computers

MDPI

Article

A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures

Muath A. Obaidat [1,*], Suhaib Obeidat [2], Jennifer Holst [3], Abdullah Al Hayajneh [4] and Joseph Brown [1]

[1] Center for Cybercrime Studies, CUNY-John Jay College of Criminal Justice, New York, NY 10019, USA; joseph.brown1@jjay.cuny.edu
[2] Computer Science and Network Engineering, Bloomfield College, Bloomfield, NJ 07003, USA; suhaib_obeidat@bloomfield.edu
[3] Department of Computer Science, CUNY-John Jay College of Criminal Justice, New York, NY 10019, USA; jholst@jjay.cuny.edu
[4] Professional Security Studies, New Jersey City University, Jersey City, NJ 07305, USA; aalhayajneh@njcu.edu
* Correspondence: muobaidat@ccny.cuny.edu

Received: 10 May 2020; Accepted: 27 May 2020; Published: 30 May 2020

check for updates

Abstract: The Internet of Things (IoT) has experienced constant growth in the number of devices deployed and the range of applications in which such devices are used. They vary widely in size, computational power, capacity storage, and energy. The explosive growth and integration of IoT in different domains and areas of our daily lives has created an Internet of Vulnerabilities (IoV). In the rush to build and implement IoT devices, security and privacy have not been adequately addressed. IoT devices, many of which are highly constrained, are vulnerable to cyber attacks, which threaten the security and privacy of users and systems. This survey provides a comprehensive overview of IoT in regard to areas of application, security architecture frameworks, recent security and privacy issues in IoT, as well as a review of recent similar studies on IoT security and privacy. In addition, the paper presents a comprehensive taxonomy of attacks on IoT based on the three-layer architecture model; perception, network, and application layers, as well as a suggestion of the impact of these attacks on CIA objectives in representative devices, are presented. Moreover, the study proposes mitigations and countermeasures, taking a multi-faceted approach rather than a per layer approach. Open research areas are also covered to provide researchers with the most recent research urgent questions in regard to securing IoT ecosystem.

Keywords: security; privacy; cyber-attack; threat; mitigations; risk; cryptography; vulnerability; intrusion; encryption-key

1. Introduction

The Internet of Things (IoT) encompasses a wide range of application domains, including home, health, manufacturing and supply chain, agriculture, transportation, city and utilities. Physical devices in these domains are increasingly being connected to each other and the Internet [1]. These devices include home IoT devices, such as smart door locks, thermostats and appliances, connected cars, wearables, health-related devices, such glucose monitoring systems and pacemakers, industrial devices, such as manufacturing sensor networks and supply chain radio frequency identification (RFID) tags, agricultural devices, such as greenhouse sensors and irrigation controllers, and city services, such as street lighting and water distribution systems [2].

The IoT presents many benefits to individuals, organizations and municipalities alike. Devices that make home life more convenient are available and inexpensive, and remote sensors can monitor areas that are difficult to access [3]. Smart city IoT technology allows municipalities to track energy consumption and monitor the environment [4]. In both hospital settings and remote care monitoring, medical IoT devices can improve patient outcomes and reduce human errors [5]. The proliferation of IoT devices across application domains has attracted interest on many fronts, including investors, business and academia [3].

However, the IoT also presents challenges to security and privacy. Firstly, the hardware used to power the IoT is very limited compared to traditional IT devices like desktops, laptops and smartphones. IoT hardware has limited memory and processing capacity, from tens of kB of RAM at the lowest end sensors, to devices like the Raspberry Pi that can run an operating system [6]. While traditional IT devices can be updated, IoT devices usually do not allow updates by the user [7] and are also usually not subject to regular security patches and updates [8]. Limited processing capacity also limits the ability to run typical cryptographic protocols. The heterogeneity of device hardware and protocols makes it difficult to have a unified security solution [7]. Secondly, the vast amount of data collected by IoT devices gives rise to privacy concerns. New smart devices promise convenience and better living, but the variety and quantity of user data collected, analyzed, transported and stored at all layers of the IoT architecture is a vulnerability, allowing threats to user privacy.

A variety of approaches have been taken in defining layered IoT security architectures and frameworks. Earlier research [7] suggested a three-layer model with Perception, Transportation and Application layers where the Perception layer represents the physical sensors and actuators, e.g., RFID tags, that interact with the physical world, the Application layer provides smart functionality to the IoT users, and the Network layer transports information between the other two layers using various wireless technologies. More recent research presents security architectures defining additional layers. A Processing layer that represents an intelligent interface between the Application and Network layers is added in [9], where information from the Physical layer is processed through services including data mining, parallel computing and cloud computing. The authors of [10] present a five-layer security architecture, with an End-User layer representing the IoT devices, an Edge Network layer with servers that collect, process and provide storage for data from the devices, a Core Network layer that transports the processed data from the Edge Network layer to a Service and Storage layer, with data servers, software servers, and control servers. The data servers store the data processed on the edge network for further analysis, the software servers hold applications and operating system images, and the control servers manage the data and software servers; the fifth layer is a Management layer that provides overall management of the Service and Storage layer. A six-layer end-to-end view of security architecture is provided in [11], encompassing an application layer, a cloud layer, and information transmission layer, a gateway information layer, an internal communications layer, and end device layer.

Attacks may target a specific layer of any security architecture framework because of vulnerabilities in that layer. In this paper, we will review attacks and security challenges on the Perception (Physical) layer, the Network layer and the Application layer. The IoT devices in the Physical layer are resource constrained and may be in an open, unprotected environment, vulnerable to physical damage, tampering and forgery attacks [7,12–14]. The Network layer is critical to the transport of information between IoT devices and Application layer processes; Denial of Service (DoS) attacks can threaten the availability of network services [15,16] and vulnerabilities in the wireless protocols lead to additional security threats [13]. The Application layer that processes data from the IoT devices and provides smart functionality to users is vulnerable to exploits of software errors, application protocol weaknesses and permissions [13,16].

Security is of utmost importance in the IoT, especially in application domains that have systems critical to individual and community safety [17]. For example, connected cars and smart transportation systems need to be secure to prevent accidents and injury, as well as to protect the privacy of drivers who might be tracked as they travel on the roads [18]. Medical and health monitoring devices need to be secure to ensure that the information the devices monitor, collect, or report is correct and that life critical devices remain available and operating [19]. Researchers were able to breach an IoT-connected camera and retrieve images [20]. This kind of security breach can pose a threat to both individual privacy and corporate secrecy depending on the location of the camera. IoT devices can not only be the target of attack, but they can be harnessed to attack another system [21], just as traditional computers have been recruited into botnets to launch attacks.

There are three basic security requirements, confidentiality, integrity and availability, commonly known as the Confidentiality, Integrity and Availability (CIA) triad [22]. These security principles apply to the IoT as they do to the Internet as a whole [23]. If there is a loss of any one of these basic requirements, there is some impact to the individual or organization involved. The National Institute for Standards and Technology (NIST) provides definitions for Low, Moderate and High potential impacts due to loss of confidentiality, integrity or availability in FIPS 199 [24]. A loss of availability in one IoT application might not have the same impact as a similar loss in another IoT application [25]. In addition to providing a taxonomy of attacks by Perception (Physical), Network, and Application layers, we will consider the potential impact of attacks on the CIA triad according to the NIST definitions in a representative IoT device.

While mitigation and countermeasures can be taken for a specific attack, because of the interconnectedness and heterogeneity of the IoT network, a security strategy should take a more comprehensive, multi- and cross-layer approach [7]. Trade-offs between functionality and constrained device capabilities can be made across architecture layers [26–28]. Cryptography and encryption can provide confidentiality and integrity of data on devices and of data as it is transported through the network [29–31]. Blockchain networks have also been presented as a multi-layer countermeasure to provide security to IoT [32,33]. End-to-end security is a comprehensive mitigation approach to protect wireless communication between devices, adapted to the specific protocols in use [34]. Authentication applies to all layers, to verify and identify devices prior to sending or receiving data [35] and user identity, using various techniques, including access controls [36–39]. Given the heterogeneous nature of the IoT environment, standardization of protocols across devices and networks can mitigate security threats [30,36,40–45]. Addressing security countermeasures, including standardization, is a current open area of research for IoT.

Contribution

In addition to discussing recent surveys on IoT security, this paper makes the following contributions:

- Review the latest related security and privacy similar studies in IoT;
- Discuss proposals for IoT security architectures and frameworks in recent literature;
- Provide a taxonomy of attacks on IoT;
- Present classification of attacks' impacts according to NIST's FIPS 199 definitions on loss of Confidentiality, Integrity and Availability (CIA) due to attacks on select smart devices;
- Discuss a multi-faceted approach to mitigation and countermeasures in IoT security;
- Allocate a section on open research area pertain to IoT ecosystem.

The rest of this paper is organized into the following sections: Section 2 provides an overview of IoT; related work is presented in Section 3; the need for security is explored in Section 4; Section 5 discusses IoT security architecture and frameworks; Section 6 provides a taxonomy of attacks, threats and vulnerabilities in IoT and possible impact of attacks on CIA security objectives; mitigation and countermeasures are discussed in Section 7; Section 8 reviews current open research areas; the paper concludes and comments on future work in Section 9.

2. IoT Overview

2.1. Internet of Things (IoT)

The desire to collect and capture data, exchange and share information automatically, remotely, at any time and without interruption help push forward the creation of Internet of Things (IoT). IoT is defined as a network of Internet-connected objects/devices with embedded sensors that have the ability to collect and send or exchange data. Today, there is a plethora of devices that are interconnected but with no network standard or clearly defined boundary.

Despite IoT's future promise of many beneficial applications, there are grave concerns about the security of IoT, especially with regards to the lack of privacy, insufficient user authentication and authorization, and weak or non-existent data encryption [46].

With the arrival of IoT, it is of paramount importance to expediently develop and embrace security-standards ensuring secure IoT-device design, connectivity, and accessibility. IoT will undoubtedly be the next big thing in our digital age after connecting people through social networks [47]. IoT will provide the connectivity of people and Things (devices around them) and of the networks of connected Things.

The world of IoT can be thought of as a "social network" for Things—connected devices, such that interaction occurs, not just between humans and devices, but among devices themselves.

2.2. Application and Scope of Internet of Things

The benefits of IoT on our daily activities are evident. However, when the IoT was first adopted in the late 1960s [48], security issues were not fully appreciated and, therefore, security was not a design goal. Today, security has become crucial for IoT survival and vast adoption. IoT applications and devices are permeating all aspects of our daily lives. In healthcare, IoT, including Wireless Sensor Network (WSN) and Wireless Body Area Network (WBAN), has become an essential component of many healthcare environments [49–51]. In the home environment, IoT devices have extended into our living spaces enabling home automation and creating intelligent, hyper-connected homes. Household devices ranging from power outlets, light bulbs, thermostats, and more are now packaged with networking capabilities allowing for wireless remote control. Just about every home appliance can be replaced with an automated and remotely controllable alternative. As shown in Figure 1, we are surrounded by IoT devices and applications in our homes, cars, trains, streets, transportations, agriculture, and businesses.

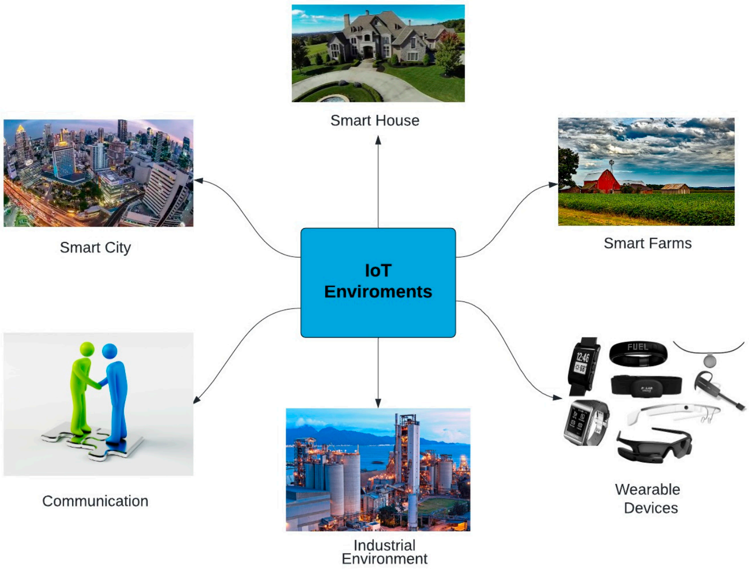

Figure 1. Internet of Things environments.

Alam et al. [52], citing Statistic's estimates and predictions, indicate that by 2025, with the current rate of expanding, as shown in Figure 2, IoT connected devices will reach over 75 billion.

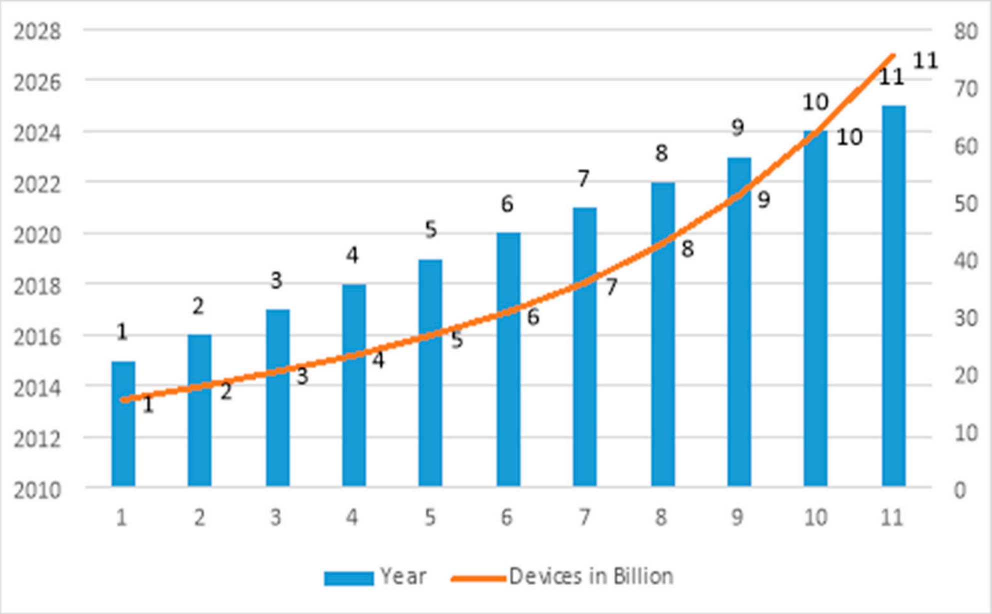

Figure 2. Internet of Things (IoT) expected devices by 2025 (in billions) [53].

2.3. *Sheer Volume of Devices Lacking Sophistication*

In general, IoT devices lack complexity and are designed to be compatible with and adaptable to our everyday Internet devices. With the increasing number of IoT devices, new vulnerabilities will emerge, unforeseen design flaws will surface, resulting in higher chances of system compromise. With this in mind, it is crucial to strike a balance between embracing a technology in a timely manner while without making compromises on the necessary protection of the Privacy, Confidentiality, Integrity and Availability of our networks and our data [47].

According to a recent report by Symantec [53,54], there were a massive number of attacks on IoT devices between 2017 and 2018, and the average number of attacks was around 5200 attacks per month. Figure 3 shows the top source-countries for these attacks on IoT [53].

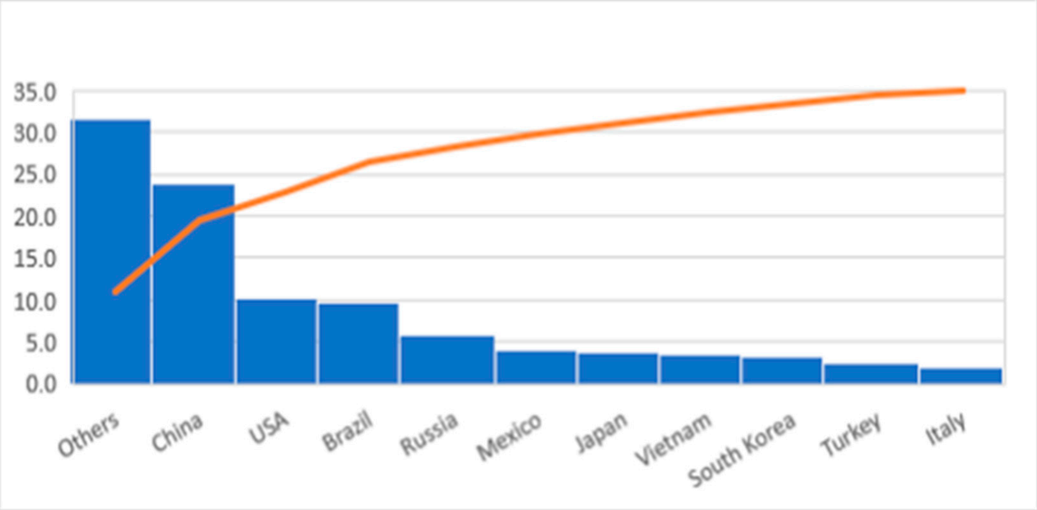

Figure 3. Source countries for IoT attacks.

Comparing this recent report to a previous one also by Symantec [54], IoT devices are still under massive attacks every year, albeit in a different ways and sources. Table 1 shows attacks on different types of IoT devices.

Table 1. Attacks on different IoT devices.

Device Type	Vulnerability Possible Exploits/Attacks
Cars	Chrysler car company had to recall 1.4 million vehicles after researchers proofed that attackers are able take control of the vehicle remotely
Smart home devices	Millions of homes are affected. Multiple vulnerabilities in a lot of commercially smart home devices such as smart door lock that could be hacked and opened remotely without using a password
Medical devices	Multiple vulnerabilities in medical devices such as insulin-pumps, Xray and CT-scanners devices, and implantable sensors
Smart TVs	Millions of Internet-connected televisions are vulnerable multiple attacks such as click fraud, data theft, and ransomware
Embedded devices	Everyday devices such as routers, watches, cameras, and smart phones using the same hard embedded code SSH and HTTPS server certificates left by manufactures leaving other millions of devices vulnerable to attacks such as interception and interruption

Ferrag et al. [55] conducted a comprehensive survey on IoT authentication protocols. They categorized protocols based on the targeted IoT environment. Sfar et al. [56] discussed security challenges in IoT devices and discussed access control, privacy, and identification security aspects. A systemic approach has been followed in which each component was presented, discussed, and highlighted to ensure the security for IoT components.

2.4. Privacy Concerns, IoT's

Privacy concerns are the biggest issue for IoT. We cannot talk about IoT without addressing the privacy concerns that come with it. The convenience of new technology and the eagerness to adopt it usually outpace the need to ensure security and privacy. However, in the world of IoT, the privacy issue is too significant to ignore. The benefits of big data can result in the premature adoption of IoT technology before it is fully developed. Data that IoT devices collect is both enormous in magnitude and diverse in nature. There are a lot of fundamental security questions we have to bear in mind, such as how data is collected, processed, transported and stored.

Privacy concerns are raised through all the layers of the IoT architecture. Attempting to minimize these security concerns has led to identifying security concerns depending on the IoT layer they reside in, as shown in Table 2.

Table 2. Privacy concerns in IoT.

Layer/Function	Privacy Concerns
Application	• Who has access to the data, information reports? • What does it use for?
Transportation/Network	• Data transmitted across networks encrypted? • In general, Wireless networks, Cloud services are vulnerable.
Perception/Sensor	• The vast majority of devices collect personal information such as name, address, date of birth, and some intrusively gather information about the user's taste of music, food preferences, not to mention health and credit card information.

Luckily, we can use the standard C-I-A triad (Confidentiality, Integrity, and Availability) to structure the way we approach the challenge of providing security [57]:

- Confidentiality-It ensures that only authorized users can access the data and information reports and only to the extent they need that access.
- Integrity-It ensures that data are secured and encrypted and only modified by authorized users during transmission, processing, and storage.
- Availability-Although it is essential to secure the data and information, we have to make sure data is available in a timely manner; otherwise, it may lose its value, e.g., in emergency and medical applications.

As pointed out earlier, IoT devices are susceptible to attacks not only during data collection, exchange, and transmission phases, but also at the design stage. This gives very little confidence and limited assurance about the IoT's confidentiality, integrity, and availability of data. If those issues are not resolved, we will face even more significant security and privacy problems. Fortunately, despite its rapid growth, IoT is still in its infancy. With the right focus and enhanced effort on security at the design and development stage and throughout the product life cycle, IoT will be able reach its full potential and truly be of benefit without compromising anyone's security, especially privacy.

2.5. Phases of Data as They Pass through IoT's Different Layers

The goal of IoT is to collect and process data and information and make meaningful, informative, visually enhanced data presentations for end users (humans, applications, machines, or devices) [58]. Those end users will either consume the information and data or intelligently use that information or data to determine what action to take. Data passing through IoT's layers can be organized into phases, as shown in Table 3 [59,60]:

Table 3. Data passing through IoT's layers.

Phase	Layer	Process
Phase 1	Perception layer	Data perception and collection from the sensors
Phase 2	Perception layer	Data storage on sensors
Phase 3	Perception layer	Data processing on the sensors
Phase 4	Transporting/Network layer	Data transmission
Phase 5	Application layer	Data delivery, data presentation for end users, output devices

At each phase, we see the transformation of the data and have inherent vulnerabilities that can be exploited by attackers.

2.6. IoT Wireless Protocols and Standards

As shown in Table 4, depending on the IoT layer, there are different wireless protocols that can be used in the Application and Message layer, Network and Transport layer, and Datalink layer [61,62]. There are different common types of IoT wireless technology, such as Bluetooth, radio frequency identification (RFID), Wi-Fi, Low-Power Wide Area Networks (LPWANs), Cellular (4G/5G), and Zigbee. Each of these wireless technologies has its strengths and weaknesses in various network criteria; thus, a suitable protocol can be selected based on the specific use of the IoT [63,64].

Table 4. IoT wireless protocols.

Layer	Protocols
Application and Message Layer	JSON, HTTP, RESTFUL, XML, FTP, Etc ...
Network and Transport Layer	IPv6, TLS, 6LoWPAN, 6lo, TCP/UDP, Etc ...
Datalink Layer	Bluetooth, ZigBee, WiFi, 4G/5G/LTE, IEEE 802.15.4e, Etc ...

Depending on the IoT layer's model, most of the standards and protocols for IoT layers are proposed by the Institute of Electrical and Electronics Engineers (IEEE), International Telecommunication Union

(ITU), and Internet Engineering Task Force (IETF) [62]. When it comes to the data link layer, IEEE is mostly used. For example, IEEE 802.15.4e is the data link standard for several MAC behaviors [65]. For the network, security firmware, and management, IETF new standards are mainly used [66]. ITU-T defined global standard recommendations for IoT and clarified the concept and scope of such standards worldwide [29].

3. Related Work

Many surveys have focused on IoT security and privacy in the past five years. The authors of [67] selected and surveyed commercially available and frequently used IoT programming frameworks from major cloud providers that supported rapid IoT application development. They compared the approaches taken to security and privacy at the programming level of the frameworks. They found that the frameworks did support security to some degree, but design flaws could cause security issues and the frameworks did not adequately consider the vast number of microcontrollers with minimal hardware security present in the IoT network.

In [68], Machine-to-Machine (M2M) applications are enumerated in major application domains, including Automotive, e-Health, Smart Metering, City Automation and Home Automation. A taxonomy of attacks against M2M is presented, categorized by the target of the attack, whether physical, logical or data. Scalability, heterogeneity, constrained resources, and a variety of end-to-end communication protocols are identified as challenges for M2M. The authors note that while most existing solutions addressed authentication and privacy, they did not address confidentiality.

The IoT is represented by three layers, Application, Transportation, and Perception in [7], and for each layer they enumerate the potential attack types. They also review communication protocols, security issues and possible solutions by layer. They find that the Perception layer is the most vulnerable due to the physical availability of these devices that sense and monitor in the IoT environment. The difference between traditional IT security requirements and IoT security requirements is also discussed and the need for a multi-layer and cross-layer approach to security is advocated.

The authors in [69] provide a comprehensive survey of attacks on IoT networks, covering both common and specific types of attacks in IoT applications. They focus on Smart Home, Smart Grid and Vehicular Ad hoc Network (VANET) applications in IoT and the related wireless networking technologies. They provide a taxonomy of attacks between each of these applications and the relevant wireless network, as well as classifying those attacks. They review existing solutions and found no common solution that would apply to all attacks, leading them to recommend more sophisticated schemes, including cryptography specifically adapted to the resource constrained IoT devices.

IoT applications in the domains of Industry, Personal Medical Devices, and Smart Home are discussed in [70], along with general IoT security requirements to protect data privacy and security. They find that most security threats to IoT are related to data leakage and loss of service. They also describe threats to Smart Home and classify different types of attacks by threat level, from low to extremely high, including possible solutions.

IoT in healthcare is the focus of [5] with applications categorized by healthcare setting, including clinical care, remote monitoring, and context awareness. They present the network topology of healthcare IoT networks and describe frameworks for health information service models and Wide Body Area Networks (WBAN) for healthcare applications, noting that there are no well-defined architectures in IoT in healthcare [50]. They identify challenges for healthcare in IoT, including scalability, data privacy and security, and low-powered devices, and enumerate requirements for WBAN in IoT in healthcare [50,51].

Blockchain as a security solution for IoT is discussed in [61]. A taxonomy of security issues by layer is provided. Security issues and potential solutions are categorized by groupings of the layers of the protocol stack, with low level including the Hardware, Physical and Data Link layers, intermediate level including Network and Transport layers, and high level encompassing the

Application layer. Blockchain-based solutions are discussed, though they note that blockchain itself is not without vulnerabilities.

The authors of [15] describe a three-layer IoT architecture divided between Perception, Network and Application layers and posits that the security goals of confidentiality, integrity, and availability (CIA-triad) apply to the IoT. They divide security challenges into two categories, technological, which contains challenges such as the heterogeneity of IoT hardware, wireless networking technologies and scalability, and security, which contains the CIA-triad and end-to-end security. Security challenges are discussed by layer and countermeasures, including authentication, trust establishment, federated architecture, and security awareness, are discussed.

An overview of IoT architecture and the interoperability of interconnected networks is provided in [71], as well as an analysis of security issues and mitigation strategies. They believe that the ease in conducting attacks against IoT is a significant threat. They discuss security constraints for hardware, software and networks, and present requirements for information security, access level security, and functional security. A taxonomy of attacks is categorized by device properties, adversary location, access level, attack strategy, and damage level, as well as by host and protocol.

The authors in [72] discuss security goals and requirements for IoT, including data confidentiality, privacy and trust, while also providing a background of threats, attacks and vulnerabilities pertaining to IoT system components. They also provide an analysis of the motivations and capabilities of the intruders who would threaten the IoT. Intruders are classified into three main types, individuals, organized criminal groups, and state intelligence units; the motivation and capabilities of each are discussed.

Classification of the IoT in a corporate environment into four component layers, including connected objects, transportation, storage and data mining, API and GUI, is done in [73], with multiple technologies possible in each layer. A taxonomy of threats and attacks for each of these components is provided. A case study is undertaken to demonstrate the operation of these components in connected thermostat devices, offering threat scenarios and corresponding mitigation measures, showing how an attacker could compromise one layer and use the trust between layers to gain access to additional resources.

A taxonomy and comparison of smart technologies in a host of application domains, Smart Cities, Smart Homes, Smart Grid, Smart Building, Smart Transportation, Smart Health, and Smart Industry, is discussed in [74], along with the objectives and characteristics of each smart technology. The authors believe that the unique capabilities of the IoT and smart technologies bring new opportunities to businesses and consumers. They present case studies from four countries that they believe were successful examples of IoT and smart technology use to improve life, safety, efficiency and environmental monitoring.

An end-to-end view of IoT is taken in [20], where the authors describe three main components, things, cloud, and controllers, where the cloud serves as a middleman for the things and controllers. The authors define ten major functionalities in their end-to-end view, including upgrading, pairing, binding, local and remote authentication and control, relay and big data analytics by cloud, and sensing and notification. They argue that security in IoT needs to be considered across five dimensions, hardware, software, OS/firmware, networking, and data. A detailed analysis of a connected camera system's functionalities and communications between the three main components is made, as well as a discussion of their implementation of remote attacks that successfully gave them control of the camera.

The authors of [75] believe that understanding the difference between traditional IT systems and cyber-physical systems is important to comprehending the security requirements of cyber-physical systems. A proposal of a cyber-physical system model with three parts, (i) physical, for those devices that directly connect with the physical world, (ii) cyber-physical, where connections between the physical and cyber worlds are made, and (iii) cyber, which has no connection to the physical world, is made. They present a comprehensive review of cyber-physical systems, choosing four major applications, Industrial Control Systems (SCADA), Smart Grid, Medical Devices, and Smart Cars, as representative systems for further analysis. A review of general threats applicable to cyber-physical systems in general, as well as threats targeted to each of the four major applications, is made, including the source, target, motivation, attack vector, and possible consequence of each attack. The causes of general and application-specific vulnerabilities, examples of real-life attacks, and controls are also discussed.

A comparison of IoT reference models, the early three-level model, the alternative five-level model, and the CISCO seven-level model is made in [76]. A detailed taxonomy of attacks, security requirements, and countermeasures is made for the Edge-side levels, including Edge Nodes, Communication, and Edge Computing (Fog). The authors believe that the traditional CIA-triad of confidentiality, integrity, and availability is not sufficient to provide full security in IoT and thus consider the expanded IAS-Octave security requirements in their discussion of attacks and countermeasures. They see the enormous growth of insecure IoT devices in the wild and the privacy implications to the vast amount of data present in the IoT environment as major challenges to be addressed.

IoT applications are classified into major application domains and the critical security issues relevant to each domain are discussed in [77]. They divide IoT applications themselves into four main layers, including Application, Middleware, Network, and Sensing. For each of these layers, including the Gateways that connect them, they present the various attacks and security issues to which the layer is susceptible. Because of the heterogeneity of the IoT infrastructure and the high level of connectedness between IoT devices and systems, the authors believe major improvements are needed to make IoT secure and to protect the large amount of private information generated by devices. They categorize existing IoT security solutions into four distinct approaches, blockchain, fog computing, edge computing, and machine learning. For each of these approaches to IoT security, they present the particular security issues that the solution can address, but they also acknowledge that these solutions are not without their own security issues.

A comprehensive look at IoT security is presented in [78]. The services and protocols in the layers of the IoT protocol stack they categorize as Semantics, Application, MAC/Adaptation/Network, and Physical/Perception are enumerated. Threats to IoT in general and at each of the four layers are detailed. A major contribution of this survey is a review of major malware attacks on IoT devices and an analysis of the malware attack methodology, from the preparatory phase, through the infiltration, execution and propagation phases, to finally the hideout and clean-up phase. The authors see current IoT security as inadequate against these malware attacks and so propose guidelines for an IoT security framework that would provide comprehensive security for IoT. Each security measure in the proposed framework is designed to counter a particular threat to IoT.

The authors in [25] propose a taxonomy of vulnerabilities in IoT grouped into nine classes that include weaknesses in the hardware, software, and resources available in the IoT system. They examine the vulnerabilities in the context of layers, security impact, attacks, countermeasures, and situational awareness capabilities. As part of this examination, they consider impact and attacks on the general security principles of confidentiality, integrity and availability. A unique contribution of this survey is an empirical analysis of darknet data passively collected from a/8 network telescope. This data is correlated with third-party information to determine the number of unique devices, manufacturers of the devices, countries of traffic origin, and the business sectors involved.

In [79], the authors approach IoT as a security object to be protected and detail specific IoT properties that are critical to security. They present vulnerabilities according to the particular IoT asset or property being targeted by attackers as well as enumerating IoT device vulnerabilities recorded in the National Institutes of Standards and Technology (NIST) National Vulnerability Database (NVD). Among the components of IoT that they see as security objects to be protected are data, devices, communications, applications and clouds. They propose a combination of hardware and software solutions as well as proper access control, organizational policies and shared threat detection and intelligence for IoT information security.

Viewing the IoT as a collection of features that are representative of IoT devices as opposed to traditional IT devices is the approach taken in [80]. These features include aspects of IoT devices, such as constrained, unattended, mobile, ubiquitous, diversity, myriad, intimacy and interdependence that have impact on security and privacy. These features relate to the vast number of connected devices in a heterogeneous technical and application environment. Threats, challenges and solutions for each feature are described. The authors conclude that vulnerabilities related to the features they call "constrained" and "interdependence" would be exploited by attackers more in the future.

The authors in [81] propose a four-layer reference model, with each layer, Cloud, Network, Edge Computing and Perception, having a set of building blocks. In developing an IoT attack model they take a multi-layer approach, considering the general building block types, including physical objects, protocols, data, and software, as IoT assets. After identifying attack surfaces by building block asset and IoT security requirements, including confidentiality, integrity and availability, as well as the extended IAS-octave, the authors present a taxonomy of attacks, compromised security requirements and countermeasures by each building block asset category.

A different approach to IoT security is taken in [56]. Instead of dividing the IoT into layers by technological function, the authors consider the various actors, relationships and interactions in the IoT. This systemic and cognitive approach is presented as a tetrahedron with four nodes representing the person, the intelligent object or device, the process, and the technical ecosystem. The edges between the nodes reflect the relationships and tensions between them. This theoretical model is further illustrated by a case study in the Smart Manufacturing application domain. The edges that relate to security are presented in more detail, including privacy, trust, identification and access control. The authors believe the increased expectation for objects and networks to be intelligent and act on their own requires IoT security to become more context aware, adaptive and similarly autonomous.

In [2], the authors focus on nine major application domains of IoT, including smart healthcare, grid, home, wearables, transportation, manufacturing, agriculture, supply chain and city. For each of these application domains, they present security requirements, including confidentiality, integrity and availability, as well as the extended IAS-Octave. Additionally, system models, threat models that include the comparative level of threats, and protocols and technologies applicable to each application domain are presented in detail. Solutions to address the limitations of IoT devices, namely their low power and capacity, are discussed, including cryptographic primitives, authentication protocols, hardware, application-specific, and current lightweight solutions.

Finally, most IoT surveys have focused on IoT devices as the target of attacks. The authors of [21] consider the IoT device as the enabling force in an attack on another target that is not necessarily another IoT device. The authors limit their work to verified attacks, whether they occurred in the real world or were produced by researchers. Their model of IoT-enabled attacks includes the adversary, the IoT device, and the actual target, which is typically a critical system. The access, means and motivation of the adversary are examined, as are the vulnerabilities at different IoT system layers and the direct, indirect and non-existent connections between the IoT device and the target system. They propose a risk methodology that assesses threat, vulnerability and impact levels to provide a risk profile for different IoT systems. Attacks in IoT application domains SCADA, Smart Power Grids, Intelligent Transportation Systems, E-Health and Medical Systems, and Smart Home and Automation are analyzed, with the authors finding that the closeness of device and target, exploitation of network and physical communication, and the extension of IoT device functionality played a role in the viability of an attack across all of the aforementioned application domains.

4. The Need for Security

The explosive growth, proliferation of IoT devices and the integration of IoT into our daily life has created an Internet of Vulnerabilities [82,83]. The convenience and comfort that IoT deliver to us comes with a security and privacy toll. Until recently, IoT devices were not completely secured. Security and privacy are delimiting factors in adopting and deploying IoT devices in many fields, sectors, services and applications such as mission critical applications [11,82].

A report by the TCS Global Trend Study, July 2015. Internet of Things: the complete reimaginative force [84] stated that reliability and security are the two main inhibiting factors for industry to deploy IoT in many fields and sectors to provide services. Traditional security techniques will not function well in the IoT environment due to the complexity, heterogeneity and the scale of IoT-enabled ecosystem [85,86]. This is mainly due to the fact that IoT devices are small in size, have low energy, low battery lifetime, memory size limitations, and low processing power to run complex encryption protocols. Identity allocation, management and the authentication of billions of IoT devices also play a role in this [85,86].

To gain insight into the need for security in IoT, we need to put security and privacy into action through practical IoT applications. In a smart health care environment, heart suffering or diabetics patients via pacemakers or insulin pumps, respectively. Patients can be monitored remotely via telehealth provision for their conditions. These IoT implants provide health monitoring but can be compromised. If these IoT implants were hacked and patients' data were breached, it can put their life at risk. Moreover, if the authenticity of information from these devices cannot be verified, then that is another life-threatening situation [85]. Some of the security and privacy concerns in this context are as follows: (i) Who has access to a patient's information? (ii) Is information communicated over the wireless medium encrypted? (iii) Is the data stored securely? (iv) What personal information about the patient is being collected and more?

In an IoT-enabled smart home, for example, if the heating control system is compromised, the hacker will gain access to the home network and from there to the home security system, which jeopardizes the physical security of the home occupants. Some of the security and privacy concerns that arise from this case are as follows: (i) Who has access to the home security system? (ii) Is the data communicated by different components of the smart home encrypted? (iii) Does the actuator accept data from authenticated sources and more?

In the previous two cases we just touched based on two wide spread practical scenarios that clearly show the need for security in IoT-enabled systems and services. The more IoT-enabled services and applications, the more vulnerabilities are ready to exploit by an adversary.

5. IoT Security Architectures and Frameworks

Urien proposes a four-quarter security architecture, based on a secure element [87]. It uses an Arduino board as a General Purpose Unit (GPU) to coordinate three subsystems: a WiFi SoC in charge of communication, a secure element (SE) performing TLS protocol operations and defining object identity, and sensors and actuators. The GPU has a limited SRAM size of 8KB, which is the most critical resource. The entire system is controlled using a mobile App. The WiFi unit implements the IEEE 802.11i security protocol and provides a TCP/IP stack with client and server features. The SE has a smartcard form factor, supports Java Virtual Machine (JVM), and runs software written in the Javacard language. The system uses a digital temperature sensor for the sensors and actuators unit.

Liu et al., propose a four-layer security architecture consisting, top-to-bottom, of information application security at the application layer, information processing security at the processing layer, information transmission security at the network layer, and information processing security at the perceptual layer [9].

Protection at the perceptual layer is in the form of physical security of the sensing devices themselves, authentication, and Wireless Sensor Network (WSN) security [49]. Authentication can be done using asymmetric encryption to the ensure security of a node's ID. Some of the attacks on a WSN include fake routing information, selective forwarding and black hole attacks [49]. Mitigating methods include integrated security policies such as encryption algorithms, key distribution strategies, intrusion detection mechanisms, and secure multi-path routing strategies.

At the network layer, issues of longer-distance transmission, such as mobile communication networks and long-distance cable networks, are tackled. Issues to account for include the denial of service attacks, unauthorized access, man-in-the-middle attacks, and virus attacks. The processing layer acting as an interface between the network and the application layers needs to ensure data integrity and confidentiality.

Obaidat et al., propose a six-layer security architecture [11] consisting of top-to-bottom security, application security, cloud security, information transmission security, gateway information security, internal communications security, and end-device security. At the application layer, they identify authentication as the most important, yet often overlooked, mechanism to employ. The cloud layer is to address data protection, privacy policies, and secure connections. The information transmission security layer handles reliable secure communication throughout the system. This includes wired, wireless and mobile networks. The gateway information security layer handles heterogeneity at the network edge using control and protocol security. Internal communications security handles security under the perimeter. Finally, the end-device security layer ensures physical IoT-device security. It is worth mentioning that the architecture is based on an end-to-end security framework.

Sridhar and Smys propose end-to-end security architecture [34]. They address the three domains of the communication in an IoT infrastructure, namely, the sensing device domain, network domain, and cloud domain. Mutual authentication is achieved through an authentication-delegation process. Key management is accomplished using a dedicated Master Key Repository. Communication between nodes and device gateway and between device gateway and cloud service gateway is conducted using symmetric encryption while communication of these gateways with the Master Key Repository is done using asymmetric encryption. The repository generates a key-pair sharing its public key with the gateways via a one-time handshake. Lee et al., proposed a three-factor mutual authentication protocol for multi-gateway IoT environments to solve the existing security weaknesses in two factor authentication protocols [46]. The proposed scheme protects IoT ecosystem against existing threats such as user impersonation attacks, gateway spoofing attacks, and session key disclosure [46]. Due to resource limitations in IoT, a lightweight authentication mechanism is needed. Yu et. al., in [88], proposed a secure and lightweight three-factor authentication scheme for IoT in cloud computing environment to secure IoT devices against attacks that were not previously addressed by previous mechanisms such as session key disclosure, replay attacks and user impersonation. In addition, it provides mutual authentication and anonymity.

Olivier et al., propose an IoT security architecture based on software-defined networking (SDN) [89]. The architecture is meant for securing wired, wireless, ad hoc networks, and object networking (devices such as sensors, tablets, smart phones and the like).

The network is assumed to be heterogeneous with nodes that have more resources being SDN-capable, while others with limited resources are not. Nodes with limited resources are assumed to be in the vicinity of an SDN-capable node. The larger network is referred to as an extended SDN domain that is divided into multiple domains, where a domain represents an enterprise network or a data center. Each domain can have or more controllers for managing the devices within that domain. To allow for scalability, the authors introduce a Border Controller that sits at the edge of each domain. The architecture is not hierarchical, rather control functions are not distributed on multiple controllers, while routing functions and security rules are distributed across edge controllers.

Each SDN domain has its own security policies and management strategy. SDN controllers are responsible for authenticating network devices, and once a device is authenticated, a controller will push the appropriate flow entries to the access switch. As opposed a master/slave model, all border controllers follow equal interaction mode having read/write access to the switch. This means they have to synchronize their operations.

Edge controllers are also responsible for establishing connections and exchanging information with other SDN border controllers. An edge controller exchanges its security rules with controllers of other domains following a concept of a grid of security.

Unlike other SDN-based schemes that assume a single controller and hence a single point of failure in case the controller is attacked, this scheme uses edge controllers working together in a distributed fashion in order to guarantee the independence of each domain in case of failure.

Ling et al. present an end-to-end view of IoT security meant as a guide to design a secure and privacy-preserving IoT system [20,90]. By focusing on standalone IoT systems consisting of three components (thing, controller and cloud) they identify 10 basic IoT functionalities related to security and privacy. These functionalities are listed and described in Table 5.

Table 5. Identified functionalities and their description.

Functionality	Description
Upgrading	Updates to IoT-device (thing) firmware
Pairing	The process of connecting a controller, e.g., a mobile app, to the IoT thing.
Binding	Configuring the thing through the controller once pairing is done.
Local Authentication	Takes place when the controller resides on the same local network as the thing. Thing may provide an open port for the controller to connect to. Thing should authenticate user to allow for further actions from user.
Local Control	Ability to locally control thing through sending user-commands after authentication.
Remote Authentication	When the controller is away from the home network, it may not be able to connect directly to the thing because the latter is probably behind NAT. In this case, it must use a cloud service to authenticate.
Remote Control	Ability to control thing while away from the home network through the cloud.
Relay	Cloud is to relay the authentication and control messages between the thing and controller. Cloud may need to authenticate both thing and controller using its own authentication servers.
Big Data Analytics	The cloud may collect data from the thing, the user, and may also contact other clouds for data on other things.
Sensing and Notification	A thing may report on environment or actions, e.g., room temperatures or number of login attempts.

To secure an IoT system, the authors identify five dimensions: hardware, operating system and firmware, software, networking and data generated and maintained within the system. The 10 functionalities span these five dimensions.

As a case study, the exploiting an IP camera system manufactured by Edimax is presented under this view of IoT security and privacy. They focus on remote attacks when the controller is away from the home network. Using three types of attacks, they are able to remotely control any camera. These attacks are: device scanning attack, brute force attack, and device spoofing attack.

Through identifying two major challenges in IoT networks, Guo et al., propose a five-layer IoT architecture [10]. The first of these challenges is interoperability due to high degree of disparity between different nodes in terms hardware architecture, embedded operating system, applications and functionalities. The second is management of both devices and resources. An example of the first is the need to update software and settings while an example of the latter is the ability to gather data from myriad devices in a timely manner.

The authors propose centralized management of resources including operating system (OS), applications, and data, while improving scalability using transparent computing (TC). TC refers to the decoupling of the software stack from the underlying hardware and separating computing unit from storage. In this model, OS, applications and data are considered resources that can be centrally managed and scheduled by the server. Prior to such scheduling, an IoT device acts as a lightweight terminal with no OS, yet is capable of executing small segments of code or data as demanded by the server (called block-streaming).

The architecture consists of five layers: the end-user layer, edge network layer, core network layer, service and storage layer, and management layer. The end-user layer is comprised of the IoT devices running a resident software such as MetaOS such that they are capable of booting various operating systems as instructed by the Edge network layer.

The edge network layer is made of devices such as servers. They perform two types of tasks: (a) collecting and processing user data gathered by the end-user layer. Processed data is sent to the service and storage layer through the network layer, (b) providing computing and storage services to IoT devices. The core network layer provides the communication infrastructure and is used for communication between the edge network layer and service and storage layer.

The service and storage layer consists of different types of servers. Data servers for storing data received from the edge network layer and providing such data for analysis. Software servers for storing OS images and applications to make available to IoT and edge devices. Finally, control servers control and manage both data and software servers. The Management layer manages service and storage layer servers, and assigns tasks to the control server, such as adding and updating software.

Liu et al., propose a security framework for IoT based on a future Internet Architecture named MobilityFirst [91]. MobilityFirst addresses, among many others, two major issues with the Internet of today, mobility at scale and security. These are achieved by cleanly separating human-readable names, globally unique identifiers (GUIDs), and network location information. To that end, two services are used, a name certification and resolution service (NCRS) is used to securely bind a human-readable name to a GUID while a global name resolution service (GNRS) is used to securely map a GUID to a network address (NA). By allowing the GUID to be a cryptographically verifiable identifier (e.g., a public key), trustworthiness is improved. Separation of the location information (NA) from the identity (GUID) enables users to request content by name without worrying about the current network address. This results in seamless mobility at scale.

The authors adopt the MobilityFirst architecture in addressing IoT needs in terms of scalability, mobility, content retrieval, inter-operability, and security. While many of these are clearly needed in an IoT setting, mobile IoT may not be. A mobile IoT application scenario is Vehicular Ad hoc Networks (VANETs). Sensors can be installed in moving vehicles to collect data and make it available to relevant applications through the underlying IoT infrastructure.

The authors propose a framework comprised of four components: devices, applications, MobilityFirst network, and IoT middleware as shown in Figure 4. Devices are the things of the IoT network, capable of sensing, actuating and communicating. Applications are used by users to both consume data after being processed and feed back into the system.

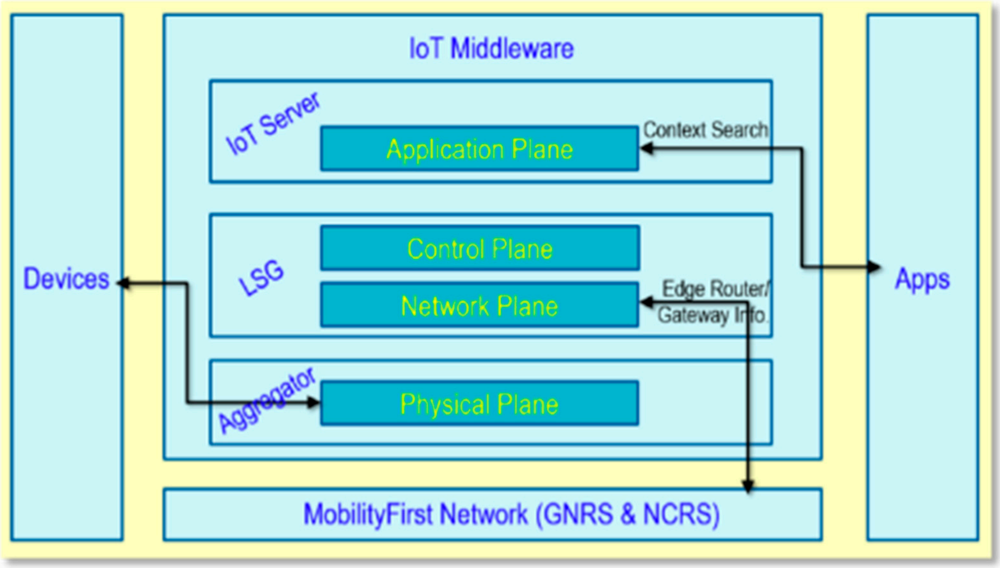

Figure 4. Components of the IoT MobilityFirst architecture, reproduced from [91].

The IoT middleware is further divided into three functional layers, Aggregator, Local Service Gateway (LSG), and the IoT server. The aggregator provides sensor abstraction hiding the hardware specifics for the underlying sensors and presenting a unified interface for querying and subscribing to the sensor data. The aggregator passes collected raw data to the LSG layer.

The LSG connects the IoT system to the global Internet. It might process raw data provided by the aggregator for context refining and aggregation purposes. The LSG also publishes the information, along with a data GUID, access control policy, and the storage location information (either human-readable names or NA), to the IoT server. Applications (users) can query the IoT server regarding where to fetch the data from through its edge router. After that, it can fetch the data from either a storage location or directly from the aggregator. In enforcing access control, the IoT server may decide to handle it itself or delegate it to the NCRS/GNRS.

Huang et al., propose a security framework for IoT that is meant to strike a balance between security and usability [92]. Three main scenarios were user experience is important are considered: a body-area network, a home network, and a hotel network. Two additional scenarios were also considered: logistics IoT and an office IoT. To better understand user perceptions of the importance of security vs. usability, and how willing users are to trade one for another, a survey is conducted. User were asked about three aspects of security: authenticity, integrity, and availability.

The survey results show that while different aspects of security matter differently depending on the application, security matters to all users and in all applications. This is particularly the case when it comes to access systems and payment systems.

The proposed framework, named SecIoT, is composed of sensors that communicate to a central node, e.g., a web server, which is connected to the Internet. The central node stores, processes, and delivers data to users. Users can also control objects via this unit. The central unit also provides interoperability when communicating with other IoT networks. An all-IP 5G network is assumed, such that either the gateway or even the IoT nodes are equipped with a 5G SIM card so they are able to communicate.

Two forms of authentication are used: users when connecting to the central node to enquire or control objects, and objects when providing data to the central unit. A single-sign-on mechanism is used to authenticate users, while a Multi-channel security protocol (MCSP) is used for authenticating devices. In MCSP, a no-spoofing and no-blocking (NSB) out-of-band channel is used to communicate security properties (e.g., public key). Examples of NSB channels are emails, SMS messages, phone calls, and even face-to-face conversations. Using a user's mobile phone or email address, it is easy to exchange public keys between the mobile phone and the IoT central service provider using, e.g., public key infrastructure.

The second component of the framework is providing a successful secure channel. This is relatively easy to accomplish once authentication takes place. The public key distributed during authentication can be used to ensure secure communication.

For authorization, role-based access control is proposed. The role is more encompassing than simply a job role. It could include the user's context, e.g., location being in the vicinity or location, access during business hours.

The last component is a risk indicator, which helps users assess their current configurations and choices in terms of security risks. The risk indicator provides information in three elements: asset identification, threat identification, and risk evaluation.

Colombo and Ferrari et al., propose Fine-Grained Access Control (FGAC) to NoSQL databases, which have been gaining popularity in the data storage and analysis layer of IoT platforms [93–96]. The papers attribute this adoption of NoSQL databases in IoT to several reasons, including performance, scalability, support for handling high volumes of data, and the ease of interaction with external applications.

NoSQL databases support multiple data models, with document-oriented being the most popular. MongoDB, the most popular NoSQL datastore, follows this data model. Using this model, a database is made of collections, each collection has a number of documents within, and each document contain key-value pairs [93,97].

A major shortcoming of NoSQL databases, however, is the poor data protection mechanism they offer; e.g., MongoDB, integrates a role-based access control model operating at collection level only. For handling sensitive IoT data, the database could greatly benefit from the integration of FGAC [95,97].

The authors propose the integration of a purpose-based model operating at document level into MongoDB and even at field level, which supports content-and context-based access control policies similar to those of Oracle VPD (Virtual Private Database). They also extend FGAC to map-reduce systems. An extracted key-value pair is dynamically modified on the basis of the specified FGAC policies, before the mapping phase starts the processing [93,97].

In recent years, fog-based access control has been proposed to move the computational complexity from the core to the edge. To dynamically control context-sensitive access to cloud data resources, a novel approach was proposed in [38], which combines the benefits of fog computing and context-sensitive access control solutions. The new model reduces administrative efforts and processing overheads. For comprehensive look at the context-aware access control schemes for cloud and fog networks as well as open research issues, the reader is encouraged to refer to the study in [39].

Irshad created a review and comparison of IoT security frameworks [98]. To survey the available literature, three search phrases were used: "IoT Security Framework", "IoT Security", and "IoT Information Security Governance" and four security frameworks were identified and compared as a result. The results of comparing these frameworks were presented in a table format and are reproduced as shown in Table 6.

Table 6. Comparison of four IoT Security Frameworks [98]. An X indicates a criterion that is insufficiently developed.

Security Framework	**Policies, Standards, Process Adaption and Secure IOT Components**	**Security**	**Service Level Agreement**	**Applicability**
Cisco Security Framework	Authentication Authorization Network Enforced Policy Secure Analytics: Risk and Assurance	Threat Detection, Anomaly Detection, Predictive Analysis contextual- Awareness	X	Infrastructure Framework
Floodgate Security Framework	Software APIs to enable secure boot Hardware root of trust integration Software based vTPM for legacy systems Integration for secure remote firmware updates.	Runtime Integrity Validation (RTIV) Application Guarding APIs Internet security (DDOS)	Identify the threats and Floodgate firewall IDS Supp Compliance support Security Evaluation	Best Fit in Infrastructure Security Framework
Constrained Application Protocol Framework (COAP)	IoT Smart Objects Protocol suites. CoAP, UDP, 6LoWPAN IEEE 802.15.4e provide the easy mapping to HTTP at the gateway	X	X	Best Fit in Application Security Framework
Object Security Framework for IoT (OSCAR)	Technological Trends and Design Goals Producer-Consumer Model Fitting the Concept with the REST Architecture and CoAP Object Security Approaches	Access Control Confidentiality Authenticity Availability	Analyzed and extracted risks of utilizing cloud computing by using the Risk Breakdown Structure (RBS) method.	Based on Object Security Approaches Best Fit in application Security

Krishna and Gnanasekaran also compare different IoT security protocols [99]. Protocols are classified based on the layer at which they operate. Nine different schemes are compared, three at the perceptual layer, two at the network layer, and four at the application layer. These are compared in terms of the issues they address, the solution they provide, and their limitations.

Issues addressed include the life style of the elderly, absence of real-time data from nodes, and data integrity at the perceptual layer, security of home devices and device security at the network layer, and e-health information systems and environmental changes at the application layer.

6. Attacks, Threats and Vulnerabilities

6.1. Perception/Physical Layer

The security challenges at this layer rise from the fact that the IoT device is residing in an open unprotected environment. In addition, it is because of the nature of IoT nodes and devices that have limited resources. [12,13,83]. Physical layer challenges include physical damage and tampering with the IoT device [7,13]. Attacks at this layer are centered on the idea of forging information [14]. The following threats/attacks are the most common at the physical layer in IoT devices.

Node capture/tampering/physical damage attack: This could be either by physically tampering with the hardware components of the node or device, or replacing the entire node with a malicious node. The aim of the attacker is to gain access and control the node or IoT device. This could also be by damaging the functionality of the hardware components or compromising the sensitive information in the device, such as keys necessary for communications. Injection, using the device's interface to inject malicious code that spreads to the rest of the network [13,15,100–104] and physically damaging the IoT node or device to hinder the availability and proper functionality of the system [104]. Since IoT nodes are usually operated outside in an unprotected environment, they are vulnerable to such attacks. The attacker with physical access to the node or device might reprogram it, tamper with the software components, and reconfigure or extract cryptographic information [14,105–108]. The extraction of security information: after gaining access to the device driver, an attacker can steal the encryption keys [13,15,76,100,101,109–111].

Physical Attacks/Tampering: against RFID tags: Some of the physical attacks against tags include probe attack, circuitry manipulation, clock glitching and material removal [112]. These attacks enable the attacker to gain access to information from the tag or modifying the tags for forgery [13,76,83,112].

Hardware Trojan: The attacker changes the design of the integrated circuit (IC) before or throughout the production process to add the hardware Trojan. This enables the attacker to gain access to data or the software implemented on the integrated circuit (IC) [76]. The attacker builds a certain trigger mechanism into the circuitry to enable activating this mechanism later on. This type of hardware Trojan attack includes both externally and internally activated Trojans.

Denial of Service (DoS) Attacks: IoT nodes are vulnerable to DoS attacks due to the fact that nodes and devices in IoT system have limited resources, such as power, battery, memory and processing capabilities [7,13]. DoS attacks at the node include, but are not limited to, sleep deprivation, outage attacks and battery draining. Because of the small batteries that IoT nodes have, they are vulnerable to this attack where the attacker depletes the battery to move the node into shutdown state [113–116]. This has very serious consequences in case of an emergency where the node cannot function and report the emergency. Moreover, keeping the node awake and preventing it from going into sleep mode would cause the DoS attack through sleep deprivation. A node might not function properly due to an outage attack. This could be as a result of code injection, unauthorized access, or the node being defective due to manufacturing error [13,76]. In case of DoS attacks against the RFID tag, the tag reader is not able to read the tag due to jammed radio frequency (RF) channel. This makes the tags unavailable which in turn causes DoS [76,110].

Node Jamming attack: In this attack, the attacker transmits a noise signal over the communication channel to interfere with the IoT radio signal to occupy the transmission media that will cause jamming of the signal. The aim of the attacker is to corrupt the transmitted signal from legitimate nodes by introducing and increasing the number of collisions that will lead to unnecessary retransmissions. This causes power consumption that leads to fast depletion of the resources. Continuously jamming the signal will disable the communications between IoT nodes and devices. This ultimately causes DoS of the IoT node preventing communication to the nodes or the entire system [13,101,102,104,109–111,117,118].

Replication/duplication of a node/device attacks: A malicious node is inserted into the system that appears to be genuine by duplicating the information (i.e., hardware, software and configuration) of a genuine node. This attack uses the duplicated node to redirect traffic, drop packets, or gain access to sensitive information such as the shared encryption keys [13,76,100,101,119,120].

Social Engineering: The aim of the attacker is to have the users of an IoT system perform specific acts by manipulating them to do such acts [104]. The attacker has to interact with the IoT user to get the information of interest or perform a certain action.

Malicious code injection attacks: The attacker infects an IoT node by injecting a malicious code to the node or device which gives the attacker full access or control of the node or the entire IoT system [104]. This attack could drain the network resources which leads to DoS attack in WSN [49]. Moreover, viruses could be injected into nodes [13,100,111,121].

Malicious Node Injection: This is used to carry out MiTM attack by introducing a malicious node between two or more legitimate genuine nodes. The attacker will be able to monitor, modify and eavesdrop on the communications between two IoT devices in the system. This is considered an insider threat since the attacker must physically exist and insert the node into the network [84].

Camouflage/Corrupted/Malicious Node attack: In this attack, a fraudulent node is inserted or attacks a legitimate node to hide at the edge. This node later could be used to perform traffic analysis, send and redirect packets [76,120,122]. By using a corrupted/malicious node, the attacker aim is to gain access to the system [12], which could include getting access to other nodes, the network and its communications [76,100,111,120,122]. This might halt the entire network.

False data injection attacks: The attacker injects information to replace existing true information that is initially collected by the IoT device. This device will then transmit the erroneous information to the intended destination [13].

Replay attacks (or freshness attacks): The goal of the attack is to have a malicious node or device gain the trust of the rest of the IoT nodes or devices. This is accomplished through communicating with the destination node or device using legitimate identification information that has already established communications with the destination node or device [13,15,102].

Cryptanalysis attacks and side-channel attacks: The attacker aim is to get the encryption key. Predicting the encryption key by obtaining the cipher-text or plain text from the communication [110,111]. The effectiveness of the cryptanalysis attack is very low. To maximize the effectiveness of such an attack, a side-channel attack is used. In this attack, some techniques are applied to get the encryption key. One of these techniques is the timing technique, where the attacker analyzes the time it takes to perform the encryption process and from that the attacker can predict the encryption key [13,15,102,103,111]. The way the side-channel attack is launched against RFID tag is that the attacker extracts information by intercepting wireless communications between different parties and processing it. The attacker then looks for patterns to launch its attack [13,110]. In a non-network side-channel attack, the continuous transmission of the electromagnetic waves delivers private information about the status of the node or the owner of it, even though the node or device is not transmitting information [76,123].

Eavesdropping and interference: The wireless communication channel is very vulnerable to this attack as most IoT nodes and devices communicate wirelessly. The attacker can interfere and eavesdrop on the transmitted information fairly easily over the wireless channel since this is broadcast transmission in nature and for this reason it is challenging to trace [13,102,109,110]. This is considered a passive attack as the attacker does not do anything besides listening. In the case of eavesdropping against RFID tags, the attacker intercepts the communications over the RF channel to sniff messages and perform some traffic analysis to extract some sensitive information [15,76].

RF interference on RFIDs: The attacker sends noise signal to cause interference with the RFID to obstruct it from performing its normal functions [110,111,124]. Once the noise signal interferes with the radio frequency signal, communication between nodes becomes very difficult, which could partially disable the network and ultimately lead to DoS [100,104,110,111].

Sleep deprivation/sleep denial attacks: The battery lifetime of most IoT nodes or devices is very limited. To extend the lifetime of an IoT node or device, they are programmed to go into sleep mode in order to save energy. In this attack, the node is prevented from going into sleep mode so that it drains its resources in the shortest time possible. Due to the fast consumption of its resources, the battery, by keeping the node awake, this will result in a shutdown state of the IoT node or device [13,15,100,104,111,125].

Tag Cloning or spoofing attacks against RFID tags: The attacker copies the target victim's RFID tags information into another RFID tag, which is replicating another genuine tag. This is accomplished by capturing the communications between the RFID tag and its reader or physical tampering [76,104,126,127]. The attacker will copy information from the compromised RFID tag and copy it into another RFID tag as described in Figure 5 below. This information can be the Identifier (ID) or Electronic Product Code (EPC), which is a serial number that is broadcasted and can be read by any within range reader, or key for memory access [127]. The purpose is to mislead the reader, which gives the attacker access to sensitive information by RFID impersonation [76,104,126,127]. According to [16], the reader cannot recognize the difference between a genuine RFID tag and a compromised RFID tag.

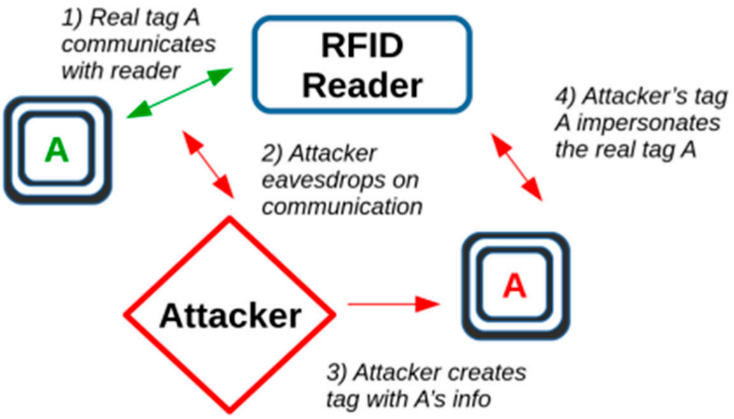
1) Real tag A communicates with reader
RFID Reader
A
2) Attacker eavesdrops on communication
4) Attacker's tag A impersonates the real tag A
Attacker
A
3) Attacker creates tag with A's info

Figure 5. Tag cloning attack.

Tracking attacks against RFID tags: Since these tags are usually unprotected, anyone can read them. This provides the attacker with a wealth of tracking information about objects or individuals. This becomes more dangerous when this tag is tied to sensitive personal information [76,128,129]. Tracking information about individuals could be related to their movement, financial transactions and social communications by fixed readers that reads all passing by RFID tags. This date will then be correlated to come up with a pattern [129]. This is a major concern and threat to people's privacy. In the case of objects, this might cause dangerous and chaotic situations when infrastructure relies on RFIDs that might lead to a Denial of Service (DoS) attack.

6.2. Network Layer Attacks

One of the main functions of this layer is to transmit information. The main challenge is to keep the network available and functional. Moreover, the wireless links are susceptible to different security threats [13].

DoS attacks: This attack can drain IoT resources to the point that a device becomes unavailable and cannot provide services [15,16]. This attack can take different forms at different layers of the IoT architecture. At the network layer, it can overwhelm the network by generating an enormous amount of traffic, as shown in Figure 6 below, or attack the IoT network protocols, which leads to the unavailability of an IoT device or system [15,16]. This includes many attacks, such as SYN flood, UDP flood, ping of death, etc. [13,104]. One of the main threats is leaking unencrypted information about the user [16].

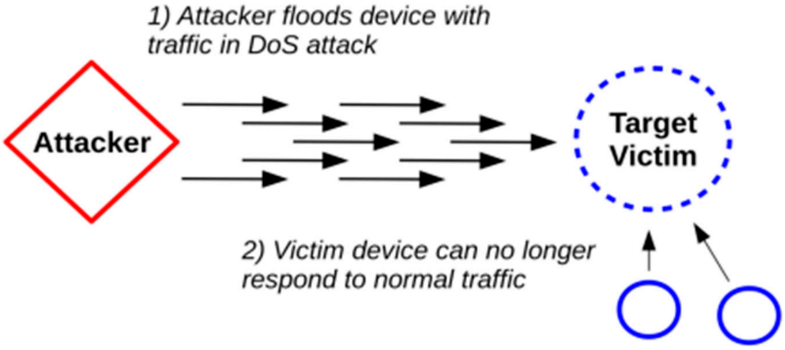
1) Attacker floods device with traffic in DoS attack
Attacker
Target Victim
2) Victim device can no longer respond to normal traffic

Figure 6. Attacker floods the victim with traffic in a DoS attack.

Spoofing attacks: The attacker uses spoofing attacks to spread malicious information through the IoT system [104]. IoT spoofing includes IP spoofing [130], where the attacker spoofs an IP address of a genuine node or device in the IoT system to gain access to the system. This allows the attacker to send contaminated data that appears to be from legitimate node or device. In RFID, spoofing is when the attacker uses legitimate spoof RFID tag information and spread data through the system that appears to be from a genuine RFID tag to execute harmful or illegal activity [13,102,103,110,131]. This is achieved by targeting the RFID signal. The attacker then uses this tag information to transmit its own data [132] as if it were the original owner of the spoofed tag id [133], which allows the attacker to gain access to the system [100,104,111].

Selective forwarding: In this attack, the attacker targets a victim by either dropping some or all packets destined to a certain IoT node or delay the forwarding of packets [13,102,109]. This attack can disrupt communications between different parties in the IoT system by causing DoS by selectively forwarding packets [134].

Packet replication attack: The attacker retransmits/replays previously received packets to the entire network or to a cluster of nodes in the IoT system, which will drastically degrade the performance of the system due to the overuse and consumption of resources such as power, memory and bandwidth [76,109]. This is considered as one of three different attacks of injecting fraudulent packets.

Man in the middle attack: This is a real time attack where the attacker places itself between two IoT devices or nodes using a malicious device [16,135]. By being in the middle of communications between two different entities, the attacker gains access to the traffic being communicated between the two victims' devices. This attack infringes the privacy, integrity and confidentiality of information being exchanged between the two victims [13,15,16,102,111,136]. This attack can be launched remotely by employing the communications protocols used in IoT system [71,100,104].

Sinkhole attacks: In this attack, a compromised IoT node or device broadcast false metrics about its capabilities to its neighboring nodes in order to attract these nodes to use it as a forwarding node (next hop) in their routing path [137]. The compromised node or device will attract so much traffic to it, then it drops these packets or inspect it and gain access to sensitive information [13,16,102,104,111,138]. In a Wireless Sensor Network (WSN), all packets generated from WSN nodes are redirected to the same sink point where they are later dropped instead of being forwarded to their destination [139]. This is carried out by the malicious node announcing fake preeminent routes using different metrics, such as having optimal bandwidth, minimum delay, shortest path, etc. [100,109,111].

Routing information attacks: Such attacks targets the routing protocols employed in IoT systems. Routing information is modified to cause routing loops, dropping packets, increase latency [104], forward false information or result in network segmentation [13,102,104,111,140]. Routing protocols at the network layer are vulnerable to impersonation, spoofing, and routing attacks [104,110,141].

The attacker might use this attack to drop, redirect, spoof or send misleading error messages throughout the system. There are many types of routing attacks, such as altering (change the routing information), Wormhole, Sybil attack, Black hole, Gray hole, and Hello flood [134,142,143] all described below. Address Resolution Protocol (ARP), Domain Name System (DNS) poisoning and Internet Control Message Protocol (ICMP) redirect are redirection attacks against the network layer and are carried out to disrupt the communications between two devices in the IoT system [76,100,109,110].

Wormhole attacks: In this attack, two malicious IoT nodes or devices are placed in two far away locations throughout the IoT system with one hop private link in between them which is exclusively used by the attacker. Through the false one hop transmission link (a wormhole tunnel) between the two malicious nodes or devices, many IoT devices will choose the malicious devices or nodes as a next hop in their routing path [13,102,109,144]. In other words, this attack will record messages from one geographic zone and replay it in another geographic zone [144]. Once there is an amount of traffic flowing through the tunnel between the two malicious nodes, the attacker can drop or delay the traffic which can be very critical and have serious consequences in case of critical mission applications. This attack can be carried out by either compromising an IoT device which is known as in-band wormhole or through out-of-band wormhole when high-gain directional antenna is used [144].

Sybil attacks: The attacker compromises an IoT device that can pretend to have many genuine identities in the IoT system and imitate them [16,104,145,146]. Having different identities, the compromised device (Sybil device) sends fabricated information to its neighboring devices. In addition, routes that include the Sybil device as a forwarding node could be deceived that many routes are available when there is only one route available where all traffic transmitted will go. This can lead to different attacks, such as a DoS or jamming attack [13,111]. In a sybil attack, sybil nodes with fraudulent identities are added or used which could outnumber the genuine nodes in the network [76]. An example of this attack would be a voting system where a malicious node claims the identity of many nodes and impersonates them to vote on their behalf [147].

Black hole attack: A malicious node is inserted in the network and advertises wrong routing information to its neighboring nodes that it has the shortest path to the destination [142]. Upon receiving the packets, the malicious node either processes or drops the packets [76,109]. In a gray hole attack, the malicious node drops some selected packets. The attacker captures packets at one site in the network and then tunnels them to a different site [76,142]. In a hello flood attack [76,134,148], the attacker inserts a malicious node with high transmission radius and then uses it to broadcast the hello message to nodes within the transmission range claiming to be their neighbor. This could be used to launch other attacks [76].

RFID unauthorized access: Due to the absence of an RFID tag authentication process (i.e., no standardized secure authentication procedure) and accessibility, these tags are vulnerable to attacks and are easy target to manipulate [100,104,111]. The information contained in the tag can easily be modified, or deleted by the attacker [13,104,149,150].

Sniffing attack: The attacker uses certain tools, applications or devices to capture traffic on the network and perform analysis to carry out an actual attack [16].

Traffic analysis attacks: Due to the wireless medium characteristics in IoT, which mainly relies on RFID technology, the attacker analyzes the traffic using a sniffing tool to get confidential information [15,16,119,151]. This is usually the initial step in launching the actual attack. This type of reconnaissance might include port scanning, vulnerability scanning and network sniffing [100,104,111,152]. In addition, this attack can be used on encrypted traffic. The more of the traffic that is captured and analyzed, the more that can be extracted from the packets captured [16].

6.3. Application Layer Attacks

The role of the application layer is to assist in providing on-demand services to the user. The layer also processes data from the network layer. This layer is mainly vulnerable to software attacks (i.e., the exploitation of vulnerabilities in programs or application layer protocols) and lifetime permissions [13,16]. These attacks target accessing sensitive information of IoT users, which leads to violations of data confidentiality and users' privacy.

Phishing attack: The attacker uses infected email or phishing website, as shown in Figure 7 below to get users' private information (i.e., authentication credentials) such as ID and password [16,100,104,111,153]. The attacker gains access to sensitive information such as login credentials once the victim accesses their email account [16].

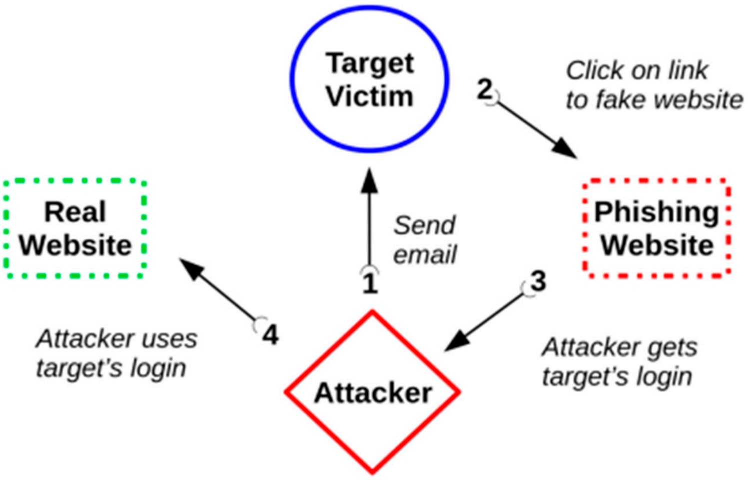
Target Victim
2
Click on link to fake website
Real Website
Send email
1
Phishing Website
3
4
Attacker uses target's login
Attacker
Attacker gets target's login

Figure 7. An attacker tricks the victim in a phishing attack.

Malicious virus/worm/trojan horse, spyware: IoT applications suffer from vulnerabilities to malware that can replicate and disseminate on its own which is considered to be one of the most challenging attacks to the IoT system [104]. Once the attacker succeeds in infecting the IoT application, s/he will intrude into the system and gain access to sensitive confidential information [102,111]. In addition, malicious software can infect the system, which could lead to DoS, tampering with or stealing data [100,108,111].

Malicious scripts: These scripts contaminate the application by adding or modifying the software in order to purposely cause harm to the IoT system and its functionality [104]. An attacker achieves his goal when the victim tries to access a service on the internet since IoT applications are all internet based. The attacker can send a malicious script to the user when the latter requests a service from the internet. Executing an ActiveX script by the user might give the attacker an access to the system [100,106,111] Examples of such scripts are Java attack applets and ActiveX scripts. The attacker can access confidential data or cause the system to crash [104].

XMPPilot attack: The attacker uses the command line tool XMPPilot to launch an attack against the XMPP connection established between client and server. The attack prevents the encryption of communications on the client side. This enables the attacker to monitor the communications [118].

Denial of service: Attackers can gain access to the application layer and confidential sensitive information in a database as a result of DoS or DDoS, which will cause service unavailability [7,100,111,120,153].

Software vulnerabilities: Software vulnerabilities are still considered a main threat since software engineers and developers do not consider writing secure code because of an absence of standardization to do so. This enables attackers to launch attacks such as buffer overflows, as explained below, for example, to redirect the execution to malicious code [7,16,100,122].

Code injection: The attacker exploits some vulnerabilities in the programs. The main aim of code injection is to get credentials, expose the confidentiality data, gain access to the system, steal data, or propagate worms to infect other IoT devices in the system. HTML and script injections are the most common types of code injection [7,16,153].

Buffer overflow: The attacker takes advantage of vulnerabilities in the program to carry out the attack as most programs have some security issues related to pre-allocated memory. The attacker writes a piece of code that is larger than the fixed pre-allocated memory size for a certain program. The consequences are modifying other information stored in other memory locations, interruption of program control flow and redirecting the control of the program to run malicious code redirecting the stack pointer. Many mechanisms exist to launch the attack, such as string buffer overflow, heap or stack overflow, and integer overflow [16].

Data aggregation distortion: the attacker modifies the data collected by a node and forwards it to the base station. So, the base station will gather false information about the observed surroundings [100,109].

Sensitive Data Permission/Manipulation: The attack exploits the vulnerabilities in IoT design flaws and, in particular, in the permission model to control applications [16]. The main target of this attack is based on communications between smart devices and smart applications. In this scenario, the smart device sends sensitive data to the application where the latter monitors the smart device [16]. This might have serious consequences on users and violate their privacy.

Clock Skewing: The attacker desynchronizes the IoT devices' clocks by generating bogus timing information. This causes victims' devices to be out of sync with the aggregation nodes [100,109].

Data leakage: An attacker, by exploiting vulnerabilities in the IoT application or service, is able to access sensitive and confidential data [7].

Authentication and Authorization: At the time of writing this paper, there is no standardized authentication mechanism for IoT devices. Therefore, no authentication mechanism exists to fit all kinds of IoT devices requirements [16]. For example, when updating an application, the attacker might use the update to inject a harmful payload to gain access to an IoT device or have control over the IoT device or system [16].

6.4. Impact of Attacks on Security Objectives

Attacks may affect the security objectives of Confidentiality, Integrity, and Availability (the CIA triad). The potential impact of the loss of one of these three security objectives is defined in NIST's publication FIPS 199 [24]:

- Low: limited effect on operations, assets, or individuals
- Moderate (Mod): serious effect on operations, assets, or individuals
- High: severe or catastrophic effect on operations, assets or individuals
- Not applicable: only applies to Confidentiality

The potential impact may vary due to the context in which an attack occurs. In Table 7, we consider the potential impact of select attacks on the CIA triad for user information depending on the general type of device at which the attacks are directed. In one case, the attacks are directed at a smart light bulb, in the other, at a smart health monitor; the difference in applications can make a difference in the severity of the impact [25].

Table 7. Potential impact of attacks on Confidentiality, Integrity and Availability.

Sample Attacks	**Potential Impact on Confidentiality of User Information**		**Potential Impact on Integrity of User Information**		**Potential Impact on Availability of User Information**	
	Smart Home Heating Control	**Smart Health Monitor**	**Smart Home Heating Control**	**Smart Health Monitor**	**Smart Home Heating Control**	**Smart Health Monitor**
RFID tag tracking	Low/Mod	Low/Mod	Low	Low/Mod	Low	Low/Mod
Denial of Service (DoS)	Low	Low/Mod	Low	Low	Low	Mod/High
Man in the Middle	Low/Mod	Low/Mod	Low	Mod/High	Low	Mod/High
Traffic analysis	Low/Mod	Low/Mod	Low	Low	Low	Low/Mod
Phishing	Low/Mod	Low/Mod	Low	Low/Mod	Low	Low
Malicious virus/worm	Low/Mod	Low/Mod	Low	Low/Mod	Low	Mod/High

7. Mitigation and Countermeasures

Mitigation and countermeasures against threats and attacks may be developed for and directed at each layer of the IoT architecture, but they may also be considered more broadly across multiple layers, as summarized in Figure 8, and described in detail below.

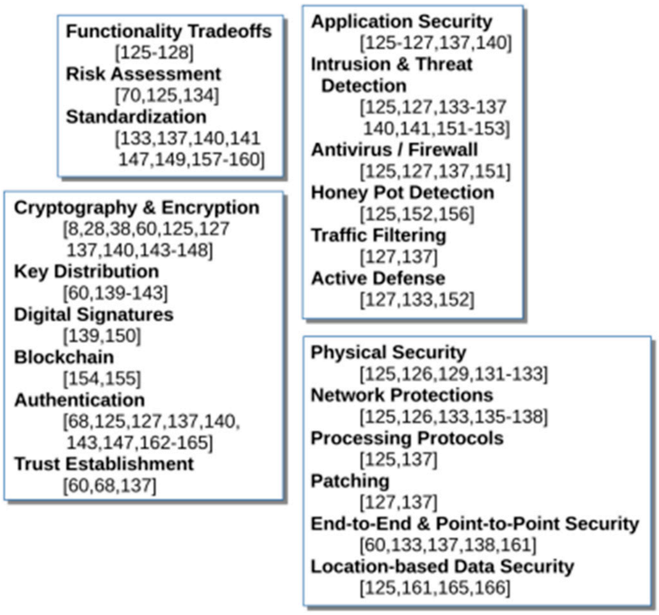

Figure 8. Mitigation and countermeasures across a wide spectrum.

7.1. Functionality Trade-Offs

Because of the limited resources present on IoT devices, trade-offs must be made between functionality and device capabilities on all respective IoT layers [26–28]. In order to best manage these functionality trade-offs while maintaining the greatest level of security, certain architectures can be adapted. This includes the "Event Driven Architecture" (EDA) Model, or alternatively the "Event Driven Adaptive Security Model" (EDAS). Because of the nature of IoT devices, adaptive security models tend to be strongest for creating a functionality trade-off architecture, but also must be balanced with system capabilities [154].

7.2. Physical Security

Physical Layer-directed security can primarily be mitigated by the physical security of device design. Individual device components should not be interchangeable, for example [155]. Techniques that provide anonymity, such as the "Zero-Knowledge" technique [156] or "K-anonymity" technique [157], mitigate physical layer security risks by hiding sensitive information such as location and address [26]. Physical security also goes hand-in-hand with chosen protocols; the assessment of device and program needs alongside connection protocols assists in determining functionality and risk trade-offs [158]. For example, RFID is more vulnerable to tracking, while WiFi is more vulnerable to eavesdropping [27]. Physical security can also simultaneously mitigate threats in other layers. The interlocking nature of functional elements in IoT means that a more secure physical environment results in more secure application and processing layers. Some studies have proposed this through SIM-based authentication alongside key agreements, or suggesting a lack of direct device to device communication at all [159]. Some research has indicated that malware can be detected physically as well as in software; this has been considered through "path delay testing", "temperature analysis", and "power based analysis" [158].

7.3. Risk Assessment

Dynamic risk assessment techniques provide confidentiality and assist in avoiding security breaches, especially on the physical layer [100]. Risk assessment can also mitigate vulnerability on the application layer alongside preexisting architectures [26,160].

7.4. Network Protections

Network protections such as routing security through pathing algorithms and security aware ad-hoc routing (SAR) can prevent attacks from adversaries by adding security measurements to packets [161] and applying confidentiality toward sensor nodes in IoT systems [26,162]. Network security options also exist on the application layer, particularly in protocols used for communication security; this is derivative of the wireless communication used at the top level. For example, protocols with TCP-based transport can use TLS/SSL for security to mitigate eavesdropping or man-in-the-middle attacks, while UDP-based transport systems can use DTLS [27]. Some studies have suggested a methodology of securing networks through non-routable TCP/IP addressing, a stark contrast to the typical network computing done elsewhere. The application of such prevents data traffic from being maliciously intercepted by sniffing or injected into by man-in-the-middle attacks [159]. Further network protections can be achieved through communication protocols which support M2M communication, such as AMQP or MQTT. The protocol used is dependent on the needs of the system; AMQP assures reliability by guaranteeing delivery, while MQTT is best on limited-memory devices that require a "publish-subscribe" architecture for data transfer. Furthermore, it has been proposed that moving from IPv4 to IPv6 for IoT devices can help with improved network security by more specific identification, especially due to the mass deployment of these devices versus non-IoT computational counterparts [30]. Alternatively, it has been proposed to eliminate modern paradigms and opt for a peer-to-peer networking protocol [163].

7.5. Key Distribution

As much as encryption and cryptographic techniques are vital for the security of all data transfers, key distribution minimizes cyberattack risks and can function within lightweight frameworks [34]. Key distribution techniques are dependent on the form of cryptography deployed by other aspects of the individual device as well as by the wider IoT ecosystem. These must be paired alongside processing power. Some forms of pre-distributed keys can provide greater security and less processing power, but may result in reverse engineering risks. Certain studies have shown hybrid encryption systems can be paired alongside key distribution systems to mitigate such risks, however [36,164]. Key administration is another element that goes hand-in-hand with key distribution. Key administration must be considered alongside secure routing systems and detection systems trilaterally. Safe key distribution methodologies can minimize protection risks in cryptographic frameworks [40,165]. Key distribution systems should also only be arranged in IoT networks in which pre-authentication make sense; otherwise, key distribution schemes can demand resources from IoT devices without proportionally secure returns [36,166].

7.6. Cryptography and Encryption

In order to avoid tampering and ensure the confidentiality, privacy, and integrity of data transactions, data between devices must be encrypted. There is a debate as to whether symmetric or asymmetric encryption is preferred, but generally because of device limitations, algorithms which consume less power are preferred. Algorithms such as RSA have been applied with success in the past, encryption, combined with authentication, can also help prevent illegal access to nodes [29]. Cryptographic hash mechanisms are used to check data integrity for data transmission between nodes and detection of errors on the network layer [31]. Homomorphic encryption is often used within the processing layer as a secure measure of data transmission, but requires high computing power.

Encryption, in general, can be applied to overcome various interception or sniffing style of cyberattacks, as well as circumvent otherwise exploitable side-channel attacks [26,167]. Furthermore, encryption can be applied in various forms, and should be designed and allocated according to device resources and functionality. The balance of functionality and processing power in a device should be equivalent to the framework of cryptography used within it, as well as the risk assessment of using said device in its respective setting [36,168]. The use of shared key cryptography for secure communication reduces the overhead for IoT gateways, which compared is important due to lower power consumption capabilities [34]. While symmetric key and/or public key cryptography suites provide better security than alternatives, their high-power consumption is often a challenge. However, lightweight alternative frameworks can provide similar security standards on minimal hardware, on which additional research has been conducted [41,168,169]. Some studies have shown that Hybrid encryption models are the best for securing information robustness and confidentiality in data exchanges at optimal speeds, without having to sacrifice power consumption [8,57]. Service Level Agreements (SLA) can be used to provide data encryption within the processing layer [30]. Since many encryption suites are compromised because of misconfiguration or user error, it is important to deploy accurate user configurations in addition to cryptographic systems for security [28]. Since devices are not heterodox, deployed encryption standards can differ between devices. Devices that communicate with each other should optimally use the same cryptographic suites. Alternatively, a standardized cryptographic method would eliminate many of the risks arising from device heterodoxy [42]. Multi-factor cryptographic schemes are best suited for larger networks with vital security applications, such as in smart cities or healthcare systems [166].

7.7. Digital Signatures

Digital signatures, encapsulated often in hybrid encryption technique models, are one specific cryptographic technique used in heterogeneous deployments to prevent cyberattacks and ensure both the integrity and confidentiality of transmitted data. These techniques require lower processing speeds than algorithms such as AES, and also faster processing speeds than RSA [164]. Digital signatures can also be deployed as a measure of warding off “puppet attacks.” However, certain forms of digital signatures are dependent on the routing protocols used by individual IoT devices [170].

7.8. Processing Protocols

Protocols in the processing layer, such as “Fragmentation redundancy” scattering, minimize data theft by splitting and allocating data into fragments between a cloud and a direct transfer between devices [26]. End-to-end data protection frameworks are best suited for transmissions that happen in this layer as well for assuring the security of data during its life cycle between devices. Service Level Agreements can be implemented to ensure protections for sensitive data, and also to reduce DoS attacks [30].

7.9. Application Security

Application layer security, through Access Control Lists, can moderate traffic by whitelisting or blacklisting both incoming and outgoing requests [26,36]. Similar to physical layer selections, the assessment of protocols used in the application layer can help to balance risk with functionality. Bluetooth leaves open the risk of “bluejacking”, for example, so applications built around Bluetooth should not be created in a way that their functionality lends themselves to this risk outweighing the functionality of the device [27]. Proper access control helps ensure confidentiality, while authentication in the application layer helps ensure integrity. “Service Level Agreement[s] (SLA)” and “Virtual Machine Monitor[s] (VMM)” are processes deployed in the application layer alongside Intrusion Detection Systems in order to achieve availability and protect data during downtime or malicious attacks [30]. Data loss prevention systems can also be implemented within IoT networks in order to prevent data theft [28,36].

7.10. Patching

Regular updates to software and firmware on IoT devices can help to mitigate vulnerabilities and lower risks associated with individual devices. However, this is often left to user responsibility, as auto-patching software must be balanced alongside other security measures against available system resources [28,30].

7.11. Intrusion and Threat Detection

Intrusion Detection Systems (IDS) secure ecosystems by producing alarms when detecting threats that either are hostile, suspicious, or uncertain within the application layer [26,36,159,171]. The application of intrusion and threat detection can be used to quell vulnerabilities that are not picked up upon by active defensive systems or firewalls; since anomalies are recorded, logs can be traced to malicious or suspicious activities. For this reason, it is important for threat detection systems to transcend all IoT layers; threat detection must include "physical damages, attacks, malicious codes, vulnerabilities, [and] misuses" [172]. Because of the often small storage on IoT devices, best practice is for security warnings from these systems to be forwarded to a secondary source, such as over email, SMS, or logs on a remote cloud [172]. There are two popularly used types of IDS for IoT devices, "Host-based Intrusion Detection Systems (HIDS)" and "Network-based Intrusion Detection Systems (NIDS)". They typically are deployed for securing the network layer, but can also run on the application layer depending on the needs of the device [30]. In a general sense, most well-known forms of network attacks can be prevented by an IDS, which include brute forcing, DDoS attacks, and malware requests [28]. If nuances in security as distinguished by sensors can be detected by threat detection systems, then systems can be stated to be more secure on the physical layer [40]. Due to the sheer diversity of the IoT ecosystem, some studies have recommended the introduction of adaptive intrusion systems to better combat against vulnerabilities arising from a heterogeneous environment. This has been recommended through the notion of using machine learning techniques as opposed to matching threats to database records [36,173].

7.12. Antivirus/Firewall

Web application scanners can help identify threats, especially when deployed alongside firewalls for detecting potential attackers. Firewalls, when deployed alongside ACLs, can block unauthorized access and assist in packet filtration on the application layer. Antivirus software can also work on this layer to detect and mitigate known threats, vulnerabilities, and cyberattacks from a database, but must be balanced with computational power for the device they are stored on [26]. Since Antivirus software and firewalls are not universal, they are best paired alongside IDS and/or Honeypot detection software in order to best mitigate attacks [28,30,171].

7.13. Blockchain

Some studies have proposed blockchain as a multi-layer solution for securing IoT networks. Blockchain networks can be deployed in either centralized or decentralized models, with their own weaknesses and strengths. The former is better for processing large data transfers from heterogeneous devices, while the latter is better for flexibility and real-time services. Blockchain can help standardized transactions among different forms of devices, as well as increase trust factors between heterodox communications or device functionalities which cross-communicate. Proposed blockchain techniques ensure an increased level of security through global trust and universal identification, standardized and high-level authentication, contextual privacy, and exponential mitigation against high-level attackers without an exponential increase in capabilities, which diminish IoT flexibility [32,33].

7.14. Honeypot Detection

Honeypot detection is another form of intrusion and/or threat detection based on system and network architecture. Instead of simply logging vulnerabilities or attacks, honeypot detection helps prevent attacks by the presentation of a separate zone outside of the typical scope of the network, such as in a "DMZ"; in this approach, vulnerabilities can still be detected and logged without putting the rest of the IoT network at larger risk [26,172]. Because honeypot detection systems do not need to be stored within the device itself, but just on the same network, they can act as a tool for measuring the dynamic nature of threats and preventing intrusion without burdening system resources [174].

7.15. Standardization

The lack of universal standards for IoT devices has resulted in a largely heterodox field, which has spawned a complexity for developing cross-device security methods. Researchers [43,44] have suggested that the standardization of security protocols would be one form of mitigating risks which spawn from device nuances [36,41]. In lieu of a lack of standardization, some studies have suggested a lack of device to device communication at all to prevent cross-device communication vulnerabilities from arising [159]. Standardization is most important on the network layer rather than the physical layer. Standardized protocols ensure a safe and simplified ecosystem for cross-device communications [30,36]. Just as the standardization of protocols for home and professional computing helped create a more secure world wide web, research has shown that a foundational standardization of protocols helps ensure an "interoperability" of security between IoT devices [40,42,45]. Software-defined networking (SDN) has also been proposed as an alternative to hardware standardization, which ensures a similarly secure return with a greater level of manufacturing and performance flexibility [175].

7.16. Traffic Filtering

Filtering traffic signals between IoT devices on the physical layer, even without IDS or threat detection on software-based layers, is one form of securing IoT networks and preventing malicious signals or cross-communications. Depending on the filter, this is also one way of implementing security despite a lack of device standardization [30]. Traffic filtering employed alongside an IDS can result in a significant decrease in malicious attacks, as well as general lessened risks within an IoT ecosystem [28].

7.17. End-to-End and Point-to-Point Security

End-to-end security mitigates risks in any wireless communication between devices, regardless of the protocol used; however, different suites must be applied depending on the protocol(s) used within respective layers [34]. Similarly, point-to-point connectivity solutions, which may take the form of IPSec VPNs or MPLS, provide similar security as end-to-end, but with greater power consumption needs [30,159]. It has also been noted that one critical strength of end-to-end security trust models is the circumvention of tertiary vulnerabilities. As cloud-reliant systems are only as secure as the remote systems facilitating processes and security, end-to-end security systems circumvent security risks proposed by such [176]. End-to-end security has also been proposed as a form of maintaining data integrity and privacy within a peer-to-peer networking system, although it is not inherently dependent on that form of networking architecture [163].

7.18. Authentication

Secure authentication is important for risk mitigation across all layers. On the physical layer, device authentication and identification must take place before signals are sent or received [35]. Authentication mechanisms prevent illegal access to data on sensor nodes in the network layer. The most common type of attack on this layer are DoS attacks, which authentication can assist in preventing [26]. Furthermore, authentication techniques can be deployed in a variety of ways, depending on the needs of the device and device application(s); these are usually, in best practice, deployed alongside access controls [36]. Various forms of authentication can be done through key exchanges, username/password (login) systems, or unique techniques such as "Identity Authentication and Capability-based Access Control (IACAC)" [37]. Furthermore, Message Authentication Codes used for device authentication can help prevent man-in-the-middle attacks [13]. An issue often pointed to for authentication is the heterodoxy of the IoT ecosystem; while some research has suggested standardization for this, authentication can still be achieved through methods such as cryptography suite-based access control, or a multitude of other formats. However, this heterodoxy means that devices which are not homogeneous and require safeguarded authentication should not be used within the same network [36,41]. Different forms of authentication are implemented at different layers, with respective security nuances based on such. Physical authentication can be achieved versus RFID-based identity authentication, whereas application authentication can be achieved through prior mentioned forms of authentication such as login or key exchanges. In comparison to these forms of authentication, physical authentication can help secure software layers additionally, but software layers cannot secure physical layers bi-directionally [177]. Applying authentication methods into sensor nodes of IoT devices is required in order to prevent malicious attacks; some studies have suggested that this is best achieved through symmetric cryptography suites. Furthermore, authentication should be setup in a distributive form, so users and nodes can only ever be authenticated to aspects that access needs to directly be attained. This can be done, for example, through Attribute-Based Access Control (ABAC); studies such as [30] propose that ABAC is most suitable over other access control methods because it requires minimal resources, is based on attribute instead of user, and uses randomized values per-session [30]. ABAC could potentially be used as a defense against man-in-the-middle, sniffing, replay, and node capture attacks [30]. Devices that connect to cloud servers and "control" devices are most in need of forms of user authentication, as well as input validation [28]. Authentication can also be deployed as a way of circumventing spoofing attacks on geospatial data [178]. Multi-factor authentication can ensure a high layer of security, but at the cost of flexibility of capabilities. In highly sensitive environments however, this trade-off is important to consider [166].

Another promising method for access control, which has been proposed within the sphere of IoT, has been NoSQL authentication. NoSQL provides performance, flexibility, and scalability for handling high data volumes, and has already found a place within the data storage and analysis layer(s) of the Internet of Things [93]. Using NoSQL as a framework for authentication within the Internet of Things is thus intuitive, especially because of the aforementioned need for implementation of access controls. Studies such as [93] have shown that NoSQL datastores can be used to implement access controls. In the past, using NoSQL for this purpose has been subject to criticism, as NoSQL datastores suffer from poor data protection; the aforementioned study [93] proposes a fix to this, and thus a possible springboard for IoT systems, by the integration of "fine-grained access controls" (FGAC). FGAC has previously been used in other systems, such as social networks and service and mobile applications [93]. The usage of FGAC allows for straightforward enforcement mechanisms and policy encoding, which suit the access control needs of IoT devices. [93]

7.19. Trust Establishment

Third parties are often introduced for trust establishment techniques, such as third-party-based key exchanges, or certification. In order to do this, devices must be able to access third parties typically, or have these trust stores built into their architecture by default. Trust stores help with safeguarding uniform transactions and preventing untrusted communications and attacks, but, depending on their implementation, must also be balanced with reverse engineering risks, or the need for constant remote authentication [34]. Trust establishment is best used alongside authentication frameworks or mechanisms in order to prevent trust tampering. This goes hand in hand with key distribution; best practices show that unique device IDs and distributive permissions are best practices [13,30].

7.20. Active Defense

In contrast to antivirus or firewallesque software, "deep packet inspection" has been proposed as a method of real-time detection of abnormal data or behavior. This type of behavior often indicates malicious activity; this behavior could be contrasted with IDS systems, but done directly as traffic is received or sent, rather than within a separate software process [159]. Active defense can be considered the primary segment of defense architecture and can encapsulate a number of other mechanisms, such as backup, authentication, access control, and encryption; however, this is based on both the needs and capabilities of the device. As active defense cannot inherently prevent all forms of threats, but generally known or up-front ones instead, it is important to be coupled with other mitigation tactics [172]. Active defense techniques are most important for devices with remote connections, such as to cloud servers, and are best deployed alongside antivirus, IDS, and firewalls, as a system administrator would otherwise secure a non-IoT computational network [28].

7.21. Location-based Data Security

GPS spoofing occurs as an attack within the network layer. Techniques such as the "GPS Location Technique" [179] have been used to successfully mitigate location-based system attacks [26]. In order to counter spoofing, techniques that match identity and location to service requests can be deployed [176]. Authentication, as well as geo-spatial validation, can be deployed in order to combat most vital spoofing attacks [178].

8. Open Research Ideas

Current open areas of research into Internet of Things have primarily been focused on addressing countermeasures for recognized security and usability flaws. More broadly, this has included topics such as security, scalability, and standardization, as described in Figure 9. Research has been focused on areas of improvement surveyed for application in fields such as smart environments (such as cities), and healthcare. As such, there has been an emphasis on the aforementioned importance of universalized security paradigms and standardization of device operations [27,42,180]. This has manifested in studies over proposed architectures and protocols; although there has not been a consensus on this, some proposals have been shown to be more recurrent than others, such as structural decentralization [181] and involvement of blockchain [32,33,163,182].

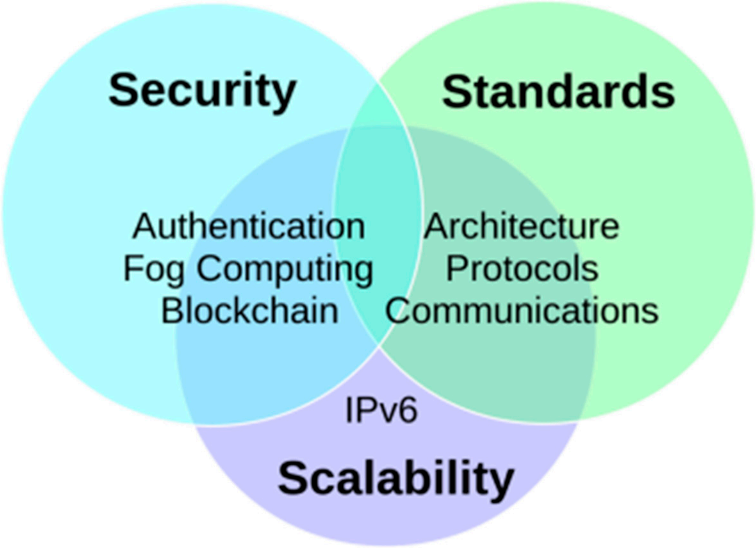

Figure 9. Open research areas.

Architectural Internet of Things research has primarily been divided into two fields from a wider pool of options, three-layer architecture and SoA-based architecture [180]. However, alternate architectural frameworks have been drafted and proposed as a result of distinct perspective issues in individual layers, such as the physical and network layers. These new architectures have largely been driven by a secure desire for standardization, especially within the field of research itself, due to dissonance in research resulting from industry fragmentation [183].

The lack of standardization within the field has created a vacuum for large-scale deployability. Because of the "multidisciplinary" nature of the field, research has demanded a universal, international standardization for Internet of Things protocols and communications [27,184]. Standardization, however, has proved to be a regulatory challenge, because of the mass variation of both consumer and industrial needs within the field internationally, as operations which result from legal and physical challenges, as shown for example by the impact of 5G technology, as well as the recent trend of technology-focused digital legislature, such as the European GDPR [35].

The relationship between the wider Internet and the Internet of Things has remained a tenuous topic for both security and functionality reasons. Open research has been done into the development of Web-based APIs for the purpose of devices securely accessing the web for functional reasons [185] as well as theoretical implementation of TCP as a transport-layer protocol, based on past historical applications of such in the field [186]. While this research exists, there has yet to be a generalized consensus on the usability of such in a wider scope. This, of course, relates back to the issue of lack of standardization, as the development and applicable testing of protocols and other proposals are predicated on their ability to be universally deployed, which is not currently viable without a consensus within the field [30,187].

Similarly, lack of standardization is also an issue that has pervaded studies into security improvements. However, it has not had as critical of an effect, due to many security proposals being intrinsically proposed in a vacuum for mitigating threats within certain architectures, or as a response to certain externalities [187]. Authentication, for example, has remained an open area of research; consensus agrees that authentication must be utilized in any secure Internet of Things architecture, but individual application of such has differed. Some open-ended papers have proposed protocols for key management schemes to strengthen resilience against cyber attacks [45,166,188]. Other research has taken a more generalized approach, surveying threats (which have shown to be more widely agreed upon) and proposing hybrid encryption schemes to protect against both data theft and hijacking [189]. However, besides standardized practices, other challenges are proposed for Internet of Things devices compared to more traditional computing; balancing security alongside energy consumption and available resources, for example, has remained a large problem, due to the complexities of stronger encryption competing with available system resources [158,187,189]. Looking to balance such attributes, studies have shown a sharp contrast in proposed solutions; some have proposed authentication through continuous authorization, or authentication based on direct user interaction [189]. Other studies have taken the route of providing security through cloud, or "fog computing" solutions [183]. Many studies, however, have incorporated security concerns into architectural proposals; this, typically, has intersected with proposals for Blockchain and decentralization [32,33,163,181,182]. Going back to Section 3 and in particular discussing access c, many approaches have been proposed to provide control access.

The usage of "fog computing" as a proposed solution has spurred a diverse sector of research [190]. The term itself, "fog computing", refers to a computing architecture which extends cloud computing methodology through employing peer entry nodes as middle-men between communicative devices and cloud networks. Some studies focus on more peer-to-peer based implementations, while others treat fog-computing as a layer in otherwise traditional cloud-computing architectures [190]. "Fog computing" has competed against cloud-computing within IoT spheres by providing similar security benefits but with overcoming many of the challenges cloud-computing otherwise faces, such as "latency requirements" or "bandwidth" or "resource" "constraints" [190]. Similar to cloud-computing, it allows for external and on-demand access to additional computing resources and virtual infrastructures with remote deployability and management [190]. As this is an open field of research, however, exact implementations of fog computing are not fully agreed upon. Many of the considered benefits have overlapped between studies, but implementations have widely varied. Some studies, for example, believe that Blockchain should be used to foster fog computing paradigms [191], while others believe that fog computing should simply act as a middleware-type framework for otherwise traditional cloud computing methods [192]. The exact architecture is also highly debated between studies [190,192,193]; some focus on optimized architecture for real time performance [190,192], while others are focused more on synchronization between nodes [193]. Others acknowledge the need for both synchronization and real-time efforts, but instead focus on adjacent implementations, such as sensor virtualizations [190].

While both Blockchain and decentralized architectures (generally, peer-to-peer or end-to-end) are fairly common, even within such proposals, there is a large distinction between papers as to theoretical implementation of such, and little case study or proof of concept within the field, due to the inherent large scale of such proposals [187]. Blockchain is often used as a means of proposing trust-based systems for ensuring integrity and non-repudiation [182]. Proposals have been more uniform among peer-to-peer studies, generally focusing on challenging the status quo by providing decentralized solutions based on improving scalability and privacy [176]. Most of these proposals have discussed forms of end-to-end encryption in tandem, but there are disagreements stemming from such, for example, how to distribute keys, or how to ensure standardization within a decentralized system across different hardware, manufacturers, and applications [159,176,180].

Other research has been conducted on scalability, which also intersects with proposals of standardization and security. Solutions regarding IPv6 for the further scalability of device connectivity has been proposed [194] but has yet to manifest as proof of concept with tangible results outside of theory. The scalability of the Internet of Things has remained an open topic, since, while it relies on standardization, it is also immediately striking as relevant technology is rolled out to consumer and industrial causes [187].

9. Conclusions

IoT is exponentially becoming part of our daily lives to increase efficiency, provide unlimited services, to increase the quality of life, and provide convenience via connecting different technologies, devices, and applications. As the number of IoT devices increases and adopted in different domains and applications, the number of threats and enormous security and privacy risks increase, creating an Internet of Vulnerabilities (IoV).

In this survey paper, we perform an in-depth systematic, comprehensive review and taxonomy of the state of the art and urgent security and privacy concerns that most matter to IoT. First, we present an overview of IoT, its underlying technologies and its limitations, approaches, as well as applications of IoT in different domains. Then, we follow that up with the coverage of previous diverse and significant similar related work that has been done for the past few years and the contribution of each work. Moreover, we explain the need for security in the context of IoT and why it is different from other systems due to its different applications' heterogeneity. In addition, we explore the most recent IoT security frameworks that address security and privacy concerns in IoT and propose a solution to maintain security and give more opportunities for IoT to become an integral part of different domains and fully embraced.

Moreover, the paper investigates attacks, threats and vulnerabilities and provides classification of them based on the severity and impact according to NIST's FIPS 199 definitions on the violation of Confidentiality, Integrity and Availability (CIA), which, to the best of our knowledge, is a unique contribution of this work and the first article to describe attacks, threats and vulnerabilities based on this criterion. Furthermore, we provide a multi-faceted approach to the mitigation of, and countermeasures to, these security concerns.

Finally, we discuss several current research challenges associated with IoT ecosystem that need further research and investigation in order for IoT to be fully adopted from convenience to mission-critical applications.

Author Contributions: Conceptualization, M.A.O.; writing—original draft preparation, M.A.O., S.O., J.H., A.A.H. and J.B.; writing—review and editing, M.A.O. and S.O.; visualization, S.O.; supervision, M.A.O.; project administration, M.A.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Sha, K.; Wei, W.; Andrew Yang, T.; Wang, Z.; Shi, W. On security challenges and open issues in Internet of Things. *Future Gener. Comput. Syst.* **2018**, *83*, 326–337. [CrossRef]
2. Samaila, M.G.; Neto, M.; Fernandes, D.A.B.; Freire, M.M.; Inácio, P.R.M. Challenges of securing Internet of Things devices: A survey. *Secur. Priv.* **2018**, *1*, e20. [CrossRef]
3. El-Shweky, B.E.; El-Kholy, K.; Abdelghany, M.; Salah, M.; Wael, M.; Alsherbini, O.; Ismail, Y.; Salah, K.; AbdelSalam, M. Internet of things: A comparative study. In Proceedings of the 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 622–631. [CrossRef]
4. Hassan, A.M.; Awad, A.I. Urban Transition in the Era of the Internet of Things: Social Implications and Privacy Challenges. *IEEE Access* **2018**, *6*, 36428–36440. [CrossRef]
5. Dhanvijay, M.M.; Patil, S.C. Internet of Things: A survey of enabling technologies in healthcare and its applications. *Comput. Netw.* **2019**, *153*, 113–131. [CrossRef]
6. Ojo, M.O.; Giordano, S.; Procissi, G.; Seitanidis, I.N. A Review of Low-End, Middle-End, and High-End Iot Devices. *IEEE Access* **2018**, *6*, 70528–70554. [CrossRef]
7. Frustaci, M.; Pace, P.; Aloi, G.; Fortino, G. Evaluating Critical Security Issues of the IoT World: Present and Future Challenges. *IEEE Internet Things J.* **2018**, *5*, 2483–2495. [CrossRef]
8. Yu, S.; Wang, G.; Liu, X.; Niu, J. Security and Privacy in the Age of the Smart Internet of Things: An Overview from a Networking Perspective. *IEEE Commun. Mag.* **2018**, *56*, 14–18. [CrossRef]
9. Liu, S.; Yue, K.; Zhang, Y.; Yang, H.; Liu, L.; Duan, X. The Research on IOT Security Architecture and Its Key Technologies. In Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 October 2018; pp. 1277–1280.
10. Guo, H.; Ren, J.; Zhang, D.; Zhang, Y.; Hu, J. A scalable and manageable IoT architecture based on transparent computing. *J. Parallel Distrib. Comput.* **2018**, *118*, 5–13. [CrossRef]
11. Obaidat, M.; Khodiaeva, M.; Obeidat, S.; Salane, D.; Holst, J. Security Architecture Framework for Internet of Things (IoT). In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 0154–0157.
12. Zhao, K.; Ge, L. A Survey on the Internet of Things Security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, Sichuan, China, 14–15 December 2013; pp. 663–667.
13. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
14. Anderson, R.; Kuhn, M. Tamper resistance-a cautionary note. In Proceedings of the Second USENIX Workshop on Electronic Commerce, Oakland, CA, USA, 18–21 November 1996; pp. 1–11.
15. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
16. Chen, K.; Zhang, S.; Li, Z.; Zhang, Y.; Deng, Q.; Ray, S.; Jin, Y. Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *J. Hardw. Syst. Secur.* **2018**, *2*, 97–110. [CrossRef]
17. Wolf, M.; Serpanos, D. Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. *Proc. IEEE* **2018**, *106*, 9–20. [CrossRef]

18. Ali, Q.; Ahmad, N.; Malik, A.; Ali, G.; Rehman, W. Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy. *Appl. Sci.* **2018**, *8*, 1964. [CrossRef]
19. Alam, M.M.; Malik, H.; Khan, M.I.; Pardy, T.; Kuusik, A.; Le Moullec, Y. A Survey on the Roles of Communication Technologies in IoT-Based Personalized Healthcare Applications. *IEEE Access* **2018**, *6*, 36611–36631. [CrossRef]
20. Ling, Z.; Liu, K.; Xu, Y.; Jin, Y.; Fu, X. An End-to-End View of IoT Security and Privacy. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7. [CrossRef]
21. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
22. Sadique, K.M.; Rahmani, R.; Johannesson, P. Towards Security on Internet of Things: Applications and Challenges in Technology. *Procedia Comput. Sci.* **2018**, *141*, 199–206. [CrossRef]
23. Ahanger, T.A.; Aljumah, A. Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms. *IEEE Access* **2019**, *7*, 11020–11028. [CrossRef]
24. NIST Computer Security Division. *F. I. P. S. Standards for Security Categorization of Federal Information and Information Systems*; NIST FIPS 199; NIST: Gaithersburg, MD, USA, 2004.
25. 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. Tutor.* **2019**, *21*, 2702–2733. [CrossRef]
26. Ahmed, A.W.; Khan, O.A.; Ahmed, M.M.; Shah, M.A. A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT. *IJACSA* **2017**, *8*, 489–501.
27. Datta, P.; Sharma, B. A survey on IoT architectures, protocols, security and smart city based applications. In Proceedings of the 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, 3–5 July 2017; pp. 1–5.
28. Rajendran, G.; Ragul Nivash, R.S.; Parthy, P.P.; Balamurugan, S. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–6.
29. Internet of Things Global Standards Initiative. Available online: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (accessed on 25 March 2020).
30. Ghadeer, H. Cybersecurity Issues in Internet of Things and Countermeasures. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Bellevue, WA, USA, 21–23 October 2018; pp. 195–201.
31. Dinker, A.G.; Sharma, V. Attacks and challenges in wireless sensor networks. In Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 16–18 March 2016; pp. 3069–3074.
32. Li, C.; Zhang, L.-J. A Blockchain Based New Secure Multi-Layer Network Model for Internet of Things. In Proceedings of the 2017 IEEE International Congress on Internet of Things (ICIOT), Honolulu, HI, USA, 25–30 June 2017; pp. 33–41.
33. Singh, M.; Singh, A.; Kim, S. Blockchain: A game changer for securing IoT data. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 51–55.
34. Sridhar, S.; Smys, S. Intelligent security framework for IoT devices cryptography based end-to-end security architecture. In Proceedings of the 2017 International Conference on Inve ntive Systems and Control (ICISC), Coimbatore, India, 19–20 January 2017; pp. 1–5.
35. Zheng, Y.; Dhabu, S.S.; Chang, C.-H. Securing IoT Monitoring Device using PUF and Physical Layer Authentication. In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 27–30 May 2018; pp. 1–5.
36. Ullah, I.; Shah, M.A.; Wahid, A.; Waheed, A. Protection of enterprise resources: A novel security framework. In Proceedings of the 2017 International Conference on Communication Technologies (ComTech), Slamabad, Pakistan, 19–21 April 2017; pp. 98–103.
37. Mahalle, P.N.; Anggorojati, B.; Prasad, N.R.; Prasad, R. Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *J. Cyber Secur. Mob.* **2013**, *1*, 309–348.

38. Kayes, A.S.M.; Rahayu, W.; Dillon, T.; Chang, E. Accessing Data from Multiple Sources through Context-Aware Access Control. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 551–559. [CrossRef]
39. Kayes, A.S.M.; Kalaria, R.; Sarker, I.H.; Islam, M.S.; Watters, P.A.; Ng, A.; Hammoudeh, M.; Badsha, S.; Kumara, I. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxon. Open Reseach Issues. *Sensors* **2020**, *20*, 2464. [CrossRef]
40. Jaswal, K.; Choudhury, T.; Chhokar, R.L.; Singh, S.R. Securing the Internet of Things: A proposed framework. In Proceedings of the 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 5–6 May 2017; pp. 1277–1281.
41. Sedrati, A.; Mezrioui, A. Internet of Things challenges: A focus on security aspects. In Proceedings of the 2017 8th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 4–6 April 2017; pp. 210–215.
42. Florea, I.; Ruse, L.C.; Rughinis, R. Challenges in security in Internet of Things. In Proceedings of the 2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet), Targu Mures, Romania, 21–23 September 2017; pp. 1–5.
43. Amadeo, M.; Molinaro, A.; Paratore, S.Y.; Altomare, A.; Giordano, A.; Mastroianni, C. A Cloud of Things framework for smart home services based on Information Centric Networking. In Proceedings of the 2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC), Calabria, Italy, 16–18 May 2017; pp. 245–250.
44. Naoui, S.; Elhdhili, M.E.; Saidane, L.A. Security analysis of existing IoT key management protocols. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–3 December 2016; pp. 1–7.
45. Agarwal, Y.; Dey, A.K. Toward Building a Safe, Secure, and Easy-to-Use Internet of Things Infrastructure. *Computer* **2016**, *49*, 88–91. [CrossRef]
46. Lee, J.; Yu, S.; Park, K.; Park, Y.; Park, Y. Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments. *Sensors* **2019**, *19*, 2358. [CrossRef] [PubMed]
47. Al Hayajneh, A.; Bhuiyan, M.Z.A.; McAndrew, I. Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN). *Computers* **2020**, *9*, 8. [CrossRef]
48. The History and Future of the Internet of Things. Available online: https://www.itransition.com/blog/iot-history (accessed on 25 March 2020).
49. Al Hayajneh, A.; Bhuiyan, M.Z.A.; McAndrew, I. A Novel Security Protocol for Wireless Sensor Networks with Cooperative Communication. *Computers* **2020**, *9*, 4. [CrossRef]
50. Hayajneh, T.; Griggs, K.; Imran, M. Secure and efficient data delivery for fog-assisted wireless body area networks. *Peer-to-Peer Netw. Appl.* **2019**, *12*, 1289–1307. [CrossRef]
51. Tao, H.; Bhuiyan, M.Z.A.; Abdalla, A.N.; Hassan, M.M.; Zain, J.M.; Hayajneh, T. Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare. *IEEE Internet Things J.* **2019**, *6*, 410–420. [CrossRef]
52. Alam, T. A Reliable Communication Framework and Its Use in Internet of Things (IoT). *IJSRCSEIT* **2018**, *3*, 450–456.
53. Broadcom, Symantec, Internet Security Threat Report, Volume 24. Available online: https://www.broadcom.com/support/security-center (accessed on 11 March 2020).
54. Broadcom, Symantec, Internet Security Threat Report, Volume 21. Available online: https://www.broadcom.com/support/security-center (accessed on 11 March 2020).
55. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication Protocols for Internet of Things: A Comprehensive Survey. *Secur. Commun. Netw.* **2017**, *2017*, 1–41. [CrossRef]
56. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Netw.* **2018**, *4*, 118–137. [CrossRef]
57. Singh, D.; Pati, B.; Panigrahi, C.R.; Swagatika, S. Security Issues in IoT and their Countermeasures in Smart City Applications. In *Advanced Computing and Intelligent Engineering*; Pati, B., Panigrahi, C.R., Buyya, R., Li, K.-C., Eds.; Springer: Singapore, 2020; Volume 1089, pp. 301–313, ISBN 9789811514821.
58. Yassine, A.; Singh, S.; Hossain, M.S.; Muhammad, G. IoT big data analytics for smart homes with fog and cloud computing. *Futur. Gener. Comput. Syst.* **2019**, *91*, 563–573. [CrossRef]

59. Guimaraes, V.G.; de Moraes, R.M.; Obraczka, K.; Bauchspiess, A. A Novel IoT Protocol Architecture: Efficiency through Data and Functionality Sharing across Layers. In Proceedings of the 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 29 July–1 August 2019; pp. 1–9.
60. Xhafa, F.; Kilic, B.; Krause, P. Evaluation of IoT stream processing at edge computing layer for semantic data enrichment. *Futur. Gener. Comput. Syst.* **2020**, *105*, 730–736. [CrossRef]
61. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Futur. Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
62. Salman, T.; Jain, R. A Survey of Protocols and Standards for Internet of Things. *arXiv* **2019**, arXiv:1903.11549. [CrossRef]
63. 6 Leading Types of IoT Wireless Tech and Their Best Use Cases. Available online: https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases (accessed on 4 April 2020).
64. Chi, T.; Chen, M. A frequency hopping method for spatial RFID/WiFi/Bluetooth scheduling in agricultural IoT. *Wirel. Netw.* **2019**, *25*, 805–817. [CrossRef]
65. Kurunathan, H.; Severino, R.; Koubaa, A.; Tovar, E. DynaMO—Dynamic Multisuperframe Tuning for Adaptive IEEE 802.15.4e DSME Networks. *IEEE Access* **2019**, *7*, 122522–122535. [CrossRef]
66. 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]
67. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27. [CrossRef]
68. Barki, A.; Bouabdallah, A.; Gharout, S.; Traore, J. M2M Security: Challenges and Solutions. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1241–1254. [CrossRef]
69. Benzarti, S.; Triki, B.; Korbaa, O. A survey on attacks in Internet of Things based networks. In Proceedings of the 2017 International Conference on Engineering & MIS (ICEMIS), Monastir, Tunisia, 8–10 May 2017; pp. 1–7.
70. Abdur, M.; Habib, S.; Ali, M.; Ullah, S. Security Issues in the Internet of Things (IoT): A Comprehensive Study. *IJACSA* **2017**, *8*, 383–388. [CrossRef]
71. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. In Proceedings of the 2015 IEEE World Congress on Services, New York, NY, USA, 27 June–2 July 2015; pp. 21–28.
72. Abomhara, M.; Køien, G.M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *JCSM* **2015**, *4*, 65–88. [CrossRef]
73. Dorsemaine, B.; Gaulier, J.-P.; Wary, J.-P.; Kheir, N.; Urien, P. A new approach to investigate IoT threats based on a four layer model. In Proceedings of the 2016 13th International Conference on New Technologies for Distributed Systems (NOTERE), Paris, France, 18 July 2016; pp. 1–6.
74. Ahmed, E.; Yaqoob, I.; Gani, A.; Imran, M.; Guizani, M. Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges. *IEEE Wirel. Commun.* **2016**, *23*, 10–16. [CrossRef]
75. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-Physical Systems Security—A Survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
76. Mosenia, A.; Jha, N.K. A Comprehensive Study of Security of Internet-of-Things. *IEEE Trans. Emerg. Topics Comput.* **2017**, *5*, 586–602. [CrossRef]
77. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access* **2019**, *7*, 82721–82743. [CrossRef]
78. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of Threats to the Internet of Things. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1636–1675. [CrossRef]
79. Miloslavskaya, N.; Tolstoy, A. Internet of Things: Information security challenges and solutions. *Cluster Comput.* **2019**, *22*, 103–119. [CrossRef]
80. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet Things J.* **2019**, *6*, 1606–1616. [CrossRef]
81. Akram, H.; Konstantas, D.; Mahyoub, M. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *IJACSA* **2018**, *9*, 090349. [CrossRef]

82. Obaidat, M.; Khodjaeva, M.; Holst, J.; Ben Zid, M. Security and Privacy Challenges in Vehicular Ad Hoc Networks. In *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks for the IoV*; Mahmood, Z., Ed.; Springer International Publishing: Cham, Switzerland, 2020; pp. 223–251, ISBN 978-3-030-36167-9.
83. Khodjaeva, M.; Obeidat, M.; Salane, D. Mitigating Threats and Vulnerabilities of RFID in IoT through Outsourcing Computations Using Public Key Cryptography. In *Security, Privacy and Trust in the IoT Environment*; Springer: Berlin/Heidelberg, Germany, 2019.
84. Internet of Things: The Complete Reimaginative Force: TCS Global Trend Study-July 2015. Available online: https://www.criticaleye.com/inspiring/insights-servfile.cfm?id=4255 (accessed on 27 May 2020).
85. Patel, C.; Doshi, N. *Internet of Things Security: Challenges, Advances, and Analytics*, 1st ed.; Auerbach Publications: Boca Raton, FL, USA, 2019; ISBN 9780429454448.
86. Chaudhuri, A. *Internet of Things, for Things, and by Things*, 1st ed.; Auerbach Publications; CRC Press/Taylor & Francis Group: Boca Raton, FL, USA, 2018; ISBN 9781315200644.
87. Urien, P. An innovative security architecture for low cost low power IoT devices based on secure elements: A four quarters security architecture. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018; pp. 1–2.
88. Yu, S.; Park, K.; Park, Y. A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment. *Sensors* **2019**, *19*, 3598. [CrossRef]
89. Olivier, F.; Carlos, G.; Florent, N. New Security Architecture for IoT Network. *Procedia Comput. Sci.* **2015**, *52*, 1028–1033. [CrossRef]
90. Ling, Z.; Liu, K.; Xu, Y.; Gao, C.; Jin, Y.; Zou, C.; Fu, X.; Zhao, W. IoT Security: An End-to-End View and Case Study. *arXiv* **2018**, arXiv:1805.05853.
91. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet* **2017**, *9*, 27. [CrossRef]
92. Huang, X.; Craig, P.; Lin, H.; Yan, Z. SecIoT: A security framework for the Internet of Things: SecIoT: A security framework for the Internet of Things. *Secur. Comm. Netw.* **2016**, *9*, 3083–3094. [CrossRef]
93. Colombo, P.; Ferrari, E. Fine-Grained Access Control within NoSQL Document-Oriented Datastores. *Data Sci. Eng.* **2016**, *1*, 127–138.
94. Colombo, P.; Ferrari, E. Enhancing MongoDB with purpose based access control. *IEEE Trans. Dependable Secure Comput.* **2015**, *14*, 591–604. [CrossRef]
95. Colombo, P.; Ferrari, E. Towards virtual private NoSQL datastores. In Proceedings of the 2016 IEEE 32nd International Conference on Data Engineering (ICDE), Helsinki, Finland, 16–20 May 2016; pp. 193–204.
96. Ulusoy, H.; Colombo, P.; Ferrari, E.; Kantarcioglu, M.; Pattuk, E. GuardMR, fine-grained security policy enforcement for MapReduce systems. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, Singapore, 14–17 April 2015; pp. 285–296.
97. Colombo, P.; Ferrari, E. Enhancing NoSQL datastores with fine-grained context-aware access control: A preliminary study on MongoDB. *Int. J. Cloud Comput.* **2017**, *6*, 292–305. [CrossRef]
98. Irshad, M. A Systematic Review of Information Security Frameworks in the Internet of Things (IoT). In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia, 12–14 December 2016; pp. 1270–1275.
99. Krishna, B.V.S.; Gnanasekaran, T. A systematic study of security issues in Internet-of-Things (IoT). In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Coimbatore, India, 10–11 February 2017; pp. 107–111.
100. Ahemd, M.M.; Shah, M.A.; Wahid, A. IoT security: A layered approach for attacks & defenses. In Proceedings of the 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 19–21 October 2017; pp. 104–110.
101. 101. Lee, C.; Zappaterra, L.; Kwanghee, C. Hyeong-Ah Choi Securing smart home: Technologies, security challenges, and security requirements. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 67–72.
102. Puthal, D.; Nepal, S.; Ranjan, R.; Chen, J. Threats to Networking Cloud and Edge Datacenters in the Internet of Things. *IEEE Cloud Comput.* **2016**, *3*, 64–71. [CrossRef]

103. Atamli, A.W.; Martin, A. Threat-Based Security Analysis for the Internet of Things. In Proceedings of the 2014 International Workshop on Secure Internet of Things, Wroclaw, Poland, 7–11 September 2014; pp. 35–43.
104. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187.
105. Wang, X.; Chellappan, S.; Gu, W.; Yu, W.; Xuan, D. Search-based physical attacks in sensor networks. In Proceedings of the 14th International Conference on Computer Communications and Networks, ICCCN 2005, San Diego, CA, USA, 17–19 October 2005; pp. 489–496.
106. Parno, B.; Perrig, A.; Gligor, V. Distributed Detection of Node Replication Attacks in Sensor Networks. In Proceedings of the 2005 IEEE Symposium on Security and Privacy (S&P'05), Oakland, CA, USA, 8–11 May 2005; pp. 49–63.
107. Zorzi, M.; Gluhak, A.; Lange, S.; Bassi, A. From today's INTRAnet of things to a future INTERnet of things: A wireless- and mobility-related view. *IEEE Wirel. Commun.* **2010**, *17*, 44–51. [CrossRef]
108. Hernandez, G.; Arias, O.; Buentello, D.; Jin, Y. Smart Nest thermostat: A Smart Spy in Your Home. In Proceedings of the Black Hat, Las Vegas, NV, USA, 6–7 August 2014.
109. Kaur, D.; Singh, P. Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack. *ACEEE Int. J. Netw. Secur.* **2014**, *5*, 1.
110. Laeeq, K.; Shamsi, J.A. A Study of Security Issues, Vulnerabilities and Challenges in Internet of Things. In *Securing Cyber-Physical Systems*; Pathan, A.K., Ed.; CRC Press: Boca Raton, FL, USA, 2015; p. 221.
111. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37.
112. Weingart, S.H. Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. In *Cryptographic Hardware and Embedded Systems—CHES 2000*; Koç, Ç.K., Paar, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1965, pp. 302–317, ISBN 9783540414551.
113. Martin, T.; Hsiao, M.; Dong, H.; Krishnaswami, J. Denial-of-service attacks on battery-powered mobile computers. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications, Orlando, FL, USA, 14–17 March 2004; pp. 309–318.
114. Khouzani, M.H.R.; Sarkar, S. Maximum Damage Battery Depletion Attack in Mobile Sensor Networks. *IEEE Trans. Automat. Contr.* **2011**, *56*, 2358–2368. [CrossRef]
115. Agah, A.; Das, S.K. Preventing DoS attacks in wireless sensor networks: A repeated game theory approach. *IJ Netw. Secur.* **2007**, *5*, 145–153.
116. Vasserman, E.Y.; Hopper, N. Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. *IEEE Trans. Mob. Comput.* **2013**, *12*, 318–332. [CrossRef]
117. Li, M.; Koutsopoulos, I.; Poovendran, R. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks. *IEEE Trans. Mob. Comput.* **2010**, *9*, 1119–1133.
118. Billure, R.; Tayur, V.M.; Mahesh, V. Internet of Things-A study on the security challenges. In Proceedings of the 2015 IEEE International Advance Computing Conference (IACC), Banglore, India, 12–13 June 2015; pp. 247–252.
119. Halim, T.; Islam, M.R. A Study on the Security Issues in WSN. *Int. J. Comput. Appl.* **2012**, *53*. [CrossRef]
120. Walters, J.P.; Liang, Z.; Shi, W.; Chaudhary, V. Wireless sensor network security: A survey. *Secur. Distrib. Grid. Mob. Pervasive Comput.* **2007**, *1*, 367.
121. Chan, H.; Perrig, A.; Song, D. Random key predistribution schemes for sensor networks. In Proceedings of the 19th International Conference on Data Engineering (Cat. No. 03CH37405), Bangalore, India, 5–8 March 2003; pp. 197–213.
122. Padmavathi, D.G.; Shanmugapriya, M.D. A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *arXiv* **2009**, arXiv:0909.0576.
123. Mohsen Nia, A.; Sur-Kolay, S.; Raghunathan, A.; Jha, N.K. Physiological Information Leakage: A New Frontier in Health Information Security. *IEEE Trans. Emerg. Topics Comput.* **2016**, *4*, 321–334. [CrossRef]
124. Li, L. Study on security architecture in the Internet of Things. In Proceedings of the 2012 International Conference on Measurement, Information and Control, Harbin, China, 18–20 May 2012; pp. 374–377.
125. Bhattasali, T.; Chaki, R.; Sanyal, S. Sleep Deprivation Attack Detection in Wireless Sensor Network. *IJCA* **2012**, *40*, 19–25. [CrossRef]

126. Burmester, M.; Munilla, J.; Ortiz, A. Comments on "Unreconciled Collisions Uncover Cloning Attacks in Anonymous RFID Systems" . *IEEE Trans. Inf. Forensic Secur.* **2018**, *13*, 2929–2931. [CrossRef]
127. Chen, X.; Liu, J.; Wang, X.; Zhang, X.; Wang, Y.; Chen, L. Combating Tag Cloning with COTS RFID Devices. In Proceedings of the 2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Hong Kong, China, 11–13 June 2018; pp. 1–9.
128. Juels, A.; Rivest, R.L.; Szydlo, M. The blocker tag: Selective blocking of RFID tags for consumer privacy. In Proceedings of the 10th ACM Conference on Computer and Communication Security (CCS 2003), Washington, DC, USA, 27–30 October 2003; p. 103.
129. Weis, S.A.; Sarma, S.E.; Rivest, R.L.; Engels, D.W. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Computing*; Hutter, D., Müller, G., Stephan, W., Ullmann, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2802, pp. 201–212, ISBN 978-3-540-24646-6.
130. Mukaddam, A.; Elhajj, I.; Kayssi, A.; Chehab, A. IP Spoofing Detection Using Modified Hop Count. In Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, Victoria, BC, Canada, 13–16 May 2014; pp. 512–516.
131. Sopori, D.; Pawar, T.; Patil, M.; Ravindran, R. Internet of Things: Security Threats. *IJARCET* **2017**, *6*, 5.
132. Mitrokotsa, A.; Rieback, M.R.; Tanenbaum, A.S. Classifying RFID attacks and defenses. *Inf. Syst. Front.* **2010**, *12*, 491–505. [CrossRef]
133. Grover, A.; Berghel, H. A Survey of RFID Deployment and Security Issues. *J. Inf. Proc. Syst.* **2011**, *7*, 561–580. [CrossRef]
134. Wallgren, L.; Raza, S.; Voigt, T. Routing Attacks and Countermeasures in the RPL-Based Internet of Things. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 794326. [CrossRef]
135. Padhy, R.P.; Patra, M.R.; Satapathy, S.C. Cloud computing: Security issues and research challenges. *IJCSITS* **2011**, *1*, 136–146.
136. Li, C.; Qin, Z.; Novak, E.; Li, Q. Securing SDN Infrastructure of IoT–Fog Networks from MitM Attacks. *IEEE Internet Things J.* **2017**, *4*, 1156–1164. [CrossRef]
137. Sehrawat, H.; Singh, Y. Detecting Sinkhole Attack in Wireless Sensor Networks. *IJESPR* **2018**, *47*, 6.
138. Parvathy, K. Security Attacks on Network Layer in Wireless Sensor Networks-An Overview. *IJRASET* **2017**, *5*, V.
139. Ali, S.; Khan, M.A.; Ahmad, J.; Malik, A.W.; Rehman, A. Detection and prevention of Black Hole Attacks in IOT & WSN. In Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23–26 April 2018; pp. 217–226.
140. Hamid, M.A.; Rashid, M.O.; Hong, C.S. Routing Security in Sensor Network: Hello Flood Attack and Defense. *IEEE ICNEWS* **2006**, *2*, 2–4.
141. Lokulwar, P.P.; Deshmukh, H.R. Threat analysis and attacks modelling in routing towards IoT. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 721–726.
142. Karakehayov, Z. Using REWARD to detect team black-hole attacks in wireless sensor networks. In Proceedings of the Workshop Real-World Wireless Sensor Networks, Stockholm, Sweden, 20–21 June 2005; pp. 20–21.
143. Revathi, B.; Geetha, D. A survey of cooperative black and gray hole attack in MANET. *IJ Comput. Sci. Manag. Res.* **2012**, *1*, 2.
144. Lee, P.; Clark, A.; Bushnell, L.; Poovendran, R. A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems. *IEEE Trans. Automat. Contr.* **2014**, *59*, 3224–3237. [CrossRef]
145. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The Sybil attack in sensor networks: Analysis & defenses. In Proceedings of the Third International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 26–27 April 2004; pp. 259–268.
146. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil Attacks and Their Defenses in the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 372–383. [CrossRef]
147. Farooq, M.U.; Waseem, M.; Khairi, A.; Mazhar, S. A Critical Analysis on the Security Concerns of Internet of Things (IoT). *IJCA* **2015**, *111*, 1–6. [CrossRef]
148. Singh, V.P.; Jain, S.; Singhai, J. Hello flood attack and its countermeasures in wireless sensor networks. *IJ Comput. Sci.* **2010**, *7*, 23.

149. Kim, D.S.; Shin, T.-H.; Lee, B.; Park, J.S. Access Control and Authorization for Security of RFID Multi-domain Using SAML and XACML. In *Computational Intelligence and Security*; Wang, Y., Cheung, Y., Liu, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4456, pp. 887–893, ISBN 9783540743767.
150. Uttarkar, R.; Kulkarni, R. Internet of Things: Architecture and Security. *IJ Comput. Appl.* **2014**, *3*, 4.
151. Khoo, B. RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 19–22 October 2011; pp. 709–712.
152. Thakur, B.S.; Chaudhary, S. Content sniffing attack detection in client and server side: A survey. *IJACR* **2013**, *3*, 7.
153. Swamy, S.N.; Jadhav, D.; Kulkarni, N. Security threats in the application layer in IOT applications. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Coimbatore, India, 10–11 February 2017; pp. 477–480.
154. Javed, M.A.; Ben Hamida, E. Adaptive security mechanisms for safety applications in Internet of Vehicles. In Proceedings of the 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), New York, NY, USA, 17–19 October 2016; pp. 1–6.
155. Zheng, Z.; Jin, S.; Bettati, R.; Reddy, A.L.N. Securing cyber-physical systems with adaptive commensurate response. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017; pp. 1–6.
156. Ogunnaike, R.M.; Lagesse, B. Toward consumer-friendly security in smart environments. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 612–617.
157. Sun, G.; Chang, V.; Ramachandran, M.; Sun, Z.; Li, G.; Yu, H.; Liao, D. Efficient location privacy algorithm for Internet of Things (IoT) services and applications. *J. Netw. Comput. Appl.* **2017**, *89*, 3–13. [CrossRef]
158. Koley, S.; Ghosal, P. Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions. In Proceedings of the 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), Beijing, China, 10–14 August 2015; pp. 517–520.
159. Lee, C.; Fumagalli, A. Internet of Things Security—Multilayered Method for End to End Data Communications Over Cellular Networks. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 24–28.
160. Rudd, E.M.; Rozsa, A.; Günther, M.; Boult, T.E. A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1145–1172. [CrossRef]
161. Shah, S.A.; Simnani, S.S.; Banday, M.T. A Study of Security Attacks on Internet of Things and Its Possible Solutions. In Proceedings of the 2018 International Conference on Automation and Computational Engineering (ICACE), Great Noida, India, 3–5 October 2018; pp. 203–209.
162. Asplund, M.; Nadjm-Tehrani, S. Attitudes and Perceptions of IoT Security in Critical Societal Services. *IEEE Access* **2016**, *4*, 2130–2138. [CrossRef]
163. Spathoulas, G.; Karageorgopoulou, A. Security and Privacy in the Internet of Things Using Blockchain Technology. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 20–31 May 2019; pp. 284–290.
164. Narang, S.; Nalwa, T.; Choudhury, T.; Kashyap, N. An efficient method for security measurement in internet of things. In Proceedings of the 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT 2018), Chennai, India, 15–17 February 2018; pp. 319–323.
165. El Hajjar, A. Securing the Internet of Things Devices Using Pre-Distributed Keys. In Proceedings of the 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), Berlin, Germany, 4–8 April 2016; pp. 198–200.
166. Banerjee, S.; Odelu, V.; Das, A.K.; Srinivas, J.; Kumar, N.; Chattopadhyay, S.; Choo, K.-K.R. A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment. *IEEE Internet Things J.* **2019**, *6*, 8739–8752. [CrossRef]

167. Negalign, W.H.; Xiong, H.; Assefa, A.A.; Gemechu, A.Y.; Geresu, D.M. Outsourced Attribute-Based Signcryption in the Cloud Computing. In Proceedings of the 2018 15th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 14–18 December 2018; pp. 40–44.
168. Muthavhine, K.D.; Sumbwanyambe, M. An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect. In Proceedings of the 2018 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 6–7 March 2018; pp. 114–119.
169. Khan, Z.A.; Herrmann, P. A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, China, 27–29 March 2017; pp. 1169–1176.
170. Pu, C.; Carpenter, L. Digital Signature Based Countermeasure Against Puppet Attack in the Internet of Things. In Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, UK, 25–28 September 2019; pp. 1–4.
171. Gupta, N.; Naik, V.; Sengupta, S. A firewall for Internet of Things. In Proceedings of the 2017 9th International Conference on Communication Systems and Networks (COMSNETS), Bengaluru, India, 4–8 January 2017; pp. 411–412.
172. Liu, C.; Zhang, Y.; Li, Z.; Zhang, J.; Qin, H.; Zeng, J. Dynamic Defense Architecture for the Security of the Internet of Things. In Proceedings of the 2015 11th International Conference on Computational Intelligence and Security (CIS), Shenzhen, China, 19–20 December 2015; pp. 390–393.
173. Anthi, E.; Williams, L.; Burnap, P. Pulse: An adaptive intrusion detection for the Internet of Things. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT-2018, London, UK, 28–29 March 2018; pp. 1–4.
174. Surnin, O.; Hussain, F.; Hussain, R.; Ostrovskaya, S.; Polovinkin, A.; Lee, J.; Fernando, X. Probabilistic Estimation of Honeypot Detection in Internet of Things Environment. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 17–20 February 2019; pp. 191–196.
175. Liu, Y.; Kuang, Y.; Xiao, Y.; Xu, G. SDN-Based Data Transfer Security for Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 257–268. [CrossRef]
176. Bhattarai, S.; Wang, Y. End-to-End Trust and Security for Internet of Things Applications. *Computer* **2018**, *51*, 20–27. [CrossRef]
177. Li, D.-Y.; Xie, S.-D.; Chen, R.-J.; Tan, H.-Z. Design of Internet of Things System for Library Materials Management using UHF RFID. In Proceedings of the 2016 IEEE International Conference on RFID Technology and Applications (RFID-TA), Shunde, China, 21–23 September 2016; pp. 44–48.
178. Zhang, P.; Nagarajan, S.G.; Nevat, I. Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things. *IEEE Internet Things J.* **2017**, *4*, 2199–2206. [CrossRef]
179. Ahmad, M.; Farid, M.A.; Ahmed, S.; Saeed, K.; Asharf, M.; Akhtar, U. Impact and Detection of GPS Spoofing and Countermeasures against Spoofing. In Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Sindh, Pakistan, 30–31 January 2019; pp. 1–8.
180. Kaur, K. A Survey on Internet of Things—Architecture, Applications, and Future Trends. In Proceedings of the 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 15–17 December 2018; pp. 581–583.
181. Conoscenti, M.; Vetrò, A.; De Martin, J.C. Peer to Peer for Privacy and Decentralization in the Internet of Things. In Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina, 20–28 May 2017; pp. 288–290.
182. Urien, P. Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues. In Proceedings of the 2018 3rd Cloudification of the Internet of Things (CIoT), Paris, France, 2–4 July 2018; pp. 1–4.
183. IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT). IEEE P2413/D0.4.5, December 2018, 1–264. Available online: https://standards.ieee.org/standard/2413-2019.html#Standard (accessed on 28 May 2020).

184. Hassan, Q.F. On Standardizing the Internet of Things and Its Applications. In *Internet of Things A to Z: Technologies and Applications*; IEEE: Piscataway, NJ, USA, 2018; pp. 191–218.
185. Sahni, N.; Bose, J.; Das, K. Web APIs for Internet of Things. In Proceedings of the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India, 19–22 September 2018; pp. 2175–2181.
186. Gomez, C.; Arcia-Moret, A.; Crowcroft, J. TCP in the Internet of Things: From Ostracism to Prominence. *IEEE Internet Comput.* **2018**, *22*, 29–41. [CrossRef]
187. Chopra, K.; Gupta, K.; Lambora, A. Future Internet: The Internet of Things-A Literature Review. In Proceedings of the 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 14–16 February 2019; pp. 135–139.
188. Celia, L.; Cungang, Y. (WIP) Authenticated Key Management Protocols for Internet of Things. In Proceedings of the 2018 IEEE International Congress on Internet of Things (ICIOT), Seattle, WA, USA, 25–30 June 2018; pp. 126–129.
189. Shahzad, M.; Singh, M.P. Continuous Authentication and Authorization for the Internet of Things. *IEEE Internet Comput.* **2017**, *21*, 86–90. [CrossRef]
190. Wei, X.; Wu, L. A New Proposed Sensor Cloud Architecture Based on Fog Computing for Internet of Things. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Piscataway, NJ, USA, 14–17 July 2019.
191. Zhu, X.; Badr, Y. Fog Computing Security Architecture for the Internet of Things Using Blockchain-Based Social Networks. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018.
192. Popovic, I.T.; Rakic, A.Z. The Fog-Based Framework for Design of Real-Time Control Systems in Internet of Things Environment. In Proceedings of the 2018 International Symposium on Industrial Electronics (INDEL), Banja Luka, Bosnia and Herzegovina, 1–3 November 2018.
193. Olaniyan, R.; Maheswaran, M. Multipoint Synchronization for Fog-Controlled Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 9656–9667. [CrossRef]
194. Ziegler, S. Considerations on IPv6 scalability for the Internet of Things—Towards an intergalactic Internet. In Proceedings of the 2017 Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–4.