sensors

MDPI

Review

A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis

Hichem Mrabet [1,2], Sana Belguith [3,*], Adeeb Alhomoud [4] and Abderrazak Jemai [5]

[1] Department of IT, College of Computing and Informatics, Saudi Electronic University, Medina 42376, Saudi Arabia; h.mrabet@seu.edu.sa
[2] SERCOM-Lab., Tunisia Polytechnic School, Carthage University, 1054 Tunis, Tunisia; Abderrazak.Jemai@insat.rnu.tn
[3] School of Science, Engineering and Environment, University of Salford, Manchester M5 4WT, UK
[4] Department of Science, College of Science and Theoretical Studies, Saudi Electronic University, Riyadh 11673, Saudi Arabia; a.alhomoud@seu.edu.sa
[5] INSAT, SERCOM-Lab., Tunisia Polytechnic School, Carthage University, 1080 Tunis, Tunisia; Abderrazak.Jemai@insat.rnu.tn
* Correspondence: S.Belguith@salford.ac.uk

Received: 29 May 2020; Accepted: 23 June 2020; Published: 28 June 2020

Abstract: The Internet of Things (IoT) is leading today's digital transformation. Relying on a combination of technologies, protocols, and devices such as wireless sensors and newly developed wearable and implanted sensors, IoT is changing every aspect of daily life, especially recent applications in digital healthcare. IoT incorporates various kinds of hardware, communication protocols, and services. This IoT diversity can be viewed as a double-edged sword that provides comfort to users but can lead also to a large number of security threats and attacks. In this survey paper, a new compacted and optimized architecture for IoT is proposed based on five layers. Likewise, we propose a new classification of security threats and attacks based on new IoT architecture. The IoT architecture involves a physical perception layer, a network and protocol layer, a transport layer, an application layer, and a data and cloud services layer. First, the physical sensing layer incorporates the basic hardware used by IoT. Second, we highlight the various network and protocol technologies employed by IoT, and review the security threats and solutions. Transport protocols are exhibited and the security threats against them are discussed while providing common solutions. Then, the application layer involves application protocols and lightweight encryption algorithms for IoT. Finally, in the data and cloud services layer, the main important security features of IoT cloud platforms are addressed, involving confidentiality, integrity, authorization, authentication, and encryption protocols. The paper is concluded by presenting the open research issues and future directions towards securing IoT, including the lack of standardized lightweight encryption algorithms, the use of machine-learning algorithms to enhance security and the related challenges, the use of Blockchain to address security challenges in IoT, and the implications of IoT deployment in 5G and beyond.

Keywords: wearable and non-wearable devices; IoT; communication protocol; security attacks and countermeasures; data analysis

1. Introduction

The Internet of Things (IoT) is considered to be a worldwide network of uniquely addressable interconnected objects, using sensing features, employing communication protocols, exploiting computational capability, and providing services and capacity to analyze data. IoT objects can be doorbells, sensors, Digital Video Recorders (DVRs), light bulbs, electric switches, and home

assistant devices. Juniper Research estimates there will be over 46 billion IoT-connected objects by 2021, including devices, sensors and actuators, which represents an increase of 200% compared to 2016 (https://www.i-scoop.eu/internet-of-things-guide/connected-devices-2021/). Near-Field Communications (NFC) and Wireless Sensor and Actuator Networks (WSAN) associated with Radio-Frequency IDentification (RFID) make up the core of the IoT network [1]. The convergence of the Internet and sensor networks is fruitful, and is leading to a new paradigm called machine-to-machine (M2M) communication over the Internet by enabling a very large number of autonomous and self-organized devices [2]. The core concept of IoT is that every object in the network has many capabilities, such as identifying, sensing, and processing data, therefore enabling communication with a wide variety of other devices and services through the Internet to provide services to humanity.

IoT application domains fall into several categories, including utilities, transport and supply chain, environment and agriculture, health, personal home, and manufacturing and industry [3]. Industry 4.0 is a new trend, introducing new technologies to the manufacturing field, such as IoT, cyber-physical systems, big data, cloud computing, the semantic web, and virtualization [4]. As with any trend, many cyber-physical attacks target manufacturers that use Industry 4.0 systems [5], such as the Maroochy water services attack in Australia [6], the steel mill attack in Germany [7], the New York Dam attack [8], and the Norwegian Hydro aluminum attack (www.bbc.com/news/technology-47624207) in 2000, 2014, 2016, and 2019, respectively.

IoT, being an emerging technology as well as having huge number of devices deployed and connected to the Internet, represents a fertile field for attacker threats, and therefore new cyber-security issues related to IoT have appeared. Many threats threatening IoT devices have been 2 defined, including network, physical, environment, cryptanalysis, and software attacks [9]. Network attacks include man-in-the-middle (MITM), replay, masquerade, and distributed denial of service (DDoS) attacks [10]. To overcome these risks to IoT systems, communication protocols should be secure, lightweight encryption algorithm should be implemented, IoT platform security features should be enforced, and advanced techniques should be applied to filter and predict different security threats.

Security in IoT is of extreme importance, as any successful attack may paralyze a whole manufacturing, transport, health system, etc. sector. IoT is a combination of devices, network protocols, and technologies that each have their own vulnerabilities, which increases the attack surface across the whole IoT network. In other words, several attacks against IoT have been inherited from underlying technologies.

Contributions — There has been no standard until now for IoT architecture. However, different architectures have been proposed for IoT, such as three-layer [11], middle-ware-based architecture [12], service-oriented architecture (SOA) [13,14], four-layer [15], and five-layer [12].

Architecture previously proposed in the literature is highlighted in this paragraph. The basic model is called three-layer architecture, and it is composed of perception, network, and application layers [11,12,16]. Four-layer architecture covers perception, network, middleware, and application layers [13,15,16]. The role of the middleware layer involves service management, data storage, and service composition [15]. A proposed five-layer architecture includes objects, object abstraction, service management, application, and business layers [12].

To add advanced features to IoT such as IoT data, machine-learning algorithms, and light encryption algorithms, we propose in this paper a new IoT architecture, as shown in Figure 1. The proposed IoT architecture is based on five layers, including a perception layer, a network/protocol layer, a transport layer, and a data and cloud services layer. As shown in Figure 1, the physical layer involves different sensors and IoT devices such as a Wireless Sensors Network (WSN), QR Codes, Wireless Body Area Network (WBAN), Radio-Frequency IDentification (RFID) devices, etc.

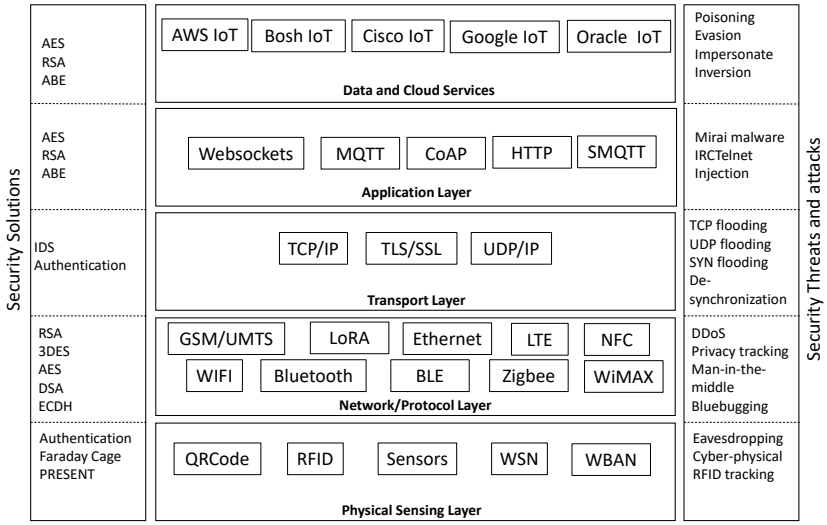

Figure 1. The proposed IoT architecture.

The network and protocol layer covers different wired and wireless network protocols involved in an IoT system, such as Wi-Fi, ZigBee, Ethernet, Bluetooth, LTE, 5G, etc. The transport layer involves TCP/IP, UDP/IP, and Transport Layer Security (TLS)/secure sockets layer (SSL) suite protocols. For the application layer, we cover the various application protocols developed to meet the IoT requirement in terms of low power consumption and small device capacity, such as Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), and Message Queuing Telemetry Transport (MQTT). Finally, the data and cloud services layer presents the main cloud-based IoT frameworks.

In Table 1, common IoT attacks are highlighted. We also provide security control suggestions to mitigate the harm to IoT devices caused by these attacks.

The paper focuses on analyzing security issues inherited by each layer component, while presenting deployed security measures and mechanisms to defeat prominent attacks.

Table 1. Common attack against IoT devices according to the new architecture.

Layer	Common Attack	Description	Security Countermeasures
Data and Cloud services	Poisoning	input of incorrect training data/labels to decrease the accuracy of classification/clustering process	Data sanitization.
	Evasion	Generating an adversarial sample leading to evade system from detection spam and malware.	Retraining learning models by classifier designers with adversarial samples.
	Impersonate	Unauthorized access based on deep neural network DNN algorithm.	Defensive distillation on DNN.
	Inversion	Gathering information about ML models to compromise the data privacy.	Differential privacy (DP) technique and data encryption.
Application	Mirai malware	Gain access to IoT device by using a default Telnet or SSH account	Disabling/changing default account of Telnet and SSH account.
	IRCTelnet	Forcing Telnet port to infect LINUX operating system of IoT device.	Disabling Telnet port number.
	Injection	Untrusted data is sent to an interpreter as part of a command or query.	Input validation control.
Transport	TCP flooding	Sending many packets through TCP protocol to stop or to reduce his activities.	A classifier based on SVM to detect and prevent DDoS TCP flooding attack.
	UDP flooding	Sending a large number of packets through UDP protocol to stop or to reduce his activities.	A flow-based detection schema on router using a state machine and a hashing table.
	TCP SYN flooding	Tentative to open an externally connection without respecting to the TCP handshake procedure.	SYN-Cookies consist on coding client SYN message to change the state in the server side.
	TCP desynchronization	Tentative to break the packet sequence by injection a packet with a wrong sequence number.	Authentication for all packets in the TCP session.
Network/protocol	Man-in-the-middle	Violate the confidentiality and integrity in data transfer.	Intrusion-detection system (IDS) and virtual private network (VPN).
	DDoS	Making network resource unavailable for its intended use	Ingress/Egress filtering, D-WARD, Hop Count Filtering and SYN-Cookies.
	Replay	Manipulate the message stream and reorder the data packets.	Timeliness of Message.
Physical	Eavesdropping	Infer information sent by IoT devices via network	Faraday cage.
	Cyber-physical	Physically attacking a device	Use of fault-detection algorithm to identify the faulty nodes.
	RFID Tracking	to disable tags, modify their contents, or imitate them	Faraday cage.

Application Mirai malware & Gain access to IoT device by using a default Telnet or SSH account & Disabling/changing default account of Telnet and SSH account. IRCTelnet & Forcing Telnet port to infect LINUX operating system of IoT device. & Disabling Telnet port number. Injection & Untrusted data is sent to an interpreter as part of a command or query. & Input validation control Transport & TCP flooding & TCP flooding consists of sending many packets through TCP protocol to stop or to reduce his activities. & A classifier based on SVM to detect and prevent DDoS TCP flooding attack. UDP flooding & UDP flooding consists of sending a large number of packets through UDP protocol to stop or to reduce his activities. & A flow-based detection schema on router using a state machine and a hashing table. TCP SYN flooding & TCP SYN flooding is a tentative to open an externally connection without respecting to the TCP handshake procedure. & One effective solution is called SYN-Cookies consist on coding client SYN message to change the state in the server side. TCP desynchronization & TCP desynchronization is defined as a tentative to break the packet sequence by injection a packet with a wrong sequence number. & Authentication is required for all packets in the TCP session. Network/protocol & Resource exhaustion, flooding, replay and amplification & Vulnerability of Transport Layer Security (TLS) to resource exhaustion, flooding, replay and amplification attacks & Using DTLS instead of TLS Man-in-the-middle & When a hacker tries to violate the confidentiality and integrity when two end-point transfer data. & Intrusion-detection system (IDS) and virtual private network (VPN). DDoS & Is an attempt to make a machine or network resource unavailable for its intended use & Ingress/Egress filtering, D-WARD, Hop Count Filtering and SYN-Cookies. Replay & The intruder may manipulate the message stream and maliciously reorder the data packets to change the meaning of the message & Timeliness of Message Physical sensing & Eavesdropping & Called also sniffing or snooping attack, it occurs when someone tries to pick up information sent by IoT devices via network Faraday cage is an effective solution for eavesdropping attack Cyber-physical & When a sensor is physically attacked or compromised by cyber-attack Using a localized fault-detection algorithm to identify the faulty nodes in WSN RFID Tracking & Is to disable tags, modify their contents, or imitate them & Faraday cage is an effective solution for RFID tracking attack.

As shown in Table 1, common IoT attacks can be classified into 5 classes:

- Data and cloud services layer attacks include poisoning, evasion, impersonation, and inversion.
- Application layer attacks include Mirai malware, IPCTelnet malware, DDoS, and injection.
- Transport layer attacks include resource exhaustion, flooding, replay, DDoS attack, and amplification attacks.
- Network and protocol layer attacks include man-in-the-middle, DDoS, and replay attacks.
- Physical sensing layer attacks include eavesdropping, cyber-physical, and tracking attacks.

A scenario to describe the realistic use of the proposed architecture could be an e-health application, in which the perception layer captures a physical parameter via a sensor implemented in a patient's body. Then, the job of the network and transport layers is to send the data to the application layer by selecting the suitable communication and lightweight encryption protocol based on power processing and energy consumption of the IoT device. The application layer will select the appropriate application protocol (i.e., MQTT, CoAP, or other) to communicate the data to the right user (i.e., doctor or medical staff). Finally, the data will be stored in the cloud layer and will be useful for future data analysis and prediction by using the appropriate machine-learning algorithm.

Existent Surveys — Internet of things security issues have attracted a lot of research, in which several published survey papers have studied IoT architecture, applications, and security issues. The survey authored by Al-Fuqaha et al. [12] covers the main IoT element-enabling technologies and the principle common IoT standards. In [11], the authors address the security of IoT frameworks such as AWS, Azure, and Calvin architecture. The authors in [16] provide a survey of the most common architectures proposed for IoT e-health applications, smart society applications, and cloud service and management solutions. Moreover, [4] addresses IoT in terms of the requirements of smart factories to enable standard Industry 4.0 protocols in the next industrial revolution. Key IoT applications in

industries are presented in [13] including the food supply chain, the iDrive system provided by the BMW car company, and an environment monitoring system for firefighting based on RFID tags. Buton et al. [17] introduced a security analysis of IoT based on an in-depth analysis of the use of WSNs, their vulnerabilities and their major security threats. Recently, Hussain et al. [18] presented a review of machine learning applied in IoT, and their main advantages and limitations.

Position of our paper — In this survey paper, we combine different aspects related to IoT technologies in one compact IoT architecture, covering IoT physical devices and sensors, communication and network protocols, a transport layer, an application layer, and data and cloud services. This architecture is based on a modification of OSI architecture, considering the security vulnerabilities and threats. In addition to existent OSI layers, we define a cloud and data layer, which involves several publicly available IoT frameworks providing IoT data storage, processing, and analysis. This architecture is extended to involve machine-learning applications that process data and protect IoT components. Furthermore, we present a discussion of current challenges facing IoT security solutions, such as the lack of standard encryption algorithms adapted for IoT devices. We also explore the application of novel techniques to secure IoT, such as the use of Blockchain in IoT and machine-learning models, as well as reviewing the potential of 5G network applications, and their reliance on IoT.

Paper Organization — This survey is organized as follows. Section 2 presents the main components of the physical sensing layer, and the related security threats and countermeasures. The IoT network and communication protocols and their related security issues and solutions are reviewed in Section 3. Section 4 introduces an overview of the transport layer protocol and its main security countermeasures. The application layer protocols are studied in Section 5, detailing their main security features. Section 6 reviews the well-known cloud-based IoT frameworks, while reviewing the main security measures they are implementing. Finally, a discussion of open issues and research opportunities is conducted in Section 7, before the survey paper is concluded in Section 8.

2. Physical Sensing Layer

2.1. Underlaying Technologies

The components of the physical sensing layer mainly involve but are not limited to QR codes, sensors, RFIDs, WSANs, and WBANs. In the state of the art, RFID uses a universal unique identifier called an Electronic Product Code (EPC) to identify objects in the IoT network. It supports various applications in several areas, such as logistics and supply-chain management, aviation, food safety, retailing, and public utilities. Likewise, the RFID system is characterized by its small size, very low cost, and no limitation to battery life. The second element that defines the core of the IoT network is WSAN, which can provide high radio coverage and communication paradigm, is peer-to-peer, while wireless sensor networks support sensing, computing, and communication capabilities in a passive system [1]. However, IoT benefits from the tracking capabilities offered by RFID tags [2]. WBAN stands for the wireless body area network and is defined as a set of sensors implemented in a patient's body to capture health parameters, including temperature, blood pressure, and glucose rate. The different sensors communicate the human vital signals to a health monitoring system via Bluetooth or ZigBee protocol.

2.2. Security Threats and Solutions

RFID is described by ISO/IEC 18000. However, RFID suffers from weak privacy. In addition, physical threats to RFID system disable tags, modify their content, and imitate them [19]. According to [9], a Faraday cage, tag-killing, tag-blocking, and re-encryption are effective solutions for RFID tracking attacks.

In the state of the art, the three kinds of attacks against the perception layer are eavesdropping, cyber-physical, and RFID tracking. An eavesdropping attack, also called a sniffing or snooping attack,

occurs when someone tries to pick up information sent by IoT devices via a network. A cyber-physical attack happens when a sensor in a WSN is physically attacked or compromised by a cyber-attack (called a faulty node). Various solutions have been proposed to overcome this attack, such as using a localized fault-detection algorithm to identify the faulty nodes in WSN [20], using a decentralized intrusion-detection system model for the WSN [21], and introducing a derived intrusion-detection probability in both homogeneous and heterogeneous WSNs [22]. A RFID tracking attack attempts to disable tags, modify their contents, or imitate them. Various security solutions are proposed to overcome this attack, such as using a localized fault-detection algorithm to identify the faulty nodes in the WSN [23], using a decentralized intrusion-detection system model for the WSN [21], and introducing a derived intrusion-detection probability in both homogeneous and heterogeneous WSNs [24]. Physical threats to the RFID system are disabling tags, modifying their content, and imitating them [19]. According to [9], a Faraday cage, tag-killing, tag-blocking, and re-encryption are effective solutions against eavesdropping and RFID tracking attacks. RFID is described by ISO/IEC 18000. In addition, a Faraday cage is one of the effective solutions for RFID consumer privacy against eavesdropping and tracking attacks [9]. Since WBAN uses wired and wireless protocol to communicate sensitive patient data, it can be vulnerable to malicious attacks such as eavesdropping, spoofing, and tampering, leading to a compromise of the privacy of the protected health information system [25]. Various solutions have been proposed in the literature to enforce access control and security communication between WBAN and external users (i.e., doctors and medical staff) such as the cyphertext policy attribute-based encryption (CP-ABE) where access is granted to the user who has at least d out of n attributes of the patient-related data [26,35].

3. Network and Protocol Layer

3.1. Underlaying Technologies/Background

Communication protocols are a main component of the IoT systems, enabling the establishment of communication and exchange of data between IoT devices and other distant parts of the network. The network and protocol layer includes ZigBee [27], 3G/4G/5G wireless communication [28], Wi-Fi [29], and Bluetooth [16]. In Table 2, we address the standard security feature (i.e., encryption protocol and key length), and advantages and disadvantages for the most relevant data-link communication protocols. Some research works divide IoT communication protocols into two sub-layers—sensor-based network and gateway network [16].

The sensor-based network relies on different protocols used by devices to communicate between each other. These protocols include but are not limited to Bluetooth, Bluetooth Low Energy (BLE), Worldwide Interoperability for Microwave Access (WiMAX), Wi-Fi, ZigBee, etc. [27,29]. The gateway network is responsible for routing data from/to a low-power lossy network (LLN) to/from the Internet or a close-by Local Area Network (LAN). These protocols include Ethernet, 3G/4G/5G, 6LoWPAN, etc. [28,30].

Table 2. Most relevant IoT communication protocols.

Communication Protocol	*Standards*	*Encryption Protocol*	*Energy Consumption*	*Advantages*	*Disadvantages*
6LoWPAN	IEEE 802.15.4	AES	Low	Low processing	Lack of authentication
RPL	IETF RPL	AES	Low	Low processing	Vulnerability to many attacks
NFC	ISO/IEC 14443	RSA, DSA	Low	Simplicity of deployment	Limited Range
Bluetooth	IEEE 802.16	AES, ECDH	Medium/Very Low (BLE)	Low consumption	Privacy/Identity Tracking
Wi-Fi	IEEE 802.11i/e/g	AES	High	Mobility and efficiency	Limited reachability
Zigbee	IEEE 802.15.4	AES	Low	Low-cost, low-energy devices	one-time transmission of the unprotected key
WiMAX	IEEE 802.16	RSA	Medium	Supports authentication	Limited mobility
3G/4G/5G	UMTS/LTE	RSA, 3DES	Medium	Portability	Battery limitation

Various basic communication protocols are used in IoT networks to ensure communication among all objects for wired and wireless networks. Bluetooth is described by the IEEE 802.15.1 standard. In its 4.2 version, Bluetooth uses the Federal Information Processing Standard (FIPS)-compliant elliptic curve

Diffie–Hellman (ECDH) algorithm for key generation (i.e., Diffie–Hellman key, or DH key). However, Bluetooth suffers from easy privacy/identity tracking. Wi-Fi is described by the IEEE 802.11i/e/g standard and it can support AES 128 key length. Mobility and efficiency are the most important benefit, while limited reachability (i.e., in the range of 100 m) is the main disadvantage [12]. ZigBee presents low-cost, low-energy devices, and one-time transmission of the unprotected key as an advantage and a disadvantage, respectively [9]. WiMAX is described by the IEEE 802.16 standard, which is a collection of wireless broadband standards. WiMAX provides data rates from 1.5 Mb/s to 1 Gb/s. NFC technology was developed by Philips and Sony in 2002 to provide contactless communication [31]. NFC is a short-range half-duplex communication protocol. NFC relies on coupling between the receiver and the sender. NFC works within a few centimeters under an operating frequency equal to 13.56 MHz. 3G and 4G mobile communication protocols are standardized by the universal mobile telecommunications system (UMTS) and Long-Term Evolution (LTE), respectively. IPv6 over LoWPAN (6LoWPAN) is a low-cost communication network allowing wireless connectivity between devices with limited power and processing capability. A 6LoWPAN typically includes devices that work together to connect the physical environment to real-world applications, e.g., wireless sensors. 6LoWPAN is standardized by the IEEE 802.15.4-2003 standard (IEEE802.15.4).

3.2. Security Threats and Countermeasures

Several common attacks have been launched against IoT communication protocols in which the attack can target most communication protocols such as eavesdropping against Bluetooth, NFC, Wi-Fi, etc. [32]. Man-in-the-middle attacks and Denial of Service (DoS) attacks also can be launched against various IoT communication protocols. To address different attacks, such as eavesdropping and replay attacks, RSA and Diffie–Hellman algorithms are the emergent solution for LTE-advanced (LTE-A)'s security features [33]. Some other attacks are dedicated to specific protocols, such as attacks against Bluetooth that are defined as follows:

- Bluejacking: This is the use of Bluetooth for sending unsolicited messages to other enabled devices. This attack exploits the Object Exchange (OBEX) protocol which is used by Bluetooth-enabled devices for exchanging data and commands [34].
- Bluebugging: This is an attack where the attacker exploits devices by manipulating the devices into compromising its own security, leading to unauthorized access of the device. The Bluebug attack focuses on or uses AT Commands (ASCII Terminal) when performing attacks [36,37].
- Bluesmack: This is an attack that causes denial of service to Bluetooth devices. This attack sends a Logic Link Control and Adaptation Protocol (L2CAP) ping request, which is similar to the ICMP ping attack, leading to devices being knocked out after receiving an oversized packet, which in turn leads to a DoS [38].

Since smart objects have a limited calculation capacity, restricted energy, and limited memory, lightweight encryption algorithms are widely used in the IoT field, such as in RFID tags, sensors, and healthcare devices [39]. Additionally, the lightweight concept for IoT is extended to lightweight attribute-based encryption schema for cloud applications [40–42], lightweight collaborative key management protocol [43], lightweight protocol for smart home authentication and key-session exchange [44,45]. Many IoT protocols have been proposed for different ISO layers, such as link layer (802.15.4, PLC), network layer (RPL, 6LoWPA), presentation layer (TLS, 802.1AR, 802.1X), and application layer (CoAP) [46]. Since 6LoWPA takes advantage of the IEEE 802.15.4 standard for low-rate wireless networks and IPv6, it provides low processing and a lack of authentication as an advantage and a disadvantage, respectively [9]. RPL uses the Advanced Encryption Standard (AES) protocol with key length of 128 [47]. RPL can support point-to-point communication and multi-cast routing in lower power networks [46]. However, its vulnerability to many attacks, such as forwarding, sinkhole, Sybil, Hello flooding, wormhole, black hole, and DoS, is the greatest disadvantage of RPL [9]. NFC is described by the ISO/IEC 14443 standard and it can support various cryptosystems including

RSA, digital signature algorithm (DSA), and elliptical curve digital signature algorithm (ECDSA) with a key length of up to 128 [48]. However, it presents a limited range between different active readers. A common attack in the network layer is the man-in-the-middle (MIM) attack. Two effective solutions for preventing MIM attacks are the use of an Intrusion-Detection System (IDS) and a Virtual Private Network (VPN). With the increasing use of IoT, botnet infections targeting IoT devices have become a noticeable threat. IoT devices suffered from a powerful botnet infection in 2016 due to the Mirai botnet malware [49]. According to [50] the latter botnet could infect and take control of more than 49,000 IoT devices distributed across 164 countries. Alhomoud el al. [49] identify botnets as a cluster of nodes infected by the same malware, where each node can serve as a bot (derived from the word robot) and is capable of performing certain actions or executing commands automatically, and mimicking human activates. One of the most common uses of botnets is to launch DDoS attacks. DDoS is an attempt to make a machine or network resource unavailable for its intended use to break the availability of a system or the network. Ingress/Egress filtering, D-WARD, Hop Count Filtering, and SYN-Cookies are DDoS attack countermeasures [23].

4. Transport Layer

4.1. Underlaying Technologies

The transport layer offers two services—a connection-oriented protocol, named TCP, for reliable application, and connectionless protocol for unreliable applications. TCP uses TLS to ensure a secure transport layer. However, UDP uses DTLS to secure the transport layer. By default, the lightweight connectivity protocol MQTT does not include a security layer. Therefore, the user is responsible for defining a security protocol, either TLS or SSL, and to enable a certificate and session key management [17]. Likewise, TLS and SSL are vulnerable against various kinds of attacks such as BEAST, CRIME, Heartbleed, and RC4. The basic form of MQTT, without a security protocol and with the weakness of TLS and SSL, is called an MQTT exploit.

4.2. Security Threats and Solutions

One of the most important weaknesses of the transport layer in IoT is the vulnerability of the TLS protocol to resource exhaustion, flooding, replay, and amplification attacks. A replay attack happens when the intruder manipulates a message stream and maliciously reorders the data packets to change the meaning of the message [27] . To protect IoT devices from a replay attack, setting the timeliness of the message is an effective security control. A DDoS attack can be considered to be a network/transport and application layer attack. The taxonomy of attacks against the transport layer caused by the DDoS is classified into TCP flooding, UDP flooding, TCP SYN flooding, and TCP desynchronization. TCP flooding and UDP flooding consist of sending many packets through the TCP and UDP protocol to stop or to reduce its activities. TCP SYN flooding is can open an external connection without respecting the TCP handshake procedure. TCP desynchronization, also called TCP hijacking, is defined as an attempt to break the packet sequence by injecting it with a wrong sequence number. In the state of the art, two solutions have been proposed to overcome the TLS issue. One is to use DTLS, and the other is to use an end-to-end tunnel to protect a low = power and lossy network [27]. Recently, various proposed solutions based on machine learning (ML) to detect DoS and DDoS have been proposed in the literature, such as the unsupervised clustering model, the Linear Vector Quantization (LVQ) model of Artificial Neural Network (ANN), and the Back-Propagation (BP) model of ANN. A pertinent classifier based on Support Vector Machine (SVM) to detect and prevent DDoS TCP flooding attacks upgrades the K-nearest, naive Bayes, and multilayer perceptron in terms of performance [51]. Finally, one effective solution against the MQTT exploit is to secure the MQTT protocol by implementing the attribute-based encryption through the elliptic curve [52].

5. Application Layer

5.1. Underlaying Technologies

Our IoT architecture application layer includes application protocols. Various application protocols have been developed to meet the IoT requirement in terms of low power consumption and small device capacity such as Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), Data Distribution Service (DDS), and Message Queuing Telemetry Transport (MQTT). MQTT is a specific application protocol that potentially enhances machine-to-machine communication between a client and a server. MQTT protocols can work under various data-link layer protocols, such as Ethernet and Wi-Fi. Additionally, they are characterized by being very lightweight and are a very effective solution to exchanging small messages between a broker (i.e., a server) and nodes (i.e., clients). Currently, the most important challenge for MQTT is adaptation to emergent technologies, such as LTE, 5G wireless, and mobile communications. Several advantages have been provided by MQTT, such as routing for small, cheap, low-power and low-memory devices in low-bandwidth and vulnerable networks [12]. MQTT was standardized in 2013, and presents three QoS levels. Likewise, an extension of MQTT is called Secure MQTT (SMQTT), and was proposed to tackle security issues. This extension is based on TCP/IP Internet suite protocol as depicted in Table 3. Many applications use MQTT, such as healthcare and Facebook notifications.

Table 3. SMQTT stack protocol.

OSI Layer	Protocol
Application	SMQTT
Session	SSL/TLS
Transport	TCP
Network	IPv4 and IPv6
Data-link	Ethernet/Wi-Fi

5.2. Security Threats and Solutions

Mirai malware, IRCTelnet, and injection are the common IoT attacks in the application layer. Mirai malware attack happens when a hacker tries to gain access to an IoT device by using a default Telnet or SSH account [53]. Therefore, to stop these attacks, the default accounts of Telnet and SSH should be disabled or changed. Likewise, IRCTelnet is based on forcing a Telnet port to infect the LINUX operating system of an IoT device [54]. One security measure to prevent an IRCTelnet attack is to disable the Telnet port number. According to the 2017 OWASP application security flaws review, the ten most critical web application security risks are: injection, broken authentication, sensitive data exposure, XML external entities (XXE), broken access control, security misconfiguration, cross-site scripting (XSS), insecure deserialization, and using components with known vulnerabilities (www.owasp.org, OWASP Top 10—2017 The Ten Most Critical Web Application Security Risks). Furthermore, injection is defined as untrusted data that is sent to an interpreter as part of a command or query to bring down the application using this data. An effective security control to prevent the user from entering more or less than the required format, and to prevent a hacker from abusing an application system, is input validation control [55]. SMQTT is proposed to improve MQTT security characteristics based on lightweight encryption. Many papers have proposed various versions of MQTT to enhance security features by adding encryption algorithms such as AES and Rivest–Shamir–Adleman (RSA) [56]. The security of the communication for SMQTT is provided through widespread SSL and transport layer security (TLS) protocols. In the state of the art, many variations of TLS, such as wireless TLS (WTLS) and datagram TLS (DTLS), are used in mobile communications and UDP-based applications, respectively, to ensure data privacy and integrity. In this section, we highlight the security protocols most used in IoT communication to ensure data confidentiality and privacy. Data confidentiality is

guaranteed by encryption protocols. Additionally, data is sanitized, and privacy is preserved. Table 4 presents the most important lightweight encryption algorithms for IoT in terms of key size, average execution time of 1000 iterations, and applications for both symmetric and asymmetric algorithms. Symmetric cipher algorithms support message integrity checks, encryption, and entity authentication. Additionally, asymmetric cipher algorithms provide non-repudiation and key management [57].

Table 4. Lightweight encryption algorithms for IoT.

	Algorithm	*Key Size*	*Execution Time*	*Application*
Symmetric	PRESENT	64 bits block with 80/128-bit length key	27.9	RFID
	CELFIA	128 bits block with 80/128/192 bits length key	-	Used by Sony for Digital Right Management
Asymmetric	RSA	1764 Bytes	19.33	Authentication
	Elliptic Curves	1272 Bytes	87.03	Pervasive Computing

PRESENT is a symmetric lightweight algorithm using a 64-bit block with 80/128-bit key length [58]. In addition, CLEFIA is proposed in the ISO/IEC 29192-2 light cryptography standard, the CRYPTREC project for the revision of the e-Government-recommended ciphers list in Japan, and it is employed by the Sony Corporation for digital rights management [59]. Additionally, RSA and elliptic curve (EC) are asymmetric lightweight algorithms. Moreover, RSA uses common public-key cryptography algorithms, and EC is very useful in pervasive computing [60,61]. Furthermore, three variants of EC algorithms are implemented—ECDAC for digital signature, ECIES for data encryption, and ECDH for key exchange [46].

6. Data and Cloud Services Layer

The development of applications for IoT faces many challenges due to the complexity of distributed computing, the involvement of different programming languages, and the variety of communication protocols. Therefore, the development of IoT applications requires the management of both hardware and software components, along with the handling of full infrastructure and delivery of functional and non-functional requirements. These challenges have led to the emergence of a cloud-based IoT programming framework launched by the major IoT stakeholders to provide ready-to-use/develop IoT applications.

The cloud-based IoT frameworks introduce a set of rules and protocols aimed at organizing data management and message exchange between the parties involved in the IoT network, such as devices, the cloud system, and users. These frameworks enable a simplified high-level deployment of IoT applications while hiding the complexity of the underlaying protocols.

In this section, we review the performance of the five main IoT frameworks based on public clouds, namely Amazon AWS IoT, CISCO IoT Cloud Connect, Google Cloud IoT, Oracle IoT Ecosystem, and Bosch IoT Suite. We have chosen these frameworks in the absence of a standardized framework, as they are the best-known ones. We focus on reviewing the security features provided by these frameworks as well as the inherited security threats by using public cloud architecture.

The cloud-based IoT frameworks are built on three main components: smart devices such as sensors, tags, etc., the cloud servers providing storage and processing of IoT data, and the users represented by the applications that access cloud-stored data and communicate with the devices. The frameworks also include the protocols that are needed to communicate between all the entities.

In Table 5, we compare the security features provided by the selected IoT frameworks. Providing a secure framework relies mainly on ensuring confidentiality, integrity, availability, authentication, and access control [55].

To ensure secure communication while transferring and accessing IoT data, various protocols are used by the aforementioned IoT frameworks, including Hypertext Transfer Protocol Secure (HTTPS), IPsec, transport layer security (TLS), datagram transport layer security (DTLS), and MQTT over TLS. Basically, SSL is used by AWS, Google Cloud and Oracle IoT Ecosystem.

Table 5. Security Features of Cloud-based IoT frameworks.

Cloud-Based IoT Framework	*Confidentiality*	*Integrity*	*Access Control*	*Authentication*	*Secure Communication*	*Encryption Protocol*
AWS IoT	SSL-protected, API endpoints	SSL-protected, API endpoints	Policy-based	X.509 certificates	SSL	TLS
Google IoT	ATLS	ATLS	Cloud IAM ACLs	ATLS RSA 2048	HTTPS, SSL	AES, 3DESTLS/S/MIME
Oracle IoT	SSL	PKI: Checksums	Roles-based	PKI : X.509 certificates, Kerberos	SSL	3DES, TSDP
CISCO IoT	IPsec	IPsec	Segment data based on destination	X.509 certificates	IPsec, TLS, MQTT over TLS	TLS, AES, RSA
Bosh IoT	WPA2	WPA2	No access control	SSID/Password	DTLS	LWM2M

AWS IoT is composed of four components, namely the device gateway, the rules engine, the registry, and the device shadows (https://docs.aws.amazon.com/iot-device-management/index.html). The device gateway is an intermediate component enabling communication between devices and cloud services via the MQTT protocol. The rules engine is responsible for processing the exchanged messages to forward them to the AWS, the subscribed devices, or a non-AWS service. The registry unit assigns an identifier to every connected device, while storing metadata to enable their tracking. The device shadow is a virtual device image created and stored in the cloud, enabling the saving of the last online state of the device and enforcement of future changes to the state once it goes online again. In a nutshell, the framework enables the management of IoT devices using its shadow even when it is not connected to the network.

To ensure confidentiality, integrity and availability, AWS proposes SSL-protected API endpoints (https://docs.aws.amazon.com/iot-device-management/index.html). AWS security modules ensure authentication and authorization. AWS authentication is based on X.509 certificates. On the other hand, AWS authorization is based on identity and access management (users, groups, and roles). Additionally, AWS Cognito identity modules are used to create unique user identities [11].

Google Cloud uses three kinds of encryption protocols to ensure the protection of data at the application layer. These are AES, TLS and secure/multipurpose Internet mail extensions (S/MIME) (http://cloud.google.com/security/encryption-in-transit). Likewise, Google cloud uses application layer transport security (ATLS) to guaranty confidentiality, integrity and authentication among different services. Also, Google Cloud suggests various access control options, such as cloud identity and access management as well as access control lists (ACLs).

The Oracle IoT solution is based on transparent sensitive data protection (TSDP) to ensure confidentiality and integrity. In addition, to improve data security, Oracle employs data masking and sub-setting to comply with the payment card industry data security standard (PCI-DSS) (www.oracle.com/technetwork/database/security/security-compliance).

CISCO IoT platform architecture is composed of four layers. These are an embedded systems and sensors layer, a multi-service edge layer, a core layer, and a data center cloud layer. The core layer includes IP/MPLS, security management, and network service. CISCO proposes an IoT/M2M security framework. Strong authentication is well provided by using AES and RSA for digital signature and key transport (www.cisco.com/secure-iot-proposed-framework, CISCO Kinetic Security Technical Paper). To ensure secure data traffic and data management, The CISCO Cloud solution employs HTTPS over IPsec, and SNMP over IPsec, respectively. Likewise, authorization and access control in CISCO IoT Cloud Connect uses segment data based on destination.

The architecture of the Bosch IoT suite expects an identity management module for users, roles, relations, and permissions. Regarding Bosch cross-domain applications (i.e., case of XDL120), confidentiality and integrity are based on the Wi-Fi-protected access 2 (WPA2) provided by the standard IEEE 802.11i/e/g white-listing of MAC addresses (https://www.digikey.co.uk/en/supplier-centers/b/bosch-cds). Furthermore, XDL120 employs DTLS to ensure a secure communication of transmitted sensor parameters and lightweight M2M (LWM2M) communication protocols.

In addition, cloud-based IoT frameworks provide access to machine-learning functions, enabling the processing of collected IoT data.

Research has identified multiple applications of machine learning in IoT contexts. The taxonomy of ML in IoT contexts for big data analysis is presented in Table 6. These ML models are categorized into three categories—classification, regression, and clustering [62]. The ML classification family

includes K-Nearest Neighbors (KNN), Naive Bayes (NB), and SVM. The ML clustering family involves K-means, a density-based approach to spatial clustering of applications with noise (DBSCAN), and the Feed Forward Neural Network (FFNN). The ML regression family covers Linear Regression (LR) and Support Vector Regression (SVR).

Table 6. Machine-learning trends for IoT.

	Algorithm	*Complexity for Prediction*	*Advantages*	*Disadvantages*	*IoT Applications*
Classification	KNN	O(np)	Easy to update in online setting	Unscalable to large data sets	Smart Citizen, Smart Tourism
	Naive Bayes	O(p)	Fast and highly scalable	Strong feature independence assumptions	Smart Agriculture, Spam filtering, Text categorization
	SVM	$O(n_{sv}p)$	Good for unbalanced data	The lack of transparency of results	Real-Time Prediction: Detection of Intrusion, attacks and malware.
Regression	Linear regression	O(p)	Processing under high rate	Very sensitive to outliers	Energy Applications, Market Prediction
	SVR	$O(n_{sv}p)$	Useful and flexible technique	More complicated	Intelligent transportation systems, Smart Weather
Clustering	K-means	O(n2)	Very fast and highly scalable	Difficult to predict the number of clusters (K-Value)	Smart Cities, Smart Home, Smart Citizen, Intelligent Transport
	DBSCAN	O(n2)	fast and robust against outliers	Performance is sensitive to the distance metric	Smart Citizen, Smart Tourism
	Feed Forward Neural Network	O(n2)	Non-linearity and robustness	Longer time for training	Smart Health

One important application of KNN clustering machine learning is to enable smart tourism and tourist pattern tracking. Then main advantage of KNN is that the online settings are easy to update; however, KNN is unscalable to large datasets. NB is applicable in many fields, such as spam filtering, text categorization, and automatic medical diagnosis [63]. Due to applying Bayes' theorem with the "naive" assumption of independence between the features, Naive Bayes classification is fast and highly scalable. The most important application of SVM is real-time prediction, which makes it suitable for real-time intrusions and attack detection. In addition, SVM has the capability to deal with high-dimensional datasets. Nonetheless, SVM suffers from a lack of transparency of results. LR can process at a high rate [64], and this algorithm is useful in many applications, such as economics, market analysis, and energy usage (to analyze and predict the energy usage of buildings, for example). However, LR is very sensitive to outliers. SVR uses the same basic idea as SVM, a classification algorithm, but applies it to predict real values rather than a class. SVR informs the presence of data non-linearity, and a prediction model is provided. Additionally, SVR is a useful and flexible technique, helping the user to deal with limitations pertaining to the distributional properties of underlying variables (https://rpubs.com/linkonabe/SLSvsSVR). The applications of SVR include the forecasting of financial markets, prediction of electricity prices, estimation of power consumption, and intelligent transportation systems [65]. The K-means clustering algorithm is present in many IoT applications, such as smart city, smart home, smart citizen, and air traffic control [66]. The most important benefits of K-means includes the high scalability and speed. However, K-means presents various disadvantages such as difficulty in predicting the number of clusters (K-Value), and sensitivity to scale. DBSCAN is an effective ML clustering algorithm, especially for large datasets. In addition, DBSCAN is very suitable for smart cities and for anomaly detection in temperature data applications [67]. Nonetheless, in the case of a dataset with large differences in densities, the clustering process is not efficient. Likewise, the performance of the model is sensitive to the distance metric used for determining whatever region is dense [68]. FFNN is a neural network trained with a back-propagation learning algorithm. The major advantages of FFNN are its adaptability without support of the user, non-linearity, and robustness. FFNN suffers from having a high number of weights in the neural network and requiring a longer time for training. The application fields of FFNN are smart health and chemistry (i.e., for the prediction of multi-state secondary structures).

The Generative adversarial network (GAN) is a pertinent type of machine learning that is receiving increased attention from researchers, based on two networks—generative network and discriminative network. The first network is used to generate new candidates from a known dataset, while the second serves as candidate evaluation. New emergent applications of GAN are applied in various fields, such as semi-supervised salient object detection in cloud-fog IoT devices [69] and high-resolution image generation [70]. On the other hand, the disadvantage of the Floor of Log algorithm associated with KNN and SVM is a promising supervised technique based on compressed features for power reduction of mobile devices running face-recognition applications [71].

7. Open Research Issues and Future Directions

Ensuring a fully secure IoT network is still a challenge that can hold back complete adoption of IoT application in daily life. There are multiple open issues and challenges to the provision of more secure IoT networks that constitute great opportunities for researchers. The first deciding factor in terms of security that will shape the future direction of IoT is the building of a standard architecture to ensure secure and reliable communication from a perception layer until cloud layer-like TCP/IP architecture in an Internet context. The second factor is the specification and selectin of the required lightweight encryption algorithm that fulfils IoT device capacity in terms of processing power and energy consumption. In this section, we review some future directions that will enable secure and private IoT application by either developing dedicated solutions, or adopting novel application of existing technologies.

7.1. The Lack of Standardized Lightweight Encryption Algorithms for IoT Applications

Efforts are being made to define a standard for lightweight encryption algorithms that are designed for IoT applications. Many requirements need to be fulfilled as IoT devices are resource-constrained devices. The main obstacles for proposing lightweight security algorithms for all IoT applications are the limited capacity of IoT devices in terms of energy consumption, processing power, and memory capacity. A minimum requirement for each lightweight security algorithm should be defined, such as key size, energy consumption, and execution time. Several encryption algorithms have been designed to suit IoT applications. Conventional algorithms have been applied to secure IoT including tiny encryption algorithm (TEA), which provides lower memory use and ease of implementation on both hardware and software scales [72]. AES has been also adopted to provide secure communication between IoT devices [73]. Though an attribute-based encryption algorithm requires high computation costs, several lightweight versions have been designed to suit IoT applications, such as reduced computation algorithms [40,74], offloading heavy computations to an edge [75], or cloud server [26].

7.2. Use of Machine Learning to Enhance Security in IoT

Recently, there has been an increased interest in targeting the use of machine-learning models to secure IoT applications [76].

Meidan et al. proposed [77] a Random Forest model, which is a supervised machine-learning algorithm, to extract features from network traffic data to detect unauthorized IoT devices.

Distributed Denial of Service (DDoS) attacks are increasing against IoT networks with the emergence of various techniques such as botnets [78]. In [77], a machine learning-based DDoS attack-detection mechanism is presented. This proposed solution enables the collection of IoT data, extracting the features and binary classification of IoT traffic to detect malicious traffic that initiates a DDoS attack. To build this mechanism, the authors used a variety of ML classifiers, namely random forests, K-nearest neighbors, support vector machines, decision trees, and neural networks.

Machine-learning algorithms have been also used for intrusion detection [79]. Zhao et al. [80] proposed a machine-learning-based intrusion-detection system that matches IoT characteristics requiring real-time monitoring. The authors based their solution on a dimension-reduction algorithm and a classifier. Principal Component Analysis (PCA) is used to decrease the size of the dataset of features to be analyzed. Furthermore, SoftMax regression and K-nearest are the two neighbor algorithms applied in the solution.

7.3. Blockchain in Smart IoT

Blockchain (BC) can be useful in many application fields, such as logistics and supply-chain management, Industry 4.0, the food industry, smart grid, and wireless network virtualization, to add more security features, to handle a large amount of data, and to support different components working

together in a distributed decentralized network [81]. A decentralized BC platform can provide better protection in terms of security and privacy compared to the classical centralized architecture [82]. However, decentralized consensus algorithms suffer from high energy consumption and computing power, and cannot be implemented in IoT devices with limited resources and mobile edge servers. For instance, various frameworks based on BC have been proposed by exploiting built-in cryptography mechanisms and by combining a smart contract concept to enable the automated enforcement of some conditions in the real world [83,84]. In 5G applications communication systems and beyond, BC can enhance spectral efficiency and provide much better 5G traffic optimization while preserving privacy when different IoT devices share a link condition [85]. Despite all the advantages offered by BC technology and the related proposed frameworks based on it to improve security components, to the best of our knowledge there is no proposed framework that can provide a complete secured solution providing the confidentiality, integrity and availability (CIA) triad, preserving privacy, and offering multi-factor or remote authentication. Therefore, we believe that securing BC-based solutions for IoT is a big challenge for researchers in the future.

7.4. Securing 4G/5G and beyond Applications

Ferag and al. [86] presented a taxonomy of attacks against 4G/5G cellular networks based on four classes, including attacks against privacy, attacks against availability, attacks against integrity and attacks against authentication. Despite various countermeasures being provided to preserve privacy and authentication based on cryptography methods, human factors, and intrusion-detection systems to meet the security requirements for IoT in the 5G context, we believe that more research effort is necessary to achieve this goal. Some security issues related to the 5G network need to be resolved, such as the absence of a dataset for network intrusion detection in 5G scenarios. Furthermore, location and identity privacy are not preserved for 5G fog radio access network (F-RAN) and 5G cloud radio access network (C-RAN). Finally, recent research work regarding capacity extension of a massive MIMO channel [87] using new waveforms to enhance the performance of a 5G mobile system and to raise the number of connected IoT devices [88] needs to be enforced against privacy breaches and intrusion attacks in the C-RAN and F-RAN architecture.

8. Conclusions

In this paper, an IoT five-layer architecture is proposed based on potential security threats and countermeasures. Furthermore, the common attacks against IoT devices are exhibited, and the required countermeasures are reviewed. Indeed, IoT trends include securing the most relevant communication protocols, mitigating the security issues of the most important IoT platforms, and applications of the most important machine-learning trends to mitigate and predict security threats and risks. The main security features of IoT business platforms are addressed in terms of confidentiality, integrity, access control, authentication, secure communication, and encryption protocols. Finally, open research issues and future directions towards secure IoT devices and applications are discussed by providing standardized lightweight encryption algorithms, using machine-learning and blockchain, and enforcing security measures for 4G/5G mobile system applications and beyond.

Funding: This research received no external funding.

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

References

1. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805.
2. Whitmore, A.; Agarwal, A.; Da Xu, L. The Internet of Things—A survey of topics and trends. *Inf. Syst. Front.* **2015**, *17*, 261–274.
3. Asghari, P.; Rahmani, A.M.; Javadi, H.H.S. Internet of Things applications: A systematic review. *Comput. Netw.* **2019**, *148*, 241–261.

4. Mabkhot, M.M.; Al-Ahmari, A.M.; Salah, B.; Alkhalefah, H. Requirements of the smart factory system: A survey and perspective. *Machines* **2018**, *6*, 23.
5. Oueslati, N.E.; Mrabet, H.; Jemai, A.; Alhomoud, A. Comparative Study of the Common Cyber-physical Attacks in Industry 4.0. In Proceedings of the 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), Tunis, Tunisia, 20–22 December 2019; pp. 1–7.
6. Abrams, M.; Weiss, J. *Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia*; The MITRE Corporation: Bedford, MA, USA, 2008.
7. Maple, C. Security and privacy in the internet of things. *J. Cyber Policy* **2017**, *2*, 155–184.
8. Ustundag, A.; Cevikcan, E. *Industry 4.0: Managing the Digital Transformation*; Springer: Berlin/Heidelberg, Germany, 2017.
9. Gloukhovtsev, M. IoT Security: Challenges, Solutions & Future Prospects. Available online: https://education.dellemc.com/content/dam/dell-emc/documents/en-us/2018KS_Gloukhovtsev-IoT_Security_Challenges_Solutions_and_Future_Prospects.pdf (accessed on 20 June 2020).
10. 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.
11. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27.
12. 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.
13. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
14. Hammoudeh, M.; Epiphaniou, G.; Belguith, S.; Unal, D.; Adebisi, B.; Baker, T.; Kayes, A.; Watters, P. A service-oriented approach for sensing in the Internet of Things: intelligent transportation systems and privacy use cases. *IEEE Sens. J.* **2020**. doi:10.1109/JSEN.2020.2981558.
15. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Voumn. 3, pp. 648–651.
16. Ray, P.P. A survey on Internet of Things architectures. *J. King Saud Univ. Comput. Inf. Sci.* **2018**, *30*, 291–319.
17. Butun, I.; Österberg, P.; Song, H. Security of the Internet of Things: Vulnerabilities,Attacks, and Countermeasures. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 616–644.
18. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: current solutions and future challenges. *IEEE Commun. Surv. Tutor.* **2020**. doi:10.1109/COMST.2020.2986444.
19. Khattab, A.; Jeddi, Z.; Amini, E.; Bayoumi, M. RFID security threats and basic solutions. In *RFID Security*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 27–41.
20. Chen, J.; Kher, S.; Somani, A. Distributed fault detection of wireless sensor networks. In *Proceedings of the 2006 Workshop on Dependability Issues in Wireless ad hoc Networks and Sensor Networks*; ACM Press: New York, NY, USA, 2006, pp. 65–72.
21. da Silva, A.P.R.; Martins, M.H.; Rocha, B.P.; Loureiro, A.A.; Ruiz, L.B.; Wong, H.C. Decentralized intrusion detection in wireless sensor networks. In *Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*; ACM Press: New York, NY, USA, 2005; pp. 16–23.
22. Wang, Y.; Wang, X.; Xie, B.; Wang, D.; Agrawal, D.P. Intrusion detection in homogeneous and heterogeneous wireless sensor networks. *IEEE Trans. Mob. Comput.* **2008**, *7*, 698–711.
23. Aamir, M.; Zaidi, M.A. A survey on DDoS attack and defense strategies: From traditional schemes to current techniques. *Interdiscip. Inf. Sci.* **2013**, *19*, 173–200.
24. Osanaiye, O.; Ogundile, O.; Aina, F.; Periola, A. Feature selection for intrusion detection system in a cluster-based heterogeneous wireless sensor network. *Facta Univ. Ser. Electron. Energ.* **2019**, *32*, 315–330.
25. Zou, S.; Xu, Y.; Wang, Y.; Li, Z.; Chen, S.; Hu, B. A Survey on Secure Wireless Body Area Networks. *Secur. Commun. Netw.* **2017**, *2017*, 1–9.
26. Belguith, S.; Kaaniche, N.; Laurent, M.; Jemai, A.; Attia, R. Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. *Comput. Netw.* **2018**, *133*, 141–156.
27. Kasmi, M.; Bahloul, F.; Tkitek, H. Smart home based on Internet of Things and cloud computing. In Proceedings of the 2016 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Hammamet, Tunisia, 18–20 December 2016; pp. 82–86.

28. Ejaz, W.; Anpalagan, A.; Imran, M.A.; Jo, M.; Naeem, M.; Qaisar, S.B.; Wang, W. Internet of Things (IoT) in 5G wireless communications. *IEEE Access* **2016**, *4*, 10310–10314.
29. Madakam, S.; Lake, V.; Lake, V.; Lake, V.; Internet of Things (IoT): A literature review. *J. Comput. Commun.* **2015**, *3*, 164.
30. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
31. Coskun, V.; Ozdenizci, B.; Ok, K. A survey on near field communication (NFC) technology. *Wirel. Pers. Commun.* **2013**, *71*, 2259–2294.
32. Bapat, C.; Baleri, G.; Inamdar, S.; Nimkar, A.V. Smart-lock security re-engineered using cryptography and steganography. In *International Symposium on Security in Computing and Communication*; Springer: Singapore, 2017; pp. 325–336.
33. Vafaei, R. Encryption of 4G Mobile Broadband Systems. Available online: https://d1wqtxts1xzle7.cloudfront.net/37977538/Encryption_of_4G__mobile_broadband_.pdf?1435043247=&response-content-disposition=inline3B+filename3DEncryption_of_4G_mobile_broadband_system.pdf&Expires=1593318157&Signature=MnmQQhPUPwG2WDpoyoCvAN-lZ6QLH12S2wML3LHG9gPs5A3toNnjj60SKgXTmq~Bnb98RjoN5C5H8O8F~aACu8hu7KcBqvXaJiwtoE~rkwZWemqW7XMc-fclkKJTbSf-CFEY6vqc9FoeHmWMzBHcw4QDjgZvyKSsCtAYISPT6Vcu1bh7c4ToHumNNlVrjd37dUMOw83RCurhhbWxiIvf2R9DfVRWmBSZZTOC6gOVDsyQ77EMA7Uo7l97OKZYSGZ82xhblzPa~ye0e3Dz92tDSZGVs2zZB9Wg9GyU8ZZPasB2MNtHpOrXvoAZ3--c2FWXHpzDnwBFJIZqviQaG1RVFw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (accessed on 20 June 2020).
34. Mira, F.; Alsmadi, I. Review of Analysis on IoT Components, Devices and Layers Security. In Proceedings of the 2019 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 4–6 November 2019; pp. 1–6.
35. Belguith, S.; and Kaaniche, N.;Hammoudeh, M. Analysis of attribute-based cryptographic techniques and *In Transactions on Emerging Telecommunications Technologies*; Wiley Online Library,pp.e3667.
36. Laurie, A.; Herfurt, M.H.M. Hacking Bluetooth enabled mobile phones and beyond–Full Disclosure. In Proceedings of the 21st Chaos Communication Congress, Berliner Congress Center, Berlin, Germany, 27–29 December 2004.
37. Liao, M. Bluetooth Vulnerabilities in Data Security of Mobile Phones. Available online: https://docs.lib.purdue.edu/dissertations/AAI1535052/ (accessed on 20 June 2020).
38. Becker, A.; Paar, I.C. *Bluetooth Security & Hacks*; Ruhr-Universität Bochum: Bochum, Germany, 2007.
39. Katagi, M.; Moriai, S. *Lightweight Cryptography for the Internet of Things*; Sony Corporation: Tokyo, Japan, 2008; pp. 7–10.
40. Belguith, S.; Kaaniche, N.; Russello, G. CUPS: Secure opportunistic cloud of things framework based on attribute-based encryption scheme supporting access policy update. *Secur. Priv.* **2019**. doi:10.1002/spy2.85.
41. Belguith, S.; Kaaniche, N.; Russello, G. Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT. In *Proceedings of the 15th International Joint Conference on e-Business and Telecommunications-Volume 1: SECRYPT*; SciTePress: Setúbal, Portugal, 2018; pp. 135–146.
42. Yao, X.; Chen, Z.; Tian, Y. A lightweight attribute-based encryption scheme for the Internet of Things. *Future Gener. Comput. Syst.* **2015**, *49*, 104–112.
43. Saied, Y.B.; Olivereau, A.; Zeghlache, D.; Laurent, M. Lightweight collaborative key establishment scheme for the Internet of Things. *Comput. Netw.* **2014**, *64*, 273–295.
44. Belguith, S.; Kaaniche, N.; Mohamed, M.; Russello, G. Coop-daab: Cooperative attribute based data aggregation for internet of things applications. In *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*; Springer: Berlin/Heidelberg, Germany, 2018, pp. 498–515.
45. Belguith, S.; Kaaniche, N.; Mohamed, M.; Russello, G. C-ABSC: cooperative attribute based signcryption scheme for internet of things applications. In Proceedings of the 2018 IEEE International Conference on Services Computing (SCC), San Francisco, CA, USA, 2–7 July 2018; pp. 245–248.
46. Mektoubi, A.; Hassani, H.L.; Belhadaoui, H.; Rifi, M.; Zakari, A. New approach for securing communication over MQTT protocol A comparaison between RSA and Elliptic Curve. In Proceedings of the 2016 Third International Conference on Systems of Collaboration (SysCo), Casablanca, Morocco, 28–29 November 2016; pp. 1–6.

47. Salman, T.; Jain, R. Networking protocols and standards for internet of things. *Internet Things Data Anal. Handb.* **2015**, *2015*, 215–238.
48. Dragomir, D.; Gheorghe, L.; Costea, S.; Radovici, A. A survey on secure communication protocols for IoT systems. In Proceedings of the 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, Greece, 26–30 September 2016; pp. 47–62.
49. Alhomoud, A.; Namanya, A.P.; Disso, J.P.; Awan, I. A Se/f/-healing Framework for Enterprise networks to combat Botnets infections. Available online: https://repository.nauss.edu.sa/bitstream/handle/123456789/64743/A/20Self-healing/20Framework/20for/20Enterprise/20networks/20to/20combat/20Botnets/20infections.pdf?sequence=5 (accessed on 20 June 2020).
50. Antonakakis, M.; April, T.; Bailey, M.; Bernhard, M.; Bursztein, E.; Cochran, J.; Durumeric, Z.; Halderman, J.A.; Invernizzi, L.; Kallitsis, M.; et al. Understanding the mirai botnet. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16–18 August 2017; pp. 1093–1110.
51. Kotey, S.D.; Tchao, E.T.; Gadze, J.D. On Distributed Denial of Service Current Defense Schemes. *Technologies* **2019**, *7*, 19.
52. Singh, M.; Rajan, M.; Shivraj, V.; Balamuralidhar, P. Secure MQTT for Internet of Things (IoT). In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015; pp. 746–751.
53. 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.
54. Rizvi, S.; Kurtz, A.; Pfeffer, J.; Rizvi, M. Securing the internet of things (IoT): A security taxonomy for IoT. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 163–168.
55. Greene, S.S. *Security Program and Policies: Principles and Practices*; Pearson Education: London, UK, 2014.
56. Iova, O.; Picco, P.; Istomin, T.; Kiraly, C. Rpl: The routing standard for the internet of things... or is it? *IEEE Commun. Mag.* **2016**, *54*, 16–22.
57. Tiwari, S.; Trivedi, M.C.; Mishra, K.K.; Misra, A.; Kumar, K.K. *Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS-2018*; Springer: Berlin/Heidelberg, Germany, 2018; Vol. 851.
58. Poschmann, A.Y. Lightweight Cryptography: Cryptographic Engineering for a Pervasive World. Ph.D. Thesis, Ruhr University Bochum, Bochum, Germany, 2009.
59. Shirai, T.; Shibutani, K.; Akishita, T.; Moriai, S.; Iwata, T. The 128-bit blockcipher CLEFIA. In *International Workshop on Fast Software Encryption*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 181–195.
60. Tewari, A.; Gupta, B. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *Int. J. Adv. Intell. Paradig.* **2017**, *9*, 111–121.
61. Odelu, V.; Das, A.K. Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography. *Secur. Commun. Netw.* **2016**, *9*, 4048–4059.
62. Mahdavinejad, M.S.; Rezvan, M.; Barekatain, M.; Adibi, P.; Barnaghi, P.; Sheth, A.P. Machine learning for Internet of Things data analysis: A survey. *Digit. Commun. Netw.* **2018**, *4*, 161–175.
63. Hammoudeh, M.; Newman, R. Information extraction from sensor networks using the Watershed transform algorithm. *Inf. Fusion* **2015**, *22*, 39–49.
64. Derguech, W.; Bruke, E.; Curry, E. An autonomic approach to real-time predictive analytics using open data and internet of things. In Proceedings of the 2014 IEEE 11th International Conference on Ubiquitous Intelligence and Computing and 2014 IEEE 11th International Conference on Autonomic and Trusted Computing and 2014 IEEE 14th International Conference on Scalable Computing and Communications and Its Associated Workshops, Bali, Indonesia, 9–12 December 2014; pp. 204–211.
65. Wu, C.H.; Ho, J.M.; Lee, D.T. Travel-time prediction with support vector regression. *IEEE Trans. Intell. Transp. Syst.* **2004**, *5*, 276–281.
66. Hammoudeh, M.; Newman, R.; Dennett, C.; Mount, S. Interpolation techniques for building a continuous map from discrete wireless sensor network data. *Wirel. Commun. Mob. Comput.* **2013**, *13*, 809–827.

67. Hammoudeh, M.; Newman, R.; Dennett, C.; Mount, S.; Aldabbas, O. Map as a service: A framework for visualising and maximising information return from multi-modalwireless sensor networks. *Sensors* **2015**, *15*, 22970–23003.
68. Campello, R.J.; Moulavi, D.; Sander, J. Density-based clustering based on hierarchical density estimates. In *Pacific-Asia Conference on Knowledge Discovery and Data Mining*; Springer: Berlin/Heidelberg, Germany, 2013, pp. 160–172.
69. Wang, C.; Dong, S.; Zhao, X.; Papanastasiou, G.; Zhang, H.; Yang, G. Saliencygan: Deep learning semi-supervised salient object detection in the fog of iot. *IEEE Trans. Ind. Inform.* **2019**, *16*, 2667–2676.
70. Alqahtani, H.; Kavakli-Thorne, M.; Kumar, G. Applications of generative adversarial networks (gans): An updated review. In *Archives of Computational Methods in Engineering*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 1–28.
71. Peixoto, S.A.; Vasconcelos, F.F.; Guimarães, M.T.; Medeiros, A.G.; Rego, P.A.; Neto, A.V.L.; de Albuquerque, V.H.C.; Rebouças Filho, P.P. A high-efficiency energy and storage approach for IoT applications of facial recognition. *Image Vis. Comput.* **2020**, *96*, 103899.
72. Rajesh, S.; Paul, V.; Menon, V.G.; Khosravi, M.R. A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. *Symmetry* **2019**, *11*, 293.
73. Yu, W.; Köse, S. A lightweight masked AES implementation for securing IoT against CPA attacks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2017**, *64*, 2934–2944.
74. Belguith, S.; Kaaniche, N.; Russello, G. PU-ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 924–927.
75. Belguith, S.; Kaaniche, N.; Hammoudeh, M.; Dargahi, T. PROUD: Verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted IoT applications. *Future Gener. Comput. Syst.* **2019**, *111*, 899–918.
76. da Costa, K.A.; Papa, J.P.; Lisboa, C.O.; Munoz, R.; de Albuquerque, V.H.C. Internet of Things: A survey on machine learning-based intrusion detection approaches. *Comput. Netw.* **2019**, *151*, 147–157.
77. Doshi, R.; Apthorpe, N.; Feamster, N. Machine learning ddos detection for consumer internet of things devices. In Proceedings of the 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 24 May 2018; pp. 29–35.
78. Carlin, A.; Hammoudeh, M.; Aldabbas, O. Defence for distributed denial of service attacks in cloud computing. *Procedia Comput. Sci.* **2015**, *73*, 490–497.
79. Carlin, A.; Hammoudeh, M.; Aldabbas, O. Intrusion detection and countermeasure of virtual cloud systems-state of the art and current challenges. *Int. J. Adv. Comput. Sci. Appl.* **2015**, *6*. doi:10.14569/IJACSA.2015.060601.
80. Zhao, S.; Li, W.; Zia, T.; Zomaya, A.Y. A dimension reduction model and classifier for anomaly-based intrusion detection in internet of things. In Proceedings of the 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, USA, 6–10 November 2017; pp. 836–843.
81. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for internet of things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094.
82. Wan, J.; Li, J.; Imran, M.; Li, D. A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Trans. Ind. Informat.* **2019**, *15*, 3652–3660.
83. Lin, C.; He, D.; Huang, X.; Choo, K.; Vasilakos, V. BSeIn: A blockchain-based secure mutual authentication with fine grained access control system for industry 4.0. *J. Netw. Comput. Appl.* **2018**, *116*, 42–52.
84. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2019**, *6*, 2188–2204.
85. Kure, E.; Engelstad, P.; Maharjan, S.; Gjessing, S.; Zhang, Y. Distributed uplink offloading for IoT in 5G heterogeneous networks under private information constraints. *IEEE Internet Things J.* **2019**, *6*, 6151–6164.
86. Ferrag, M.; Maglaras, L.; Argyriou, A.; Kosmanos, D.; Janicke, H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *J. Netw. Comput. Appl.* **2018**, *101*, 55–82.

87. Mhatli, S.; Mrabet, H.; Dayoub, I. Extensive Capacity Simulations of Massive MIMO Channels for 5G Mobile Communication System. In Proceedings of the 2019 2nd International Conference on Computer Applications and Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–6.
88. Mrabet, H. Performance Investigation of New Waveforms in CRAN Architecture for 5G Communication Systems. In Proceedings of the IEEE 2020 3rd International Conference on Computer Applications and Information Security (ICCAIS), Riyadh, Saudi Arabia, 19–21 March 2020, pp. 1–5.