*sustainability*

MDPI

*Review*

# State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions

**Ritika Raj Krishna [1], Aanchal Priyadarshini [1], Amitkumar V. Jha [1], Bhargav Appasani [1], Avireni Srinivasulu [2] and Nicu Bizon [3,4,*]**

[1] School of Electronics Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar 751024, India; ritikaraj11a@gmail.com (R.R.K.); aanchal233100@gmail.com (A.P.); amit.jhafet@kiit.ac.in (A.V.J.); bhargav.appasanifet@kiit.ac.in (B.A.)
[2] Department of Electronics and Communication Engineering, K. R. Mangalam University, Gurugram 122103, India; avireni@ieee.org
[3] Faculty of Electronics, Communication and Computers, University of Pitesti, 110040 Pitesti, Romania
[4] Doctoral School, Polytechnic University of Bucharest, 313 Splaiul Independentei, 060042 Bucharest, Romania
* Correspondence: nicu.bizon@upit.ro

**Abstract:** The Internet of Things (IoT) plays a vital role in interconnecting physical and virtual objects that are embedded with sensors, software, and other technologies intending to connect and exchange data with devices and systems around the globe over the Internet. With a multitude of features to offer, IoT is a boon to mankind, but just as two sides of a coin, the technology, with its lack of securing information, may result in a big bane. It is estimated that by the year 2030, there will be nearly 25.44 billion IoT devices connected worldwide. Due to the unprecedented growth, IoT is endangered by numerous attacks, impairments, and misuses due to challenges such as resource limitations, heterogeneity, lack of standardization, architecture, etc. It is known that almost 98% of IoT traffic is not encrypted, exposing confidential and personal information on the network. To implement such a technology in the near future, a comprehensive implementation of security, privacy, authentication, and recovery is required. Therefore, in this paper, the comprehensive taxonomy of security and threats within the IoT paradigm is discussed. We also provide insightful findings, presumptions, and outcomes of the challenges to assist IoT developers to address risks and security flaws for better protection. A five-layer and a seven-layer IoT architecture are presented in addition to the existing three-layer architecture. The communication standards and the protocols, along with the threats and attacks corresponding to these three architectures, are discussed. In addition, the impact of different threats and attacks along with their detection, mitigation, and prevention are comprehensively presented. The state-of-the-art solutions to enhance security features in IoT devices are proposed based on Blockchain (BC) technology, Fog Computing (FC), Edge Computing (EC), and Machine Learning (ML), along with some open research problems.

**Keywords:** Internet of Things; security; threats; privacy; vulnerabilities; Blockchain

check for updates

**Citation:** Krishna, R.R.; Priyadarshini, A.; Jha, A.V.; Appasani, B.; Srinivasulu, A.; Bizon, N. State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. *Sustainability* **2021**, *13*, 9463. https://doi.org/10.3390/su13169463

Academic Editor: Zubair Baig

Received: 30 May 2021
Accepted: 18 August 2021
Published: 23 August 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

## 1. Introduction

We live in a time when technology is an essential requirement for all humans, and the evidence is the increased dependence on technology in almost every aspect of our lives. Today's world is evolving with the rapidly growing Internet of Things (IoT)-based application [1]. The rise of the IoT has been a glorious phenomenon in recent years. The physical and virtual objects implanted with sensors, software, and other technologies are interlinked together in IoT [2]. It envisages communicating and sharing data with other devices and systems worldwide over the Internet. Further, IoT is like an array of network-enabled devices that exclude traditional computers such as laptops and servers.

IoT has sprawled everywhere, starting from the healthcare sector to the big industries. It is now implantable, wearable, and portable, resulting in a pervasive and interactive

world [3]. It modifies the physical objects around us into smart objects, creating an information environment that increasingly changes human living standards. For instance, IoT devices track and collect essential measurements (such as blood pressure, blood sugar level, pulse rate, etc.) in real time, allowing emergency alerts to improve the odds of a patient's survival [4]. Moreover, autonomous and self-driving vehicles prevent drivers from deviating from paths or accidents while providing them assistance to reach their destinations. In addition, those definitions are expanded to provide automatic emergency alerts of the closest road and medical assistance in the event of an accident. IoT also covers many aspects of modern industries, including manufacturing, assembly, packing, logistics, smart cities, and aviation industries [5]. Some of the essential IoT-based application domains in health, commerce, communication, and entertainment are shown in Figure 1.


**Figure 1.** Important IoT application domains.

To implement IoT, the traditional technology had to undergo some major modifications. For example, to convert an isolated device into a transmitting device, there is a need to increase small computing devices' memory and processing capacity while dramatically reducing their size [6]. Further, the creation of various lightweight, secure protocols for communication between different IoT devices is equally important. The improvements to the conventional networks to help the operation of the IoT ecosystem have their own set of consequences. However, the unprecedented growth of interconnected devices has crippled the IoT ecosystem. Consequently, there exists enough scope for threats and attacks in IoT-based applications.

The Global Vice President at New Net Technologies (NNT), Dirk Schrader, stated that IoT-based computers have become the crown jewels of cybercriminals. He also said that less than 42% of businesses can detect insecure IoT devices. Hence, for researchers to develop well-grounded solutions to trace and avert these threats, they must first understand the threats and attacks to make the IoT environment safe, secure, and reliable. There are three significant aspects to consider while examining the IoT from a security perspective. To begin with, there are a massive number of smart devices, possibly billions. This suggests that the IoT would be the most complex man-made system ever in terms of the number of entities involved [7]. Second, they are essentially heterogeneous, with respect to the functionality, protocol stacks, radios, operating systems (some objects do not even have one), energy sources, identities, and so on [8]. Third, each smart object is owned by a company or a person, and it is managed by the same or a different company or individual. Millions of businesses and individuals are in control of a subset of the smart objects in their management domains. From the standpoint of protection, privacy, and trust, how this control is technically upheld is a critical issue.

The attack surface in the IoT domain has increased significantly, as have the possible threats to the protection of these entities in the domain [9]. For example, the security threats to the autonomous and self-driving industry may lead to disastrous consequences. Autonomous vehicles are vulnerable to sensor-based attacks. By manipulating the sensors (e.g., linear acceleration sensor, magnetic sensor, etc.), attackers may collect data, transfer malware to it, or trigger a malicious activity [10]. Furthermore, smartphones and embedded systems contribute to a digital ecosystem for global communication that simplifies lives by being sensitive, flexible, and responsive to human needs. However, on the other hand, security cannot be assured due to vulnerabilities in IoT. When a user's signal is disrupted or intercepted, their privacy may be jeopardized, and their information may be leaked.

The state-of-the-art survey on various aspects of IoT, including security, privacy, and robustness, has been presented in [11] by Chen et al. The authors focused on specific issues of IoT interface positioning and localization. The development of lightweight block cipher algorithms has been proposed to be used in devices for data encryption and decryption [12]. A desktop review and qualitative analysis have been performed by Gamudani et al. in [13] to compute performance analysis of attacks. Cryptographic approaches have been discussed in [14] as a method of ensuring long-term security approaches. Different layer architectures of IoT and security issues associated with them have been discussed with possible countermeasures using Blockchain (BC) in [15]. The survey on security aspects of IoT has been presented by Alaba et al. in [16], covering the scope of security countermeasures in some other allied paradigms, including Machine-to-Machine (M2M), Cyber-Physical System (CPS), and Wireless Sensor Networks (WSNs). In [17], Abomhara et al. discussed various applications of IoT and the security threats related to them, including vulnerabilities, intruders, and some other attacks. The threats concerning security and privacy in IoT architecture have been presented without counter measuring techniques by Kozlov et al. in [18].

The organization of the paper is as follows. The state-of-the-art motivation and contributions of this research are presented in Section 2. The background of the IoT as the foundation to the security threats and attacks is presented in Section 3. Section 4 deals with the IoT reference model and the protocol stack. The state-of-the-art review on the vulnerabilities with threats and attacks taxonomy in the IoT paradigm is presented in Section 5. Security goals and a roadmap in IoT are presented in Section 6. Section 7 deals with the state-of-the-art security solution for IoT framework using ubiquitous technologies, such as BC, FC, EC, and ML. Some of the open research problems are discussed in Section 8. The last section deals with the conclusion of the article with future scope for research.

## 2. State-of-the-Art, Motivation, and Contributions of This Research

### *2.1. Trends in Literature and Motivation*

There is an ample amount of work in literature focusing on the IoT from various perspectives. Particularly, aspects such as applications, architecture, protocols, and standards are extensively covered in the literature. However, threats and attacks in IoT are comparatively less explored. The analysis from one of the world's largest databases, i.e., SCOPUS, can be used to understand the relevance of the particular aspects of IoT. If we search the number of articles in the SCOPUS database that focus on IoT architecture, IoT architecture and threats, and IoT architecture and attacks, then it can be corroborated from the search results that the threats and attacks analysis of IoT architecture is sparsely explored in the literature, which can be validated from the SCOPUS statistics seen in Figure 2. Further, there is rapid growth in the interest of the researchers towards threats and attacks analysis in the IoT architecture. This can be corroborated from the number of articles pertaining to the threats and attacks analysis in IoT architecture, which was four and zero, respectively, in 2010, and rapidly increased to 73 and 157, respectively, up to the third quarter of the year 2021 (approximately).

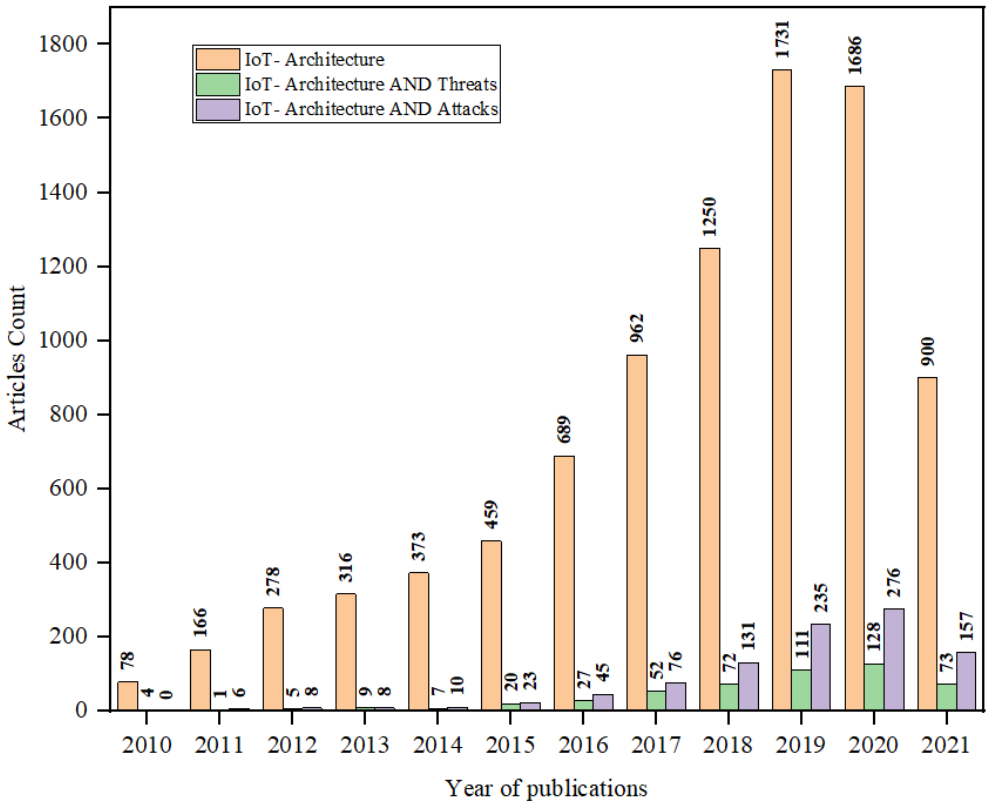



**Figure 2.** Literature statistics on IoT architecture, IoT architecture and threats, and IoT architecture and attacks.

A similar trend can be seen with respect to the protocols and standards in the IoT paradigm. The publication statistics obtained from the SCOPUS database for the articles on IoT protocols, IoT protocols and threats, and IoT protocols and attacks are shown in Figure 3. The plotted statistics reveal that the threats and attacks analysis in IoT protocols were sparsely explored in the past 10 years. Nevertheless, these aspects are gaining rapid momentum, which can be corroborated from the published articles on threats and attacks analysis in IoT protocols, which were six and five, respectively, in 2010, and have increased to 160 and 254, respectively, by the third quarter of 2021 (approximately). In a nutshell, the increasing interests of the researchers in the paradigm of IoT architecture and protocols,

which are sparsely explored from threats and attacks point-of-view, is the motivating factor for the present work.

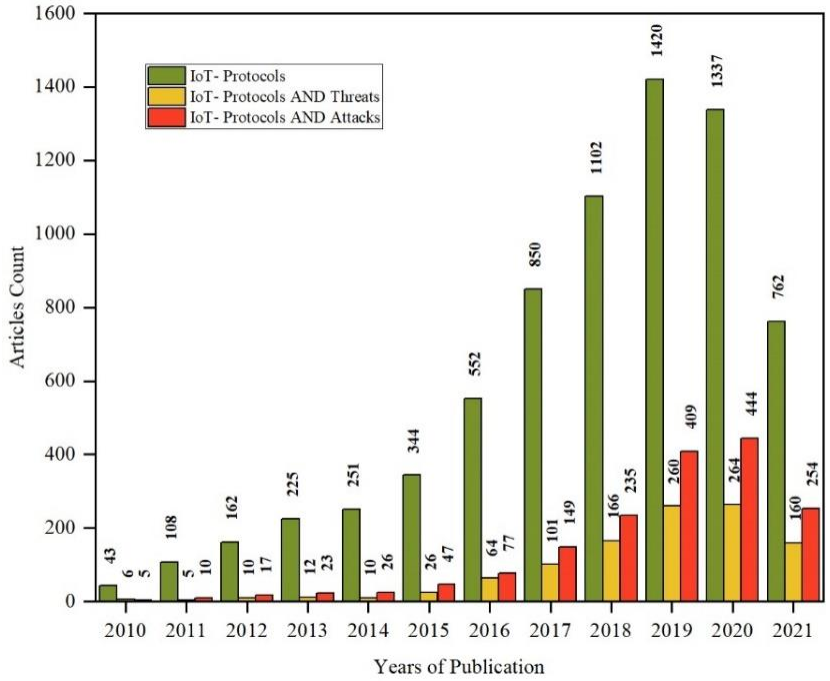



**Figure 3.** Literature statistics on IoT protocols, IoT protocols and threats, and IoT protocols and attacks.

The other motivating factor for the present work is the threats and attacks analysis and possible solutions using ubiquitous technologies, such as BC, Fog Computing (FC), Edge Computing (EC), and Machine Learning (ML). The threats and attacks analysis and possible solutions in architecture, protocols, and standards have gained significant momentum in the past few years, corroborating the upwards trend in the published articles as per the SCOPUS database statistics shown in Figure 4.

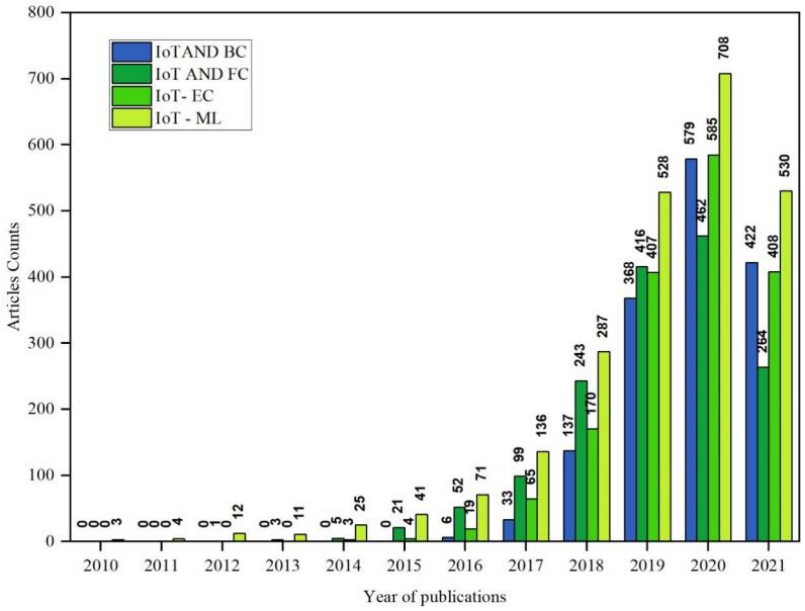



**Figure 4.** Literature statistics on IoT and BC, IoT and FC, IoT and EC, and IoT and ML from SCOPUS database.

IoT is far behind in realizing its true potential due to the lack of interoperability. The most comprehensive review on security standards and interoperability goals is presented by Lee et al. [19]. To comprehensively review the existing architectures, protocols, and standards is one of the promising means to address the interoperability issues in IoT and other challenges. If we look at the trend of the type of documents in the SCOPUS database, it can be seen that researchers are significantly contributing with Review articles (12.2%) being the third most in number behind Articles (50.8%) and Conference papers (29.1%). These statistics obtained from the SCOPUS database are shown in Figure 5. Conclusively, the present work is a review that comprehensively surveys the existing work and presents the possible solution in the context of threats and attacks pertaining to the architecture, protocols, and standards in the IoT paradigm.

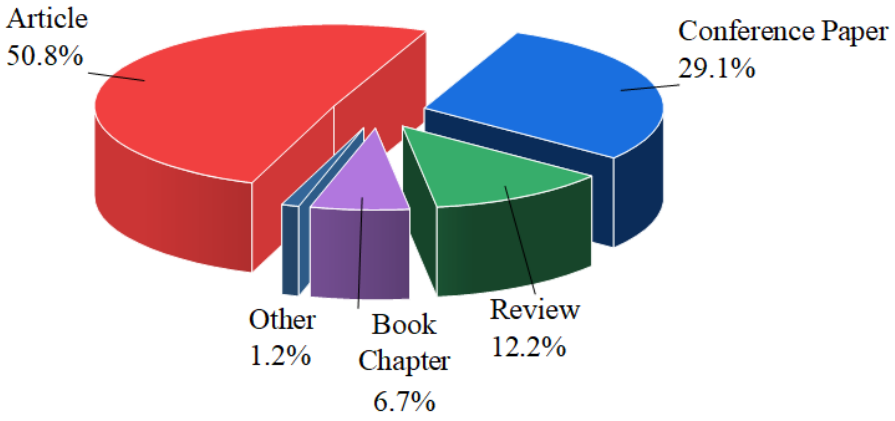



**Figure 5.** Literature trends from SCOPUS database.

### *2.2. Comparison with Existing Surveys*

Several works have surveyed IoT, its architecture, its reference model, communication protocols, etc., from the perspective of security, threats, and vulnerabilities with possible countermeasure methodologies. In this section, some of the existing surveys are discussed and compared with the present work.

Many works in the literature cover the various aspects of the threats and attacks in IoT. Authors in [20–26] cover the taxonomy of the threats and attacks pertaining to the IoT. These works mainly focus on two broad categories: the architecture of IoT and protocols/standards in IoT. Despite covering the threats and attacks taxonomy, only a few of these works present the possible countermeasures. However, none of these works present countermeasures of threats and attacks based on ubiquitous technology such as BC, FC, EC, and ML. Such ubiquitous technologies in analyzing the threats and attacks have been surveyed in scattered ways by the authors in [27–37]. A comprehensive review of all these technologies to combat IoT threats and attacks is not available.

The comprehensive survey on security and attacks with possible countermeasures solutions has been presented by Abosata et al. in [20], where authors consider the application-specific IoT architecture belonging to industrial IoT. Mann et al. in [21] presented the classification of attacks pertaining to the IoT environment. For attack classification, authors have considered a three-layer architecture comprising devices, gateway, and cloud with respect to the possible attack type. The countermeasures have also been discussed. Ogonji has comprehensively presented a threat taxonomy for the IoT environment in [22], including two broad categories: security threat and privacy threat. The authors of this survey presented taxonomy and countermeasures for the three-layer domain-specific IoT architecture. The state-of-the-art survey on intrusion detection for mitigating the impact of threats and attacks on IoT systems has been presented by Zarpelão et al. [23]. The authors proposed four attributes in the survey: intrusion detection placement strategy, detection method, security threats, and validation. A similar extensive survey by Hajiheidari et al. discusses the state-of-the-art intrusion detection system for IoT environment with a detailed

taxonomy of the attacks responsible for intrusion in IoT at various layers [24]. The seminal survey using the top-down approach on various aspects of security in the IoT environment from application-specific IoT architecture has been presented by Kouicem et al. [25]. The authors have also presented the detailed taxonomy of security solutions covering several application-specific IoT architectures, and they also proposed software-defined networking-based solutions to the security in IoT. Sun et al., in [26], focused on the physical layer of the IoT and presented a rich survey covering various security aspects of the protocols and standards, including the countermeasure methodologies. All these surveys are rich in content covering various aspects of threats and attacks in the context of IoT architectures or protocols. Despite presenting the possible countermeasures of threats and attacks, the countermeasures based on rapidly evolving technologies such as BC, FC, EC, ML, etc., have not been discussed to the authors' best knowledge. However, the concluding remarks of all these surveys identified some of the research gaps and provided a hint towards utilizing these technologies.

Elazhary [27] has presented an extensive survey on such computing technologies in the paradigm of IoT. Despite handling various aspects of IoT, particularly computation, processing, and analysis of voluminous IoT data, the security aspects of these data from the architecture point of view are not extensively covered in this survey. Taylor, P.J. et al., in [28], presents a seminal survey of using BC technology for providing the security countermeasures in IoT environment with some open challenges to incorporate other such technologies in the IoT for improving cybersecurity. BC as an infrastructure for IoT architecture with enhanced performance and security has been proposed by Memon et al. in [29]. In this survey, the authors have presented a comparative survey on cloud-based vs BC-based IoT architecture and identified some research gaps with some other similar technologies such as EC and FC. From the point of design objectives, a systematic survey on BC envisioning secure IoT infrastructure has been presented by Tran et al. in [30].

Fersi et al. developed a comprehensive survey in [31] about the scope of FC from the various aspects of the IoT, including enhanced data computing, network management, interoperability issues, security, etc. A similar review on FC from several perspectives, including threats and attacks countermeasures, has been presented by Atlam et al. [32]. Hamdan et al., in [33], comprehensively review the architecture of IoT based on EC. The survey is very rich from the architectural point of view; however, the threats and attacks analysis of such EC-based architecture is narrowly covered in this survey. Another pragmatic survey with EC-based architecture in IoT covering physical layer aspects is presented by Capra et al. in [34]. In this survey, the authors also cover the security aspects of hardware-based IoT architecture. Knowing the extraordinary effectiveness of the EC in IoT, the most seminal survey on the various simulator that can be used to validate the IoT model has been presented by Ashouri et al. in [35]. This survey is one of the best in its field, covering the EC-based simulation tools in IoT, which can even be exploited for modeling and analysis of threats and attacks in the IoT environment.

One of the most comprehensive surveys in the paradigm of ML to enable security and privacy in the IoT data ecosystem has been presented by Amiri et al. in [36]. This survey considers an ML-based approach for enhancing privacy in the IoT data ecosystem where a three-layer architecture comprising perception, network, and application layers of IoT has been considered. The authors also propose a similar approach of using BC with ML to enhance security on the IoT data ecosystem. The state-of-the-art review on the application of ML for intrusion detection in IoT environment has been presented by Adnan in [37]. The authors consider the three dominant attributes, namely, computational complexity, concept drift, and dimensionality, which are mitigated by integrating ML in IoT, envisioning the security of the IoT-based applications.

Some of the other seminal surveys in this context are summarized in Table 1.

**Table 1.** Some of the key literature surveys and research papers, and their scope.

| Reference | Scope of Threats and Attacks Analysis | | Technology Adopted for the Solution to Threats and Attacks | | | | Research Gap and Open Challenges | Year |
|---|---|---|---|---|---|---|---|---|
| | Architecture | Protocols and Standards | BC | FC | EC | ML | | |
| [38] | × | × | × | × | ✓ | × | ✓ | 2021 |
| [39] | × | × | × | × | × | × | × | 2020 |
| [40] | × | × | ✓ | × | × | × | ✓ | 2019 |
| [41] | × | ✓ | × | × | × | × | ✓ | 2015 |
| [42] | × | × | ✓ | × | × | × | ✓ | 2019 |
| [43] | ✓ | × | × | × | × | × | × | 2017 |
| [44] | ✓ | × | × | ✓ | ✓ | × | × | 2017 |
| [45] | × | ✓ | × | × | × | × | × | 2019 |
| [46] | × | × | × | × | ✓ | × | ✓ | 2021 |
| [47] | × | × | × | × | × | × | ✓ | 2020 |
| [48] | ✓ | × | ✓ | × | × | × | × | 2019 |
| [49] | ✓ | × | ✓ | × | × | × | ✓ | 2020 |
| [50] | × | × | × | × | × | × | ✓ | 2019 |
| [51] | ✓ | × | × | × | × | ✓ | ✓ | 2020 |
| [52] | ✓ | × | × | × | ✓ | × | ✓ | 2017 |
| [53] | ✓ | ✓ | × | × | × | × | ✓ | 2019 |
| [54] | × | ✓ | ✓ | × | × | × | ✓ | 2020 |
| [55] | ✓ | × | × | × | × | × | × | 2021 |
| [56] | × | ✓ | × | × | × | × | ✓ | 2017 |
| [57] | × | × | × | × | × | × | ✓ | 2019 |
| [58] | × | × | × | ✓ | ✓ | × | ✓ | 2020 |
| [59] | ✓ | × | × | ✓ | × | × | ✓ | 2020 |
| [60] | × | × | ✓ | × | × | × | ✓ | 2019 |
| [61] | × | ✓ | × | × | × | × | ✓ | 2019 |
| [62] | ✓ | × | × | × | × | ✓ | ✓ | 2019 |
| [63] | × | × | × | × | ✓ | × | ✓ | 2018 |
| [64] | × | × | × | ✓ | × | × | ✓ | 2018 |
| [65] | × | × | ✓ | × | × | ✓ | ✓ | 2018 |
| [66] | ✓ | ✓ | × | ✓ | ✓ | × | × | 2019 |
| [67] | ✓ | × | × | × | × | ✓ | × | 2020 |
| [68] | × | ✓ | ✓ | × | × | × | ✓ | 2019 |
| [69] | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | 2019 |
| [70] | ✓ | × | × | × | × | ✓ | ✓ | 2020 |
| [71] | ✓ | ✓ | × | × | × | × | × | 2018 |
| [72] | × | × | ✓ | × | × | × | ✓ | 2020 |
| [73] | ✓ | ✓ | × | × | × | × | ✓ | 2020 |
| [16] | ✓ | ✓ | × | × | × | × | ✓ | 2017 |
| [74] | × | × | × | × | × | × | ✓ | 2019 |
| [75] | × | ✓ | × | ✓ | × | × | ✓ | 2019 |
| This survey | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | NA |

These surveys are classified based on: (1) scope of threats and attacks analysis in IoT—architecture, protocols/standards, and general; and (2) possible technology adopted as a solution to the threats and attacks in IoT. The last entry of this table presents the scope of the present survey to highlight a clear comparative picture of the contributions of this survey.

### *2.3. Scope of the Present Survey and Contributions*

As discussed in the previous sections, the threats and attacks analysis in IoT is scattered and none of the surveys so far, to the best knowledge of the authors, covers the threats and attacks taxonomy covering architecture, protocols, and standards of IoT with possible countermeasures using rapidly evolving ubiquitous technologies, such as BC, FC, EC, and

ML, simultaneously. The threats and attacks were discussed in general without focusing on architecture and protocols [38–40]. Security concerns were addressed in [38] using EC and in [40] using BC. The research gaps were identified, and some open research problems were proposed in [38,40]. The analysis on threats and attacks based on protocols and standards without addressing security solutions was shown in [41]. On the other hand, [42] neither covers the architecture nor protocols for analyzing the threats and attacks. However, security countermeasures were discussed using BC with open research problems in [42]. In [43], threats and attacks were analyzed based on architecture without any security countermeasures. In [44], threats and attacks were discussed based on architectures with possible security countermeasures using FC and EC, but it does not identify the research gaps. Similar observations can be made throughout the seminal existing surveys discussed in Table 1. A comparative analysis reveals that none of these surveys analyze the threats and attacks covering all aspects, i.e., architecture as well as protocols and standards. In addition, the security countermeasures have not been discussed in any one of the existing surveys using all four ubiquitous technologies, i.e., BC, FC, EC, and ML, simultaneously. An extensive survey on threats and attacks analysis in the context of IoT, its challenges, taxonomy, and possible technological solutions covering the most important aspects of the IoT, such as architecture, protocols, and standards, is presented in this work. The vital contributions of the paper are highlighted below:

- This survey envisages providing a deeper insight into the IoT from the perspective of threats and attacks.
- An information-rich survey on various aspects of IoT, including threats and attacks from the literature, is presented.
- This survey presents a five-layer IoT architecture and seven-layer IoT architecture, along with the existing three-layer architecture.
- A comprehensive survey on the communication standards and protocols corresponding to three-layer, five-layer, and seven-layer IoT architectures is presented.
- The multidimensional taxonomy of threats and attacks in IoT is proposed with impact assessment on its architecture.
- With respect to communication standards and protocols, the threats and attacks corresponding to each of the proposed architectures, i.e., three-layer, five-layer, and seven-layer IoT architectures, are comprehensively reviewed.
- The potential use of ubiquitous technologies, such as BC, FC, EC, and ML, are presented in the context of security enhancement in IoT.
- The research gap, challenges, and some open problems are presented which can be further explored in the IoT paradigm.

## 3. Elementary Overview of an IoT System

The IoT is an evolving notion as a vast network of interconnected devices and services that store, share, and process data to dynamically adapt to the environment. IoT offers an ocean of opportunities, and so, many organizations aim to have IoT services integrated into their business processes. Before discussing the security threats, vulnerabilities, attacks, etc., it is pertinent to have a keen understanding of the layout of IoT. The emerging IoT technology typically consists of three levels of hardware which are integrated using software [76]. IoT devices, controllers, and peripherals constitute the first level of IoT, gateways and networks are associated with the second level, whereas cloud servers and control devices are part of the third level of IoT. Such a typical IoT system is depicted in Figure 6, followed by a brief discussion of each level.

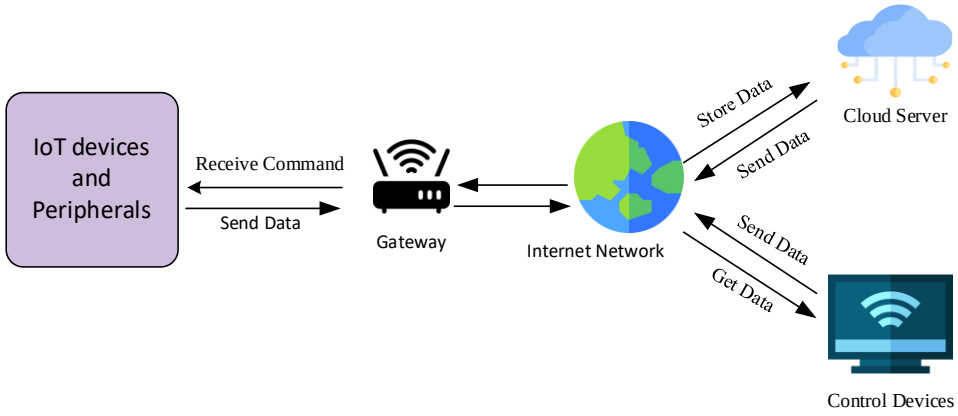



**Figure 6.** Elementary overview of an IoT system.

### *3.1. IoT Devices, Controllers, and Peripherals*

The first level consists of IoT devices, controllers, and peripherals consisting of sensors, actuators, transducers, etc. Their basic function is to capture real-time data of the outer world and convert them into information for further analysis. These devices can be connected to or implanted in any device that needs to be tracked or mounted in the environment to control the device indirectly.

The IoT devices are embedded devices capable of transmitting information across a network to improve interactions with people and with other smart objects. These smart devices make up the bottom layer of the basic IoT architecture. One of the most important features of IoT devices is their ability to use multiple sensors for different applications. Sensors in IoT gadgets are generally coordinated through the sensor hubs. A sensor hub is a single point of connection that gathers and sends data from multiple sensors to the system processing unit. Gathering data is the foremost step [77]. A sensor hub uses various transport mechanisms such as Inter-Integrated Circuit (I2C) or Serial Peripheral Interface (SPI) to transfer data between the sensors and the applications. A communication channel between sensors and applications is established by these transmitting mechanisms that accumulate sensor data through IoT devices [78].

The vulnerabilities associated with some of the sensors in the IoT paradigm are described in Table 2.

**Table 2.** A few sensor types and their vulnerabilities.

| Sensor Type | Sensor | Vulnerabilities |
|---|---|---|
| Motion Sensors | Accelerometer<br>Gyroscope<br>Linear Acceleration Sensor | Task Inference<br>False Data Injection<br>Malware Transmission |
| Environmental Sensors | Light Sensor<br>Proximity Sensor<br>Air Pressure Sensor<br>Audio Sensor<br>Temperature Sensor<br>Soil Moisture sensor<br>Noise Sensor | Eavesdropping<br>Task Inference<br>Smudge Attack<br>False Data Injection<br>Transferring Malware<br>DoS<br>Information Leakage |
| Position Sensors | GPS<br>Magnetic Sensor | Location Inference<br>Eavesdropping<br>False Data Injection |

Sensors are vulnerable to numerous security attacks and threats which might be internal or external depending upon their features [79]. To name a few, information tampering, Man-In-The-Middle Attack (MITM), Distributed Denial of Service (DDoS), jamming, etc., are some of the notable threats to the IoT sensors.

### *3.2. Gateways and Networks*

A gateway for IoT is a system or software program that connects the cloud to controller development boards, actuators, and smart devices [80]. It builds a bridge between the cloud and IoT devices. It systematically connects the field to the cloud. An IoT gateway, either a software application or a hardware appliance, is responsible for transmitting data between the cloud and IoT devices. It serves as a network router, connecting IoT devices to the cloud. It is capable of handling both inbound and outbound traffic. Inbound traffic is used for system management tasks, including upgrading device firmware, while outbound traffic is used to transfer IoT data to the cloud. The IoT gateway provides services to safely accumulate, operate, and filter data for analysis. It aids in the secure and safe transport of confederated data produced by the systems and the devices from the edge to the cloud. Ethernet, Wi-Fi, or a 4G/3G modem are used to link the IoT gateway to the cloud [81]. For data exchange and command transfer, a two-way communication channel is developed with the cloud. In an IoT environment, sensors and devices must logically communicate with other devices through the gateway or redirect the necessary data to the cloud. Some of the key functionalities of the IoT gateway are enumerated below.

- Facilitating contact with non-Internet linked or legacy devices.
- Data pre-processing, cleansing, filtering, and optimization.
- Data caching, buffering, and streaming.
- Aggregation of data.
- M2M (Machine-to-Machine) communications.
- Networking features and live data hosting.
- Data visualization and analytics.
- Security feature in data exchange.

Glancing over the number of functions and responsibilities of the IoT gateway, one can easily quote that it is essential to have a secure gateway network to carry out all the enlisted functions safely and efficiently. The gateway is prone to several different kinds of attacks which can be classified into five categories [82]:

- Physical Attack: Unauthorized access to gateway hardware or any unaccredited geographical movement.
- Software Attack: Trojan, Worms, virus, jamming, denial of services.
- Network Attack: Node capture, node subversion, node malfunctioning, message corruption, routing attacks, false node.
- Cryptanalysis Attack: Known-plaintext, Man-In-The-Middle-Attack (MITM), ciphertext only, chosen plaintext.
- Side Channel Attack: Micro probing, reverse engineering.

The state-of-the-art discussion on these attacks is comprehensively discussed later in this article.

### *3.3. Cloud Servers and Control Device*

Smart devices of the IoT are being deployed at a rapid rate. However, the amount of data they produce makes it difficult to store and process in the local platforms. The unstructured IoT data can be easily stored in a public cloud infrastructure [83]. The scalability provided by cloud computing offers a solution to this problem. Cloud computing provides flexible computing and storage tools that can be used to assist in data management. As a result, this technology can be used to analyze data generated by sensors and IoT devices. Many of the major cloud providers use object storage technology to offer low-cost, scalable storage systems. Cloud computing allows businesses to store and analyze data easily and in real time, enabling them to get the most out of their data. According to a survey conducted by Information Week [84], 65% of respondents said that "the opportunity to satisfy business demands easily" was one of the most significant factors for a company to migrate to the cloud. Since they have high-speed networks with no data ingress fees, the public cloud is an excellent place to store the vast quantities of IoT data generated by

businesses. However, the public cloud has plenty to do. Big data analysis applications that consume and process vast amounts of unstructured content have been added to the product offerings of cloud service providers. This enables companies that can potentially process data more efficiently than a private data center to build highly scalable IoT applications. Depending on the device's networking features, devices can connect to the cloud in a variety of ways. Some of these are cellular, satellite, Wi-Fi, Low Power Wide Area Networks (LPWAN) such as NB-IoT, and direct access to the Internet through Ethernet.

While the cloud has acquired universal popularity, and most IoT applications use cloud services for data storage and retrieval. However, questions about whether cloud technologies are genuinely safe and reliable are continuing to be debated. Nevertheless, cloud risks should also be addressed. The cloud is a public platform used by many people, and there could be malicious users on the cloud who pose a risk to IoT data. The cloud is vulnerable to several attacks such as SQL injection, DDoS, weak authentication, malicious applications, back doors, exploits, etc. [85]. An extensive survey on these aspects is discussed later in this survey.

## 4. IoT Reference Model and Protocol Stack

### *4.1. Three-Layer Reference Model*

The mitigation of security threats and attacks in IoT can be achieved by understanding the IoT reference model and protocol stack in-depth. There is no widely agreed-upon framework for the IoT [86]. However, different architectures have been suggested by different researchers [87]. The most basic architecture being followed widely is the three-layer reference model consisting of perception layer, network layer, and the application layer, which is illustrated in Figure 7a. The functionality of each of these layers is briefly summarized below.

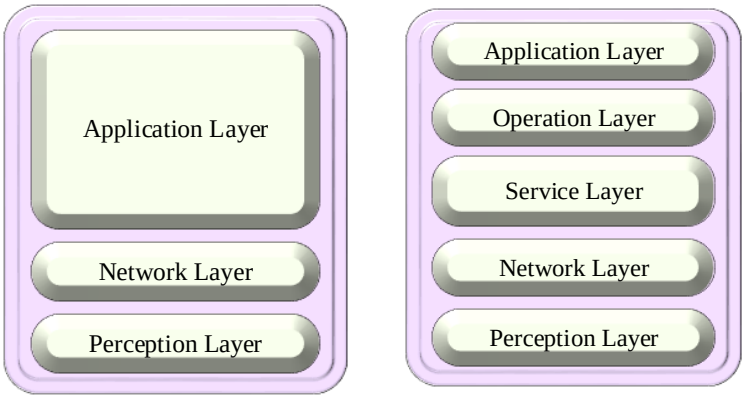
- Perception Layer: The perception layer is also often known as the physical layer. The layer deals with the various sensors affixed to the IoT devices. Sensor nodes, RFID Sensors, and other sensory technologies are provided by this layer [88]. The sensors in this layer gather data and transfer it to the network layer. Physical quantities such as temperature, humidity, light intensity, sound, etc., are measured by the sensors, which are pre-processed before they send the information to the network layer. The perception layer is primarily responsible for the data collection and its transmission to the network layer. Devices linked in short-range networks can collaborate with the help of the perception layer.
- Network Layer: The network layer is made up of network components that enable communication to take place. It facilitates the data exchanged between the IoT devices. The network layer serves as a connection between the perception layer and the application layer. It is in charge of IoT networking, which involves connecting and translating IoT devices over a network. The network layer's job is to route and relay the data obtained by the perception layer over the network. The data are sent over the Internet to other computers or IoT hubs. Wi-Fi, Bluetooth, 3G/LTE, Zigbee, Lora, and other network technologies are examples of commonly used network technologies [89].
- Application Layer: The application layer is the topmost layer of the IoT architecture, and it is responsible for accomplishing the final purpose of community service. The application layer collects data from the network layer and uses them to accomplish the ultimate objective of delivering the IoT infrastructure's intended service. The application layer is liable for offering types of assistance and decides a bunch of conventions for message passing at the application level. The application layer serves as a bridge between applications and end clients, allowing them to communicate. It defines the allocation of resources and computation in data production, processing, screening, and feature selection. The application layer is a client-driven layer that performs various tasks for the clients and offers customized assistance as per a client's pertinent requirements [90]. This IoT layer brings together the industries to create high-level intelligent application solutions such as disaster monitoring, health monitoring,

translation, fortune, medical, environmental monitoring, and global management for all intelligent applications.

### *4.2. Five-Layer Reference Model*

The architecture of IoT has been further improved by decomposing the responsibilities and functionalities of the existing three-layer architecture, resulting in a five-layer architecture [91]. A five-layer architecture consisting of a perception layer, network layer, service layer, operation layer, and application layer is proposed, which is different from that proposed by [92]. The pictorial representation of the five-layer reference model is as shown in Figure 7b. It is worthy to note that the application layer is segregated into three layers, namely, service layer, operation layer, and application layer. The functionalities of the service, operation, and application layers are briefly summarized below, whereas the perception layer and network layer hold the same responsibilities.

- Service layer: This layer envisages facilitating the use of heterogeneous IoT devices, tools, testbeds, platforms, etc., for a wide range of IoT applications. The processing of the data from the network layers is also its responsibility. Generally, the data at this layer are voluminous, for which processing, computing, and analyzing are some key challenges to be handled by this layer.
- Operation layer: This is an important layer, especially from the business point of view in IoT. The supervision of services offered by IoT, creating business models, visualization of the data, decision-making, etc., are some of the key responsibilities of this layer. Ensuring QoS across all layers is one of the vital responsibilities associated with this layer. This layer is also responsible for real-time monitoring, control, and evaluation of various application-specific parameters in an IoT environment.
- Application layer: This layer is primarily responsible for providing service to the end-users related to particular applications. There exists a wide range of applications envisaged using IoT, viz., smart city, smart home, smart agriculture, industry 4.0, healthcare, environmental monitoring, etc. This is the layer through which end users usually interact and pay for the service provided to them.




(**a**) Three-Layer Architecture. (**b**) Five-Layer Architecture.

**Figure 7.** Three-layer vs proposed five-layer architecture of IoT.

### *4.3. Seven-Layer Reference Model*

Even though the architectures of IoT are either application-specific or domain-specific, we propose a more generic IoT architecture that comprises seven layers. The seven-layer generic IoT reference model comprises a perception layer, abstraction layer, network layer, transport layer, computing layer, operation layer, and application layer. The representation of the seven-layer reference model is as shown in Figure 8. Further, the functionality of each of the layers is briefly described below.

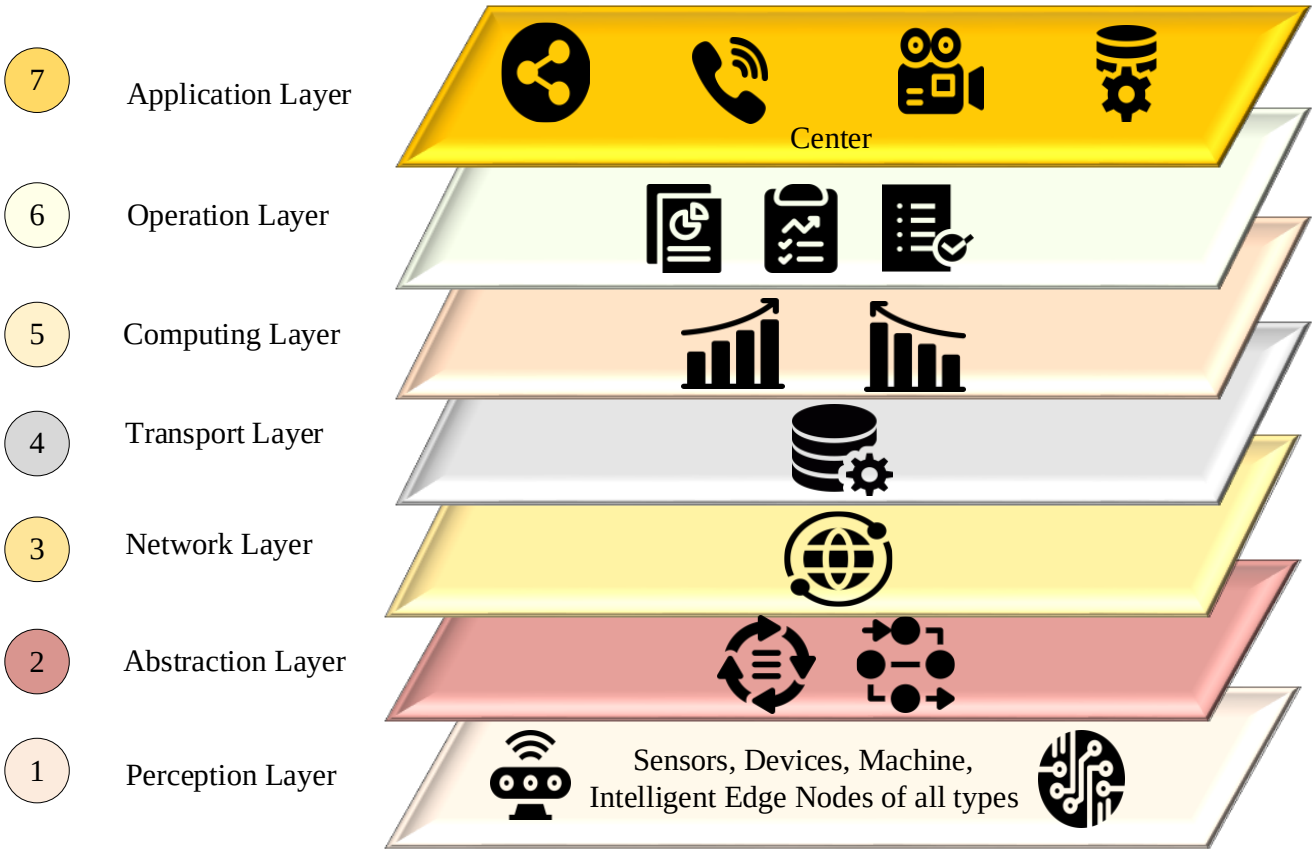



**Figure 8.** The proposed seven-layer architecture of IoT.

- Perception layer: This is the first level which consists of different IoT sensing and actuating devices such as sensors, actuators, RFID tags, controllers, etc. Being the first layer, the devices at this layer must adhere to the security protocols and standards to ensure they mitigate security threats to other layers originating from the perception layer.
- Abstraction layer: The IoT is based on a large and diverse set of items, each with specialized functionalities accessible through its dialect. Thus, this layer envisages harmonizing the potentials of other devices by providing a common language, protocol, and standard-based solutions.
- Network layer: This layer is responsible for providing various networking-related solutions to IoT devices. Routing, forwarding, security, etc., are some of the key responsibilities of this layer.
- Transport layer: This layer is responsible for transmitting the data from one service to other services within the application. The security at the transport layer is one of the key responsibilities in IoT in addition to the QoS.
- Computing layer: Voluminous data are generated and shared in IoT-based applications. The computing, processing, and analysis of such voluminous data is very cumbersome in general. Thus, this layer is associated to deal with such challenges in IoT. The integration of several burgeoning technologies such as cloud computing, big data, FC, EC, deep learning, machine learning, etc., is seen as promising at this layer for improving performance and security in IoT-based applications.
- Operation layer: This is an important layer, especially from the business point of view in IoT. The supervision of services offered by IoT, creating business models, visualization of the data, decision-making, etc., are some of the key responsibilities of this layer. Ensuring QoS in all layers is one of the vital responsibilities associated

with this layer. This layer is also responsible for real-time monitoring, control, and evaluation of various application-specific parameters in an IoT environment.

- Application layer: This layer is primarily responsible for providing service to the end-users related to particular applications. There exists a wide range of applications envisaged using IoT, viz., smart city, smart home, smart agriculture, industry 4.0, healthcare, environmental monitoring, etc. This is the layer through which end users usually interact and pay for the service provided to them.

### *4.4. IoT Protocols and Standards*

In the Internet of Things, the communication protocol is a bunch of rules set down for exchanging information between electronic gadgets. Since IoT devices are more resource-limited/dependent than traditional network devices, the protocol stack in an IoT network must be different from the traditional OSI model. IoT protocols are supposed to be small and compact. The IoT protocol stack can be considered as an augmented version of the layered TCP/IP protocol stack [93]. In recent times, many standardization efforts have been seen to reduce the efforts of all stakeholders of the burgeoning IoT, such as service providers, developers, manufacturers, programmers, operators, etc. To this extent, although there are numerous players, some of the prominent organizations involved are EPC global, the European Telecommunications Standards Institute (ETSI), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), and Institute of Electrical and Electronics Engineers (IEEE). The protocols can be broadly grouped into four categories: application protocol, service discovery protocol, connectivity and networking protocol, and other dominant protocols [94]. Some of the widely explored protocols under these categories are summarized in Table 3, whereas a detailed discussion can be found in the seminal work carried out in [41,57], of which we briefly describe some of the key protocols in the following subsections.

**Table 3.** Protocols at various layers of IoT architecture with key functionality.

| Broad Category | Dominant Protocols | | Functionality |
|---|---|---|---|
| Application protocol | CoAP, DDS, AMQP, MQTT, MQTT-SN, XMPP, HTTP REST | | Services to end-users for various applications |
| Service discovery protocol | mDNS, DNS-SD | | Domain name resolution, client pairing for service discovery |
| Connectivity and networking protocol | Routing protocol | RPL | Routing in low power lossy networks |
| | Network layer protocol | 6LoWPAN, IPv4, IPv6 | To provide networking for effective communication in IoT over the existing IPv4 and IPv6 infrastructure |
| | Data link layer protocol | IEEE 802.15.4 | To provide channel access, coordination, scheduling, and resource management tasks. |
| | Connectivity protocol | LTE-A, EPC global, IEEE 802.15.4, Z-Wave | To interconnect IoT devices at the perception layer for effective communication |
| Other dominant protocols | IEEE 1888.3, IPSec, IEEE 1905.1 | | To provide interoperability, security in an IoT environment |

- CoAP: CoAP stands for Constrained Framework Protocol. COAP is a transfer protocol similar to HTTP, but it is designed to help devices with limited resources communicate [95]. This protocol is used to communicate between low-resource IoT devices and high-resource Internet-connected devices. CoAP is a binary protocol that communicates using UDP. The semantics of CoAP are designed to be very similar to those of HTTP [96]. It has less data overhead because it is a binary protocol, and because it uses UDP, it has more flexibility in communication models and can minimize latency. One of the advantages of using HTTP semantics on top of CoAP UDP rather than HTTP TCP is that a computer can easily communicate with the cloud and other devices on the local network using the same protocol language. One of the benefits of using HTTP semantics on top of CoAP UDP rather than HTTP TCP is that a machine can communicate with the cloud and other local network devices using the same protocol language [97].
- mDNS: Multicast DNS (mDNS) is having responsibility similar to the Domain Name Space (DNS) protocol in TCP/IP. This is responsible for mapping IP addresses and names among IoT devices. Since mDNS can be used without extra configuration or memory locally, it is quite flexible with speedy response [98].
- RPL: It is an abbreviation of routing protocols for low power and noisy network (RPL). It was established to assist the creation of a robust topology across lossy lines to provide minimal routing needs [99]. The point-to-multipoint, multipoint-to-point, and point-to-point traffic models are all supported by this routing protocol [100].
- 6LoWPAN: 6LoWPAN is an abbreviated form of IPv6 over Low power Wireless Personal Area. 6LoWPAN is a low-power wireless mesh network with individual IPv6 addresses for each node [101]. This enables the node to link to the Internet directly using open standards. Data are sent as packets in the form of a wireless sensor network. The protocol is used for transporting IPv6 packet data over IEEE 802.15.4 and other networks. It offers end-to-end IPv6 access, allowing it to provide direct connectivity to a wide range of networks, including the Internet. The 6LoWPAN protocol includes a layer that aids in the adaptation of resource-constrained devices to the IP environment [102]. This allows Internet access to sensor devices. Under the low power wide area network, LoRa (Long Range) and SigFox are some of the new emerging technologies.
- IEEE 802.15.4: The IEEE 802.15.4 protocol specifies a Medium Access Control (MAC) sublayer and a physical layer (PHY) for low-rate wireless personal area networks (LR-WPAN). Some of the notable characteristics are low data rate, low cost, low power consumption, and high throughput [103]. It also provides excellent security features and can support many smart IoT devices over the networks. However, the QoS feature is not guaranteed by this protocol.
- LTE-A: It stands for Long Term Evolution- Advanced (LTE-A) and it is based on cellular communication technology. Due to the utilization of sprawling existing infrastructure, it is a cost-effective and most affordable solution for IoT. Its performance is better than some other cellular-based technology in the IoT paradigm [104].
- IEEE 1905.1: The security protocols which are best for traditional Internet-based communication seem to be inappropriate for providing security in the IoT environment. Since resource constraints are among of the prominent challenges in IoT, security protocols must be built in a way that is not resource hungry. IEEE 1905.1 is designed to solve interoperability issues in IoT. Particularly, it envisages integrating heterogenous technologies with the digital home network. Interestingly, with IEEE 1905.1 as an interoperable protocol, IEEE 802.3, IEEE 802.11, IEEE 1901, and MoCA can coexist together in an IoT environment [105].
- UDP: UDP is a connectionless protocol; here, the sender sends data without waiting for the receiver to establish a link. They are connectionless datagrams that allow for the transmission of smaller packets and cycles with less overhead and a faster wake-up time [106].

- EXI: Efficient XML Interchange is abbreviated as EXI. This is an XML representation in a small package. To support XML applications on resource-constrained devices, EXI is described as a technique that uses less bandwidth and improves encoding/decoding efficiency. EXI compression aids in the reduction of document content by creating small tags internally based on the current XML schema, processing level, and context. It assures the tags are optimized for data representation. The document is in binary format, with all of the document's data tags encoded using event codes. Event codes are binary tags that keep their value only in the EXI stream where they are allocated.

## 5. IoT Vulnerabilities, Security Threats, and Attacks

With the unprecedented growth in IoT devices with rapidly evolving technologies, the new generation IoT-based applications are at risk. Nevertheless, there is an increasing consciousness that the new age of cell phones, computers, and other gadgets might be powerless against malware and assault. Thus, the vulnerabilities, security, and attacks must be comprehensively analyzed to make envisioned IoT a reality.

### *5.1. Vulnerability*

Vulnerabilities are the defects in a framework's design or usefulness that permits the attacker to execute orders, access unapproved information, and launch distributed denial-of-service (DDoS) attack [107]. Attackers can utilize IoT gadgets with existing issues to infiltrate the networks. DNS rebinding attacks, which allow for the processing and ex-filtration of data from internal networks to new side-channel attacks, such as infrared laser inducted attacks against smart devices in homes and workplaces, are among the risks. In IoT systems, vulnerabilities can be found in several places [108].

Hardware and software systems are two central components of IoT frameworks, vulnerable to design flaws. Regardless of whether bugs are identified due to compatibility and interoperability of the equipment or efforts to remedy them, hardware flaws are very difficult to detect and even more difficult to repair. Computer bugs may exist in operating systems, programming software, and control software. Human elements and programming complexity are two factors that contribute to software configuration defects. Human flaws are normally the source of technical vulnerabilities [109]. Miscommunication between the developer and clients, lack of resources, skills, and experience, and a failure to manage and monitor the system can result from a poor understanding of the specifications introducing vulnerabilities in the IoT framework. Thus, vulnerability poses indispensable threats and attacks in the IoT environment. What follows next is the taxonomy of threats and attacks in IoT.

### *5.2. Taxonomy of Threats and Attacks in IoT*

A threat is an activity that exploits a system's security flaws and has a negative effect on it. Humans and the environment are the two main sources of security threats [110,111]. As an example, seismic tremors, typhoons, floods, and fires are all natural hazards that can cause serious damage to computer systems. Few shields can be used to protect against traumatic events since these naturally occurring events cannot be prevented. Backup and contingency planning, for example, are the best ways to protect stable infrastructures from common threats. Human threats are those that humans create, such as malicious threats that are either internal (someone has allowed access) or external (individuals or organizations operating outside the network) in nature and seek to damage or disrupt a system. Following are the different types of human threats:

- Unstructured threats: These are made up mainly of novice people who use the readily available hacking software.
- Structured threats: People aware of system vulnerabilities and can comprehend, build, and exploit code and scripts are known as structured risks.
- Advanced Persistent Threats (APT): A coordinated assault is an example of advanced persistent threats. APT is a sophisticated network attack that seeks to steal data

from high-value information in industries such as manufacturing, banking, and national defense [112].

A taxonomy of threats posing a big concern from a security perspective in the IoT environment is shown in Figure 9.

Compared to the threat that can be intentional or unintentional, the attack is always intentional and malicious to cause damage. Several security attacks persist in the IoT framework, which can be analyzed with respect to the proposed IoT reference model. A taxonomy of attacks in IoT has been presented in Figure 10. These threats and attacks pose severe challenges to the IoT environment from a security perspective. The security concern due to various threats and attacks are categorically described in the following subsections.

### *5.3. Security Concern Due to Threats and Attacks at Different Layers*

#### 5.3.1. Security Concern at Perception Layer

Since current sensor management systems and protection schemes are insufficient to protect the sensors, an attacker may use them in various ways. In general, sensor-based threats refer to passive and active malicious actions that are attempted by the manipulation of sensors for their malicious purposes. Different kinds of threats and attacks which cause serious security challenges at the perception layer are eavesdropping, battery drainages, hardware failure, malicious data injection, Sybil threat, disclosure of critical information, device compromise, node cloning, node capture, side-channel attack (SCA), tag cloning, Radio Frequency (RF) jamming, node injection, exhaustion, node outage, etc. Some of these security threats and attacks are briefly discussed below. Further, a detailed discussion on these threats and attacks is comprehensively covered in [49,57,65,67].

- Eavesdropping: Attackers can sniff the traffic generated by IoT data flow to gather users' critical information by setting similar IoT devices.
- Malicious Data Injection: False sensor data injection is a form of attack in which the sensor data used in IoT applications are forged or modified for malicious purposes. False sensor data may be injected into devices by physical access or clandestine use of different networking mediums such as Bluetooth, Wi-Fi, GPS, etc. For instance, a spoof attack in a vehicle equipped with a GPS system. To change the location of the car, the attacker sends a forged GPS signal to the system. This conceals the vehicle's true location, allowing the attacker to attack the targeted vehicle with any physical attack [113].
- Sybil Attack: The malicious nodes in this can have multiple identities of a genuine node by either impersonating it or with a fake identity through duplication. One such malicious node may have several identities simultaneously or at different instances.
- Disclosure of Critical Information: Sensors used in IoT gadgets can disclose sensitive information such as passwords, secret keys, credit card credentials, and so on. These details may be used to violate user privacy or to build a database for future attacks. One such example of this attack is eavesdropping. It is a kind of attack where a pernicious application records a discussion subtly by misusing sound sensors and extracts data from the discussion. An attacker can save the recorded discussion on a gadget or tune in to the discussion continuously. Soundcomber is one of the current instances of eavesdropping over the receiver of a cell phone. In this model, a pernicious application secretively records when a discussion is initiated from the gadget. Since the recording is carried out behind the scenes, a client is completely unaware of the chronicle [114].

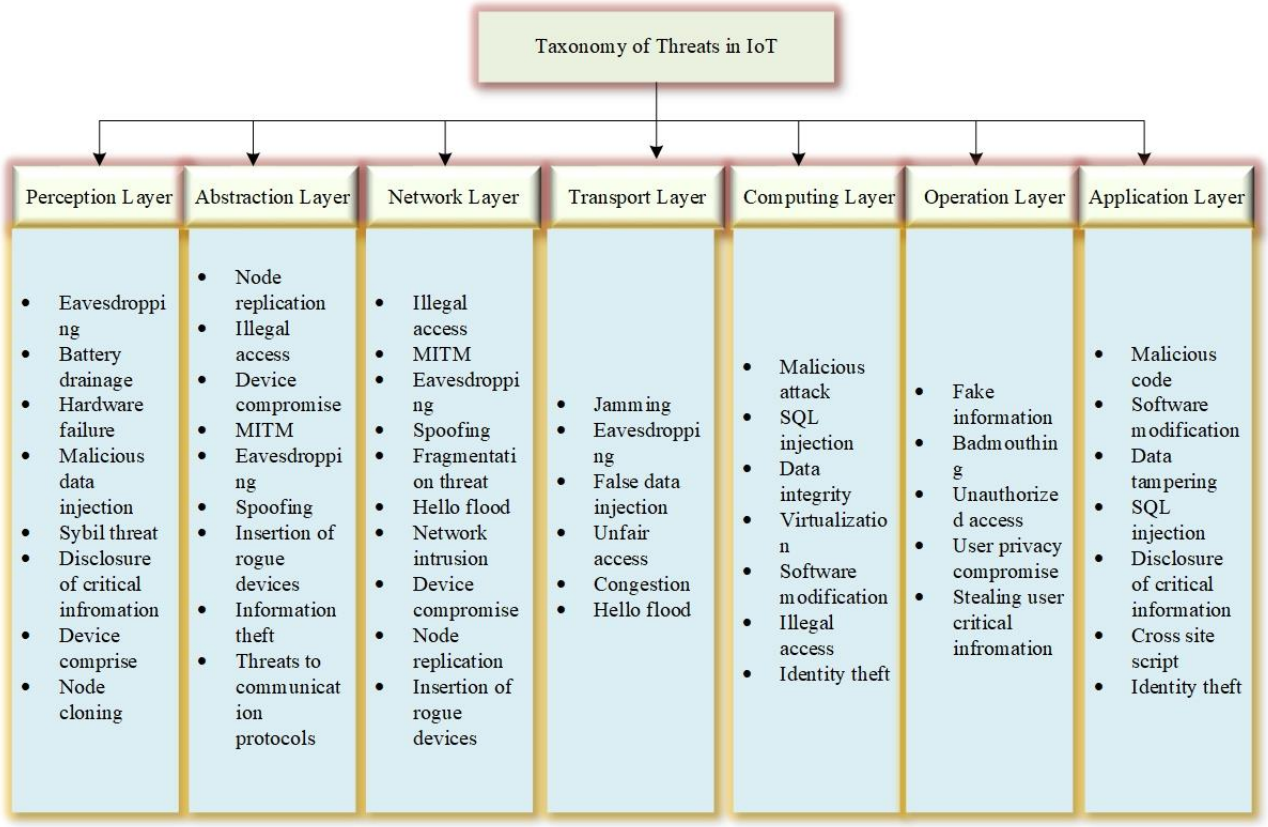



**Figure 9.** Taxonomy of threats in IoT.

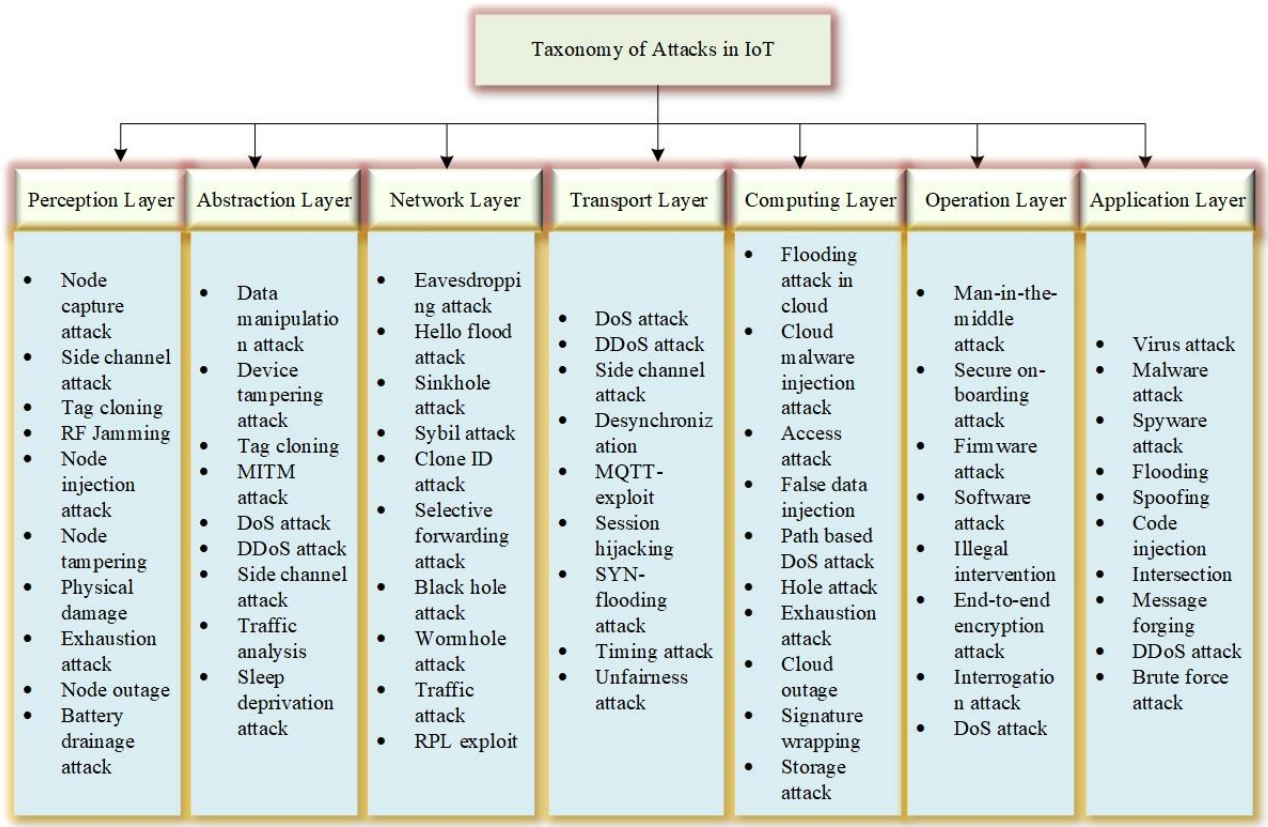



**Figure 10.** Taxonomy of attacks in IoT.

- Side-Channel Attacks: The assailant gathers information and performs the reverse engineering process to collect the encryption credentials of an IoT device while the encryption process is under way. This information cannot be collected from plaintext or ciphertext during the encryption process, but from the encryption devices. Side-channel attacks the use of certain or all data to acquire the key the device uses. Some instances of such attacks include timing attacks, power or failure analysis, and electromagnetic attacks. The opponent uses data leaks and collects block cipher keys. In the event of the attacks, an intrusion prevention system such as Boolean masking can be directed.
- Malicious Data Injection: Attackers take advantage of flaws in communication protocols to insert data into the network [115]. The intruder will tamper with the information required to control the device if the protocol does not verify the integrity of the data. The injection attack may result in code execution or system control from afar.
- Node cloning: In most cases, IoT devices such as sensor nodes and CCTV cameras are developed without hardware defects, given the lack of standardization of the IoT device design. Therefore, for unauthorized purposes, these devices can be easily forged and replicated. This is also known as the cloning of nodes. It can take place in either of the two phases, i.e., production and during operations. An internal attacker can replace an original device with an unauthorized, pre-programmed object in the former case. A node can be captured and cloned during the operational phase. Capturing nodes could further remove security parameters and substitute firmware replacement attacks.
- Exhaustion attack: Jamming or DoS attacks that have been mentioned before could lead to attacks of exhaustion. In particular, energy consumption can affect the battery-operated devices if an assailant attacks the network continuously. Repeated retransmission attempts could cause collisions with IoT MAC protocols leading to high-energy depletion. Exhaustion is a dot attack and is connected with deactivation assaults, reducing the size of the network and removing nodes permanently from the network.

#### 5.3.2. Security Concern at Abstraction Layer

Different kinds of threats and attacks which cause serious security challenges at the abstraction layer are node replication, illegal access, device compromise, MITM, eavesdropping, spoofing, insertion of rogue devices, information theft, a threat to the communication protocols, data manipulation, device tampering, tag cloning, DoS, DDoS, SCA, traffic analysis, and sleep deprivation. Some of these security threats and attacks are briefly discussed below. Further, a detailed discussion on these threats and attacks is comprehensively covered in [49,57,65,67].

- Illegal access: IoT equipment often operates without any physical protection in an untrusted environment, such as traffic light sensors, environmentally friendly sensors, agricultural sensors, smart city sensors, and much more. Problems such as illegal access and malicious change of data may arise during the processing of sensitive data.
- MITM: Man-in-the-Middle (MITM) is a system that listens in on traffic between a smart device and a gateway [116]. All traffic will be routed via the attacker's computer using the ARP poisoning technique. This attack can be avoided if the attacker is unable to see the traffic in progress. As a result, encryption is required in the protocol [117].
- Spoofing: To initiate a spoofing attack, an attacker can mimic a node. Due to its manner of assault, a spoofing attack is one of the high-risk attacks. A transmission could be recorded using a compatible portable reader. Because the attacker is impersonating the node, the retransmission may appear to be coming from a legitimate node. This threat could exist in all three layers of the IoT. Spoofing attacks that impersonate nodes are classified as authentication attacks, and they also breach the privacy principle.
- Threat to communication protocols: The fact that most current wireless communication protocols adhere to the OSI layered protocol architecture and the physical layer encryption is not reinforced with additional security methods in the upper layers of

the communication presents additional issues in IoT/CPS security design. Cellular technologies such as UMTS, GSM, and LTE, on the other hand, have their own set of security challenges. Because radio baseband stacks are implemented openly, mobile networks are vulnerable to hacking and cyber-attacks. Furthermore, aggressive attackers can use "IMSI Catching" to compromise GSM and UMTS networks.

- Tag cloning: An opponent can readily clone RFID tags by gaining direct access to a device or via reverse engineering to obtain the essential information. A tag cloning attack was described in the literature, in which an RFID scanner was unable to discriminate between legitimate and compromised tags.
- Denial-of-Service (DoS): It is a type of attack in which a device or application is maliciously denied normal operation. DoS attacks can be active attacks where an application or task is strongly denied or where passive attacks can stop another ongoing task on the device by attacking one application [118].
- DDoS: Any IoT device, network, or software program could be shut down by a distributed denial-of-service (DoS) attack, rendering the service inaccessible to its consumers. These attacks can take many different shapes. One method of attack is to generate a large amount of network traffic and send a massive request to the victim. The main goal of this attack is to make the target consumers' devices, software, network services, and resources unavailable. Furthermore, the attacker may be able to obtain sensitive information from users. DDoS attacks are more harmful than DoS attacks, which use many attacking platforms to infiltrate one or more systems
- Traffic analysis: For attackers, a network's traffic pattern may be as useful as the substance of data packets. Analyzing traffic patterns can provide valuable information about the networking topology. In WSNs, the sink nodes closer to the base station generate more transmissions than the other nodes because they relay more packets than the nodes further away. Similarly, clustering is a key scaling strategy in WSNs, and cluster heads are busier than the rest of the network's nodes. For adversaries, detection of the base station, nearby nodes, or cluster heads may be very beneficial since a denial-of-service attack or packet eavesdropping against these nodes might be very useful
- Sleep deprivation: The denial of a sleep attack on a battery-powered device will result in energy depletion. Collision attacks or repetitive handshaking, i.e., repeatedly shaking hands, can be used to carry out this attack. Request to Send (RTS) and Clear to Send (CTS) manipulate flow control signals, stopping the node from entering the stage of sleep.

#### 5.3.3. Security Concern at Network Layer

Gateways and networking systems assist in the routing and networking of data packets to their intended destinations. If the gateway communicates using wireless protocols, the attacker will use wireless attacks to link to the gateway or internal network. As a result, the attacker will be able to carry out further attacks, such as ARP poisoning, MITM, packet injection, and sniffing. Different kinds of threats and attacks which cause serious security challenges at the network layer are illegal access, MITM, eavesdropping, spoofing, fragmentation, hello flood, network intrusion, device compromise, node replication, insertion of rogue devices, sinkhole attack, Sybil attack, clone ID attack, selective forwarding attack, blackhole attack, wormhole attack, traffic attack, and RPL exploits. Some of these security threats and attacks are briefly discussed below. Further, a detailed discussion on these threats and attacks is presented in [49,57,65,67].

- Hello flood: Message flooding is amongst the biggest network layer threats. By sending multiple route establishment requests to a network or node. The nodes in the network interpret a hello message as coming from within and mark it as a communication route.
- Sinkhole: By using this approach, an attacker compromises a network's central node and overrides it in a bid to render it unavailable. An attack that uses sinkholes is

more likely to cause a major incident than a tempering attack, which involves a few affected nodes. As a result of sinkhole attacks, the whole infrastructure base could be controlled.

- Blackhole: If the malicious node experiences a Blackhole attack, it will drop all packets encountered and the entire network will be affected. Since it absorbs all routing data, it is considered a high-impact attack. By flooding malicious routing information, an intruder tries to hijack the most efficient route to a destination. Upon transmission through the malicious route, the source node continues to send packets, and the attacker drops all packets, preventing any traffic from being forwarded to the destination.
- Traffic Analysis: The attacker analyses the traffic and saves a copy for later use in this attack. As a result, the interface can be managed using the traffic that was previously communicating with the gateway. The traffic or data that have been checked are reused in a different context [119].
- Wormhole: This network attack would intercept traffic in one location and redirect it to another. As a result, it causes network congestion and efficiency problems.
- Selective forwarding: An attacker launches an SF attack by entering a network and dropping packets. Some packets are dropped casually, while others are selectively forwarded. Consequently, packet dropping can be difficult to figure out in IoT networks due to their lossy nature. As a consequence, the entire network may suffer bandwidth degradation and delay.
- RPL exploit: The IoT is made up of devices with limited resources, such as battery power, memory, and computational power. RPL is a new network layer routing protocol developed for these types of networks (routing protocol for low power and lossy networks). RPL is a lightweight routing protocol that does not contain all of the features of typical routing protocols. RPL was developed specifically for data sinks (multi-point to point communications) and has lately been adopted by the IoT. In such attacks, spiteful nodes can seek to redirect paths when data are transferred. Sinkhole attacks are a kind of routing attack in which an opponent advertises and hire a node to drive traffic [120]. Wormhole attacks can also pose a serious threat to IoT systems if associated with other attacks such as sinkhole attacks [121]. A wormhole is an out-of-band link that allows easy packet transfer between two nodes. An attacker will try to circumvent the basic security protocols in an IoT application by creating a wormhole between a compromised node and a computer on the Internet.

#### 5.3.4. Security Concern at Transport Layer

Different kinds of threats and attacks which cause serious security challenges at the transport layer are jamming, eavesdropping, false data injection, unfair access, congestion, hello flood, DoS, DDoS, SCA, desynchronization, MQTT exploit, session hijacking, SYQ-flooding, timing attack, etc. Some of these security threats and attacks are briefly discussed below. Further, a detailed discussion on these threats and attacks is comprehensively covered in [49,57,65,67].

- Desynchronization: De-synchronizing the transmissions between two nodes allows an attacker to break actual links between them. Trying to send fabricated messages to both sides of communication, such as false flag types of messages, is an example of this type of attack. By forcing them to lose their synchronization, they will lose their ability to communicate.
- Session hijacking: In session hijacking, an attacker steals the session ID and pretends to be the legitimate user to take over a user's online session. The attacker can spoof the user's session ID and do anything the authorized user can do on the network once the attacker obtains it.

5.3.5. Security Concern at Computing Layer

This part of the IoT infrastructure supports data storage and computer remote control. If cloud servers are not properly configured, they can then lead to the server and smart devices being exploited. Different kinds of threats and attacks which cause serious security challenges at the computing layer are malicious attack, SQL injection, data integrity, virtualization, software modification, illegal access, identity theft, flooding attack in cloud, cloud malware injection, access attack, false data injection, path-based DoS, hole attack, exhaustion attack, cloud outage, signature wrapping, storage attack, etc. Some of these security threats and attacks are briefly discussed below. Further, a detailed discussion on these threats and attacks is comprehensively covered in [49,57,65,67].

- Malicious Attack: As workers in the company download untrustworthy malicious software programs from the Internet, there is a good chance that the machine will be hacked. The malware would spread across the internal network, putting the whole company under its influence. The attacker would use the compromised machine to hack the IoT system connected to the network. As a result, it may result in economic loss and abasement of the company's reputation.
- SQL injection: SQL injection is a web security flaw that permits an attacker to meddle with a web application's database queries. It permits an attacker to access the information that they would not usually be able to reclaim. This may incorporate information belonging to different clients or whatever other information the application can access. An attacker may alter or erase these data, resulting in the application's content being permanently altered. In certain circumstances, an attacker can improvise a SQL injection attack to alter the basic server or other back-end foundation or carry out a distributed denial-of-service (DDoS) attack [122].
- Illegal Access: It is one of the major challenges faced by companies providing cloud services. Most enterprise proprietors are unfamiliar with cloud-based technology, which opens them to a variety of data breaks that can affect their tasks. Since cloud computing is built to be simple to use and share, it is difficult for businesses to ensure that data are only available to legal parties. On the off chance that IoT gadgets do not properly configure, the entire network will be damaged. Additionally, companies using cloud-based computing lack complete control over their networks, which requires configuring and protecting their cloud deployments on security controls provided by their cloud service providers (CSP).
- Storage Attack: It can be very difficult to detect and deal with cryptojacking. The main problem here is that hackers will slow down the activity of the device as they use the cloud storage resources, but it will continue to operate. This means it may seem that nothing is malicious and that the machines are probably just struggling with their processing capacity. Many teams in IT experience the symptoms of cryptojacking as an upgrade fault or as a sluggish Internet link, so the real issue is much longer to be resolved.
- Access Attack: Advanced persistent threat is another term for an access attack. An unauthorized individual or adversary gains access to the IoT network in this form of attack. The intruder will remain undetected in the network for an extended period. Rather than causing network harm, the ultimate goal of such a type of attack is to steal valuable information. IoT applications receive and transmit valuable data regularly, making them particularly vulnerable to such attacks.
- Software modification: An IoT device can be compromised by modifying its software or firmware by using physical or remote access to take unauthorized actions. By patching or substituting code, or by making code extensions, the vulnerability can be exploited further.

5.3.6. Security Concern at Operation Layer

Different kinds of threats and attacks which cause serious security challenges at the operation layer are fake information, badmouthing, unauthorized access, users' privacy

compromise, stealing users' critical information, MITM, secure on-boarding, firmware attack, software attack, illegal intervention, end-to-end encryption attack, interrogation attack, DoS, etc. Some of these security threats and attacks are briefly discussed below. Further, a detailed discussion on these threats and attacks is comprehensively covered in [49,57,65,67].

- Illegal Intervention: Cloud services are typically provided, monitored, and managed through APIs and software user interfaces. Although, cloud service providers are engaged diligently to improve APIs and interfaces, this boom has additionally extended safety dangers related to them. Cloud specialist organizations utilize a particular structure to give APIs to developers, making their frameworks more endangered against an attacker. In 2018, the social media platform Facebook suffered a security breach that affected around 50 million users due to a flaw [123]. API flaws, particularly when linked to user interfaces, may provide the attacker a direct path to steal employee or client credentials.
- **Unauthorized Access:** Access control is an approval system that permits authentic clients to acquire information. Multi-client access and simultaneous altering of design systems ought to be vigorous against multi-client access. When numerous clients can alter the designs of different segments of the IoT frameworks, simultaneous execution of setup changes and simultaneous altering of arrangement records effectively leads to temperamental framework status. In IoT applications, access control is important because if access is compromised, the entire IoT framework becomes susceptible to attacks.

#### 5.3.7. Security Concern at Application Layer

The application layer manages the services offered to the clients. This layer serves applications such as telehealth, industrial automation, smart metering, and so on. This layer has its own set of security concerns that are unique to each program. Different kinds of threats and attacks which cause serious security challenges at the application layer are malicious code, software modification, data tampering, SQL injection, disclosure of critical information, cross-site script, identity theft, virus attack, malware attack, spyware attack, flooding, spoofing, code injection, intersection, message forging, DDoS attack, brute force attack, etc. Some of these security threats and attacks are briefly discussed below. Further, a detailed discussion on these threats and attacks is comprehensively covered in [49,57,65,67].

- Malicious code: Malicious codes or targeted malware can easily exploit the vulnerabilities of IoT devices through the Internet, which allows hackers to compromise those devices. Further attacks can be launched on other endpoints/networking apps via the infected devices.
- Software Modification: Minor changes can lead to more complicated problems. Unexpected environment changes along with minor framework alterations and system changes may have unanticipated consequences. As the arrangement of framework develops, these results can spread to more concerning issues. If the programming mechanism is not secured, the attacker will be able to reprogram IoT devices remotely. This could result in the IoT network being hacked.
- Data tampering: During an attack of this type, the information on the end device is misrepresented by an attacker. Invaders retrieve data format and type, then insert tamper detection measures and recreate the original data. Due to this, there is considerable doubt about the precision of data collected over the network.
- Cross-site script: XSS (cross-site script) is a technique attackers use to insert malicious code into a website that is otherwise trusted. If an XSS attack is successful, the IoT system will be under the complete influence of the attacker.
- Identity Thefts: IoT systems deal with plenty of personal and sensitive information. Clients will hesitate to enlist their personal information on IoT applications if these applications are helpless against information burglary. Some of the protocols and

methodologies used to protect IoT applications from information burglary include data isolation, data encryption, privacy management, user and network authentication, etc.

- Virus attack: The objective of these attacks is to breach the confidentiality of the system. The risk of these attacks is significantly higher for smartphones, sinks, or gateways in IoT networks. Hence, IoT applications must seriously consider mitigating viruses and malware.
- Spyware attack: Installed on IoT devices without consent, spyware is an installation program that collects information. Using this type of attack, attackers are looking to gather sensitive information about users by monitoring their behavior. Signature, behavior, and specification-based techniques are some common approaches to spyware detection.
- Code Injection: Attackers usually use the simplest or easiest way to break into a device or network. If the device is endangered to spiteful scripts and misdirection as a result of inadequate code tests, it will be the first point of entry for an attacker.
- Intersection: System integrity is a critical feature of the IoT framework. When a system's integrity is compromised, there is a high risk of safety and security threats. High activity stress or irregular process conditions, network or device failures, multiple warnings, executing previously unexecuted error path code or system recovery code, or wrongly executed commands do not cause the system to crash. This necessitates extensive research.
- Brute force attack: A brute force attack involves systematically trying and guessing every possible passphrase or password combination to gain access to the system. Crypto-analysts are ultimately able to identify the correct one which allows them access to the system.

To summarize, the different threats and attacks are reported in Table 4, along with their scope in IoT architecture and protocols, their impact, and references focusing on different detection, prevention, and mitigation strategies. With reference to this table, the following abbreviations are used: PL—Perception Layer, AbsL—Abstraction Layer, NL—Network Layer, TL—Transport Layer, CL—Computing Layer, OL—Operation Layer, AL—Application Layer, AP—Application Protocols, SDP—Service Discovery Protocols, RP—Routing Protocols, NLP—Network Layer Protocols, DLLP—Data Link Layer Protocols, CP—Connectivity Protocols, ODP—Other Dominant Protocols.

**Table 4.** The scope and panoramic view of threats and attacks with detection, prevention, or mitigation strategies in IoT architecture.

| Threats/Attacks | Scope on Different Layers in IoT Architecture | Scope on Different Protocols and Standards of IoT | Impact | References Focusing Detection, Prevention, or Mitigation Strategies |
|---|---|---|---|---|
| Eavesdropping | PL, AbsL, NL, TL | AP, SDP, RP, NLP, DLLP, CP, ODP | Affect user's privacy and confidentiality | [124,125] |
| Battery drainage | PL | CP | Drain the batters of IoT devices at a much faster rate | [126] |
| Hardware failure | PL | NLP, CP | Affect the service due to failure causing unreliability | [127,128] |
| Malicious data injection | PL, | AP, SDP, ODP | Can harm applications services | [129] |
| Sybil threat | PL, NL | SDP, CP | Enhances packet drop probability | [130,131] |
| Disclosure of critical information | PL, AL | AP, SDP, | Affect user's privacy | [132] |
| Node cloning | PL | SDP, DLLP, NP, CP | Can copy the functions, data, etc., of a particular node or even capture a node | [133,134] |

**Table 4.** *Cont.*

| Threats/Attacks | Scope on Different Layers in IoT Architecture | Scope on Different Protocols and Standards of IoT | Impact | References Focusing Detection, Prevention, or Mitigation Strategies |
|---|---|---|---|---|
| Side-channel attack | PL, AbsL | SDP, RP | Indirect attack on node leaking sensitive information | [135] |
| RF jamming | PL, TL | CP | Cause interreference, and DoS | [136,137] |
| Physical damage | PL | CP, DLLP | Affect service of a node | [127] |
| Exhaustion attack | PL, CL | SDP, NLP, DLLP, CP | Affect network lifetime | [138] |
| Node outage | PL | SDP, CP | Causing unreliability | [126] |
| Node replication | AbsL | ODP, SDP, NLP | Injecting huge traffic flow | [139] |
| Illegal access | AbsL, NL, CL, OL | AP, SDP | Can steal user's confidential·data | [126] |
| Device compromise | AbsL, NL | AP, SDP, RP, NLP, DLLP, CP, ODP | Affect credibility of device | [140] |
| MITM | AbsL, NL, OL | AP, SDP, RP, NLP, DLLP, CP, ODP | Affect network resources and authenticity | [141] |
| Spoofing | AbsL, NL, AL | AP, SDP, RP, NLP, DLLP, CP | Affect trust and confidentiality | [142] |
| Threats to communication protocols | AbsL | CP, NLP, DLLP | Affect connectivity | [143] |
| Tag cloning | AbsL | SDP, RP | Affect authenticity | [144] |
| DoS | AbsL, TL, OL | AP, SDP, RP, NLP | Affect service availability resulting in huge losses | [145] |
| DDoS | AbsL, TL, AL | AP, SDP, RP, NLP | Affect reliability, and availability | [146] |
| Traffic analysis | AbsL, NL | NLP | Affect user's privacy and confidentiality | [124] |
| Sleep deprivation attack | AbsL | SDP, DLLP | Affect the network lifetime | [147] |
| Fragmentation threat | NL | NLP, RP | Affect data integrity | [148] |
| Hello flood | NL | NLP, RP | Creates unnecessary traffic in the system | [149] |
| Network intrusion | NL | NLP, RP, CP | Affect the network resources | [79] |
| Insertion of rogue devices | NL | NLP, RP, ODP, CP | Affect network security and data integrity | [150] |
| Sinkhole | NL | NLP, RP | Result in network failure | [151] |
| Clone ID attack | NL | NLP, RP | Results in other network attacks | [152] |
| Selective forwarding attack | NL | NLP, RP, DLLP | Affect data integrity | [153] |
| Blackhole attack | NL | NLP, RP | Affect entire network | [154] |
| Wormhole attack | NL | SDP, RP, NLP, DLLP, CP, ODP | Affect entire network | [155,156] |
| RPL exploit | NL | RP | Affect routing of packets | [157,158] |
| False data injection | TL, CL | DLLP, CP | Affect the legitimate information | [129] |
| Unfair access | TL | AP, SDP, RP, NLP, DLLP, CP, ODP | Affect the performance | [145] |
| Congestion | TL | AP, ODP | Can cause more packet drop and latency | [126] |
| Desynchronization | TL | SDP, RP, NLP, DLLP | Affect data integrity | [159] |
| MQTT-exploit | TL | AP | Affect transmission of packets | [160] |
| Session hijacking | TL | SDP, RP, NLP, DLLP, CP | Exploitation and tampering with the legitimate session | [161] |

**Table 4.** *Cont.*

| Threats/Attacks | Scope on Different Layers in IoT Architecture | Scope on Different Protocols and Standards of IoT | Impact | References Focusing Detection, Prevention, or Mitigation Strategies |
|---|---|---|---|---|
| SYN-flooding | TL | SDP, RP, NLP | Affect node resources such as energy and memory | [162] |
| Timing attack | TL | SDP, RP, CP | Leads to SCA | [163] |
| SQL injection | CL, AL | AP, SDR, ODP | Affect SQL database | [164] |
| Data integrity | CL | AP | Affect credibility of data | [141] |
| Virtualization | CL | AP, SDP, ODP | Affect data protection | [165] |
| Software modification | CL | AP, SDP, ODP | Affect entire application resources | [166] |
| Identity theft | CL | AP, SDP | Affect user's privacy, and data confidentiality | [167] |
| Access attack | CL | AP, SDP, RP, NLP, DLLP, CP, ODP | Can steal valuable data from the network | [126] |
| Cloud outage | CL | AP, SDP, RP, NLP, DLLP, CP, ODP | Affect cloud-related services | [166] |
| Signature wrapping | CL | AP, SDP | Affect signature algorithm resulting in eavesdropping attack | [168] |
| Storage attack | CL | AP, SDP, NLP | Affect the data storage | [166] |
| Path-based DoS attack | CL | RP, NLP | Affect application layer similar to DoS | [169] |
| Badmouthing | OL | AP, ODP | Affect the credibility | [126] |
| Unauthorized access | OL | AP, SDP, CP | Can result in stealing of critical information | [167] |
| User privacy compromise | OL | AP | Affect the privacy of users | [167] |
| Secure on-boarding attack | OL | AP, SDP, NLP, DLLP, CP | Can cause eavesdropping during on-boarding of new devices | [170] |
| Firmware attack | OL | AP, SDP, RP, NLP, DLLP, CP | Affect low-level control software of IoT | [171] |
| Software attack | OL | AP, CP | Affect software of IoT | [171] |
| End-to-end encryption attack | OL | AP | Affect privacy and integrity of the end-users | [172] |
| Interrogation attack | OL | AP, SDP, RP, NLP, DLLP, CP, ODP | Affect the channel resources | [173] |
| Malicious code | AL | AP | Can cause illegitimate access to the IoT resources | [174] |
| Virus attack | AL | AP | Affect high-end IoT devices | [175,176] |
| Malware attack | AL | AP, SDP | Affect high-end IoT devices causing user's security concern | [175,176] |
| Spyware attack | AL | AP, SDP | Indirect harm to users | [177] |
| Intersection | AL | AP, SDP | Affect privacy | [178] |
| Message forging | AL | AP | Can steal critical information | [179] |
| Brute force attack | AL | AP, SDP, ODP | Affect the user's privacy and can steal critical login information | [174] |

## 6. Security Goals and Roadmap in IoT

There are certain security objectives that IoT must essentially meet to provide undisputed services. For smooth functioning, IoT applications require secure connections with proper authentication mechanisms and data confidentiality. To ensure information security, one needs to implement the CIA triad—data Confidentiality, Integrity, and Availability.

Threats and violations in any of these areas can result in substantial damage to the system, compromise its integrity, and disrupt its activity. To be efficient in implementing effective IoT security, the following primary security objectives must be considered. These security objectives can be achieved with effective methodologies for detection, prevention, and mitigation of threats and attacks pertaining to the IoT ecosystem, described in the next section.

- Confidentiality: Confidentiality is an important security feature in the Internet of Things, but it is not always required, for example, in cases where data are exchanged with the public. In the vast majority of situations and cases, sensitive data must not be disclosed or read by unauthorized persons [180]. Sensitive information about patient data, company information, and possibly military information, as well as security accreditations, should all be kept private from unauthorized users. Confidentiality should be granted such that the information gathered or distributed is safe and only accessible to approved users. Data collected by a computer or a sensor should not be sent to other devices unless they are properly encrypted. To prevent malicious actors from accessing the collected data, only encrypted messages should be sent to neighboring devices. A data encryption system transforms each bit of data into ciphertext, followed by a two-step verification process in which two devices/components permit access only if the authentication test is passed by both the devices, and a biometric verification in which the user is uniquely identifiable and biometric authentication in which the person can be identified by his or her fingerprints.
- Integrity: Integrity should be offered to ensure data validity. Data integrity is critical since data recipients must be able to verify whether data obtained from other devices are authentic. In most cases, integrity is a necessary security property for IoT users to receive reliable services [181]. Different IoT systems have different levels of trustworthiness. As an example, because of data sensitivities, a patient observation framework would have high trustworthiness testing against arbitrary mistakes. It is integrated into the network to protect cybercrimes data in the communication process so that data manipulation cannot be carried out without the danger detected by the device. Two error detection methods are used to ensure data integrity in the inspection and cyclic redundancy search. For continuous data sync for backup purposes, a version control system is used.
- Authentication and authorization: Authenticity is related to credibility, and it means that each system in the network should be able to recognize and authenticate other devices. Since the IoT is made up of so many devices, it is critical to be able to recognize them; otherwise, malicious devices might use spoofing to target IoT networks. Due to the design of IoT settings, the possible communication between the device and device (M2M) is exacerbated by the problem of authentication in IoT connectivity. Different authentication criteria in different systems require different solutions. Some solutions, such as bank card or bank device authentication, require a high level of reliability. However, others will need to be foreign, such as e-Passport, while others will need to be local. Only approved entities (any authenticated entity) can conduct such network operations using the authorization property [182].
- Availability: The primary aim of every IoT protection system is to make data available to users promptly. The consumer should be able to obtain data from the resources right away, not only in usual circumstances but also in emergencies. Firewalls are installed in the network to protect against attacks on services such as denial-of-service attacks, which prevent data from reaching the end-user [183].
- Accountability: Accountability provides redundancy and responsibility for some activities, tasks, and the preparation of the execution of network security policies while designing security strategies to be used in a safe network [184]. Accountability cannot prevent attacks on its own, but it does help ensure that other security measures are functioning properly. Integrity and confidentiality, for example, can be rendered worthless if they are not subjected to transparency. Often, in a disapproved event, an

entity's behavior can also be traced through an accountability system, which can help determine the inside story of what occurred and who was ultimately responsible.

## 7. Scope of Security Enhancements in IoT with Burgeoning Technologies

Now, we review the state-of-the-art methodology to enhance security and privacy in an IoT environment using a few of the ubiquitous technologies such as BC, FC, EC, and ML. Despite some other technologies such as cloud computing, Big Data, embedded system, digital twin, etc., the trend in the literature unanimously shows that BC, FC, EC, and ML have huge potential to answer the security concern in the IoT ecosystem. Further, these technologies are indispensable for the IoT ecosystem, which motivates researchers to address the security concern based on these ubiquitous technologies.

### *7.1. BC for IoT*

BC technology is a network of peer-to-peer nodes that stores transactional records, known as blocks; these blocks consisting of numerous public databases are known as the "chain". The fundamental principle of BC is based on a distributed ledger. IoT devices collect real-time data from sensors, and BC ensures the security of data by deploying a decentralized, distributed, and shared ledger [185]. Any transaction in this ledger is signed with the owner's digital signature, which verifies the transaction and protects it from tampering. As a result, the data in the digital ledger are extremely stable. The BC entries are both chronological and time-stamped. In the ledger, each entry is linked to the previous entry by applying cryptographic hash keys. Individual transactions are stored in a Merkle tree, and the tree's root hash is stored in the BC. Individual transactions are represented by T1, T2, T3, and Tn in the diagram. The cryptographically hashed transactions are stored on the leaf node represented as H1, H2, H3, and so on. The hashes of the child nodes are combined to create a new root hash. The BC stores the final root hash (i.e., Ha and Hb). It can be confirmed whether the transactions associated with the root hash are secure or not, by just verifying the root node. If a single transaction is modified, all hash values on that side of the tree will be affected. The miners verify all the transactions and then a key is produced that allows the most recent transaction to be included in the ledger. This procedure renders the most recent transaction available to all network nodes. It is very difficult and time-consuming for the attackers to hack the blocks as each block is secured using cryptographic hash keys [186]. The miners are only mining to gain their bonuses and have no personal stake in the transactions. The identity of the transaction's owners is unknown to the miners. Furthermore, several miners are working on the same collection of transactions, and they are in fierce competition to link the transactions to the BC. These characteristics enable the BC to serve as a safe, distributed, tamper-proof, and open data system for IoT data. The entire process of a transaction from its inception to its commitment to the distributed chain is elucidated in Figure 11.

In academia and industry, various platforms and frameworks are being built to support the development and maintenance of BC. Ethereum, Hyperledger Cloth, Ripple, and other platforms are examples of this kind [187]. Nevertheless, the simplified general architecture of the BC is as shown in Figure 12.

The following are the key characteristics of the BC that can be exploited to enhance security and privacy in IoT.

- To create blocks, a consensus algorithm is used; involved individuals (typically miners) verify the transactions' coherence and validity.
- A monetary competition exists for block certification and the computation of a new branch, which is based on algorithms such as Proof of Work (PoW) or Proof of Stake (PoS).
- There is no third party to rely on; each individual produces his or her own keys.
- All ledger elements, such as blocks, and transactions are stored in the database.

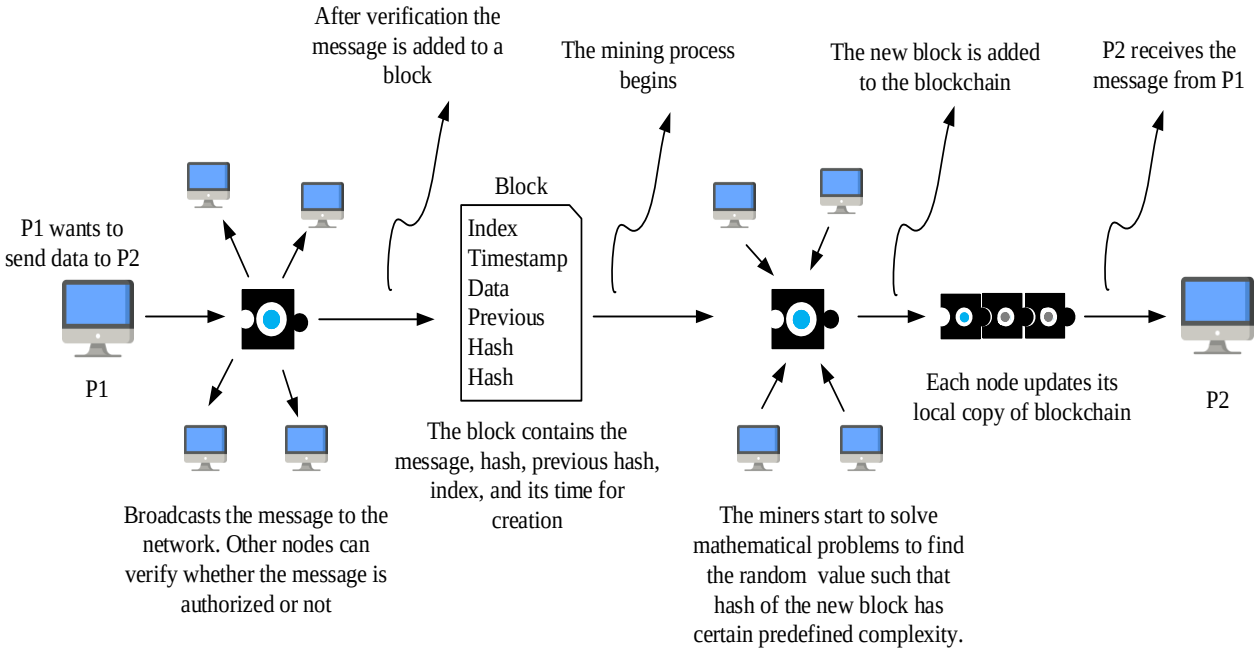



**Figure 11.** Basics of BC for enhancing security and privacy in IoT.

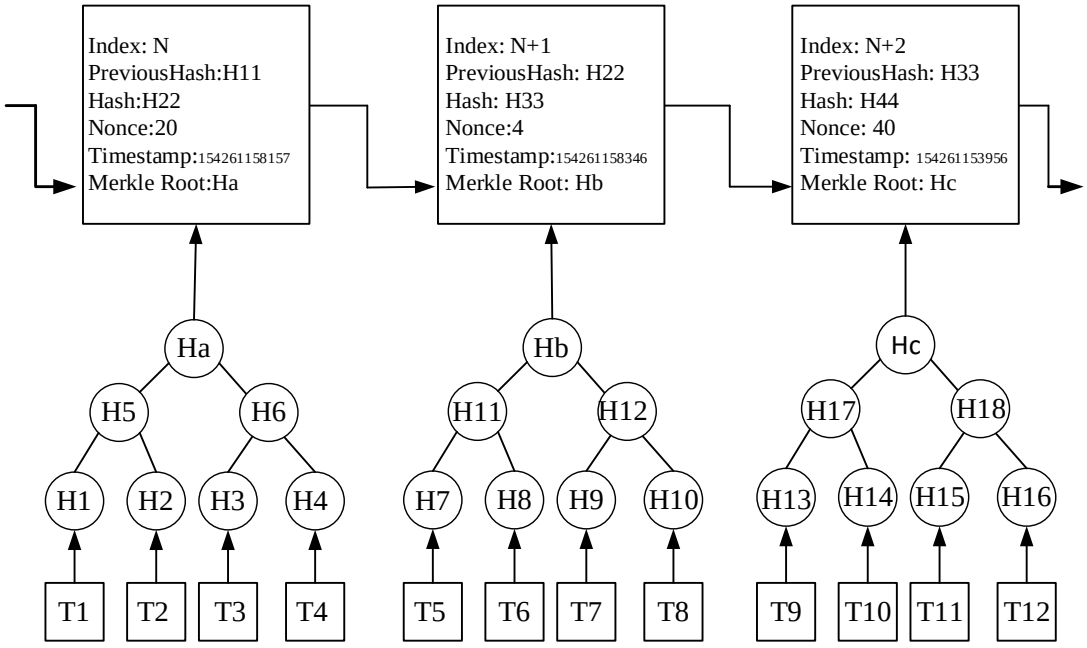



**Figure 12.** The architecture of BC.

The use of BC in IoT applications has several benefits. The followings are a summary of the main advantages of using BC in IoT applications.

- BC can be used to store the data from IoT devices: The IoT technologies incorporate a wide range of devices that are all interconnected. This arrangement is additionally associated with the cloud to empower IoT applications to be accessed from anywhere. BC is a promising method for storing and protecting such an enormous amount of data. BC is an apt solution for storing and transmitting data regardless of the layer in an IoT application.
- Terminating the centralized cloud server system: BC boosts the security of IoT frameworks by removing the centralized cloud server and establishing a peer-to-peer net-

work framework. Data pirates are mostly interested in centralized cloud servers. BC enables the distribution of data across all the nodes of the network and encrypts them.

- Forestalling illegal access: Several IoT applications necessitate a lot of contact between different nodes on a regular basis. Since BC communication is based on public and private keys, data can only be accessed by the intended party or node. If an unintended person accesses the data, the content will be nonsensical because it is protected with keys. As a result, the BC data system attempts to address a variety of security problems that IoT applications face.
- A solution for resource-constrained devices: Because of the limited resources, IoT devices are unable to store large ledgers. There have been different works toward this path to work with the assistance of BC. One of the potential solutions for IoT devices to use BC is proxy-based architecture. By setting up the proxy servers, the data can be stored in an encrypted format and the encrypted resources can be downloaded via proxy servers.
- Forestalling spoofing attack: Spoofing is a type of attack where a foreign node enters the IoT ecosystem and tries to emulate the existing nodes to be seen as a member of the original framework. This foreign node can monitor or inject malicious data into the network. The BC technology appears to be a potential solution for preventing such attacks. Each genuine client or gadget is enlisted on BC, and gadgets can undoubtedly recognize and validate each other.
- Forestalling data loss: IoT devices acquire the danger of losing information. There is a possibility that the data are lost by the sender and the recipient due to natural environmental causes. The utilization of BC can forestall such losses as it is impossible to eliminate a block once it is included in the chain.

### *7.2. FC for IoT*

The Internet infrastructure is being challenged by an unprecedented amount of data generated by IoT. The integration of IoT and the cloud has led to the development of numerous new possibilities on how to process, store, manage, and secure data. These benefits do not fully address all of the problems associated with the IoT. Cloud computing and FC complement each other rather than replace each other [188].

Computing in the fog enables processing, storage, and intelligence control to come within the proximity of the data devices. It uses two frameworks, namely Fog-Device Framework and Fog Cloud Framework [189]. With the Fog-Devices framework, different services can be delivered to a user without involving any cloud servers. Whereas the simple decisions in the Fog-Cloud-Device framework occur at the fog layer, the complex ones occur at the cloud level [190]. The architecture of the Fog-Cloud-Device framework is shown in Figure 13.

The convenience and flexibility of this structure make it possible to offer cloud computing at the network edge. The result is a reduction in distance and improved efficiency while decreasing the amount of data required to be transported into the cloud for processing, analysis, and storage. Comparing the FC with cloud-only models, data traffic between the cloud and network edge is reduced by 90%, and response times for users are cut by 20% [191]. This flexible structure extends cloud computing services to the edge of the network. Thus, it reduces the distance across the network, improves efficiency, and decreases the amount of data needed to transport to the cloud for processing, analysis, and storage.

Using fog technology, data are collected at nodes referred to as fog nodes, and the nodes can process 40 percent [192]. It reduces the latency of IoT devices by offloading traffic from the core network. According to its time sensitivity, data are directed to the cloud, fog, or aggregation nodes. By providing cryptographic computations to IoT applications, fog nodes help secure communication [193].

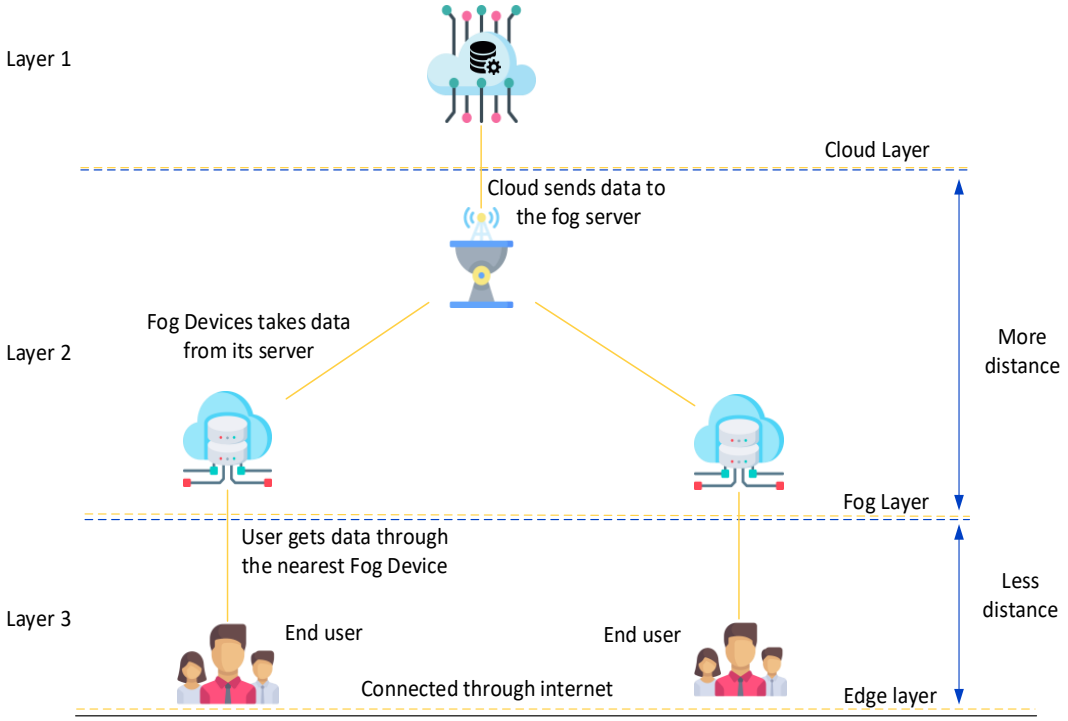



**Figure 13.** An elementary overview of FC.

FC can provide some solutions to counteract certain security threats and attacks as discussed in the earlier section. More details are provided below to demonstrate how FC can counteract these threats.

- Incident response services: Some critical applications cannot be stopped completely to resolve malware issues. When the system is running, fog nodes can help with such resolutions. It is possible to program fog nodes to provide incident response services in real time. As soon as the fog nodes detect suspicious data or requests, they can generate a warning flag for the end-user or the IoT system. Using FC, malware can be detected and problems resolved in transit. Some of the real-time services include identity recognition, intrusion detection, access management, etc.
- Resource-constraint issues: IoT devices are typically resource-constrained, which makes them an ideal target for attackers. By damaging edge devices, attackers try to exploit weak points and worm their way in. Fog nodes can support edge devices so those devices will not be attacked. For protection, fog nodes can provide more sophisticated security functions, as well.
- Eavesdropping: Rather than routing the information throughout the network, usage of fog nodes enables communication with only the end-user and fog nodes. Because the network traffic is reduced, there is less opportunity for adversaries to eavesdrop.
- Data transit attacks: Data management and storage are much more efficient when using secure fog nodes instead of IoT devices. Fog nodes provide a greater level of protection for data than end-user devices for storing data.
- Man-in-the-middle attack: A fog serves as a layer of security between the cloud and the end-user. A fog layer stands in between all threats or attacks on IoT systems, and in this layer, unusual activity can be identified and mitigated before it reaches the system.

### *7.3. EC for IoT*

Both FC and EC share similar responsibilities, such as reducing latency, reducing the volume of the data sent to the cloud, enhancing computational efficacy, incorporating heterogeneity, etc., with a common objective to bring intelligence and computing possibly

as close as to the data source. However, they are not the same. They differ in the way they operate and handle the data. For example, usually, FC takes place on the devices to which sensors are connected, such as switches, routers, gateways, access points, etc. On the other hand, EC takes place at the sensors themselves or devices which are at a one-hop distance from the sensor. Thus, the FC nodes are at more distance than the EC nodes.

Contrary to the EC, the data are transmitted from sensors to the FC nodes for processing and then sent back to the edge nodes for appropriate actions. Nevertheless, EC and FC are widely used by many companies as an extension of cloud computing. The main difference between cloud, fog, and edge stems from the location where intelligence and power computation are conducted. In the cloud, more data are processed, and users are comparatively located at a greater distance, requiring a much higher level of data processing [194]. EC uses a small edge server to overcome the problems associated with cloud computing, placed between the user and the cloud.

Figure 14 shows the EC architecture's device components, which include edge devices, fog nodes, and cloud data centers [195]. The processing power and analytical capability are provided at the edge itself in an EC framework. An application comprises devices that communicate among themselves and collaborate to calculate data [196]. The IoT application can then minimize the amount of data sent to the outside, whether to cloud or fog nodes, and this will improve the application's security.EC reduces communication costs, as all the data do not have to be moved to the cloud.

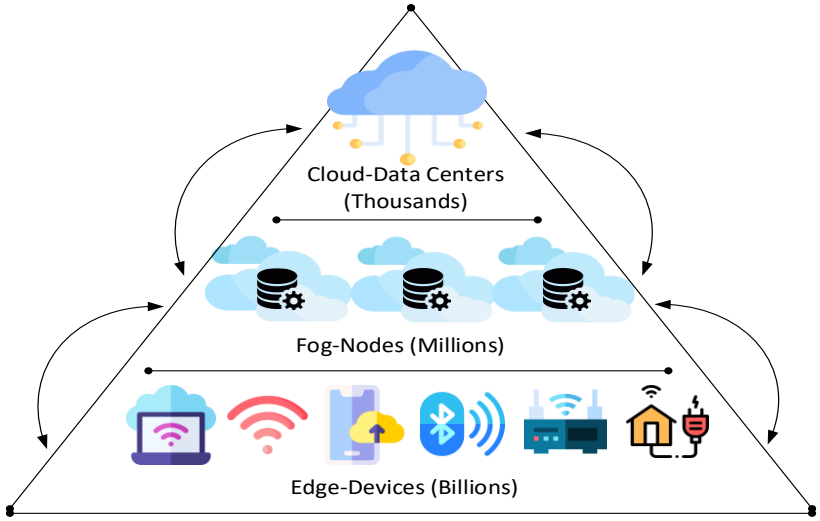



**Figure 14.** An elementary architecture of EC.

Looking at the threats and attacks causing serious security concerns to the IoT system, the following are possible solutions that can be achieved by incorporating EC with IoT.

- Data Compliance Issues: Data movement outside of borders is prohibited by many countries due to their restrictive regulatory acts, such as the GDPR (General Data Protection Regulation) of the European Union. Data sovereignty laws can be followed through EC, which keeps the data inside organizations [197]
- Data Breaches: Data are stored and processed entirely within local networks or devices in EC. In this case, no data are transferred from the source to the processor. Therefore, there is no risk of data theft or data breaches since the data are not in transit [198].
- Bandwidth Issues: Most of the data generated by IoT applications are raw and relatively of low value. As well as having a high bandwidth cost, the process of moving all the data to the cloud is also very hard in terms of security. The use of EC can enable data processing to be conducted at the edge nodes rather than sending the data to a cloud service [199].

- Safety issues: Physical safety can be compromised even if there is just a slight delay in responses. In the case of sensors that send all of their data and wait for the cloud to act, it may be too late to prevent injuries or deaths. Therefore, to achieve faster responses, devices can be deployed with EC to examine the abnormalities, process the data, and send them to the data center.

### *7.4. ML for IoT*

In recent years, the field of ML has been of major interest. For their development, many domains use ML, and it is also used for IoT security. ML seems to be an excellent way of protecting IoT devices against cyber assaults by offering an approach other than traditional methods to defend against attacks. ML refers to intelligent approaches that use example data or previous experience through learning to optimize performance criteria. Different ML algorithms have been developed to provide some non-traditional solutions to these challenges.

The basic requirement in IoT is the securing of all network-connected systems and devices. The role of ML is to use, train, and prevent data loss in IoT equipment to detect anomalies or to detect any unwanted activity in IoT systems. Consequently, ML provides a promising platform to overcome the problems in securing IoT devices.

Looking at the threats and attacks causing serious security concerns to the IoT system, the following are possible solutions that can be achieved by incorporating ML with IoT.

- DoS Attack: DoS attacks on IoT or IoT devices are a major concern. A multilayer perceptron (MLP) protocol to secure networks against DoS attacks serves as an approach for preventing such attacks [200]. Pavani, K. et al. proposed to create an MLP to improve the safety of wireless networks through particle swarm optimization and a backpropagation algorithm [201]. ML technologies help increase the accuracy of deductions and secure IoT devices vulnerable to DoS attacks.
- Eavesdropping: Attackers can sweep messages while data are being transmitted. ML techniques such as Q learning-based offloading strategy [202] or Bayesian non-parametric techniques [203] can be used to protect against such attacks. ML techniques such as Q-learn and Dyna-Q can be used to protect devices from eavesdropping, as well. Experimental evaluation and strengthening education of those schemes are presented in [204].
- Digital Fingerprinting: Digital fingerprinting is a promising solution for safe IoT systems and for the end-user to have enough confidence in applications. Digital fingerprints are widely used for smartphones, payments, car and home doors, etc. Digital fingerprinting is a dominant bio-metric identification method thanks to its low cost, reliability, acceptability, and high level of safety [205]. Aside from the advantages of digital fingerprinting, the efficiency of using this technology in IoT is varied, including fingerprint classification, improved image, and functional matching.

So far, from the discussion, it can be inferred that there is a huge potential for security enhancement in IoT using burgeoning technologies such as BC, FC, EC, and ML. The scope of possible security enhancements in IoT through the integration of these ubiquitous burgeoning technologies sprawling the appropriate layers is summarized in Table 5. Some of the research papers in literature focusing on security solutions in different capacities covering various aspects of IoT based on BC, FC, EC, and ML are shown in Figure 15. In this figure, three applications of IoT are considered, namely, healthcare, smart devices, and smart grid, for which some of the papers are presented from the literature which covers the security solutions in different capacities based on BC, FC, EC, and ML.

**Table 5.** Scope of security enhancement in IoT using burgeoning technologies.

| Burgeoning Technology | Scope of Security Enhancement in IoT |
| --- | --- |
| BC | Due to its key operational characteristics such as decentralized behavior, encryption-based communication, distributed functionality, inbuilt cryptography, authenticated access, etc., it offers security solutions against several threats and attacks across multiple layers of the IoT such as malicious data injection, disclosure of critical information, device compromise, node cloning, tag cloning, exhaustion attack, illegal access, information theft, spoofing, data manipulation, false data injection, unfair access, session hijacking, unfairness attack, fake information, unauthorized access, stealing users critical information, illegal interventions, software modification, message forging, brute force attack, etc. |
| FC | With abundant capabilities in processing, storing, managing the voluminous data, it offers security solutions against various threats and attacks such as eavesdropping, hardware failure, disclosure of critical information, device compromise, node capture attack, node tampering, battery drainages attack, node replication, illegal access, MITM, information theft, data manipulation, DoS, DDoS, false data injection, session hijacking, malicious attack, data integrity, virtualization, illegal access, cloud malware injection, illegal intervention, etc. |
| EC | The real-time services such as identity recognition, intrusion detection, access management, etc., enable EC to enhance security against several threats and attacks such as eavesdropping, battery drainage, hardware failure, node capture, DoS, DDoS, jamming, malicious attack, SQL injection, data integrity, virtualization, illegal access, flooding attack in the cloud, access attack, signature wrapping, etc. |
| ML | With enormous success in the paradigm of speech recognition, fraud detection, computer vision, spam detection, computer networks, etc., it is envisaged to solve several threats and attacks persisting to IoT. Some of these include device compromise, Sybil threat, node cloning, node capture, RF jamming, battery drainage attack, node replication, MITM, information theft, threats to communication protocols, DoS, DDoS, SCA, hello flood, congestion, MQTT-exploit, hole attack, firmware attack, illegal intervention, SQL injection, cross-site script, intersection, etc. |

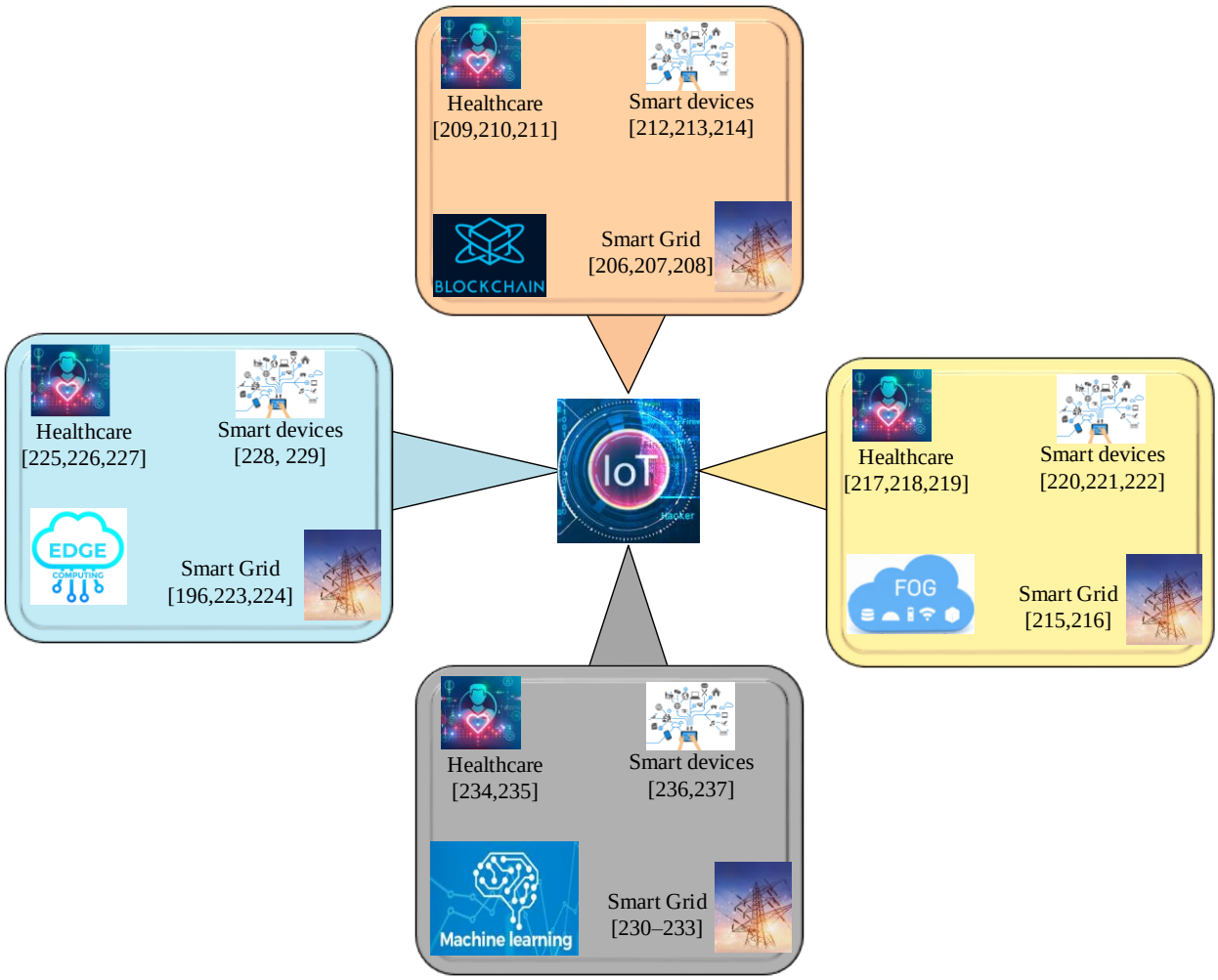



**Figure 15.** Some of the application domains of IoT and related work focusing scope for the security enhancement using burgeoning technologies [196,206–237].

## 8. Open Research Problems

Despite a successful journey so far, the IoT has many technological challenges and research issues that are yet to be explored. Some of the prominent research challenges are enumerated below.

- There is no generic validated architecture of IoT so far, i.e., most of the architectures are either domain-specific or application-specific. Thus, the security enhancement methodology may not fit the most generic architecture.
- The detailed protocols stack and its interoperability are still being explored. Due to immaturity, the exhaustive security aspects for protocols and the standards are far behind the actual realization.
- The amount of abstraction in security, the formal language to be utilized for policy encoding, and contextual IoT features to be considered for optimal usage of software-defined networking-based security mechanisms in a secure IoT framework is still an open problem.
- Given the inherent trade-off between flexibility, performance, and cost, the granularity of protection methods poses an open challenge in the provision of network slices specialized for IoT applications.
- The implementation methods and utilization of software and hardware are critical factors in BC to enhance security in IoT using BC. Being public in nature, the transactions of IoT data are still a problem of security concern that can be revealed to the public in general [238].
- Since FC is an extension to cloud computing, some of the serious concerns of cloud computing such as security and privacy are inherent to the FC, which are being extensively explored in the literature.
- EC poses serious security and privacy concerns since most of the computations are generally performed at the edge devices. However, most of the edge devices are resource-constrained in an IoT system, which may not be able to compute, analyze, and process the data securely.
- There are enormous ML algorithms. The selection of suitable algorithms is of vital importance, because choosing the incorrect algorithm will result in "garbage" output and a loss of effort, effectiveness, and accuracy. Similarly, selecting the incorrect data set will result in "garbage" input and inaccurate results. Thus, the correct data sets and appropriate algorithms are critically important, which can be explored for securing IoT environment using machine learning.
- The systematic review on vulnerabilities of BC, FC, EC, and ML and their mapping with impact on IoT are some of the research problems which can be further explored.
- The optimum resource sharing in FC is another research area that can be explored to avoid the burden on the cloud for processing the voluminous data during heavy traffic conditions.
- Further, the scope of other technologies such as artificial intelligence, big data, etc., must be also analyzed, which were shown to have great potential in IoT-based applications [239].

## 9. Conclusions

The introduction of smart computing devices using IoT has made day-to-day lives more convenient. Data analytics, automation, and smart devices have all benefited from the introduction of IoT into human life. Nevertheless, the unprecedented growth in IoT has also been crippled with many vulnerabilities and challenges. Further, the IoT's heterogeneous design expands the attack surface and adds new challenges to an already vulnerable IoT network. The successful compromise of the system's security may have fatal consequences for users. The overall security of the device must be considered to ensure that critical vulnerabilities are mitigated. Policies and protocols must be enforced as much as possible to deter threats and attacks. In this paper, we have presented a most comprehensive survey on IoT from the perspective of security threats and attacks. Further, modern threats

and attacks on the emerging IoT infrastructure, security flaws, and countermeasures are discussed in this paper. In addition, a roadmap of using ubiquitous technologies, viz., BC, FC, EC, and ML, for enhancing security in IoT are comprehensively discussed in this paper.

However, due to IoT devices' heterogeneous existence and limitations, any resolution would be ineffective and obsolete. Consequently, due to the evolving nature of technology, it is estimated that more countermeasures and vulnerabilities will be revealed in the near future. As future work, the authors are working on ML and IoT integration to enhance IoT-based applications' security under dynamically varying conditions.

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

**Funding:** There is no funding available for this research.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

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

## References

1. Jha, A.V.; Appasani, B.; Ghazali, A.N. Performance Evaluation of Network Layer Routing Protocols on Wireless Sensor Networks. In Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 17–19 July 2019; pp. 1862–1865. [CrossRef]
2. Tiwary, A.; Mahato, M.; Chidar, A.; Chandrol, M.K.; Shrivastava, M.; Tripathi, M. Internet of Things (IoT): Research, architectures and applications. *Int. J. Future Revolut. Comput. Sci. Commun. Eng.* **2018**, *4*, 23–27.
3. González-Zamar, M.D.; Abad-Segura, E.; Vázquez-Cano, E.; López-Meneses, E. IoT Technology Applications-Based Smart Cities: Research Analysis. *Electronics* **2020**, *9*, 1246. [CrossRef]
4. Internet of Things in Healthcare: Applications, Benefits, and Challenges. Available online: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html (accessed on 12 April 2021).
5. Cvar, N.; Trilar, J.; Kos, A.; Volk, M.; Stojmenova Duh, E. The Use of IoT Technology in Smart Cities and Smart Villages: Similarities, Differences, and Future Prospects. *Sensors* **2020**, *20*, 3897. [CrossRef] [PubMed]
6. Ryan, P.J.; Watson, R.B. Research Challenges for the Internet of Things: What Role Can OR Play? *Systems* **2017**, *5*, 24. [CrossRef]
7. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. *Wirel. Netw.* **2021**, *27*, 2595–2613. [CrossRef]
8. Jha, A.V.; Mishra, S.K.; Appasani, B.; Ghazali, A.N. Communication Networks for Metropolitan E-Health Applications. *IEEE Potentials* **2021**, *40*, 34–42. [CrossRef]
9. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
10. Rajendran, G.; Nivash, R.S.R.; Parthy, P.P.; Balamurugan, S. Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–6. [CrossRef]
11. Chen, L.; Thombre, S.; Järvinen, K.; Lohan, E.S.; Alén-Savikko, A.; Leppäkoski, H.; Bhuiyan, M.Z.H.; Bu-Pasha, S.; Ferrara, G.N.; Honkala, S.; et al. Robustness, security and privacy in location-based services for future IoT: A survey. *IEEE Access* **2017**, *5*, 8956–8977. [CrossRef]
12. Shin, H.; Lee, H.K.; Cha, H.Y.; Heo, S.W.; Kim, H. IoT security issues and light weight block cipher. In Proceedings of the International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Okinawa, Japan, 11–13 February 2019; pp. 381–384.
13. Gamundani, A.M. An impact review on internet of things attacks. In Proceedings of the International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 114–118. [CrossRef]
14. Kumar, N.; Madhuri, J.; Channe Gowda, M. Review on security and privacy concerns in Internet of Things. In Proceedings of the International Conference on IoT and Application (ICIOT), Nagapattinam, India, 19–20 May 2017; pp. 1–5. [CrossRef]
15. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
16. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]

17. Abomhara, M.; Køien, G.M. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.* **2015**, *4*, 65–88. [CrossRef]
18. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. *BODYNETS* **2012**, 256–262. [CrossRef]
19. Lee, E.; Seo, Y.D.; Oh, S.R.; Kim, Y.G. A Survey on Standards for Interoperability and Security in the Internet of Things. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 1020–1047. [CrossRef]
20. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors* **2021**, *21*, 3654. [CrossRef]
21. Mann, P.; Tyagi, N.; Gautam, S.; Rana, A. Classification of Various Types of Attacks in IoT Environment. In Proceedings of the 12th International Conference on Computational Intelligence and Communication Networks (CICN), Bhimtal, India, 3 November 2020; pp. 346–350. [CrossRef]
22. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. *Comput. Sci. Rev.* **2020**, *38*, 10031. [CrossRef]
23. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A survey of intrusion detection in Internet of Things. *J. Netw. Comput. Appl.* **2017**, *84*, 25–37. [CrossRef]
24. Hajiheidari, S.; Wakil, K.; Badri, M.; Navimipour, N.J. Intrusion Detection Systems in the Internet of Things: A Comprehensive Investigation. *Comput. Netw.* **2019**, *160*, 165–191. [CrossRef]
25. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. *Comput. Netw.* **2018**, *141*, 199–221. [CrossRef]
26. Sun, L.; Du, Q. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy* **2018**, *20*, 730. [CrossRef]
27. Elazhary, H. Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. *J. Netw. Comput. Appl.* **2019**, *128*, 105–140. [CrossRef]
28. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
29. Memon, R.A.; Li, J.P.; Ahmed, J.; Nazeer, M.I.; Ismail, M.; Ali, K. Cloud-based vs. blockchain-based IoT: A comparative survey and way forward. *Front. Inform. Technol. Electron. Eng.* **2020**, *21*, 563–586. [CrossRef]
30. Tran, N.K.; Babar, M.A.; Boan, J. Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. *J. Netw. Comput. Appl.* **2020**, *173*, 102844. [CrossRef]
31. Fersi, G. Fog computing and Internet of Things in one building block: A survey and an overview of interacting technologies. *Cluster Comput.* **2021**, 1–31. [CrossRef]
32. Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog Computing and the Internet of Things: A Review. *Big Data Cogn. Comput.* **2018**, *2*, 10. [CrossRef]
33. Hamdan, S.; Ayyash, M.; Almajali, S. Edge-Computing Architectures for Internet of Things Applications: A Survey. *Sensors* **2020**, *20*, 6441. [CrossRef]
34. Capra, M.; Peloso, R.; Masera, G.; Ruo Roch, M.; Martina, M. Edge Computing: A Survey on the Hardware Requirements in the Internet of Things World. *Future Internet* **2019**, *11*, 100. [CrossRef]
35. Ashouri, M.; Lorig, F.; Davidsson, P.; Spalazzese, R. Edge Computing Simulators for IoT System Design: An Analysis of Qualities and Metrics. *Future Internet* **2019**, *11*, 235. [CrossRef]
36. Amiri-Zarandi, M.; Dara, R.A.; Fraser, E. A survey of machine learning-based solutions to protect privacy in the Internet of Things. *Comput. Secur.* **2020**, *96*, 101921. [CrossRef]
37. Adnan, A.; Muhammed, A.; Abd Ghani, A.A.; Abdullah, A.; Hakim, F. An Intrusion Detection System for the Internet of Things Based on Machine Learning: Review and Challenges. *Symmetry* **2021**, *13*, 1011. [CrossRef]
38. Alwarafy, A.; Al-Thelaya, K.A.; Abdallah, M.; Schneider, J.; Hamdi, M. A Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. *IEEE Internet Things J.* **2020**, *8*, 4004–4022. [CrossRef]
39. Qiu, J.; Tian, Z.; Du, C.; Zuo, Q.; Su, S.; Fang, B. A survey on access control in the age of internet of things. *IEEE Internet Things J.* **2020**, *7*, 4682–4696. [CrossRef]
40. Parmar, M.S.; Shah, P.P. Uplifting Blockchain Technology for Data Provenance in Supply Chain. *Int. J. Adv. Sci. Technol.* **2020**, *29*, 5922–5938. [CrossRef]
41. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312. [CrossRef]
42. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204. [CrossRef]
43. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
44. 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]
45. Malik, M.; Dutta, M.; Granjal, J. A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things. *IEEE Access* **2019**, *7*, 27443–27464. [CrossRef]

46. Alshehri, F.; Muhammad, G. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. *IEEE Access* **2021**, *9*, 3660–3678. [CrossRef]
47. Stoyanova, M.; Nikoloudakis, Y.; Panagiotakis, S.; Pallis, E.; Markakis, E.K. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1191–1221. [CrossRef]
48. Viriyasitavat, W.; Da Xu, L.; Bi, Z.; Hoonsopon, D. Blockchain technology for applications in internet of things—mapping from system design perspective. *IEEE Internet Things J.* **2019**, *6*, 8155–8168. [CrossRef]
49. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 616–644. [CrossRef]
50. Cha, S.C.; Hsu, T.Y.; Xiang, Y.; Yeh, K.H. Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. *IEEE Internet Things J.* **2018**, *6*, 2159–2187. [CrossRef]
51. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
52. Mosenia, A.; Jha, N.K. A comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* **2016**, *5*, 586–602. [CrossRef]
53. 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]
54. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2521–2549. [CrossRef]
55. Serror, M.; Hack, S.; Henze, M.; Schuba, M.; Wehrle, K. Challenges and opportunities in securing the industrial internet of things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2985–2996. [CrossRef]
56. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT middleware: A survey on issues and enabling technologies. *IEEE Internet Things J.* **2016**, *4*, 1–20. [CrossRef]
57. Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the internet of things. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1636–1675. [CrossRef]
58. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2462–2488. [CrossRef]
59. Hamad, S.A.; Sheng, Q.Z.; Zhang, W.E.; Nepal, S. Realizing an internet of secure things: A survey on issues and enabling technologies. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1372–1391. [CrossRef]
60. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1676–1717. [CrossRef]
61. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
62. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network intrusion detection for IoT security based on learning techniques. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2671–2701. [CrossRef]
63. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A survey on the edge computing for the Internet of Things. *IEEE Access* **2017**, *6*, 6900–6919. [CrossRef]
64. Ni, J.; Zhang, K.; Lin, X.; Shen, X. Securing fog computing for internet of things applications: Challenges and solutions. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 601–628. [CrossRef]
65. Restuccia, F.; D'Oro, S.; Melodia, T. Securing the internet of things in the age of machine learning and software-defined networking. *IEEE Internet Things J.* **2018**, *5*, 4829–4842. [CrossRef]
66. Omoniwa, B.; Hussain, R.; Javed, M.A.; Bouk, S.H.; Malik, S.A. Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet Things J.* **2018**, *6*, 4118–4149. [CrossRef]
67. Khanam, S.; Ahmedy, I.B.; Idris, M.Y.I.; Jaward, M.H.; Sabri, A.Q.B.M. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. *IEEE Access* **2020**, *8*, 219709–219743. [CrossRef]
68. Alotaibi, B. Utilizing blockchain to overcome cyber security concerns in the internet of things: A review. *IEEE Sens. J.* **2019**, *19*, 10953–10971. [CrossRef]
69. 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]
70. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]
71. Benkhelifa, E.; Welsh, T.; Hamouda, W. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3496–3509. [CrossRef]
72. Sengupta, J.; Ruj, S.; Bit, S.D. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
73. Yugha, R.; Chithra, S. A survey on technologies and security protocols: Reference for future generation IoT. *J. Netw. Comput. Appl.* **2020**, *169*, 102763. [CrossRef]
74. Bhoyar, P.; Sahare, P.; Dhok, S.B.; Deshmukh, R.B. Communication technologies and security challenges for internet of things: A comprehensive review. *AEU-Int. J. Electron. Commun.* **2019**, *99*, 81–99. [CrossRef]

75. Bellavista, P.; Berrocal, J.; Corradi, A.; Das, S.K.; Foschini, L.; Zanni, A. A survey on fog computing for the Internet of Things. *Pervasive Mob. Comput.* **2019**, *52*, 71–99. [CrossRef]
76. Peña-López, I. ITU Internet Report 2005: The Internet of Things. Available online: https://www.comminit.com/global/content/itu-internet-reports-2005-internet-things (accessed on 12 April 2021).
77. Sikder, A.K.; Petracca, G.; Aksu, H.; Jaeger, T.; Uluagac, A.S. A survey on sensor-based threats to internet-of-things (IoT) devices and applications. *arXiv* **2018**, arXiv:1802.02041v1.
78. Hongsong, C.; Zhongchuan, F.; Dongyan, Z. Security and trust research in m2m system. In Proceedings of the 2011 IEEE International Conference on Vehicular Electronics and Safety, Beijing, China, 10–12 July 2011; pp. 286–290. [CrossRef]
79. Kumar, S.A.; Vealey, T.; Srivastava, H. Security in internet of things: Challenges, solutions and future directions. In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 5772–5781. [CrossRef]
80. Lee, S.K.; Bae, M.; Kim, H. Future of IoT networks: A survey. *Appl. Sci.* **2017**, *7*, 1072. [CrossRef]
81. Chen, H.; Jia, X.; Li, H. A Brief Introduction to IoT Gateway. In Proceedings of the IET International Conference on Communication Technology and Application (ICCTA), Beijing, China, 14–16 October 2011; pp. 1–4. [CrossRef]
82. Tan, H.; Tsudik, G.; Jha, S. MTRA: Multi-Tier randomized remote attestation in IoT networks. *Comput. Secur.* **2019**, *81*, 78–93. [CrossRef]
83. Internet of Things Challenges in Storage and Data. Available online: https://www.computerweekly.com/news/252450705/Internet-of-things-challenges-in-storage-and-data (accessed on 25 April 2021).
84. 12 Benefits of Cloud Computing. Available online: https://www.salesforce.com/in/products/platform/best-practices/benefits-of-cloud-computing/ (accessed on 25 April 2021).
85. Li, X.; Wang, Q.; Lan, X.; Chen, X.; Zhang, N.; Chen, D. Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach. *IEEE Access* **2019**, *7*, 9368–9383. [CrossRef]
86. Kepçeoğlu, B.; Murzaeva, A.; Demirci, S. Performing energy consuming attacks on IoT devices. In Proceedings of the 27th Telecommunications Forum (TELFOR), Belgrade, Serbia, 26–27 November 2019; pp. 1–4. [CrossRef]
87. Bilal, M. A Review of Internet of Things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers. *arXiv* **2017**, arXiv:1708.04560. Available online: https://arxiv.org/abs/1708.04560 (accessed on 25 April 2021).
88. Dodig, I.; Cafuta, D.; Kramberger, T.; Cesar, I. A Novel Software Architecture Solution with a Focus on Long-Term IoT Device Security Support. *Appl. Sci.* **2021**, *11*, 4955. [CrossRef]
89. Capella, J.V.; Campelo, J.C.; Bonastre, A.; Ors, R. A Reference Model for Monitoring IoT WSN-Based Applications. *Sensors* **2016**, *16*, 1816. [CrossRef]
90. Sadiku, M.N.; Tembely, M.; Musa, S.M. Home area networks: A primer. *Int. J.* **2017**, *7*, 208. [CrossRef]
91. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
92. Swamy, S.N.; Kota, S.R. An Empirical Study on System Level Aspects of Internet of Things (IoT). *IEEE Access* **2020**, *8*, 188082–188134. [CrossRef]
93. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of Things: A General Overview between Architectures, Protocols and Applications. *Information* **2021**, *12*, 87. [CrossRef]
94. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
95. Shelby, Z.; Hartke, K.; Bormann, C.; Frank, B. Constrained Application Protocol (CoAP), Draft-Ietf-Corecoap-18, Work in Progress. sl: IETF. 2013. Available online: http://tools.ietf.org/html/draft-ietf-corecoap-18 (accessed on 1 July 2021).
96. IoT Standards and Protocols Guide—Protocols of the Internet of Things. Available online: https://www.avsystem.com/blog/iot-protocols-and-standards/ (accessed on 25 April 2021).
97. Bormann, C.; Castellani, A.P.; Shelby, Z. Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Comput.* **2012**, *16*, 62–67. [CrossRef]
98. Cheshire, S.; Krochmal, M. Multicast DNS. *RFC* **2013**, *6762*. Available online: https://www.rfc-editor.org/info/rfc6762 (accessed on 1 July 2021). [CrossRef]
99. Vasseur, J.; Agarwal, N.; Hui, J.; Shelby, Z.; Bertrand, P.; Chauvenet, C. RPL: The IP routing protocol designed for low power and lossy networks. *IPSO Alliance* **2011**, 1–20. Available online: http://www.cse.chalmers.se/edu/year/2019/course/DAT300/PAPERS/rpl.pdf (accessed on 1 July 2021).
100. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.W.; Kelsey, R.; Levis, P.; Alexander, R.K. RPL: IPv6 routing protocol for low-power and lossy networks. *RFC* **2012**, *6550*, 1–157. Available online: https://datatracker.ietf.org/doc/html/rfc6550 (accessed on 1 July 2021).
101. Yang, Z.; Yue, Y.; Yang, Y.; Peng, Y.; Wang, Z.; Liu, W. Study and Application on the Architecture and Key Technologies for IOT. In Proceedings of the International Conference on Multimedia Technology, Hangzhou, China, 26–28 July 2011; pp. 747–751. [CrossRef]
102. Palattella, M.R.; Accettura, N.; Vilajosana, X.; Watteyne, T.; Grieco, L.A.; Boggia, G.; Dohler, M. Standardized protocol stack for the internet of (important) things. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 1389–1406. [CrossRef]

103. IEEE 802 Working Group. *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*; IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006); IEEE: Manhattan, NY, USA, 2011; pp. 1–314. [CrossRef]
104. Hasan, M.; Hossain, E.; Niyato, D. Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches. *IEEE Commun. Mag.* **2013**, *51*, 86–93. [CrossRef]
105. IEEE 802 Working Group. *IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies*; IEEE Std 1905.1-2013; IEEE: Manhattan, NY, USA, 2013; pp. 1–93. [CrossRef]
106. User Datagram Protocol(UDP). Available online: https://www.geeksforgeeks.org/user-datagram-protocol-udp/ (accessed on 25 April 2021).
107. Pipkin, D.L. *Halting the Hacker: A Practical Guide to Computer Security*, 2nd ed.; Prentice Hall Professional: Hoboken, NJ, USA, 2003.
108. Bertino, E.; Martino, L.D.; Paci, F.; Squicciarini, A.C. Web services threats, vulnerabilities, and countermeasures. In *Security for Web Services and Service-Oriented Architectures*; Springer: Heidelberg, Germany, 2019; pp. 25–44. [CrossRef]
109. Kizza, J.M. *Guide to Computer Network Security*, 1st ed.; Springer: Heidelberg, Germany, 2009; pp. 387–411. [CrossRef]
110. Dahbur, K.; Mohammad, B.; Tarakji, A.B. A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications, New York, NY, USA, 18–20 April 2011; pp. 1–6. [CrossRef]
111. Rainer, R.K.; Cegielski, C.G. Ethics, privacy, and information security. In *Introduction to Information Systems: Supporting and Transforming Business*; John Wiley & Sons: Hoboken, NJ, USA, 2010; Volume 3, pp. 70–121.
112. Tankard, C. Advanced persistent threats and how to monitor and deter them. *Netw. Secur.* **2011**, *2011*, 16–19. [CrossRef]
113. Coffed, J. *The Threat of Gps Jamming: The Risk to An Information Utility*; EXELIS: Herndon, VA, USA, 2014; pp. 6–10.
114. Tippenhauer, N.O.; Pöpper, C.; Rasmussen, K.B.; Capkun, S. On the requirements for successful GPS spoofing attacks. In Proceedings of the 18th ACM Conference on COMPUTER and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 75–86. [CrossRef]
115. Uluagac, A.S.; Subramanian, V.; Beyah, R. Sensory channel threats to cyber physical systems: A wake-up call. In Proceedings of the IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 301–309. [CrossRef]
116. Ge, M.; Hong, J.B.; Guttmann, W.; Kim, D.S. A framework for automating security analysis of the internet of things. *J. Netw. Comput. Appl.* **2017**, *83*, 12–27. [CrossRef]
117. Anthi, E.; Ahmad, S.; Rana, O.; Theodorakopoulos, G.; Burnap, P. Eclipse. IoT: A secure and adaptive hub for the Internet of Things. *Comput. Secur.* **2018**, *78*, 477–490. [CrossRef]
118. Sanchez Alcon, J.A.; López, L.; Martínez, J.F.; Rubio Cifuentes, G. Trust and privacy solutions based on holistic service requirements. *Sensors* **2016**, *16*, 16. Available online: https://www.mdpi.com/1424-8220/16/1/16 (accessed on 25 April 2021). [CrossRef] [PubMed]
119. Mauro, C.; Pallavi, K.; Rabbani, M.M.; Ranise, S. Attestation-enabled secure and scalable routing protocol for IoT networks. *Ad Hoc Netw.* **2020**, *98*, 102054. [CrossRef]
120. Prabadevi, B.; Jeyanthi, N. Distributed Denial of service attacks and its effects on Cloud environment-a survey. In Proceedings of the International Symposium on Networks, Computers and Communications, Hammamet, Tunisia, 17–19 June 2014; pp. 1–4. [CrossRef]
121. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6. [CrossRef]
122. Qian, L.; Zhu, Z.; Hu, J.; Liu, S. Research of SQL injection attack and prevention technology. In Proceedings of the International Conference on Estimation, Detection and Information Fusion (ICEDIF), Harbin, China, 10–11 January 2015; pp. 303–306. [CrossRef]
123. Everything You Need to Know About Facebook's Data Breach Affecting 50M Users. Available online: http://https//techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/ (accessed on 26 April 2021).
124. Zou, Y.; Wang, G. Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack. *IEEE Trans. Ind. Inform.* **2016**, *12*, 780–787. [CrossRef]
125. Chan, H.; Perrig, A.; Song, D.X. Random key predistribution schemes for sensor networks. In Proceedings of the IEEE Symposium Security Privacy, Berkeley, CA, USA, 11–14 May 2003; pp. 197–213. [CrossRef]
126. Abomhara, M.; Køien, G.M. Security and privacy in the Internet of Things: Current status and open issues. In Proceedings of the IEEE International Conference Privacy Security Mobile System (PRISMS), Aalborg, Denmark, 11–14 May 2014; pp. 1–8. [CrossRef]
127. Ashraf, Q.M.; Habaebi, M.H. Autonomic schemes for threat mitigation in Internet of Things. *J. Netw. Comput. Appl.* **2015**, *49*, 112–127. [CrossRef]
128. Znaidi, W.; Minier, M.; Babau, J.P. *An Ontology for Attacks in Wireless Sensor Networks*; RR-6704; INRIA: Rocquencourt, France, 2008.
129. Ye, F.; Luo, H.; Lu, S.; Zhang, L. Statistical en-route filtering of injected false data in sensor networks. *IEEE J. Sel. Areas Commun.* **2005**, *23*, 839–850.

130. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis & defenses. In Proceedings of the ACM Third International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 27 April 2004; pp. 259–268.
131. Sarigiannidis, P.G.; Karapistoli, E.D.; Economides, A.A. Detecting sybil attacks in wireless sensor networks using UWB ranging-based information. *Expert Syst. Appl.* **2015**, *42*, 7560–7572. [CrossRef]
132. Savola, R.M.; Abie, H.; Sihvonen, M. Towards metrics-driven adaptive security management in e-health IoT applications. In Proceedings of the 7th International Conference Body Area Network, Brussels, Belgium, 24–26 February 2012; pp. 276–281.
133. Choi, H.; Zhu, S.; Porta, T.F.L. SET: Detecting node clones in sensor networks. In Proceedings of the IEEE 3rd Int. Confernce Security Privacy Commun. Netw. Workshops (SecureComm), Nice, France, 17–21 September 2007; pp. 341–350. [CrossRef]
134. Xing, K.; Liu, F.; Cheng, X.; Du, D.H.C. Real-time detection of clone attacks in wireless sensor networks. In Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS), Beijing, China, 17–20 June 2008; pp. 3–10. [CrossRef]
135. Standaert, F.X. *Introduction to side-channel attacks. Secure Integrated Circuits and Systems*; Springer: Boston, MA, USA, 2010; pp. 27–42. ISBN 978-0-387-71829-3.
136. Wood, A.D.; Stankovic, J.A.; Son, S.H. JAM: A jammed-area mapping service for sensor networks. In Proceedings of the 24th IEEE Real-Time Systems Symposium, Cancun, Mexico, 5 December 2003; pp. 286–297. [CrossRef]
137. Hussein, A.A.; Leow, C.Y.; Rahman, T.A. Robust multiple frequency multiple power localization schemes in the presence of multiple jamming attacks. *PLoS ONE* **2017**, *12*, e0177326. [CrossRef]
138. Shabana, K.; Fida, N.; Khan, F.; Jan, S.R.; Rehman, M.U. Security issues and attacks in wireless sensor networks. *Int. J. Adv. Res. Comput. Sci. Electron. Eng.* **2016**, *5*, 81.
139. Ho, J.-W.; Wright, M.; Das, S.K. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. In Proceedings of the IEEE INFOCOM, Rio de Janeiro, Brazil, 19–25 April 2009; pp. 1773–1781. [CrossRef]
140. Wurm, J.; Hoang, K.; Arias, O.; Sadeghi, A.-R.; Jin, Y. Security analysis on consumer and industrial IoT devices. In Proceedings of the 21st IEEE Asia South Pacific Design Automation Conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 519–524. [CrossRef]
141. 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]
142. Koh, J.Y.; Nevat, I.; Leong, D.; Wong, W.C. Geo-spatial location spoofing detection for Internet of Thing. *IEEE Internet Things J.* **2016**, *3*, 971–978. [CrossRef]
143. Lough, D.L. *A Taxonomy of Computer Attacks with Applications to Wireless Networks*; Virginia Polytechnic Institute and State University: Blacksburg, VA, USA, 2001.
144. Bu, K.; Xu, M.; Liu, X.; Luo, J.; Zhang, S.; Weng, M. Deterministic detection of cloning attacks for anonymous RFID systems. *IEEE Trans. Ind. Informat.* **2015**, *11*, 1255–1266. [CrossRef]
145. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [CrossRef]
146. Mirai "Internet of Things" Malware From Krebs DDoS Attack Goes Open Source. Available online: https://nakedsecurity.sophos.com/2016/10/05/mirai-internet-of-things-malware (accessed on 30 June 2021).
147. Liu, Y.; Li, Y.; Man, H. MAC layer anomaly detection in ad hoc networks. In Proceeding of the 6th Annual IEEE SMC Information Assurance Workshop (IAW), West Point, NY, USA, 15–17 June 2005; pp. 402–409. [CrossRef]
148. Riaz, R.; Kim, K.-H.; Ahmed, H.F. Security analysis survey and framework design for IP connected LoWPANs. In Proceedings of the IEEE International Symposium Autonomous Decentralized Systems (ISADS), Athens, Greece, 23–25 March 2009; pp. 1–6.
149. Hamid, M.A.; Rashid, M.; Hong, C.S. Routing security in sensor network: Hello flood attack and defense. In Proceedings of the IEEE ICNEWS, Phoenix Park, Korea, 20–22 February 2006; pp. 2–4.
150. Murphy, J. Enhanced Security Controls for IBM Watson IoT Platform, Armonk. Available online: https://developer.ibm.com/iotplatform/2016/09/23/enhanced-securitycontrols-for-ibm-watson-iot-platform/ (accessed on 30 June 2021).
151. Teng, L.; Zhang, Y. SERA: A secure routing algorithm against sinkhole attacks for mobile wireless sensor networks. In Proceedings of the IEEE 2nd International Conference on Computer Modeling Simulation (ICCMS), Sanya, China, 22–24 January 2010; pp. 79–82.
152. Sathish, R.; Scholar, P.G. Dynamic detection of clone attack in wireless sensor networks. In Proceedings of the International Conference on Communication Systems Network Technologies, Gwalior, India, 6–8 April 2013; pp. 501–505.
153. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* **2003**, *1*, 293–315. [CrossRef]
154. Karakehayov, Z. Using reward to detect team black-hole attacks in wireless sensor networks. In Proceedings of the Workshop on Real World Wireless Sensor Network, Stockholm, Sweden, 20–21 June 2005; pp. 20–21.
155. Wang, W.; Bhargava, B.K. Visualization of wormholes in sensor networks. In Proceedings of the 3rd ACM Workshop Wireless Security, Philadelphia, PA, USA, 1 October 2001; pp. 51–60. [CrossRef]
156. Kaissi, R.Z.E.; Kayssi, A.; Chehab, A.; Dawy, Z. DAWWSEN: A Defense Mechanism Against Wormhole Attacks in Wireless Sensor Networks. Ph.D. Thesis, American University of Beirut, Beirut, Lebanon, 2005.
157. Perrey, H.; Landsmann, M.; Ugus, O.; Wählisch, M.; Schmidt, T.C. TRAIL: Topology Authentication in RPL. In Proceedings of the ACM International Conference on Embedded Wireless System and Network (EWSN), Graz, Austria, 15–17 February 2016; pp. 59–64.
158. Dvir, A.; Holczer, T.; Buttyán, L. Vera-version number and rank authentication in RPL. In Proceedings of the IEEE 8th International Conference on Mobile Ad Hoc Sensor Systems (MASS), Valencia, Spain, 17–22 October 2011; pp. 709–714. [CrossRef]

159. Accettura, N.; Piro, G. Optimal and secure protocols in the IETF 6TiSCH communication stack. In Proceedings of the IEEE 23rd International Symposium on Industrial Electronics (ISIE), Istambul, Turkey, 1–4 June 2014; pp. 1469–1474. [CrossRef]
160. Singh, M.; Rajan, M.; Shivraj, V.; Balamuralidhar, P. Secure MQTT for Internet of Things (IoT). In Proceedings of the IEEE 5th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 4–6 April 2015; pp. 746–751. [CrossRef]
161. Song, S.; Choi, H.-K.; Kim, J.-Y. A secure and lightweight approach for routing optimization in mobile IPv6. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*, 1–10. [CrossRef]
162. Neisse, R.; Steri, G.; Baldini, G. Enforcement of security policy rules for the Internet of Things. In Proceedings of the IEEE 10th International Confernce on Wireless and Mobile Computing Networking and Communications (WiMob), Larnaca, Cyprus, 8–10 October 2014; pp. 165–172. [CrossRef]
163. Xbox 360 Timing Attack. Available online: http://beta.ivc.no/wiki/index.php/Xbox_360_Timing_Attack (accessed on 30 June 2021).
164. Zhang, Q.; Wang, X. SQL injections through back-end of RFID system. In Proceedings of the International Symposium on Computer Network and Multimedia Technology, Wuhan, China, 18–20 January 2009; pp. 1–4.
165. Farris, I.; Taleb, T.; Khettab, Y.; Song, J. A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 812–837. [CrossRef]
166. Singh, J.; Pasquier, T.; Bacon, J.; Ko, H.; Eyers, D. Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet Things J.* **2016**, *3*, 269–284. [CrossRef]
167. Bose, T.; Bandyopadhyay, S.; Ukil, A.; Bhattacharyya, A.; Pal, A. Why not keep your personal data secure yet private in IoT: Our lightweight approach. In Proceedings of the IEEE 10th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, 7–9 April 2015; pp. 1–6.
168. Kumar, J.; Rajendran, B.; Bindhumadhava, B.S.; Babu, N.S.C. XML wrapping attack mitigation using positional token. In Proceedings of the International Confernce Public Key Infrastructure and its Applications (PKIA), Bangalore, India, 14–15 November 2017; pp. 36–42.
169. Deng, J.; Han, R.; Mishra, S. Defending against path-based dos attacks in wireless sensor networks. In Proceedings of the 3rd ACM Workshop Security Ad Hoc Sensor Network, Alexandria, VA, USA, 14–15 November 2005; pp. 89–96.
170. Gupta, H.; Oorschot, P.C.V. Onboarding and Software Update Architecture for IoT Devices. In Proceedings of the 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 26–28 August 2019; pp. 1–11. [CrossRef]
171. Skorobogatov, S. Fault attacks on secure chips: From glitch to flash. In *Design and Security of Cryptographic Algorithms and Devices (ECRYPT II)*; University of Cambridge: Cambridge, UK, 2011; pp. 1–64.
172. Stanciu, A.; Balan, T.-C.; Gerigan, C.; Zamfir, S. Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm. In Proceedings of the International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP), Brasov, Romania, 25–27 May 2017; pp. 1001–1006.
173. MohammadI, S.; Jadidoleslamy, H. A comparison of link layer attacks on wireless sensor networks. *Int. J. Appl. Graph Theory Wirel. Ad Hoc Netw. Sens. Netw.* **2011**, *3*, 35–56.
174. Swamy, S.N.; Jadhav, D.; Kulkarni, N. Security threats in the application layer in IoT applications. In Proceedings of the International Confernce IoT Social, Mobile, Analytics Cloud (I-SMAC), Palladam, India, 10–11 February 2017; pp. 477–480.
175. Sharmeen, S.; Huda, S.; Abawajy, J.H.; Ismail, W.N.; Hassan, M.M. Malware Threats and Detection for Industrial Mobile-IoT Networks. *IEEE Access* **2018**, *6*, 15941–15957. [CrossRef]
176. Ham, H.-S.; Kim, H.-H.; Kim, M.-S.; Choi, M.-J. Linear SVM-based Android malware detection for reliable IoT services. *J. Appl. Math.* **2014**, *2014*, 594501. [CrossRef]
177. Kaur, P.; Sharma, S. Spyware detection in Android using hybridization of description analysis permission mapping and interface analysis. *Procedia Comput. Sci.* **2015**, *46*, 794–803. [CrossRef]
178. Wolinsky, D.I.; Syta, E.; Ford, B. Hang with your buddies to resist intersection attacks. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), Berlin, Germany, 4–8 November 2013; pp. 1153–1166.
179. Grover, J.; Laxmi, V.; Gaur, M.S. Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks. *CSI Trans. ICT* **2013**, *1*, 261–279. [CrossRef]
180. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
181. Cherian, M.; Chatterjee, M. Survey of security threats in iot and emerging countermeasures. In Proceedings of the International Symposium on Security in Computing and Communication, Bangalore, India, 19–22 September 2018; pp. 591–604.
182. Sepulveda, J.; Willgerodt, F.; Pehl, M. SEPUFSoC: Using PUFs for memory integrity and authentication in multi-processors system-on-chip. In Proceedings of the GLSVLSI '18: Proceedings of the 2018 on Great Lakes Symposium on VLSI, Chicago, IL, USA, 23–25 May 2018; pp. 39–44. [CrossRef]
183. Bîrleanu, F.G.; Bizon, N. Reconfigurable computing in hardware security–a brief review and application. *J. Electr. Eng. Electron. Control Comput. Sci.* **2016**, *2*, 1–12.
184. Katsikogiannis, G.; Kallergis, D.; Garofalaki, Z.; Mitropoulos, S.; Douligeris, C. A policy-aware Service Oriented Architecture for secure machine-to-machine communications. *Ad Hoc Netw.* **2018**, *80*, 70–80. [CrossRef]
185. Laplante, P.A. Blockchain and the Internet of Things in the industrial sector. *IEEE Comput. Soc.* **2018**, *20*, 15–18.

186. Orman, H. Blockchain: The emperors new PKI? *IEEE Internet Comput.* **2018**, *22*, 23–28. [CrossRef]
187. Henry, R.; Herzberg, A.; Kate, A. Blockchain access privacy: Challenges and directions. *IEEE Secur. Priv.* **2018**, *16*, 38–45. [CrossRef]
188. Fog Computing: Focusing on Mobile Users at the Edge. Available online: https://arxiv.org/abs/1502.01815 (accessed on 1 July 2021).
189. Dastjerdi, A.V.; Buyya, R. Fog Computing: Helping the Internet of Things Realize Its Potential. *Computer* **2016**, *49*, 112–116. [CrossRef]
190. Sehgal, V.K.; Patrick, A.; Soni, A.; Rajput, L. Smart human security framework using Internet of Things, cloud and fog computing. Intelligent Distributed Computing. *Springer* **2015**, *321*, 251–263. [CrossRef]
191. Feasibility of Fog Computing. Available online: https://arxiv.org/abs/1701.05451 (accessed on 31 June 2021).
192. IoT Agenda. IoT and Big Data Analytics. Available online: https://internetofthingsagenda.techtarget.com/ (accessed on 30 June 2021).
193. Alwaris, A.; Alhothaily, A.; Hu, C.; Cheng, X. Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Comput.* **2017**, *21*, 34–42. [CrossRef]
194. Mollah, M.B.; Azad, M.A.K.; Vasilakos, A. Secure data sharing and searching at the edge of cloud-assisted Internet of Things. *IEEE Cloud Comput.* **2017**, *4*, 34–42. [CrossRef]
195. Alrowaily, M.; Lu, Z. Secure edge computing in IoT systems: Review and case studies. In Proceedings of the IEEE/ACM Symposium on Edge Computing (SEC), Seattle, WA, USA, 25–27 October 2018; pp. 440–444. [CrossRef]
196. Li, Y.; Wang, S. An energy-aware edge server placement algorithm in mobile edge computing. In Proceedings of the IEEE International Confernce Edge Comput. (EDGE), San Francisco, CA, USA, 2–7 July 2018; pp. 66–73. [CrossRef]
197. 6 Significant Issues That Edge Computing in IoT Solves. Available online: https://internetofthingsagenda.techtarget.com/feature/6-significant-issues-that-edge-computing-in-IoT-solves (accessed on 30 June 2021).
198. Premsankar, G.; Di Francesco, M.; Taleb, T. Edge computing for the Internet of Things: A case study. *IEEE Internet Things J.* **2018**, *5*, 1275–1284. [CrossRef]
199. Abbas, N.; Zhang, Y.; Taherkordi, A.; Skeie, T. Mobile edge computing: A survey. *IEEE Internet Things J.* **2018**, *5*, 450–465. [CrossRef]
200. Pavani, K.; Damodaram, A. Intrusion detection using MLP for MANETs. In Proceedings of the Third International Conference on Computational Intelligence and Information Technology (CIIT 2013), Mumbai, India, 18–19 October 2013; pp. 440–444. [CrossRef]
201. Kulkarni, R.V.; Venayagamoorthy, G.K. Neural network based secure media access control protocol for wireless sensor networks. In Proceedings of the 2009 International Joint Conference on Neural Networks, Atlanta, GA, USA, 14–19 June 2009; pp. 1680–1687. [CrossRef]
202. Xiao, L.; Xie, C.; Chen, T.; Dai, H.; Poor, H.V. A mobile offloading game against smart attacks. *IEEE Access* **2016**, *4*, 2281–2291. [CrossRef]
203. Xiao, L.; Yan, Q.; Lou, W.; Chen, G.; Hou, Y.T. Proximity-based security techniques for mobile users in wireless networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 2089–2100. [CrossRef]
204. Xiao, L.; Li, Y.; Han, G.; Liu, G.; Zhuang, W. PHY-layer spoofing detection with reinforcement learning in wireless networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 10037–10047. [CrossRef]
205. Spirina, K. Biometric Authentication: The Future of IoT Security Solutions. Available online: https://www.IoTevolutionworld.com/IoT/articles/438690-biometricauthenticationfuture-IoT-security-solutions.html (accessed on 9 February 2019).
206. Blanco-Novoa, Ó.; Fernández-Caramés, T.; Fraga-Lamas, P.; Castedo, L. An electricity price-aware open-source smart socket for the Internet of energy. *Sensors* **2017**, *17*, 643. [CrossRef]
207. Zhang, Y.; Wen, J. An IoT electric business model based on the protocol of bitcoin. In Proceedings of the 18th International Conference on Intelligence in Next Generation Networks, Paris, France, 17–19 February 2015; pp. 184–191. [CrossRef]
208. Lundqvist, T.; Blanche, A.; Andersson, H.R.H. Thing-to-thing electricity micro payments using blockchain technology. In Proceedings of the Global Internet of Things Summit (GIoTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6. [CrossRef]
209. Salahuddin, M.A.; Al-Fuqaha, A.; Guizani, M.; Shuaib, K.; Sallabi, F. Softwarization of Internet of Things infrastructure for secure and smart healthcare. *arXiv* **2018**, arXiv:1805.11011. Available online: https://arxiv.org/abs/1805.11011 (accessed on 1 July 2021).
210. Bocek, T.; Rodrigues, B.B.; Strasser, T.; Stiller, B. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In Proceedings of the IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8–12 May 2017; pp. 772–777. [CrossRef]
211. Shae, Z.; Tsai, J.J.P. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine. In Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1972–1980. [CrossRef]
212. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.A.; Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. *IEEE Internet Things J.* **2017**, *4*, 1832–1843. [CrossRef]
213. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Koreea, 19–22 February 2017; pp. 464–467. [CrossRef]
214. Samaniego, M.; Deters, R. Internet of Smart Things-IoST: Using Blockchain and CLIPS to Make Things Autonomous. In Proceedings of the IEEE International Conference on Cognitive Computing (ICCC), Honulul, HI, USA, 25–30 June 2017; pp. 9–16. [CrossRef]

215. Faruque, M.A.A.; Vatanparvar, K. Energy Management-as-a-Service Over Fog Computing Platform. *IEEE Internet Things J.* **2016**, *3*, 161–169. [CrossRef]
216. SGao, S.; Peng, Z.; Xiao, B.; Xiao, Q.; Song, Y. SCoP: Smartphone energy saving by merging push services in Fog computing. In Proceedings of the IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), Vilanova i la Geltrú, Spain, 14–16 June 2017; pp. 1–10. [CrossRef]
217. Dubey, H.; Monteiro, A.; Constant, N.; Abtahi, M.; Borthakur, D.; Mahler, L. Fog computing in medical Internet-of-Things: Architecture implementation and applications. In *Handbook of Large-Scale Distributed Computing in Smart Healthcare*, 1st ed.; Khan, S.U., Zomaya, A.Y., Abbas, A., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2017; pp. 281–321, ISBN 978-3-319-58280-1.
218. Rahmani, A.M.; Gia, T.N.; Negash, B.; Anzanpour, A.; Azimi, I.; Jiang, M. Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Gener. Comput. Syst.* **2018**, *78*, 641–658. [CrossRef]
219. Gia, T.N.; Jiang, M.; Rahmani, A.M.; Westerlund, T.; Liljeberg, P.; Tenhunen, H. Fog computing in healthcare Internet of Things: A case study on ecg feature extraction. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology, Liverpool, UK, 26–28 October 2015; pp. 356–363. [CrossRef]
220. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge Computing: Vision and Challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
221. Ni, J.; Zhang, A.; Lin, X.; Shen, X.S. Security, Privacy, and Fairness in Fog-Based Vehicular Crowdsensing. *IEEE Commun. Mag.* **2017**, *55*, 146–152. [CrossRef]
222. Markakis, E.K.; Karras, K.; Zotos, N.; Sideris, A.; Moysiadis, T.; Corsaro, A.; Pallis, E. EXEGESIS: Extreme Edge Resource Harvesting for a Virtualized Fog Environment. *IEEE Commun. Mag.* **2017**, *55*, 173–179. [CrossRef]
223. Huang, Y.; Lu, Y.; Wang, F.; Fan, X.; Liu, J.; Leung, V.C. An Edge Computing Framework for Real-Time Monitoring in Smart Grid. In Proceedings of the 2018 IEEE International Conference on Industrial Internet (ICII), Seattle, WA, USA, 21–23 October 2018; pp. 99–108. [CrossRef]
224. Oyekanlu, E.; Nelatury, C.; Fatade, A.O.; Alaba, O.; Abass, O. Edge computing for industrial IoT and the smart grid: Channel capacity for M2M communication over the power line. In Proceedings of the IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), Owerri, Nigeria, 7–10 November 2017; pp. 1–11. [CrossRef]
225. Muhammed, T.; Mehmood, R.; Albeshri, A.; Katib, I. UbeHealth: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities. *IEEE Access* **2018**, *6*, 32258–32285. [CrossRef]
226. Barik, R.K.; Dubey, H.; Mankodiya, K. SOA-FOG: Secure service-oriented edge computing architecture for smart health big data analytics. In Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, UK, 14–16 November 2017; pp. 477–481. [CrossRef]
227. Singh, D.; Tripathi, G.; Alberti, A.M.; Jara, A. Semantic edge computing and IoT architecture for military health services in battlefield. In Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 8–11 January 2017; pp. 185–190. [CrossRef]
228. Aman, M.N.; Sikdar, B.; Chua, K.C.; Ali, A. Low Power Data Integrity in IoT Systems. *IEEE Internet Things J.* **2018**, *5*, 3102–3113. [CrossRef]
229. Gope, P.; Sikdar, B. Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices. *IEEE Internet Things J.* **2019**, *6*, 580–589. [CrossRef]
230. Ahmed, S.; Lee, Y.; Hyun, S.; Koo, I. Feature Selection–Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning. *IEEE Access* **2018**, *6*, 27518–27529. [CrossRef]
231. Ozay, M.; Esnaola, I.; Vural, F.T.Y.; Kulkarni, S.R.; Poor, H.V. Machine Learning Methods for Attack Detection in the Smart Grid. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 1773–1786. [CrossRef] [PubMed]
232. Zhang, D.; Han, X.; Deng, C. Review on the research and practice of deep learning and reinforcement learning in smart grids. *CSEE J. Power Energy Syst.* **2018**, *4*, 362–370. [CrossRef]
233. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny, M.S.H. Application of Big Data and Machine Learning in Smart Grid and Associated Security Concerns: A Review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
234. Mercer, C. How Machine Learning Will Change Society. Available online: https://www.techworld.com/picture-gallery/tech-innovation/5-ways-machine-learning-will-change-society-3666674 (accessed on 1 July 2021).
235. Chen, M.; Hao, Y.; Hwang, K.; Wang, L.; Wang, L. Disease prediction by machine learning over big data from healthcare communities. *IEEE Access* **2017**, *5*, 8869–8879. [CrossRef]
236. Vito, S.D.; Francia, G.D.; Esposito, E.; Ferlito, S.; Formisano, F.; Massera, E. Adaptive machine learning strategies for network calibration of IoT smart air quality monitoring devices. *Pattern Recognit. Lett.* **2020**, *136*, 264–271. [CrossRef]
237. Punithavathi, P.; Geetha, S.; Karuppiah, M.; Islam, S.K.F.; Hassan, M.M.; Choo, K.K.R. A lightweight machine learning-based authentication framework for smart IoT devices. *Inf. Sci.* **2019**, *484*, 255–268. [CrossRef]
238. Bigini, G.; Freschi, V.; Lattanzi, E. A Review on Blockchain for the Internet of Medical Things: Definitions, Challenges, Applications, and Vision. *Future Internet* **2020**, *12*, 208. [CrossRef]
239. Sepasgozar, S.; Karimi, R.; Farahzadi, L.; Moezzi, F.; Shirowzhan, S.M.; Ebrahimzadeh, S.; Hui, F.; Aye, L. A Systematic Content Review of Artificial Intelligence and the Internet of Things Applications in Smart Home. *Appl. Sci.* **2020**, *10*, 3074. [CrossRef]