RFC 4919 [62] defines how IPv6 is used in Low-Power Wireless Personal Area Networks (LoWPANs). The devices in LoWPANs conform with our definition of constrained IoT devices. According to [62], these devices conform with the IEEE 802.15.4-2003 standard and are characterized by short-range, low bit rate, low power, and limited computational power and memory. IPv6 is used in such networks as a unique identifier for each device within the scope of the network. Other than its large address space, IP is preferential because it has been around for a long time. Therefore, its standards and regulations are readily and freely available and well-known in addition to its existing infrastructure that includes management, diagnostic, and commissioning tools [62].
- **Digital Object Identifier:** The Digital Object Identifier (DOI) is defined in the ISO 26324:2012 standard [63]. It was initially developed by the International DOI Foundation (IDF), which three publishing institutes formed [64], and later standardized by ISO 26324:2012 [63]. Later, the DOI system became the go-to tool for identifying objects digitally. The word Digital in Digital Object Identifier refers to the identifier. DOIs are meant to be unique, persistent, and permanent digital identifiers for objects. Information about an object identified by a DOI can be retrieved upon resolving the DOI. DOIs are formed of two parts, prefix and suffix, separated by a "/" and with no maximum length. The prefix identifies a unique naming authority that is responsible for assigning DOIs. The suffix is a unique identifier of objects which, for interoperability purposes, could be an existing identifier. A typical DOI, for example, is 10.100/20.

The Handle System [65,66] does the resolution of DOI. The Handle System is a set of distributed servers that allow the storage of handles that refer to digital objects. The system can efficiently and securely resolve the handles into information to locate and access the intended object. Additional services could be added, such as data confidentiality, data integrity, and non-repudiation.

- **The Electronic Product Code (EPC):** The EPC is a universal identifier for physical objects operated by GS1 [67]. It is used whenever an object needs to be tracked or identified. EPC is predominantly known as the ID used in Radio Frequency Identification (RFID). RFIDs act as data carriers holding the object's EPC to which they are attached. However, this is not always the case. EPC is not exclusively used in RFID; the latter does not always contain an EPC. When stored on computer systems, EPCs are in the form of a Universal Resource Identifier (URI), often referred to as Pure Identity EPC URI. A typical Pure Identity EPC URI in Uniform Resource Names (URN) notation, for example, is

urn : epc : id : sgtin : 0614141.112345.400

On RFID tags, and due to their memory limitations, EPCs are encoded in binary form. The resolution of EPC codes is accomplished using the Object Name Service (ONS) [11], which is based on the existing Domain Name System (DNS).

- **Object Identifier:** The Object Identifier (OID) [68] was developed jointly by ITU-T starting with ITU-T X.660 series [69], and ISO through ISO/IEC 9834-1:2012 [70].

The goal was to provide an unambiguous persistent name for objects. The OIDs are organized in a hierarchical tree structure. The top level is called the root; under it are nodes from which many arcs branch infinitely. An object's name is the path from the root downwards until the node related to that object is reached. A typical OID in dot notation, for example, is

1.2.840.113549.1

and in URN notation

urn : oid : 1.2.840.113549.1

For resolution, the OID Resolution System (ORS) is a DNS-based system that accepts queries about OIDs and returns associated information. Various objects, big and small, could be identified using OIDs, such as countries, companies, X.509 certificates, standards, and Simple Network Management Protocol Management Information Bases (SNMP MIBs), to name a few.

6.3. IoT Security

RFC 8576 [71] titled 'IoT Security: State of the Art and Challenges' gives a general overview of the security challenges facing IoT environments. IoT security drawbacks are not due to a lack of security mechanisms but have roots in the devices' design. The constrained IoT devices are meant to serve particular purposes, such as measuring temperature or detecting motion. Therefore, vendors of such devices seek to keep the designs simple and the prices low. So, most constrained IoT devices were designed without considering the security threats they may face. These facts prevent these devices from using modern security functions designed for more powerful ones. So, they either abandon security or use weak protocols and implementations [71]. In addition, and also due to the factors mentioned before, given their constrained nature and rapid development, some IoT devices do not receive necessary firmware updates as often as they should [72]. These firmware updates should be regular to avoid depriving these devices of possibly essential security updates. IoMT is one domain where security and privacy are paramount due to the sensitivity of the patient data. It is, however, vulnerable to the same attacks as other IoT devices [73–75].

Figure 5 shows the classification of some IoT attacks [76,77] based on the three-layer model for IoT architecture.

- Perception Layer Attacks
 - Node capture attack: A physical attack against IoT nodes where the attacker captures the node and gains control over it. The attacker can then either impersonate the node, block incoming and outgoing traffic, or gain unauthorized access to the network associated with the node.
 - Replay attack: Replay attacks happen when the attacker captures a legitimate message destined for the device and saves it. The attacker later retransmits (replays) the same message to trick the devices about the sender's identity. Replay attacks could allow attackers to access the network and control the devices.
 - Side-channel attack: Side-channel attacks occur due to unintentional device information leakage. This includes power consumption, acoustic emissions, or timing information. Using this information, an attacker might be able to, for example, guess the device's key based on the power consumption during encryption or decryption.
 - False data injection attack: Occurs when attackers inject false data into devices. These attacks can be carried out manually on compromised devices, using Man-in-the-Middle or malware. False data injection attacks are particularly dangerous in critical applications such as healthcare.

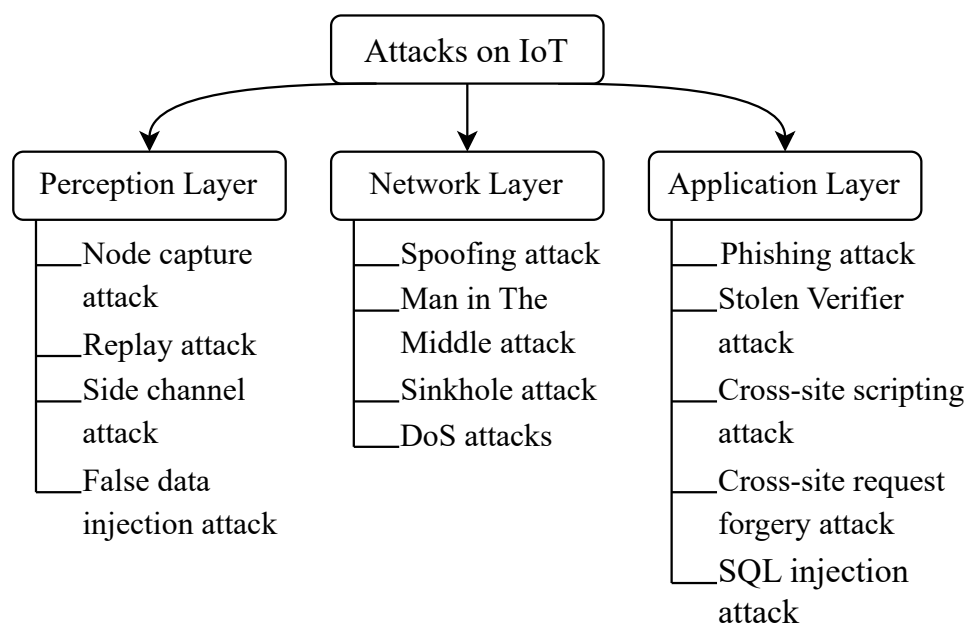


Figure 5. Attacks against IoT (three-layer architecture).

- **Network Layer Attacks**
 - **Spoofing attack:** Occurs when an attacker impersonates legitimate devices or users on the network. This is achieved by altering data to make them look like they originated from other users or devices. Spoofing includes, for example, MAC spoofing, IP spoofing, or DNS spoofing.
 - **Man in The Middle attack:** Such attacks happen while data is transmitted between devices or between a device and its backend servers. The attacker intercepts the data and could sniff, alter, or block the communication.
 - **Sinkhole attack:** Occurs when attackers redirect IoT traffic to a compromised device or malicious server instead of the legitimate destination. This is accomplished by controlling the DNS or routing infrastructure.
 - **DoS attack:** Denial of Service (DoS) attacks occur when a large number of compromised devices are used to overwhelm a target server by sending a large number of requests. The target could be a DNS server or a regular web server.
- **Application Layer Attacks**
 - **Phishing attack:** Occurs when an attacker sends a malicious file or link to users of IoT devices posing as a legitimate entity such as a service provider or a manufacturer. Malware is installed upon clicking the link or opening the file, which might grant the attacker access to the network and control over its devices.
 - **Stolen Verifier attack:** Occurs when an attacker obtains a password or an authentication token that grants them access to the network and the devices connected to it. The attacker can then impersonate the users or devices of the network, leading to possible information theft or data corruption.
 - **Cross-site scripting (XSS) attack:** An injection attack where the attacker injects malicious code into a webpage or web application. This could be, for example, the web interface for managing IoT devices. As a result, the attacker can control the devices, steal sensitive information, or corrupt data.
 - **Cross-site request forgery (CSRF) attack:** Occurs when an attacker tricks a user into performing a malicious action on the webpage the user is already authenticated to. The attacker can then gain access to the network, steal or corrupt data, or control the devices connected to that network.
 - **SQL injection attack:** Occurs when an attacker inserts malicious SQL statements into an application's input field. As a result, the attacker can corrupt, steal, or

modify data. In the context of IoT, an IoT device with a web interface that accepts user input, such as a security camera with a login page, may be vulnerable to SQL injection attacks.

The facts above drove the research community to look into IoT vulnerabilities and the consequences such vulnerabilities may have on different security objectives if exploited by attackers [78–80]. IoT has benefited from the development of new technologies, such as Blockchain [76,81,82], and the advances that leverage Machine Learning (ML) [83,84] to improve security and mitigate attacks.

6.4. IoT Interoperability

In IoT, each vendor has its own infrastructure, devices, Application Programming Interfaces (APIs), and data formats [85]. This causes an interoperability problem between different technologies. Interoperability is regarded by the ITU-T as one of its high-level requirements for IoT, stating that “interoperability is essential among heterogeneous and distributed systems for the provision and consumption of a variety of information and services” [32].

RFC 8477 [86] attributes the lack of interoperability to the lack of an encoding-independent standardization and the link between the data formats and the technology that produces it. There is no shortage of IoT standards, but their abundance and the fact that they originate from numerous organizations [87] make achieving interoperability harder. Heterogeneity could be seen as device-level heterogeneity due to the various technologies and protocols used in devices, data-level heterogeneity due to various formatting of data, and semantic heterogeneity related to how different technologies interpret data they receive from other technologies [88]. Semantic heterogeneity and achieving semantic interoperability have been studied extensively [88–91]. Due to the lack of standardization, IoT technologies send and receive data in proprietary forms. One IoT device could not understand the meaning (semantic) of what some other device sent if the latter belonged to a different technology. Solutions for semantic heterogeneity include using a middleware, ontology, and semantic web of technologies.

Several organizations issued proprietary standards in an attempt to facilitate interoperability. We present two of them: The Web of Things and OneM2M.

The Web of Things: The Web of Things (WoT) [92,93], created by the World Wide Web Consortium (W3C), is a concept that aims to enable interoperability between existing IoT technologies by connecting things in these networks to the web. WoT aims to preserve and complement existing IoT technologies rather than implement new ones. The main building blocks of the WoT are:

- **Thing Description (TD):** The TD is a central building block of WoT. It contains metadata describing the thing, a set of Interaction Affordances indicating how the thing can be used, schemas for the data exchanged with the thing for machine understandability, and web links to express the thing’s relation with other things or documents.
- **Binding templates:** These consist of reusable vocabulary and extensions to the TD format that enables a client to interact with diverse things exposing different protocols.
- **Scripting API:** An optional block that enables implementing the application logic of a thing using a common JavaScript API similar to web browser APIs.
- **Security and Privacy Guidelines:** Guidelines for secure implementation and configuration of things.

Human-assisted semantics translation would extend the WoT, allowing IoT devices to understand metadata from devices that use different semantics to increase semantic interoperability between heterogeneous devices further [94].

OneM2M: OneM2M [95] was established in 2012 as a partnership project between eight standardization bodies. The goal was to address the interoperability problem in IoT and machine-to-machine communications by promoting a global IoT standard. OneM2M does not propose a new standard but builds on the existing standards and aims to facilitate

interoperability. This is achieved by defining a common middleware between IoT devices, communication networks, and IoT applications. This middleware service layer contains a suite of common service functions (CSFs) exposed to IoT devices and applications via RESTful APIs. CSFs are general-purpose services unrelated to specific IoT domains or technologies. They can be looked at as generic operating system tools that various IoT devices and applications could use. The claim is that OneM2M allows any IoT application to connect to any IoT device, facilitating interoperability between IoT silos.

The fact that IoT is developing fast and quickly becoming a need rather than a luxury requires its challenges to be addressed. These challenges, as discussed above, are numerous and, to some extent, intertwined. The root cause lies in the constrained nature of IoT devices. Whenever a device is made with such specifications, it is automatically deprived of many tools used by today's computers and servers. Tools that deal, for example, with security, privacy, and identification are not compatible with constrained IoT. Another definite fact about IoT is the diversity due to the different technologies, each using its proprietary standards and tools. While developing new technologies is essential, the conspicuous lack of interoperability between these different technologies prevents IoT from becoming a global network. Furthermore, the lack of interoperability in IoT slows down the research backing it up, as different technologies disperse the research efforts, making progress slower and more individual to each technology rather than for the whole IoT environment.

The DNS is a valuable tool to address the challenges described in this section. However, DNS has its drawbacks, especially regarding security and privacy. In Section 7, we present its primary function, security and privacy drawbacks and the extensions developed to address them.

7. The Domain Name System

In the early stages of the Internet, a simple 'HOSTS.txt' file located on a single computer was responsible for the domain name-to-IP address translation. All hosts retrieved the 'HOSTS.txt' file via FTP. The bandwidth required to download this file was proportional to N^2 for a network of N hosts [8]. This solution worked properly when N was small, but the growth of the Internet mandated that a more scalable solution be found. The solution was the Domain Name System (DNS). The DNS is a distributed lookup service that is used to translate domain names (such as "www.afnic.fr" (accessed on 24 April 2023)) to IPv4 addresses (such as 192.134.5.37) and IPv6 addresses (such as 2001:67c:2218:302::51:231). The DNS acts as the Internet's phonebook and ensures that communications on the Internet, such as email or simple web browsing, are easily and efficiently carried out.

Many standardization documents describe the functions of DNS. The IETF regularly publishes RFCs that define or update DNS functions. Since the first steps to naming hosts were laid out in 1982 by RFC 819 [96], which was followed by RFC 920 [97] that introduced the idea of domain names, DNS has undergone many updates, some of the major ones being RFC 1034 [8] and RFC 1035 [58], which were the blueprint of today's DNS.

7.1. Function of DNS

The primary function of DNS is to map domain names to IP addresses. The domain names are usually given to resources on the Internet that users wish to access. The mapping process is referred to as domain name resolution. The DNS resolution process is depicted in Figure 6.

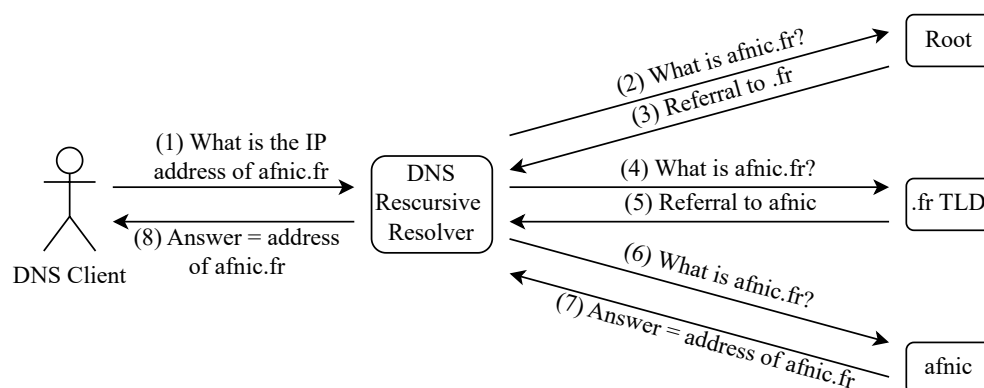


Figure 6. DNS resolution process.

For example, a user that wishes to visit the website of Afnic (Afnic is the French Internet Registry) will type in their browser “www.afnic.fr (accessed on 24 April 2023)”. The first entity that receives the request, also known as the DNS query, is the stub resolver, which is usually part of the operating system. The stub resolver then transfers the query to the DNS recursive resolver. Recursive resolvers are the main interface between users and the DNS infrastructure. After receiving the query, the recursive resolver begins a hierarchical query/response process with the name servers of DNS. Name servers are DNS servers that map domain names to IP addresses. The set of all possible domain names and their associated IP addresses is known as the DNS namespace, and name servers that could return definitive answers to queries (i.e., answer with the IP address) about a subset of the DNS namespace are said to be authoritative over that subset.

The recursive resolver first sends the query to one of the root name servers. These servers are authoritative over Top-Level Domains (TLDs) such as .com and .fr. The root name server answers with a referral to the .fr name server. The recursive resolver then sends the request to the .fr name server, which is authoritative over .fr domain names. Hence, it can answer with a referral to Afnic’s name server, which is authoritative over “www.afnic.fr (accessed on 24 April 2023)”. Lastly, the recursive resolver sends the query to Afnic’s name server, which answers with the IP address of “www.afnic.fr (accessed on 24 April 2023)”. The recursive resolver then sends back the answer to the user.

7.2. DNS Security Drawbacks

When the DNS was first deployed, privacy and security were not considered [98]. Recently published RFC 9076 [98] titled ‘DNS Privacy Considerations’ studies the security (mainly privacy) drawbacks of DNS that end users should keep in mind. The drawbacks include sending the queries in plain text, which jeopardizes privacy, using UDP, whereas most security mechanisms are designed for TCP, sending the full QNAME (Query Name, i.e., the requested domain) at every stage of the resolving process even though it is not needed, sending unnecessary DNS requests due to resource prefetching and auto-completion, cache snooping, and the passive DNS data collection by powerful companies running public DNS servers like Google [99] and Cloudflare [100]. One cannot be sure that such valuable data are not sold to third-party companies for commercial purposes or abused for surveillance and spying. Finally, the Server Name Indication (SNI), the last plain-text part of a secured web connection, is worth mentioning. The SNI is used in the case of multi-hosting to identify the intended resource requested on the webserver. SNI is still sent without encryption, which exposes the browsing habits of users [101].

We present next the most known DNS security and privacy standards and extensions. See Figure 7.

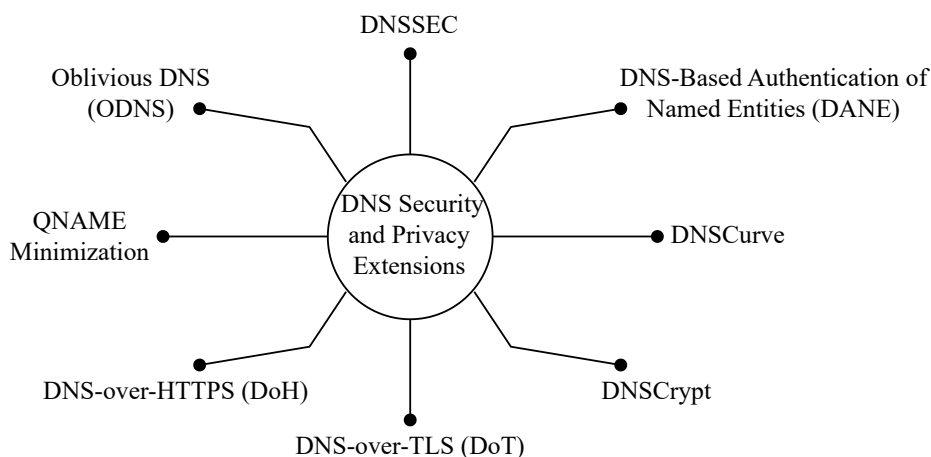


Figure 7. DNS security and privacy extensions.

7.3. DNS Security Standards

If the DNS is to be used with IoT, as discussed in Section 8, it must ensure that communications to and from the constrained IoT devices are secure. We introduce the most known DNS security standards and extensions in what follows.

DNSSEC: DNSSEC [102] stands for DNS security extensions. DNSSEC guarantees the integrity (not privacy) of DNS responses that DNS clients receive using an authentication chain. The chain starts at the root servers, which are trusted by default. Going down, every level in the hierarchy vouches for the level below it. Cryptographic signatures are added to DNS resource records to ensure the DNS client that the record they receive came from the legitimate DNS server and that it has not been tampered with on the way. The DNSSEC mechanism is presented in Figure 8.

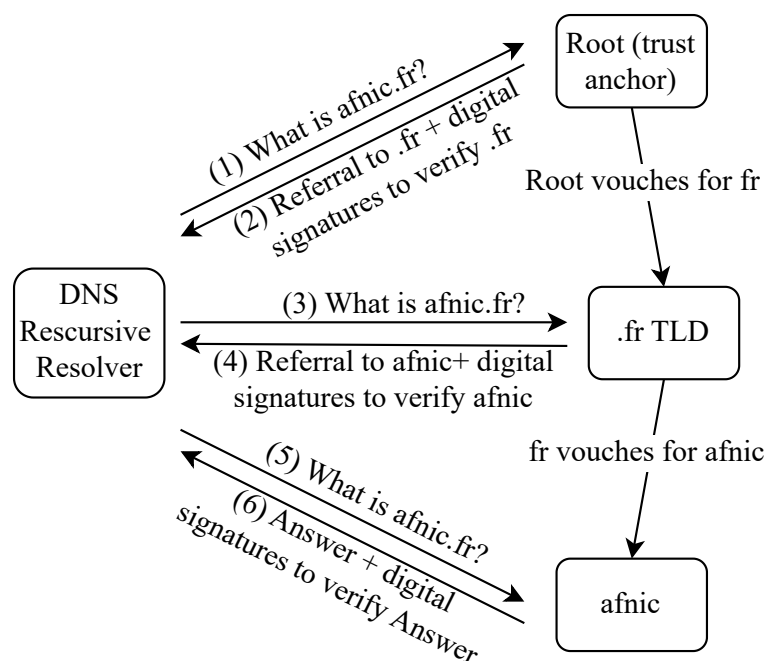


Figure 8. DNSSEC verification.

RFC 4033 [102] provides an introduction to DNS security and requirements, RFC 4034 [103] defines the Resource Records for the DNS Security Extensions, and RFC 4035 [104] is about the modifications required in the initial DNS protocols following the introduction of DNSSEC. RFC 4398 [105] discusses storing certificates in the DNS, RFC 5155 [106]

presents DNSSEC hashed authenticated denial of existence, and RFC 6014 [107] explains how the cryptographic algorithm identifiers needed to implement DNSSEC are allocated in the Internet Assigned Numbers Authority (IANA) registries.

DNS-Based Authentication of Named Entities (DANE): DNS-Based Authentication of Named Entities (DANE), which was introduced in RFC 6698 [108], is a security protocol that allows domain name owners to associate digital certificates with their domain names to provide a way to authenticate and secure Internet communications. DANE uses DNSSEC to guarantee the integrity of certificates and associated domains.

DNSCurve: DNSCurve [109] was designed in 2009 to add link-level security to DNS using elliptic-curve cryptography. In particular, DNSCurve preserves confidentiality by encrypting DNS packets, protects the integrity of DNS responses by cryptographically authenticating them, and ensures availability by protecting against Denial of Service (DoS) attacks. DNSCurve uses 256-bit public and secret keys, 192-bit nonces, and 128-bit authenticators. DNS servers that use DNSCurve distribute their public keys by encoding them in regular nameserver (NS) records, ensuring that the public key distribution system is compatible with registries and name server software. On the other hand, clients share their public keys in the queries they send.

DNSCrypt: DNSCrypt [110] acts between DNS clients and DNS recursive resolvers. It uses cryptographic signatures to verify that responses from the resolvers are authentic and have not been tampered with on the way. Anonymized DNSCrypt [111] was proposed in 2019 as an extension to further secure DNS traffic by not allowing the server to see the client's IP address.

DNS-over-TLS: DNS-over-TLS (DoT) [9,112] is one of the few IETF-standardized DNS-securing protocols (the other notable one being DNS-over-HTTPS)). Instead of the traditional UDP, DoT uses TCP and provides packet authentication and confidentiality for DNS traffic between clients and resolvers. This is achieved using TLS. A TLS session is established on TCP port 853, and DNS data are exchanged over the secure channel.

DNS-over-HTTPS: DNS-over-HTTPS (DoH) [9,113] is the other IETF-standardized DNS-securing protocol. Its goal is also to preserve the integrity and confidentiality of DNS data. Moreover, as the name indicates, DoH uses HTTPS instead of benefiting only from the TLS handshake, as with DoT. The use of HTTPS allows a web application to use DNS securely. In DoH, any DNS query with its response is an HTTPS exchange. A client encodes the DNS request into an HTTP request using an HTTP GET or POST method.

7.4. DNS Privacy Extensions

This section describes other standards that introduced changes to the DNS protocol to preserve privacy. The most valuable information an adversary could retrieve from a compromised DNS query is about the source IP address and the requested domain or Query Name (QNAME). The source IP address may reveal the person or entity making that DNS request. Revealing the QNAME gives away the browsing habits of the query issuer and their email activity or at least which email exchange the query issuer is interacting with. Such knowledge could be exploited for commercial, political, or censorship purposes. The following paragraphs detail two approaches that altered the original DNS design to ensure confidentiality in DNS query resolution.

QNAME Minimization: One of the shortcomings of DNS is that the full QNAME and query type (QTYPE) are always sent during recursive DNS resolving, regardless of the stage of the resolving. Meanwhile, the full QNAME and QTYPE are only needed when the request reaches the authoritative name server of the domain requested. For example, when resolving "www.afnic.fr" (accessed on 24 April 2023), the root name server receives a query with QNAME 'www.afnic.fr' even though it only needs to know .fr and does not need to know QTYPE. QNAME minimization [114,115] aims to allow resolvers to send minimum information at every stage of the resolution since the principle is "the less data you send out, the fewer privacy problems you have" [116]. Therefore, when sending queries to servers not authoritative for the requested domains, resolvers implementing

QNAME minimization send a different QNAME to obscure the original one. Instead of the full QNAME, they send one level longer than what the name server is known to be authoritative for.

Oblivious DNS (ODNS): ODNS [117] addresses the fact that in any privacy setup, there should always exist a party that is trusted by default. The trusted party could be any entity from the ISP to large public DNS resolver companies. When a client sends DNS requests to their designated recursive DNS resolver, the resolver has complete access to the domains requested by the client and the client's IP. Mostly, this recursive resolver is trusted not to abuse or share this data with third parties. The trust is almost baseless since one has no solid reason to trust their recursive resolver. ODNS aims to eliminate the need for that trust by preventing the recursive resolvers from associating between client identities and requested domains. ODNS uses the existing DNS infrastructure, which facilitates its deployment.

DNS was first designed with the goal of mapping between domain names and IP addresses. Several extensions and functionalities have been added to DNS since its inception. These extensions gave the DNS the needed maturity to become a reliable tool for any application that securely stores and retrieves information. DANE, for example, in which DNS is used as a complement or a total replacement of the certificate authorities for TLS handshakes, shows that DNS could play roles in areas previously thought to be out of its usual scope [118].

8. DNS and IoT

Sections 7.3 and 7.4 demonstrated the ability of DNS to evolve. In particular, we explained how DNS evolved from being a basic name-to-address translation protocol to providing security and privacy for DNS traffic. In the following subsections, we explore the state-of-the-art works leveraging the DNS infrastructure and its protocols to tackle IoT challenges by providing seamless identification, interoperability, security, and privacy for IoT devices. We conclude the section with studies from the literature that evaluate the usage of DNS in IoT and the impact of the latter on DNS. Table 5 summarizes the use cases of DNS in IoT environments.

Table 5. Summary of DNS use cases in IoT environments.

DNS for Constrained IoT	DNS for IoT Name Resolution
<ul style="list-style-type: none"> QNAME minimization [114,115] and using elliptical curves [119] DNS over CoAP (DoC) [57,120] DNS over Datagram Transport Layer Security (DTLS) [121] 	<ul style="list-style-type: none"> Object Name Service (ONS) [11] OID Resolution System (ORS) [68] IoT name resolution [122,123] Finding and localizing IoT devices [124,125] Device autoconfiguration [126–128] Device identification [129] IoT roaming [130]
DNS for IoT Security	DNS for IoT Interoperability
<ul style="list-style-type: none"> Secure IoT name resolution using DNS's security extensions (see Section 7.3/7.4). PKI for IoT [118,130] Authentication for device autoconfiguration [131,132] Malicious activity detection through DNS traffic analysis [133,134] 	<ul style="list-style-type: none"> Overlay mechanisms for IoT naming [11,64,68,135] PKI that encourages IoT Interoperability using DNS and its security extensions [130] Interoperable service discovery using mDNS/DNS-SD [136–138]

8.1. DNS for Constrained IoT

As described in Section 6.1, IoT devices are constrained in nature and have limited processing power, memory, and power resources. Since the DNS was not designed for

constrained devices, its memory and bandwidth requirements are much more than what IoT can handle.

Even though most DNS responses fit in a 512-byte UDP packet [58], measurements between recursive resolvers and authoritative servers indicate that the network behavior is relatively uniform with IP packet sizes up to 1500 bytes [139]. DNSSEC operating with RSA signatures leads to significantly higher memory requirements [140]. Such large messages increase CPU usage and require high bandwidth.

QNAME minimization [114,115] and using elliptical curves [119] can considerably reduce the bandwidth and CPU usage. DNS over CoAP is another method that uses CoAP [57] for transport. CoAP allows for HTTP-like communication on constrained nodes [120]. DNS over Datagram Transport Layer Security (DTLS) [121] is based on TLS protocol and provides encryption for queries and responses between DNS clients and servers. It is more suited for constrained IoT scenarios that support low latency and loss-tolerant communication.

The constrained nature of most IoT devices will allow adopting DNS to solve many of its challenges. The DNS accounts for constrained devices through several extensions and could function according to their constraints.

8.2. DNS for IoT Name Resolution

Given the primary role of DNS on the Internet, which is to map domain names to IP addresses, it is expected to play a significant role in resolving IoT identifiers. Like regular Internet devices, IoT devices connected to the Internet will need identifiers and systems to resolve the identifiers into addresses. Addresses would eventually be used to query IoT devices for their readings, control and manage them, or be redirected to locations containing information about the device in question.

As explained in Section 6.2, the naming conventions for the IoT are numerous and, in most cases, incompatible. One possible way to solve heterogeneity in identification schemes is for a standardization organization to develop a globally unique naming convention and ask different stakeholders in the IoT space to use it. This could be done from a purely technical point of view. For example, the large IPv6 address space allows every IoT device to have a unique IPv6 address. However, having one global naming convention for all IoT devices will be nearly impossible. Industries like retail, automobile, and defense have proprietary naming conventions that they have used for a long time. Changing that would impact their infrastructure and operations considerably.

A more feasible alternative is to keep the existing naming conventions and develop the resolving process they use. Here is where DNS could be exploited. For example, DNS was used with ENUM (Electronic Number Mapping) to map telephone numbers to web addresses [141]. Moreover, there exist several DNS-based services such as the Object Name Service (ONS) [11] and the OID Resolution System (ORS) [68] that allow registration and resolution of unique identifiers for IoT devices. This shows the feasibility of DNS playing a more global role in name resolution for IoT, which will provide a familiar and robust solution for managing IoT devices and their namespace.

The work in [122] presents the problems different IoT platforms suffer from. The shortcomings of a particular system do not cause the problems, but they are caused rather because each technology has its naming scheme that cannot seamlessly connect to other IoT technologies and controls resolution over its defined namespace. The authors propose a new scheme for peer-to-peer equal name resolution. In the proposed method, names from various technologies are hashed into a string of bits. In addition to preserving privacy by one-way hashing of the name, it allows for resolution via DNS, which only requires adding a TLD (.iot). The authors in [123] studied the use of DNS architecture for IoT devoted to transport logistics. A hierarchical organization of DNS was presented that can scale globally by translating unique URIs to network addresses that can be used to extract information about the object of interest (status, location, etc.)

The global reach of DNS and its distributed nature were used in [124], where the existing DNS architecture was used to construct a search engine for the WoT, specifically a search engine for devices and their offered service. A TLD (.env, for example) is added. Users can then use a regular browser and look up, for example, service.location.env. The DNS resolving of service.location.env would return a list of devices offering the requested service at the specific location. Choosing a specific device requires only adding a level specifying the device requested to the name. The authors in [125] proposed a scheme to represent semantic metadata of IoT devices and encode those into domain names so that devices could be found by performing DNS queries. The paper also suggests 'DNS as a source of IoT Data', where DNS could be used to store TXT information about IoT devices.

DNS can help with device autoconfiguration. Autoconfiguration comes in handy in cases where the number of IoT devices is too large to be named individually. Autoconfiguration using DNS allows devices to name themselves and register themselves in their DNS zone. DNS Name Autoconfiguration (DNSNA) for IPv6-based IoT environments was proposed in [126,127]. DNSNA provides a global framework for IoT autoconfiguration, including defining DNS name formats for such devices, name generation, and registration of the generated DNS names. DNSNA uses IPv6 Neighbor Discovery Protocol (ND) to acquire the DNS search list through IPv6 Router Advertisement (RA) or DHCPv6. Once the DNS search list is acquired, the IoT device can generate its name using the DNS search list and its information. Authors in [128] extended DNSNA to IPv4 IoT devices by proposing DNSNAv4. IoT devices can register their DNS name using a DHCP server.

Moreover, the authors in [129] proposed IoTFinder, an IoT identification method using DNS traffic analysis. IoTFinder is a machine-learning-based multi-label classifier aiming to learn statistical DNS traffic fingerprints automatically. The authors in [130] presented IoTRoam, a roaming setup for IoT devices. The use case for IoTRoam was demonstrated with a LoRaWAN network where a Device could locate and join its dedicated Join Server with the help of DNS.

IoT is still far from having a global naming scheme with a global name resolution mechanism. A single solution to fit all the technologies is not realizable. However, the problem is still manageable. Some approaches leave the pre-existing naming schemes as is and work on an upper layer. Phone numbers, for example, are different in structure in each country but can interoperate globally using international codes. The diversity would not be eliminated, but it would be manageable. DNS can help many technologies interoperate while keeping their naming schemes intact. This, as discussed earlier, is already being done between individual technologies achieving peer-to-peer interoperability via DNS.

8.3. DNS for IoT Security

IoT presents several security risks to both consumers and businesses. As discussed in Section 6.3, the security risks in IoT environments are numerous. However, despite these risks, the security mechanisms currently deployed in IoT environments are inadequate and are usually proprietary as each IoT provider develops their own closed security solution. As a result, contrary to how security is set up on the regular Internet, there is no global security mechanism with known trust anchors for IoT technologies. Moreover, the constrained nature of IoT devices deprives them of security mechanisms currently used on the Internet that require more processing power and memory than most of these devices have. Since most IoT devices are highly constrained, bootstrapping trust, supporting secure communications, and guaranteeing privacy are significant challenges.

IoT data communication often needs a gateway to translate between the IoT device (e.g., sensors communicating via protocols such as Bluetooth or LoRa) and the end-points (e.g., cloud infrastructures using HTTP over IP) in the Internet core. One of the basic requirements in IoT is to control the terms under which an IoT device is allowed to onboard into the Internet core. Like regular devices on the Internet when joining a network, IoT devices must be authenticated when onboarding to a network. Such devices need an identifier and an authentication token to be admitted to the network. IoT technologies use

different (predominantly incompatible) mechanisms when accepting new devices. On the one hand, these mechanisms are weak. On the other hand, the different mechanisms are incompatible, which worsens interoperability. DNS has been used to secure some aspects of IoT communications, whether with IoT devices joining and registering to their networks or subsequent communications.

The authors in [130] propose a Public Key Infrastructure (PKI) based on DNS for secure onboarding of IoT devices. The work in [131] built on DNSNA and added authentication. The obtained algorithm, Secure Domain Name System Name Autoconfiguration (SDNSNA) for IPv6 IoT devices, uses DNSNA for name generation and NFC-based authentication to authenticate and register their devices. The idea is that users can communicate with an authentication server using their smartphone, which can communicate with IoT devices using NFC. More on securing autoconfiguration and registration was carried out in [132] with Advanced Secure DNS name autoconfiguration with Authentication and Authorization for enterprise IoT network (ASDAI). The authors in [135] extended the EPC ONS based on DNS to dynamically support heterogeneous object code identification. The authors in [133] designed an IoT router that analyzes DNS traffic to detect if IoT devices consulted unknown DNS servers, which is usually done by malicious devices such as botnets. Botnets, which are compromised devices controlled by a Command-and-Control (C&C) server, typically use DNS to connect to that server [142,143]. DNS Filtering & Extraction Network System (D-FENS) was proposed in [134]. D-FENS sits between the client and the recursive DNS server and accepts DNS requests. It then uses a deep learning model to accurately detect and blacklist unreported malicious domains that IoT devices could connect to.

Several protocols and extensions were devised to secure the DNS and were discussed in sections IV-C and IV-D. These could benefit IoT devices using DNS. The benefits IoT could reap include security, privacy, and authentication. Moreover, as discussed earlier, DNS is no longer seen as only a mapping tool between IP addresses and domain names.

8.4. DNS for IoT Interoperability

The IoT infrastructure must incorporate different IoT connectivity technologies and hardware, software, identification, security, privacy, and resolution services. Multiple stakeholders provide these components and services. Beyond vertical integration, horizontal interoperability between devices and systems will be critical for an IoT network.

For different technologies, interoperability is the ability to communicate seamlessly. This includes exchanging and using data, services, or functionality, regardless of the underlying technology and standards. The issue of interoperability is one major drawback of IoT today. As discussed in Section 6.4, IoT technologies' lack of interoperability is a significant drawback. This has caused the IoT environment to be fragmented into many incompatible technologies. These technologies develop and implement proprietary solutions and use communication protocols and data representation methods that few other technologies can understand. Thus, users and devices of one IoT technology are almost always bound to communicate with users and devices of the same technology. This fact transformed IoT into distant islands or silos, each having its standards.

DNS could play a role in alleviating some of IoT's interoperability issues. Its robustness and distributed nature have already encouraged some organizations to resort to it when looking for IoT solutions.

The Object Name Service (ONS) [11] is EPC's [67] resolution system that is based on DNS to resolve an EPC identifier to the location of the information associated with that identifier. The work in [135] suggests an enhancement to the ONS framework that enables it to handle heterogeneous object code identification. This technique shares similarities with established conventions such as OID [68] and DOI [63,64]. In [130], the authors laid out a PKI for IoT devices with an underlying technology based on DNS and its security extensions which aims to enable interoperability between heterogeneous IoT technologies. DNS-Based Service Discovery (DNS-SD) [144] demonstrates how DNS could be used to locate named entities. DNS-SD uses DNS Service records (SRV record) to locate services

by specifying the specific service and the domain the service belongs to as `service.domain`. The client requesting the service receives a list of available services that fit the query as `instance.service.domain`, and then a service instance is chosen. DNS-SD is compatible with the standard unicast DNS and the DNS-like Multicast DNS (mDNS) [145]. DNS-SD has been used in [136] to develop an interoperable service discovery for IoT environments. Other works [137,138] also developed a solution for service discovery of resource-constrained devices based on mDNS/DNS-SD.

DNS plays a vital role in IoT interoperability. With its primary function as a naming service, along with its security extensions, DNS provides a reliable and secure way to map IoT device names to network addresses or information about these devices. This should encourage different IoT technologies to either consolidate their naming mechanisms or use services based on DNS to allow interoperability between the various naming standards. Doing this allows for building a cohesive Web of Things with distributed registries containing information about IoT devices and their services. DNS also supports dynamic updates, which allows for the automatic reconfiguration of device addresses, making it well-suited for dynamic IoT environments.

8.5. Impact of IoT on DNS

So far, we have encouraged using DNS to address many of the IoT environment's challenges as we demonstrated how DNS could mitigate these challenges. However, we have also discussed the importance of DNS as one of the cornerstones of the Internet. The significance of DNS calls for caution when exposing this vital piece of the Internet's infrastructure to IoT. The large number of IoT devices and the constrained nature of most devices could endanger DNS. IoT manufacturers usually give little to no thought to the security of their devices. These devices are seen as having specific functions and not needing much security. Moreover, the constrained nature of IoT devices prevents them from arming themselves with state-of-the-art security solutions used today on the Internet. In addition, constrained IoT devices such as sensors usually lack a user interface, so it is not easy for users to interact with them. This makes it hard for users to notice if their devices have been compromised and are being used to launch attacks.

In [146], some challenges facing DNS in IoT scenarios are explored. It mainly focuses on functionality, security, and availability problems. The work in [147] investigates whether the current DNS is ready for IoT. The authors lay out criteria that should be met before using DNS with IoT and analyze whether these criteria are met or not. The conclusions drawn could be summarized as follows:

- **Security:** Security is the main enabler of IoT, and although DNS security is enhanced, it remains too costly for constrained IoT devices.
- **Mobility:** An IoT naming service should support mobility and automatic name update. DNS is ready to provide the automatic name update, but since mobility was not accounted for when designing DNS, it lacks this feature for now.
- **Infrastructure Independence:** Name resolution should generally be independent of the underlying infrastructure. DNS could provide that with local link extensions and technologies such as cloud computing.
- **Localization:** All devices must be localizable and reachable. The authors argue that DNS is evolving to account for service deployment and name format localization.
- **Efficiency:** Efficiency is crucial for latency-sensitive IoT services. Efficiency remains a significant challenge for DNS because the DNS name resolution mechanism incurs delays due to the hierarchical delegation and unpredictable cache hits.

Even though using DNS with IoT is helpful for the IoT environment, it should be done carefully. The ability of IoT devices to reach DNS servers poses significant risks to the DNS infrastructure. This includes public DNS servers used on the Internet and private DNS setups used in isolated networks. Given the importance of DNS, these risks should not be overlooked.

The risks of using DNS with IoT could be summarized as follows:

- Complex coding at the IoT layer: The improper design of some IoT devices increases the probability of making simple mistakes when configuring them, but that could lead to DDoS (Distributed Denial-of-Service) attacks [14,15].
- DDoS attacks: The large number of IoT devices, coupled with their security vulnerabilities, allows for DDoS attacks of increased size and complexity against Internet infrastructure, which includes the DNS [14,15]. The Mirai botnet DDoS attack against the DYN DNS service provider had an unprecedented strength at the time, reaching 1.2 Tbps [12,13]. Such attacks are launched from several hundred thousand IoT devices that the attackers control. Having many devices under the attackers' control makes countering the attack harder with traditional filtering based on IP addresses. This allows such DDoS attacks to last for extended durations.
- DDoS amplification: These attacks, also known as reflection attacks, depend on open resolvers' response to a query which is usually larger than the original query. Adversaries might abuse this by sending several DNS queries but using the victim's spoofed IP address as a source for these queries. The servers then respond and send responses to the victim's machine. The massive load received by the victim could overload its memory and CPU and put it out of service [15].
- Recent DNS vulnerability: A vulnerability in several popular TCP/IP stacks used in some IT and IoT firmware was discovered in 2021. It was referred to as 'Name: Wreck', and it allows the devices to be used for remote code execution and denial of service attacks [15].

9. Discussion

This survey aimed to investigate the potential benefits of using DNS to address the IoT environments' challenges. As illustrated in Figure 1, IoT technologies face several challenges. The scale at which IoT is integrated into daily life and the prediction of larger-scale deployments in the future demand that its challenges be scrutinized and alleviated one by one.

The constrained nature of IoT devices is one of its major limitations and simultaneously helped IoT spread. The constrained IoT devices are deprived of state-of-the-art protocols. These protocols are crafted for much more powerful devices on the Internet, such as personal computers, i.e., devices with enough processing power and memory. IoT devices, on the other hand, settle for inferior protocols, especially in terms of security, which jeopardizes data sent from and received by these devices. However, the processing, memory, and power constraints of IoT devices, even though they denied using state-of-the-art protocols, helped to spread the adoption of IoT technology due to their affordability and accessibility. DNS and its constrained-friendly extensions designed specifically for IoT could help IoT devices take advantage of modern tools adapted to their constraints.

The diverse IoT technologies that are mostly isolated from one another make it difficult to create a unified system for naming and identifying IoT devices. This is due to each manufacturer's diverse communication and data representation protocols. Many of these protocols are proprietary and are not readily available for use by other technologies. The DNS, the Internet's naming system, is the natural candidate to solve this issue. The well-established DNS infrastructure encourages using it to overcome the IoT identification problem. As discussed in Section 8, many initiatives already rely on DNS for IoT name resolution. However, a global solution is yet to be found.

Close to the identification challenge, there are significant interoperability issues between IoT technologies. These technologies are run by independent authorities, have their own standards, and are not compatible with one another. The IoT environment is thus fragmented and made up of independent vertical silos where one technology cannot communicate with the others due to the lack of standardization. This is crucial for the future of IoT, as having more interoperability between most, if not all, IoT technologies helps transform IoT into a global network. Furthermore, the lack of interoperability in IoT slows down research and development efforts supporting IoT, as different technologies

disperse the research efforts, making progress more individualized to each technology rather than for the whole IoT environment. As a globally distributed infrastructure, the DNS has already significantly transformed the Internet into a cohesive network. It can continue to play a role in developing the IoT environment, turning it from independent silos to a more interconnected network.

Finally, regarding the security challenges of IoT, addressing these challenges becomes even more critical when we inspect the nature of the data that pass through such networks. The data that pass through IoT networks are mostly sensitive due to the diversity of IoT applications, from smart homes to medical and industrial applications. On the one hand, the ambitious calls to connect everything promises a prosperous and more comfortable future where additional everyday objects are connected and easily managed. On the other hand, it means higher stakes, as more data shared over the network means a higher risk of security breaches. DNS can contribute immensely to improving the security of IoT communications. DNSSEC, which is being adopted progressively in today's Internet, can be used to ensure the integrity of DNS responses received by IoT devices. This helps prevent DNS cache poisoning attacks, spoofing attacks, and other DNS-related cyber threats. DNSSEC is essential for ensuring DNS response integrity, and its adoption is critical for enhancing the security of both IoT and regular Internet communications.

Moreover, to ensure privacy, DNS offers several extensions, some already standardized, like DoT and DoH, but they still need to be more widely adopted. DNS could also be adapted to constrained IoT, as with DoC. Therefore, to save IoT networks from being the weakest security link, using DNS and its security extensions and protocols is paramount.

10. Conclusions and Future Outlook

DNS is a valuable tool that has proved its worth as a pillar of today's Internet. If used in IoT environments, it promises to address many of these environments' challenges. Users, manufacturers, and administrators of IoT networks could reap huge benefits from exploiting the potential of DNS. As discussed in this survey, IoT faces several challenges related to device limitations and constraints, lack of standards, security issues, and interoperability problems. However, DNS can effectively address these challenges, enabling the widespread adoption and integration of IoT. DNS is flexible enough to be adapted to constrained devices, as seen with its extensions tailored to such devices as DNS over CoAP (DoC), which allows IoT technologies to benefit from its power. DNS is also highly scalable and can accommodate large numbers of devices, making it well-suited for the rapidly growing IoT landscape. Additionally, it can be beneficial when it comes to IoT identification. Moreover, DNS provides a universal standard for addressing devices, which could help overcome some of the interoperability issues of IoT environments and improve efficiency and reliability in IoT systems. Finally, DNS's security extensions and ability to adapt to constrained IoT make it instrumental in ensuring that IoT systems are secure. However, it is essential to exercise caution when using DNS in IoT environments, and our survey highlighted the potential risks that IoT could pose to DNS infrastructure.

Looking towards the future, DNS is expected to integrate more into IoT environments. Some interesting domains to look into include having a global naming system similar to domain names for constrained IoT devices that preserves the privacy of IoT data. Another area of research could be the development of new DNS extensions designed for IoT environments. For example, there could be extensions that allow for more efficient and secure resolution of device names. Furthermore, location-based services and personalized content delivery could be some of the services DNS could provide to IoT technologies. In the context of Social IoT (SIoT) [148], which is a concept that aims to create a more human-centric IoT by allowing more interactions between humans and devices, DNS could play a fundamental role in facilitating connecting IoT devices to social media platforms and autoconfiguring their profiles. In addition, blockchain technologies' increased security, transparency, and decentralization can benefit IoT applications. On the one hand, Distributed Sensor Networks (DSNs) relying on blockchain technologies can highly benefit

from decentralized data storage, secure data transmission, transparency, and scalability offered by blockchains. On the other hand, DNS could also profit from blockchains, and this could provide a secure, decentralized name resolution and registration system [149,150]. Finally, IoT edge computing could benefit from DNS by leveraging DNS to discover and communicate with nearby edge computing resources.

Author Contributions: Conceptualization, I.A. and S.B.; methodology, I.A., S.B. and K.K.; validation, S.B., K.K. and B.A.; formal analysis, I.A., S.B., K.K. and B.A.; investigation, I.A.; resources, S.B. and B.A.; data curation, I.A., S.B., K.K. and B.A.; writing—original draft preparation, I.A.; writing—review and editing, I.A., S.B., K.K. and B.A.; visualization, I.A.; supervision, S.B., K.K. and B.A.; project administration, S.B.; funding acquisition, S.B. and B.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the French National Research Agency (ANR)—PIVOT (ANR-20-CYAL-0002).

Data Availability Statement: Data will be made available upon request.

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

References

1. Bulashenko, A.; Piltyay, S.; Polishchuk, A.; Bulashenko, O. New Traffic Model of M2M Technology in 5G Wireless Sensor Networks. In Proceedings of the 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 25–27 November 2020; pp. 125–131. [CrossRef]
2. Piltyay, S.; Bulashenko, A.; Demchenko, I. Wireless Sensor Network Connectivity in Heterogeneous 5G Mobile Systems. In Proceedings of the 2020 IEEE International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 6–9 October 2020; pp. 625–630. [CrossRef]
3. Report: Connected Devices Have More Than Doubled Since. 2019. Available online: <https://www.telecompetitor.com/report-connected-devices-have-more-than-doubled-since-2019/> (accessed on 24 April 2023).
4. Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2030. Available online: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/> (accessed on 24 April 2023).
5. Number of Connected IoT Devices Will Surge to 125 Billion by 2030. Available online: <https://sst.semiconductor-digest.com/2017/10/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030/> (accessed on 24 April 2023).
6. Internet of Things (IoT) Total Annual Revenue Worldwide from 2019 to 2030. Available online: <https://www.statista.com/statistics/1194709/iot-revenue-worldwide/> (accessed on 24 April 2023).
7. Global IoT Market to Grow to \$1.5trn Annual Revenue by 2030. Available online: <https://www.iot-now.com/2020/05/20/102937-global-iot-market-to-grow-to-1-5trn-annual-revenue-by-2030/> (accessed on 24 April 2023).
8. Domain Names—Concepts and Facilities; RFC 1034; Internet Society: Reston, VA, USA, 1987. [CrossRef]
9. Schmid, G. Thirty Years of DNS Insecurity: Current Issues and Perspectives. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2429–2459. [CrossRef]
10. Saidi, S.J.; Matic, S.; Gasser, O.; Smaragdakis, G.; Feldmann, A. Deep Dive into the IoT Backend Ecosystem. In Proceedings of the Proceedings of the 22nd ACM Internet Measurement Conference, Nice, France, 25–27 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; IMC '22, pp. 488–503. [CrossRef]
11. Object Name Service (ONS). Available online: <https://www.gs1.org/standards/epcis/epcis-ons/2-0-1> (accessed on 24 April 2023).
12. DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say. Available online: <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet> (accessed on 24 April 2023).
13. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Berkeley, CA, USA, 16–18 August 2017; USENIX Association: Vancouver, BC, Canada, 2017; pp. 1093–1110.
14. Hesselman, C.; Kaeo, M.; Chapin, L.; Claffy, K.; Seiden, M.; McPherson, D.; Piscitello, D.; McConachie, A.; April, T.; Latour, J.; et al. The DNS in IoT: Opportunities, Risks, and Challenges. *IEEE Internet Comput.* **2020**, *24*, 23–32. [CrossRef]
15. Aucklah, K.; Mungur, A.; Armoogum, S.; Pudaruth, S. The Impact of Internet of Things on the Domain Name System. In Proceedings of the 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 6–8 May 2021; pp. 449–454. [CrossRef]
16. HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Aledhari, M.; Karimipour, H. A survey on internet of things security: Requirements, challenges, and solutions. *Internet Things* **2021**, *14*, 100129. [CrossRef]
17. Ali, R.; Muneer, A.; Panneer Selvam, D.D.D.; Mohd Taib, S.; Ghaleb, E. *Internet of Things (IoT) Security Challenges and Solutions: A Systematic Literature Review*; Springer: Singapore, 2021; pp. 128–154. [CrossRef]

18. Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A. Internet of Things: Security and Solutions Survey. *Sensors* **2022**, *22*, 7433. [CrossRef]
19. Jmila, H.; Blanc, G.; Shahid, M.R.; Lazrag, M. A Survey of Smart Home IoT Device Classification Using Machine Learning-Based Network Traffic Analysis. *IEEE Access* **2022**, *10*, 97117–97141. [CrossRef]
20. Ashraf, I.; Park, Y.; Hur, S.; Kim, S.W.; Alroobaea, R.; Zikria, Y.B.; Nosheen, S. A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 2677–2690. [CrossRef]
21. Bhuiyan, M.N.; Rahman, M.M.; Billah, M.M.; Saha, D. Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities. *IEEE Internet Things J.* **2021**, *8*, 10474–10498. [CrossRef]
22. Ren, Y.; Xie, R.; Yu, F.R.; Huang, T.; Liu, Y. Potential Identity Resolution Systems for the Industrial Internet of Things: A Survey. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 391–430. [CrossRef]
23. Mazhar, N.; Salleh, R.; Zeeshan, M.; Hameed, M.M. Role of Device Identification and Manufacturer Usage Description in IoT Security: A Survey. *IEEE Access* **2021**, *9*, 41757–41786. [CrossRef]
24. Guo, H.; Heidemann, J. Detecting IoT Devices in the Internet. *ACM/IEEE Trans. Netw.* **2020**, *28*, 2323–2336. [CrossRef]
25. Ashton, K. That 'Internet of Things' Thing. Available online: <https://www.itrc.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf> (accessed on 24 April 2023).
26. Standardization of NB-IOT Completed. Available online: https://www.3gpp.org/news-events/1785-nb_10t_complete (accessed on 24 April 2023).
27. Kanj, M.; Savaux, V.; Le Guen, M. A Tutorial on NB-IoT Physical Layer Design. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2408–2446. [CrossRef]
28. Bluetooth® Low Energy (LE). Available online: <https://www.bluetooth.com/learn-about-bluetooth/tech-overview/> (accessed on 24 April 2023).
29. Sigfox. Available online: <https://www.sigfox.com/en> (accessed on 24 April 2023).
30. Zigbee The Full-Stack Solution for All Smart Devices. Available online: <https://csa-iot.org/all-solutions/zigbee/> (accessed on 24 April 2023).
31. LoRa Alliance®. Available online: <https://lora-alliance.org/> (accessed on 24 April 2023).
32. Overview of the Internet of Things, 2012. ITU-T Recommendation Y.4000. Available online: <https://www.itu.int/rec/T-REC-Y.2060-201206-I/en> (accessed on 24 April 2023).
33. Al-Qaseemi, S.A.; Almulhim, H.A.; Almulhim, M.F.; Chaudhry, S.R. IoT architecture challenges and issues: Lack of standardization. In Proceedings of the 2016 Future Technologies Conference (FTC), San Francisco, CA, USA, 6–7 December 2016; pp. 731–738. [CrossRef]
34. Kakkar, L.; Deepali, G.; Saxena, S.; Tanwar, S. *IoT Architectures and Its Security: A Review*; Springer: Singapore, 2021; pp. 87–94. [CrossRef]
35. Gokhale, P.; Bhat, O.; Bhat, S. Introduction to IOT Int. Adv. Res. J. Sci. Eng. Technol. **2018**, *5*, 41–44.
36. Elkin, D.; Vyatkin, V. *IoT in Traffic Management: Review of Existing Methods of Road Traffic Regulation*; Springer: Cham, Switzerland, 2020; pp. 536–551. [CrossRef]
37. Dhingra, S.; Madda, R.B.; Gandomi, A.H.; Patan, R.; Daneshmand, M. Internet of Things Mobile–Air Pollution Monitoring System (IoT-Mobair). *IEEE Internet Things J.* **2019**, *6*, 5577–5584. [CrossRef]
38. Cai, Z.; Zhou, Y.; Qi, Y.; Zhuang, W.; Deng, L. A Millimeter Wave Dual-Lens Antenna for IoT-Based Smart Parking Radar System. *IEEE Internet Things J.* **2021**, *8*, 418–427. [CrossRef]
39. Deese, A.S.; Jesson, J.; Brennan, T.; Hollain, S.; Stefanacci, P.; Driscoll, E.; Dick, C.; Garcia, K.; Mosher, R.; Rentsch, B.; et al. Long-Term Monitoring of Smart City Assets via Internet of Things and Low-Power Wide-Area Networks. *IEEE Internet Things J.* **2021**, *8*, 222–231. [CrossRef]
40. Han, H.; Ma, W.; Zhou, M.; Guo, Q.; Abusorrah, A. A Novel Semi-Supervised Learning Approach to Pedestrian Reidentification. *IEEE Internet Things J.* **2021**, *8*, 3042–3052. [CrossRef]
41. Han, J.; Lin, N.; Ruan, J.; Wang, X.; Wei, W.; Lu, H. A Model for Joint Planning of Production and Distribution of Fresh Produce in Agricultural Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 9683–9696. [CrossRef]
42. Ben-Daya, M.; Hassini, E.; Bahrour, Z. Internet of things and supply chain management: A literature review. *Int. J. Prod. Res.* **2017**, *57*, 1–24. [CrossRef]
43. Ayaz, M.; Ammad-Uddin, M.; Sharif, Z.; Mansour, A.; Aggoune, E.H.M. Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk. *IEEE Access* **2019**, *7*, 129551–129583. [CrossRef]
44. Tun, S.; Madanian, S.; Mirza, F. Internet of things (IoT) applications for elderly care: a reflective review. *Aging Clin. Exp. Res.* **2021**, *33*, 855–867. [CrossRef]
45. Aloï, G.; Fortino, G.; Gravina, R.; Pace, P.; Savaglio, C. Simulation-Driven Platform for Edge-Based AAL Systems. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 446–462. [CrossRef]
46. Nouman, M.; Khoo, S.Y.; Mahmud, M.A.P.; Kouzani, A.Z. Recent Advances in Contactless Sensing Technologies for Mental Health Monitoring. *IEEE Internet Things J.* **2022**, *9*, 274–297. [CrossRef]
47. Huynh-The, T.; Hua, C.H.; Tu, N.A.; Kim, D.S. Physical Activity Recognition With Statistical-Deep Fusion Model Using Multiple Sensory Data for Smart Health. *IEEE Internet Things J.* **2021**, *8*, 1533–1543. [CrossRef]

48. Rashid, N.; Dautta, M.; Tseng, P.; Al Faruque, M.A. HEAR: Fog-Enabled Energy-Aware Online Human Eating Activity Recognition. *IEEE Internet Things J.* **2021**, *8*, 860–868. [\[CrossRef\]](#)
49. Pivoto, D.G.; de Almeida, L.F.; da Rosa Righi, R.; Rodrigues, J.J.; Lugli, A.B.; Alberti, A.M. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *J. Manuf. Syst.* **2021**, *58*, 176–192. [\[CrossRef\]](#)
50. Mei, G.; Xu, N.; Qin, J.; Wang, B.; Qi, P. A Survey of Internet of Things (IoT) for Geohazard Prevention: Applications, Technologies, and Challenges. *IEEE Internet Things J.* **2020**, *7*, 4371–4386. [\[CrossRef\]](#)
51. Kumar, N.; Acharya, D.; Lohani, D. An IoT-Based Vehicle Accident Detection and Classification System Using Sensor Fusion. *IEEE Internet Things J.* **2021**, *8*, 869–880. [\[CrossRef\]](#)
52. Zhang, G.; Lu, D.; Liu, H. IoT-Based Positive Emotional Contagion for Crowd Evacuation. *IEEE Internet Things J.* **2021**, *8*, 1057–1070. [\[CrossRef\]](#)
53. Bianco, G.M.; Giuliano, R.; Marrocco, G.; Mazzenga, F.; Mejia-Aguilar, A. LoRa System for Search and Rescue: Path-Loss Models and Procedures in Mountain Scenarios. *IEEE Internet Things J.* **2021**, *8*, 1985–1999. [\[CrossRef\]](#)
54. Singh, R.P.; Javaid, M.; Haleem, A.; Suman, R. Internet of things (IoT) applications to fight against COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 521–524. [\[CrossRef\]](#)
55. Ndiaye, M.; Oyewobi, S.S.; Abu-Mahfouz, A.M.; Hancke, G.P.; Kurien, A.M.; Djouani, K. IoT in the Wake of COVID-19: A Survey on Contributions, Challenges and Evolution. *IEEE Access* **2020**, *8*, 186821–186839. [\[CrossRef\]](#) [\[PubMed\]](#)
56. Bormann, C.; Ersue, M.; Keränen, A. *Terminology for Constrained-Node Networks*; RFC 7228; Internet Society: Reston, VA, USA, 2014. [\[CrossRef\]](#)
57. Shelby, Z.; Hartke, K.; Bormann, C. *The Constrained Application Protocol (CoAP)*; RFC 7252; Internet Society: Reston, VA, USA, 2014. [\[CrossRef\]](#)
58. *Domain Names—Implementation and Specification*; RFC 1035; Internet Society: Reston, VA, USA, 1987. [\[CrossRef\]](#)
59. China Academy of Telecommunication Research (CATR) and Research Cluster on the Internet-of-Things (IERC). EU-China Joint White Paper on Internet-of-Things Identification. Available online: <https://www.napier.ac.uk/research-and-innovation/research-search/outputs/eu-china-joint-white-paper-on-the-internet-of-things#downloads> (accessed on 24 April 2023).
60. Alliance for Internet of Things Innovation. Identifiers in Internet of Things (IoT). Available online: https://aioti.eu/wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf (accessed on 24 April 2023).
61. Requirements and Common Characteristics of the IoT identifier for the IoT Service. 2014. ITU-T Recommendation Y.4801. Available online: <https://www.itu.int/rec/T-REC-F.748.1-201410-1/en> (accessed on 24 April 2023).
62. Montenegro, G.; Schumacher, C.; Kushalnagar, N. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*; RFC 4919; Internet Society: Reston, VA, USA, 2007. [\[CrossRef\]](#)
63. ISO 26324:2012; Information and Documentation—Digital Object Identifier System. The International DOI Foundation: Westwood, MA, USA, 2012.
64. DOI Handbook. Available online: <https://www.doi.org/hb.html> (accessed on 24 April 2023).
65. Lannom, L.; Boesch, L.C.B.P.; Sun, S. *Handle System Overview*; RFC 3650; Internet Society: Reston, VA, USA, 2003. [\[CrossRef\]](#)
66. Handle.Net Registry. Available online: <https://www.handle.net/> (accessed on 24 April 2023).
67. Gs1 EPC Tag Data Standard. Available online: <https://www.gs1.org/standards/rfid/tds> (accessed on 24 April 2023).
68. Object Identifier (OID) Repository. Available online: <http://oid-info.com/> (accessed on 24 April 2023).
69. Information Technology—Procedures for the Operation of Object Identifier Registration Authorities: General Procedures and Top Arcs of the International Object Identifier Tree. ITU-T Recommendation X.660. 2011 Available online: <https://www.itu.int/rec/T-REC-X.660-201107-1/en> (accessed on 24 April 2023).
70. ISO/IEC 9834-1:2012; Information Technology—Procedures for the Operation of Object Identifier Registration Authorities: General Procedures and Top Arcs of the International Object Identifier Tree—Part 1. ISO/IEC JTC 1/SC 6 Telecommunications and Information Exchange between Systems. Seoul, Republic of Korea, 2012. Available online: <https://www.iso.org/obp/ui/#iso:std:iso-iec:9834-1:ed-4:v1:en> (accessed on 24 April 2023).
71. Garcia-Morchon, O.; Kumar, S.; Sethi, M. *Internet of Things (IoT) Security: State of the Art and Challenges*; RFC 8576; Internet Society: Reston, VA, USA, 2019. [\[CrossRef\]](#)
72. Zandberg, K.; Schleiser, K.; Acosta, F.; Tschofenig, H.; Baccelli, E. Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check. *IEEE Access* **2019**, *7*, 71907–71920. [\[CrossRef\]](#)
73. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet Things J.* **2021**, *8*, 8707–8718. [\[CrossRef\]](#)
74. Ding, Y.; Wu, G.; Chen, D.; Zhang, N.; Gong, L.; Cao, M.; Qin, Z. DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 1504–1518. [\[CrossRef\]](#)
75. Rahman, A.; Hossain, M.S.; Alrajeh, N.A.; Alsolami, F. Adversarial Examples—Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices. *IEEE Internet Things J.* **2021**, *8*, 9603–9610. [\[CrossRef\]](#)
76. Mohanta, B.K.; Jena, D.; Ramasubbareddy, S.; Daneshmand, M.; Gandomi, A.H. Addressing Security and Privacy Issues of IoT Using Blockchain Technology. *IEEE Internet Things J.* **2021**, *8*, 881–888. [\[CrossRef\]](#)
77. Schiller, E.; Aidoo, A.; Fuhrer, J.; Stahl, J.; Ziörjen, M.; Stiller, B. Landscape of IoT security. *Comput. Sci. Rev.* **2022**, *44*, 100467. [\[CrossRef\]](#)

78. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2702–2733. [CrossRef]
79. Jurcut, A.; Ranaweera, P.; Xu, L. Introduction to IoT Security; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 2019; pp. 1–39. [CrossRef]
80. Mishra, N.; Pandya, S. Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review. *IEEE Access* **2021**, *9*, 59353–59377. [CrossRef]
81. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *Internet Things* **2018**, *1–2*, 1–13. [CrossRef]
82. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
83. Uprety, A.; Rawat, D.B. Reinforcement Learning for IoT Security: A Comprehensive Survey. *IEEE Internet Things J.* **2020**, *2020*, 3040957. [CrossRef]
84. Lv, Z.; Qiao, L.; Li, J.; Song, H. Deep-Learning-Enabled Security Issues in the Internet of Things. *IEEE Internet Things J.* **2021**, *8*, 9531–9538. [CrossRef]
85. Atiquzzaman, M.; Noura, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mob. Netw. Appl.* **2018**, *24*, 769–809. [CrossRef]
86. Jimenez, J.; Tschofenig, H.; Thaler, D. Report from the Internet of Things (IoT) Semantic Interoperability (IOTSI) Workshop 2016; RFC 8477; Internet Society: Reston, VA, USA, 2018. [CrossRef]
87. Lee, E.; Seo, Y.D.; Oh, S.R.; Kim, Y.G. A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 1020–1047. [CrossRef]
88. Rahman, H.; Hussain, M.I. A comprehensive survey on semantic interoperability for Internet of Things: State-of-the-art and research challenges. *Trans. Emerg. Telecommun. Technol.* **2020**, *31*, e3902. [CrossRef]
89. Nagowah, S.D.; Ben Sta, H.; Gobin-Rahimbux, B.A. An Overview of Semantic Interoperability Ontologies and Frameworks for IoT. In Proceedings of the 2018 Sixth International Conference on Enterprise Systems (ES), Limassol, Cyprus, 1–2 October 2018; pp. 82–89. [CrossRef]
90. Ganzha, M.; Paprzycki, M.; Pawlowski, W.; Szmeja, P.; Wasielewska, K. Towards Semantic Interoperability Between Internet of Things Platforms. *Integr. Interconnect. Interoperability IoT Syst.* **2018**, 103–127. [CrossRef]
91. Gyrard, A.; Datta, S.K.; Bonnet, C. A survey and analysis of ontology-based software tools for semantic interoperability in IoT and WoT landscapes. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 86–91. [CrossRef]
92. Web of Things (WoT) Architecture. Available online: <https://www.w3.org/TR/wot-architecture/> (accessed on 24 April 2023).
93. Datta, S.K.; Bonnet, C. Advances in Web of Things for IoT Interoperability. In Proceedings of the 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), Yilan, Taiwan, 20–22 May 2019; pp. 1–2. [CrossRef]
94. Novo, O.; Francesco, M. Semantic Interoperability in the IoT: Extending the Web of Things Architecture. *ACM Trans. Internet Things* **2020**, *1*, 1–25. [CrossRef]
95. OneM2M. Available online: <https://www.onem2m.org/> (accessed on 24 April 2023).
96. The Domain Naming Convention for Internet User Applications; RFC 819; Internet Society: Reston, VA, USA, 1982. [CrossRef]
97. Domain Requirements; RFC 920; Internet Society: Reston, VA, USA, 1984. [CrossRef]
98. Wicinski, T. DNS Privacy Considerations; RFC 9076; Internet Society: Reston, VA, USA, 2021. [CrossRef]
99. Google Public DNS. Available online: <https://developers.google.com/speed/public-dns> (accessed on 24 April 2023).
100. Cloudflare Public DNS. Available online: <https://www.cloudflare.com/dns/> (accessed on 24 April 2023).
101. Huitema, C.; Rescorla, E. Issues and Requirements for Server Name Identification (SNI) Encryption in TLS; RFC 8744; Internet Society: Reston, VA, USA, 2020. [CrossRef]
102. Rose, S.; Larson, M.; Massey, D.; Austein, R.; Arends, R. DNS Security Introduction and Requirements; RFC 4033; Internet Society: Reston, VA, USA, 2005. [CrossRef]
103. Rose, S.; Larson, M.; Massey, D.; Austein, R.; Arends, R. Resource Records for the DNS Security Extensions; RFC 4034; Internet Society: Reston, VA, USA, 2005. [CrossRef]
104. Rose, S.; Larson, M.; Massey, D.; Austein, R.; Arends, R. Protocol Modifications for the DNS Security Extensions; RFC 4035; Internet Society: Reston, VA, USA, 2005. [CrossRef]
105. Josefsson, S. Storing Certificates in the Domain Name System (DNS); RFC 4398; Internet Society: Reston, VA, USA, 2006. [CrossRef]
106. Arends, R.; Sisson, G.; Blacka, D.; Laurie, B. DNS Security (DNSSEC) Hashed Authenticated Denial of Existence; RFC 5155; Internet Society: Reston, VA, USA, 2008. [CrossRef]
107. Hoffman, P.E. Cryptographic Algorithm Identifier Allocation for DNSSEC; RFC 6014; Internet Society: Reston, VA, USA, 2010. [CrossRef]
108. Hoffman, P.E.; Schlyter, J. The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA; RFC 6698; Internet Society: Reston, VA, USA, 2012. [CrossRef]
109. DNSCurve: Usable Security for DNS. Available online: <https://dnscurve.org/> (accessed on 24 April 2023).
110. DNSCrypt. Available online: <https://www.dnscrypt.org/> (accessed on 24 April 2023).
111. Anonymized DNSCrypt. Available online: <https://github.com/DNSCrypt/dnscrypt-protocol/blob/master/ANONYMIZED-DNSCRYPT.txt> (accessed on 24 April 2023).

112. Hu, Z.; Zhu, L.; Heidemann, J.; Mankin, A.; Wessels, D.; Hoffman, P.E. *Specification for DNS over Transport Layer Security (TLS)*; RFC 7858; Internet Society: Reston, VA, USA, 2016. [\[CrossRef\]](#)
113. Hoffman, P.E.; McManus, P. *DNS Queries over HTTPS (DoH)*; RFC 8484; Internet Society: Reston, VA, USA, 2018. [\[CrossRef\]](#)
114. Bortzmeyer, S.; Dolmans, R.; Hoffman, P.E. *DNS Query Name Minimisation to Improve Privacy*; RFC 9156; Internet Society: Reston, VA, USA, 2021. [\[CrossRef\]](#)
115. de Vries, W.; Scheitle, Q.; Müller, M.; Toorop, W.; Dolmans, R.; Rijswijk-Deij, R. *A First Look at QNAME Minimization in the Domain Name System*; Springer: Cham, Switzerland, 2019; pp. 147–160. [\[CrossRef\]](#)
116. Cooper, A.; Tschofenig, H.; Aboba, D.B.D.; Peterson, J.; Morris, J.; Hansen, M.; Smith, R. *Privacy Considerations for Internet Protocols*; RFC 6973; Internet Society: Reston, VA, USA, 2013. [\[CrossRef\]](#)
117. Schmitt, P.; Edmundson, A.; Mankin, A.; Feamster, N. Oblivious DNS: Practical Privacy for DNS Queries. *Proc. Priv. Enhancing Technol.* **2019**, 2019, 228–244. [\[CrossRef\]](#)
118. Ayoub, I.; Berthaud-Müller, G.; Balakrishnan, S.; Khawam, K.; Ampeau, B. The DNS to Reinforce the PKIX for IoT Backend Servers: Implementation and Evaluation. In Proceedings of the 2022 14th IFIP Wireless and Mobile Networking Conference (WMNC), Sousse, Tunisia, 17–19 October 2022; pp. 80–84. [\[CrossRef\]](#)
119. Igoe, K.; McGrew, D.; Salter, M. *Fundamental Elliptic Curve Cryptography Algorithms*; RFC 6090; Internet Society: Reston, VA, USA, 2011. [\[CrossRef\]](#)
120. Lenders, M.S.; Amsüss, C.; Gündogan, C.; Schmidt, T.C.; Wählich, M. Securing Name Resolution in the IoT: DNS over CoAP. In Proceedings of the CoNEXT Student Workshop, Virtual, 7 December 2021; Association for Computing Machinery: New York, NY, USA, 2021; CoNEXT-SW '21, pp. 11–12. [\[CrossRef\]](#)
121. Reddy, K.T.; Wing, D.; Patil, P. *DNS over Datagram Transport Layer Security (DTLS)*; RFC 8094; Internet Society: Reston, VA, USA, 2017. [\[CrossRef\]](#)
122. Yan, Z.; Kong, N.; Tian, Y.; Park, Y.J. A Universal Object Name Resolution Scheme for IoT. In Proceedings of the 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 1120–1124. [\[CrossRef\]](#)
123. Karakostas, B. A DNS Architecture for the Internet of Things: A Case Study in Transport Logistics. *Procedia Comput. Sci.* **2013**, 19, 594–601. [\[CrossRef\]](#)
124. Kamilaris, A.; Papakonstantinou, K.; Pitsillides, A. In Proceedings of the Exploring the Use of DNS as a Search Engine for the Web of Things; Seoul, Republic of Korea, 6–8 March 2014. [\[CrossRef\]](#)
125. Fernandez, S.; Amoretti, M.; Restori, F.; Korczynski, M.; Duda, A. Semantic Identifiers and DNS Names for IoT. In Proceedings of the 2021 International Conference on Computer Communications and Networks (ICCCN), IEEE, Athens, Greece, 19–22 July 2021. [\[CrossRef\]](#)
126. Lee, S.; Jeong, J.; Park, J. DNS Name Autoconfiguration for IoT Home Devices. In Proceedings of the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangju, Republic of Korea, 24–27 March 2015; pp. 131–134. [\[CrossRef\]](#)
127. Lee, S.; Jeong, J.P.; Park, J.S. DNSNA: DNS name autoconfiguration for Internet of Things devices. In Proceedings of the 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, Republic of Korea, 31 January–3 February 2016; pp. 410–416. [\[CrossRef\]](#)
128. Lee, K.; Kim, S.; Jeong, J.P. DNSNAv4: DNS Name Autoconfiguration for Internet-of-Things Devices in IPv4 Networks. In Proceedings of the 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, 27–29 March 2017; pp. 347–351. [\[CrossRef\]](#)
129. Perdisci, R.; Papastergiou, T.; Alrawi, O.; Antonakakis, M. IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroSP), Genoa, Italy, 7–11 September 2020; pp. 474–489. [\[CrossRef\]](#)
130. Balakrishnan, S.; Bernard, A.; Marot, M.; Ampeau, B. IoTRoam: design and implementation of an open LoRaWAN roaming architecture. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021.
131. Lee, K.; Kang, H.; Jeong, J.P.; Kim, H.; Park, J.S. Secure DNS name autoconfiguration for IPv6 internet-of-things devices. In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 19–21 October 2016; pp. 564–569. [\[CrossRef\]](#)
132. Kim, T.H.; Reeves, D.; Dutta, R. Advanced Secure DNS Name Autoconfiguration with Authentication for Enterprise IoT Network. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6. [\[CrossRef\]](#)
133. von Sperling, T.L.; de Caldas Filho, F.L.; de Sousa, R.T.; e Martins, L.M.C.; Rocha, R.L. Tracking intruders in IoT networks by means of DNS traffic analysis. In Proceedings of the 2017 Workshop on Communication Networks and Power Systems (WCNPS), Brasília, Brazil, 16–17 November 2017; pp. 1–4. [\[CrossRef\]](#)
134. Spaulding, J.; Mohaisen, D. In Proceedings of the Defending Internet of Things Against Malicious Domain Names Using D-FENS; Seattle, WA, USA, 25–27 October 2018; pp. 387–392. [\[CrossRef\]](#)
135. Ding, D.; Li, M.; Zhu, Z. Object Naming Service Supporting Heterogeneous Object Code Identification for IoT System. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018; Volume 1, pp. 545–554. [\[CrossRef\]](#)

136. Djamaa, B.; Richardson, M. *Towards Scalable DNS-Based Service Discovery for the Internet of Things*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2014; pp. 432–435. [\[CrossRef\]](#)
137. Stolikj, M.; Verhoeven, R.; Cuijpers, P.J.L.; Lukkien, J.J. Proxy support for service discovery using mDNS/DNS-SD in low power networks. In Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, Australia, 19 June 2014; pp. 1–6. [\[CrossRef\]](#)
138. Stolikj, M.; Cuijpers, P.J.L.; Lukkien, J.J.; Buchina, N. Context based service discovery in unmanaged networks using mDNS/DNS-SD. In Proceedings of the 2016 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–11 January 2016; pp. 163–165. [\[CrossRef\]](#)
139. DNS 2XL. Available online: <https://labs.apnic.net/?p=1386> (accessed on 24 April 2023).
140. Ager, B.; Dreger, H.; Feldmann, A. Predicting the DNSSEC overhead using DNS traces. In Proceedings of the 2006 40th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 22–24 March 2006; pp. 1484–1489. [\[CrossRef\]](#)
141. Hoeneisen, B.; Mayrhofer, A. *ENUM Validation Architecture*; RFC 4725; Internet Society: Reston, VA, USA, 2006. [\[CrossRef\]](#)
142. Li, W.; Jin, J.; Lee, J.H. Analysis of Botnet Domain Names for IoT Cybersecurity. *IEEE Access* **2019**, *7*, 94658–94665. [\[CrossRef\]](#)
143. Dietrich, C.J.; Rossow, C.; Freiling, F.C.; Bos, H.; Steen, M.v.; Pohlmann, N. On Botnets That Use DNS for Command and Control. In Proceedings of the 2011 Seventh European Conference on Computer Network Defense, Gothenburg, Sweden, 6–7 September 2011; EC2ND '11, pp. 9–16. [\[CrossRef\]](#)
144. Cheshire, S.; Krochmal, M. *DNS-Based Service Discovery*; RFC 6763; Internet Society: Reston, VA, USA, 2013. [\[CrossRef\]](#)
145. Cheshire, S.; Krochmal, M. *Multicast DNS*; RFC 6762; Internet Society: Reston, VA, USA, 2013. [\[CrossRef\]](#)
146. Hamzic, A.; Olofsson, I. DNS and the Internet of Things: Outlining the Challenges Faced by DNS in the Internet of Things. Master's Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2016.
147. Yan, Z.; Li, H.; Zeadally, S.; Zeng, Y.; Geng, G. Is DNS Ready for Ubiquitous Internet of Things? *IEEE Access* **2019**, *7*, 28835–28846. [\[CrossRef\]](#)
148. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The Social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [\[CrossRef\]](#)
149. Xia, P.; Wang, H.; Yu, Z.; Liu, X.; Luo, X.; Xu, G.; Tyson, G. Challenges in Decentralized Name Management: The Case of ENS. In Proceedings of the 22nd ACM Internet Measurement Conference, Nice, France, 25–27 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; IMC '22, pp. 65–82. [\[CrossRef\]](#)
150. Rajendran, B.; Palaniappan, G.; Dijesh, R.; Bindhumadhava Bapu, S.; Sudarsan, S.D. A Universal Domain Name Resolution Service—Need and Challenges—Study on Blockchain Based Naming Services. In Proceedings of the 2022 IEEE Region 10 Symposium (TENSYP), Mumbai, India, 1–3 July 2022; pp. 1–6. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.