IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 July 2022, accepted 31 August 2022, date of publication 8 September 2022, date of current version 20 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3205351

SURVEY

Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions

MAHMOUD ABBASI[1], (Member, IEEE), MARTA PLAZA-HERNÁNDEZ[1], JAVIER PRIETO[1], (Senior Member, IEEE), AND JUAN M. CORCHADO[1,2,3]

[1]BISITE Research Group, Edificio Multiusos I+D+I, University of Salamanca, 37007 Salamanca, Spain
[2]AIR Institute, IoT Digital Innovation Hub, 47011 Valladolid, Spain
[3]Department of Electronics, Information and Communication, Faculty of Engineering, Osaka Institute of Technology, Osaka 535-8585, Japan

Corresponding author: Mahmoud Abbasi (mahmoudabbasi@usal.es)

This work was supported by the IoTalentum Project within the Framework of Marie Skłodowska-Curie Actions Innovative Training Networks (ITN)-European Training Networks (ETN), which is funded by the European Union Horizon 2020 Research and Innovation Program under Grant 953442.

ABSTRACT Communication systems and networks are evolving as an integral part of not only of our everyday life but also as a part of the industry, fundamental infrastructures, companies, etc. Current directions and concepts, such as the Internet of Things (IoT), promise the enhanced quality of life, greater business opportunities, cost-effective manufacturing, and efficient operation management through ubiquitous connectivity and deployment of smart physical objects. IoT networks can collect, preprocess, and transmit vast amounts of data. A considerable portion of this data is security- and privacy-critical data, which makes IoT networks a tempting option for attackers. Given that these networks deal with the actual aspects of our lives and fundamental infrastructures (e.g. smart grids), security in such networks is crucial. The large scale of these networks and their unique characteristics and complexity bring further vulnerabilities. In this study, we focus on the IoT application layer, security requirements, threats, and countermeasures in this layer, and some of the open issues and future research lines.

INDEX TERMS Internet of Things, security, privacy, requirements, taxonomy.

I. INTRODUCTION

Generally, the Internet of Things (IoT) refers to the growing network of smart-physical devices that can sense and act on their surroundings, pre-process data, communicate, and share data to achieve their ultimate goals [1]. In other words, IoT systems play an active part in different aspects of human life, including daily activities, industry, self-driven cars, retail, healthcare, smart grids, business, farming, etc. The successful implementation of IoT-enabled systems in diverse areas has led to significant growth in the number of connected things. It is forecasted to reach several billion in the upcoming year [2]. Cisco predicts that over 500 billion things (e.g., sensors, actuators, and cars) will be connected to the Internet by the end of 2025. A study by the McKinsey Global Institute reveals an estimated annual economic impact of IoT, and its application areas will be around 3.9 to 11.1 trillion USD worldwide by 2025 [3].

Accordingly, many industries and companies are extending IoT-powered products, services, and solutions to break into and dominate the market [4]. In addition, the main aim of IoT is to transform the way we live and work by developing smart devices and services that carry out our daily tasks. Smart cities, smart agriculture, smart transportation, smart healthcare, smart environment, etc., are some of the ideas introduced in connection with IoT [5].

Despite these promising developments and efforts, there are still several issues hindering the full and practical deployment of IoT in the real world. One of the key challenges that IoT deals with and must be overcome is security [6]. Due to the fact that these systems are increasingly used in diverse aspects, fundamental questions bring up about the security of such systems. Many investigations have provided proof of security and privacy vulnerabilities such as authentication,

The associate editor coordinating the review of this manuscript and approving it for publication was Xiangxue Li.

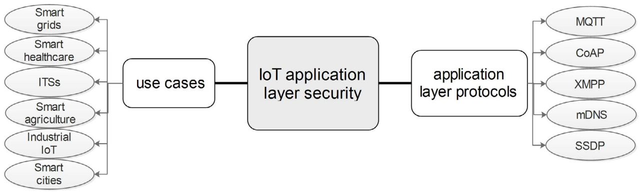

FIGURE 1. Key elements of the IoT application layer.

authorization, Denial-of-Service (DoS) attacks, and information leakage in IoT-powered systems [7], [8], [9]. Indeed, not only the number of IoT security threats are growing, but also their complexity [10].

IoT security has become an overriding concern among research communities, industry, and the public, necessitating further extensive research. To this end, the main aim of this paper is to identify and examine the fundamental security requirements for the IoT application layer and then to understand and categorize security threats in the IoT application layer. Furthermore, the paper analyzes existing security countermeasures at the application layer of IoT.

In the field of IoT security, several survey articles have been published, e.g., [6], [7], [8], [11], [12], [13], [14]. Nevertheless, the lack of clear focus and direction in some of these papers is evident, especially those related to the IoT application layer. In other words, few studies have been carried out to individually examine IoT layers' security aspects. In an attempt to fill this critical gap and in response to concerns about the security of the IoT application layer, our main objective is to investigate a structural survey of the security of the application layer by presenting the major security requirements, threats, and existing solutions. Also, open issues and future research lines are provided. The primary contributions of our paper are as follows:

- We examined the surveys that reviewed the security of the IoT application layer and then highlighted its advantages and limitations.
- We identified and represented the main security requirements of the IoT application layer. Moreover, these security requirements are categorized based on IoT use cases and protocols.
- We introduced the key security threats and the countermeasure for those threats in the IoT application layer for both IoT use cases and protocols (see Fig. 1).
- Finally, we discussed open challenges and future research lines of the IoT application layer's security.

The rest of the paper is structured as follows: Section II provides the background to our study and its motivation. Related published surveys are reviewed and discussed in Section III. Section IV investigates the key security requirements in the IoT application layer. The provided classification, security threats, and potential solutions for the IoT application layer are discussed in Section V. Section VI illustrates the challenges and future research directions. Finally, our paper is concluded in Section VII.

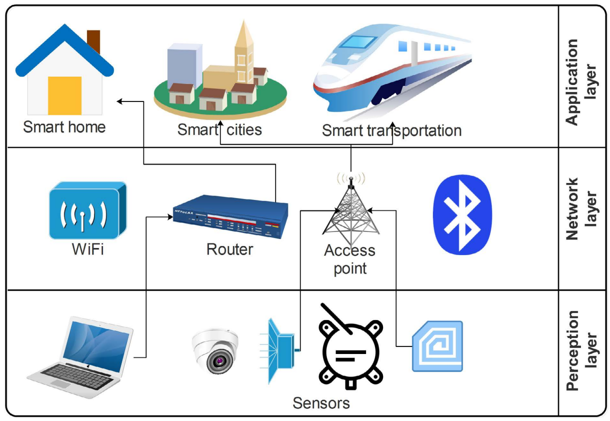

FIGURE 2. Three-layer IoT architecture.

II. BACKGROUND AND MOTIVATION

IoT can be described as a computing and communication concept focusing on the interconnection between things and/or between things and people. Kevin Ashton firstly presented the IoT paradigm in 1998. In an IoT network, it is possible to have various heterogeneous devices and communication protocols to gather and interchange data with other nodes in the network [15].

The definition of the most adopted IoT architectures and the description of the IoT layers and their functions is essential to understanding IoT networks. Research communities and industries have introduced multiple IoT architectures. Broadly speaking, IoT architectures can fall into three main [16]:

1) Three-layer architecture: It is the most common architecture introduced for IoT networks [17]. As the name indicates, there are three layers in this architecture, including the application layer, the network layer, and the perception layer.
2) Four-layer architecture: This IoT architecture model is roughly similar to the three-layer architecture, except that it has an extra layer, the data processing layer.
3) Five-layer architecture: Compared to the three-layer architecture, this one includes two additional layers, the business layer and the data processing layer.

In this study, the three-layer architecture is used as a reference for the definition of the IoT layers and their tasks, as this architecture is the most common architecture for IoT (see Fig. 2). Furthermore, our central focus is on the IoT application layer to narrow the search and investigate the topic as carefully as possible.

A. APPLICATION LAYER

This layer is designed as the top layer in the IoT architecture [18]. The application layer accepts the network-level data from the middle layer and uses this data to deliver desired services and/or operations. For example, the application layer can provide the data analysis service to find valuable details for forecasting the condition of physical devices.

B. NETWORK LAYER

It is designed as the middle layer in the three-layer IoT architecture. It is also named the transmission layer [19]. One of its major functions is to route the pre-processed data supplied by the perception layer. In other words, this layer sends the data to the IoT devices, services, etc., through the communication network. The network layer consists of various components, such as different devices (e.g., gateway, hub, and cloud) and different communication protocols (e.g., WiFi and cellular network) [20].

C. PERCEPTION LAYER

The sensor layer is another name for this IoT layer [21]. The perception layer is implemented as the bottom layer in the three-layer IoT architecture. It is capable of interacting with physical objects and entities in an IoT network via smart devices such as Radio Frequency Identification (RFID) tags and various sensors.

As mentioned, IoT security is crucial. This is mainly due to the fact that there is a growing number of IoT devices integrated into security- and safety-critical services and applications, such as smart cities, industrial automation, e-health, and smart mobility [7]. Moreover, IoT devices are capable of collecting, pre-processing, and transmitting security-critical and sensitive private data; hence, they are vulnerable targets for various intruders [22], [23]. Accordingly, to offer the greater and safe functionality of IoT systems, it is vital to strengthen the security of the underlying components, especially their protocols, devices, and data, against adversary agents [24]. Compared with the traditional communication systems, IoT systems are more prone to security attacks due to [12], [25]:

- Most IoT networks adopt wireless protocols for communications (e.g., WiFi and Sigfox), where malicious actors could obtain confidential data by eavesdropping on the wireless channel [26].
- Most IoT devices are resource-constrained in terms of power, storage, computation, and memory. Hence, they cannot support complex security mechanisms [27].
- The ever-increasing complexity and heterogeneity of IoT systems also complicate the security issues faced by such systems [28].
- Most IoT systems use centralized data management approaches (e.g. cloud and local servers). These centralized approaches make the overall system vulnerable because of single point of failure and probability of security attacks [29].

Motivated by the importance of IoT security, especially the IoT application layer, as well as the lack of a comprehensive survey on the IoT application layer's security, we try to fill the gap by providing an extensive survey on this topic. The research gap will be discussed further in the following sections.

As mentioned, this paper considers the three-layer IoT architecture. The paper's primary focus is on the application layer and providing a taxonomy of security requirements, security threats, and potential solutions. To achieve the aims of our study, the security of the IoT application layer is investigated from two different points of view, including IoT use cases and IoT application layer protocols. These are discussed in more detail in Sections IV and V.

In the next section, we review the surveys and papers related to the security of the IoT application layer and highlight their contributions and limitations.

III. RECENT SURVEYS ON THE SECURITY OF THE IoT APPLICATION LAYER

A number of papers reviewed the security aspects of IoT, e.g., [8], [23], [30], [31]. There are also some papers in the literature that focus on the security aspects of a specific IoT layer, e.g., physical layer [32], [33], perception layer [34], [35], and network layer [36], [37], or some papers investigate IoT security from a technological point of view, e.g., blockchain [38], [39], machine learning [40], [41], and network virtualization [42], [43]. Nevertheless, a limited body of literature focuses on IoT security from the point of view of the *application layer*. This section provides an overview of the existing work that discusses IoT application layer security and compares them with our study.

Maybe the most relevant paper to our study is [44]. In this paper, the authors surveyed the security of the IoT application layer. The paper mainly discussed the challenges of conventional security measures, such as authentication, key management, and cryptography. However, this work differs from our survey because it did not provide any specific classification for investigating security challenges and relevant solutions in the IoT application layer. Furthermore, this survey did not discuss the security of the IoT use cases, and their discussion on IoT application protocols is limited to the commonly used protocols, such as AMQP, MQTT, and XMPP.

In [45] Nebbione *et al.* conducted an in-depth survey on the IoT application layer protocols. More specifically, they investigated the most widespread IoI application layer protocols and their security threats. Nevertheless, the paper did not cover the security of IoT use cases, e.g., smart cities and smart grids, as an important aspect of the IoT application layer.

Similar studies have been performed in [46], [47], [48], and [49]. The authors provided a brief overview of IoT application protocols and their security vulnerabilities in these papers without considering potential solutions. The papers did not cover any security aspects regarding the IoT use cases. In addition, the studies only investigated a limited number of IoT application protocols.

The authors in [50] reviewed conventional and recent advances in the application layer protocols of IoT systems and the importance of the application layer protocols in IoT use cases, such as Industrial IoT, healthcare, and smart cities. Moreover, they discussed machine learning as a solution for the dynamicity and intelligence of the IoT application layer protocols. However, their review did not cover security requirements, threats, and potential solutions.

The authors in [51] provided a detailed survey of IoT security based on a five-layer IoT architecture, including physical, network, transport, application, and data/cloud service layers. Considering the fact that the authors had to overview all the five layers, they barely investigated the IoT application layer, especially the key security requirements and attacks.

Rizvi *et al.* [52] discussed the security requirements and challenges that IoT faces in the different layers, including perception, application, and network layers. Given trust in IoT systems, the authors referred to privacy, availability, and reliability as the primary security classes. However, the authors did not provide enough detailed information concerning security requirements in each layer, potential countermeasures, and security of the IoT use cases.

Tripathi *et al.* [53] reviewed the existing application layer DoS attacks and defense actions. In this paper, attacks against IoT application layer protocols are identified, discussed and classified. Moreover, the authors compared the existing defense mechanisms based on relevant factors.

Rahman *et al.* [54] conducted a brief survey on the IoT application layer protocols' security, focusing on the CoAP protocol. Moreover, the authors discussed solutions to these security challenges, such as adopting compressing mechanisms and key management processes.

The authors in [55] introduced IoT and its different layers. Then, they discussed security in IoT based on a three-layered architecture, including perception, middleware, and application layer. Moreover, they investigated the IoT's protocol stack (e.g., 6LoWPAN and IEEE 802.15.4) and security requirements for these protocols. Despite these positive points, the authors did not cover the IoT application layer's security, including use cases and application protocols, in enough detail as they focused on all three layers.

In Table 1, a summary of the reviewed papers is provided based on their contributions and focus, i.e., IoT use cases or application protocols.

To the best of our knowledge, most of the existing surveys of the IoT application layer's security do not fully cover fundamental aspects of this layer, i.e., IoT uses cases and IoT application layer protocols. Compared to the existing survey papers, the main aim of our paper is to give a comprehensive view of the security of the IoT application layer. To this end, the following section answers the following question:

What are the fundamental security requirements of the IoT application layer regarding IoT use cases and IoT application layer protocols?

IV. SECURITY REQUIREMENTS OF THE IoT APPLICATION LAYER

Before introducing the security threats of the IoT application layer, it is important to discuss the security requirements that this layer must fulfill for the correct operation of the IoT systems. Failure to comply with a security requirement may bring security challenges to the system. The key security requirements in the IoT application layer are listed below. These requirements have been identified through careful investigation of the papers related to the security of IoT use cases and the security of IoT application protocols [56], [57], [58], [59], [60], [61], [62], [63], [64] (see Fig. 3).

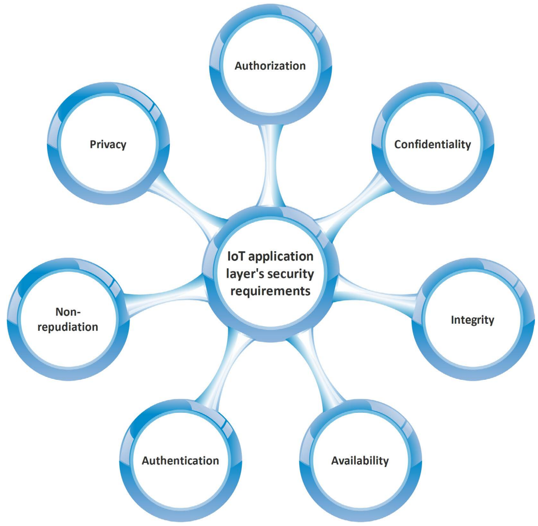

FIGURE 3. Key security requirements of the IoT application layer.

To find related papers on the topic, different keywords have been used, including "security and IoT," "security and IoT application layer," "security and IoT application layer protocols", "privacy and security and IoT application layer," "privacy and security and IoT application layer protocols," etc. We searched well-known digital libraries and academic publishers, including IEEE, Elsevier, ScienceDirect, ACM, Springer, MDPI, etc., to download the literature for our work. Moreover, for each IoT use case and IoT application layer protocol discussed in this paper, we went through the same process to find the related literature.

A. CONFIDENTIALITY

When a communication system deals with private/sensitive information, confidentiality is a critical security requirement that needs to be satisfied [65]. Confidentiality refers to protecting information from unauthorized access or those who are not allowed to view it [14]. Confidentiality may also refer to preserving the IoT devices and equipment from unauthorized access.

Confidentiality protection is challenging when considering the IoT use cases due to the different involved devices and components [66]. For example, an Intelligent Transportation System (ITS) has various devices such as smartphones, vehicles, roadside stations, cameras, and sensors. In some IoT use cases (e.g., IIoT and smart grids), the lack of confidentiality countermeasures can lead to the loss of customer and vendors' data and intellectual property such as trade secrets [67].

Confidentiality, especially confidentiality of transmissions/communications, is also an essential security requirement in IoT application layer protocols [68]. To this end, many IoT application layer protocols try to preserve

TABLE 1. An overview of existing literature surveys on IoT application layer security. (✔: The paper investigated the determining factor; ⊕: The paper partially covered that factor; ✖: The papers did not consider that factor.)

Study	Year	Contribution and focus	IoT use cases	IoT application protocols	Identified requirements
[54]	2016	Provides a security analysis of IoT protocols and potential solutions, with a focus on the CoAP protocols	✖	⊕	Confidentiality Integrity Authentication
[46]	2017	Giving a brief overview of the IoT application layer protocols' security	✖	⊕	N/A
[47]	2017	Provides a short overview of the IoT application layer protocols' security, with a focus on MQTT protocol	✖	⊕	Confidentiality Integrity Availability
[52]	2018	Given a three-layered architecture, conducts a brief survey of IoT layers' security	✖	✖	Privacy Availability Reliability
[48]	2019	Focusing on the IoT application layer protocols, their security, and potential solutions	✖	⊕	N/A
[51]	2020	Providing an overview of the IoT security based on a five-layered architecture	✖	⊕	Confidentiality Integrity Access control Authentication Secure communication Encryption protocols
[45]	2020	Discussing the security of the IoT application layer protocols and solutions	✖	✔	Confidentiality Integrity Authenticity Authorization
[49]	2020	A general discussion on the IoT application layer's security and some solutions	✖	✖	N/A
[55]	2020	Investigation the security of IoT on the basis of a three-layered architecture	✖	⊕	Authentication Identification Privacy Data management
[44]	2021	Providing a review on privacy and security of the IoT application layer	✖	⊕	Confidentiality Integrity Authenticity Authorization Availability
[50]	2021	Provides a review of traditional and recent advances in the IoT application layer protocols	✖	✖	Confidentiality Integrity Availability Authentication Privacy
[53]	2021	Provides an overview of application layer DoS attacks and potential solutions	✖	✖	N/A
[Our work]	2022	Conducting a comprehensive review of the IoT application layer's security, including IoT use cases and application protocols. The review covers IoT application layer's security requirements, threats, and potential solutions	✔	✔	Confidentiality Integrity Availability Authentication Authorization Non-repudiation Privacy

confidentiality through built-in mechanisms, such as Transport Layer Security (TLS) and Data TLS (DTLS) protocols [69]. The lack of appropriate confidentiality measures by IoT application layer protocols can cause the disclosure of sensitive information by attackers.

As described in the next section, several security attacks can threaten the confidentiality of an IoT application layer by disclosing information.

B. INTEGRITY

Data/message integrity means that a message was not changed over its life cycle (i.e., between sending and receiving). In other words, it refers to data's consistency, accuracy, and validity over workflow [70]. In IoT systems, integrity can safeguard the system against the unapproved spread, destruction, or changing of messages.

In IoT use cases, it is essential to ensure the integrity of communication and computation between different system entities, such as various sensors, actuators, controllers, human agents, etc. This is mainly due to the fact that these entities can collect massive amounts of important data. For example, in a smart agriculture scenario, many IoT sensors and smart meters capture different types of data, e.g., humidity, temperature, and water data [71]. The altering of this data can lead to severe damage to other involved operations, e.g., changes in the pH of agricultural water and the applied nutrient solution for plants. In another instance, the lack of data integrity in the industrial automation scenario can lead to damaging consequences, such as hiding and altering crucial details related to the safety parameters of industrial machinery or standards, degradation of product quality, and industrial machinery breakdown [72].

In IoT application layer protocols, messages, and communication integrity are paramount. Hence, built-in plugins and additional mechanisms are deployed to preserve the integrity [73].

C. AVAILABILITY

Availability is vital in IoT systems and guarantees that service and network continue to operate even in the presence of faults or malicious activities [74]. For availability, not only security is required but also a fault management process (i.e., fault detection, isolation, and then correction of the abnormal condition of the network).

For IoT systems, especially safety- and mission-critical IoT systems, such as smart grids and ITS, it is vital to guarantee the availability of the systems since these systems deal with the safety of the users and the real-time functional requirements. For example, to guarantee the safety of passengers, ITS's involved devices need to be able to operate and communicate with each other [75]. The forecasting of potential bottlenecks and providing bandwidth need to be considered. In the context of IoT application layer protocols, the availability of nodes and the environment are important and can be compromised by various threats [45].

D. AUTHENTICATION AND AUTHORIZATION

This is one of the principal requirements for any communication system and ensures that the right users (e.g., patients and physicians in a smart healthcare system) or devices (e.g., nodes and aggregators) can get access to the resources or take certain actions, and the services provided by an IoT network [76]. For example, granting access to electronic health records and patient records. In the vast majority of IoT applications, e.g., in vehicular networks and ITSs, the authentication of all users and messages is critical as it can prevent serious security threats such as Sybil attacks [77].

Considering IoT application layer protocols, authentication/authorization is a key security requirement as there are various authorization-related vulnerabilities. Accordingly, some application layer protocols use built-in authorization services, and some deploy custom solutions for authentication [78]. We will discuss these solutions in the next section in more detail.

E. NON-REPUDIATION

In communication systems and networks, non-repudiation refers to the assurance that any entity participating in communication can not deny having been involved in all or part of a communication event. Satisfying non-repudiation guards IoT systems against false denials related to communication [79]. The primary objective of non-repudiation is to handle disputes about an event's happening or not happening. This can be done through gathering, maintaining, making available, and confirming indisputable evidence about the declared event [80]. Non-repudiation is an essential security requirement for ITSs, especially in VANETs and V2V communications. This is mainly because non-repudiation can protect communications from false denial activities [81]. The loss of event data can lead to security risks against non-repudiation.

F. PRIVACY

Based on [82], the definition of privacy in IoT environments is: "privacy is a term related to persons, and their data, especially personal or sensitive data, which emphasizes the need to protect data should not be exploited, accessed without the permission of the owner, or used in a way that the owner doesn't expect". Privacy in IoT systems is paramount because, in such systems, many devices are connected to the Internet to send data to other devices and/or communication systems. This data can be personal raw or sensitive data that should not be exposed to a third party. For example, one can refer to the mobility data in VANETs and V2V communications. Given the IoT application layer, the attackers in this layer can destroy privacy through a known vulnerability, such as cross-site scripting attacks and buffer overflow [83].

In the next section, we will introduce security threats that can compromise the above-mentioned security requirements. Moreover, different potential countermeasures to prevent and mitigate security threats are reviewed.

V. SECURITY THREATS AND SOLUTIONS IN THE IoT APPLICATION LAYER

The security of the IoT application layer, i.e., IoT applications and application layer protocols, is an integral part of the system design. IoT application layer protocols are the foundation for communications among various IoT use cases, devices, and running services. In other words, IoT application layer protocols serve as an interface between the IoT use cases and end-users [84]. Hence, considering the vital role of the application layer in all of the IoT use cases, security at this layer is crucial. The intruders in the IoT application layer are probably going to disturb security through different attacks, such as injection attacks, unauthorized access, cross-site scripting attacks, etc., [85].

A. FOCUSING ON THE IoT USE CASES

Following extensive review and analysis, we have identified six crucial IoT applications: smart grids, smart healthcare, ITS, smart agriculture, IIoT, and smart cities. In the following sections, we discuss the security aspects of these applications.

1) SMART GRIDS

The main security goals in smart grids are confidentiality, integrity, and availability [86]. Concerning these security requirements, one can refer to the following security threats.

a: THREATS

Several types of attacks target *confidentiality* in smart grids, including password-pilfering attacks, traffic analysis attacks, eavesdropping attacks, unauthorized access, false data injection attacks, and password theft attacks. The main objective of these attacks is to gain the desired information [87]. Another group of attacks tries to destroy the *integrity* of smart grids, such as data tampering attacks, wormhole attacks, data injection attacks, spoofing attacks, data manipulation attacks, man-in-the-middle attacks, and masquerading attacks [56]. The main goal of these attacks is to change the original data payload. The *availability* of smart grids can also be endangered through the availability-related attacks, such as jamming, wormhole, DoS attacks (e.g., teardrop, LDoS, puppet, and smurf), buffer overflow, masquerading, man-in-the-middle attacks, and spoofing attacks [88].

In addition, using monitoring technologies such as Advanced Metering Infrastructure (AMI) may cause privacy violation risks for users (privacy issues) [57]. For example, extracting habitual information patterns by adversaries or disseminating industrial information. Moreover, the massive number of deployed devices and the heterogeneity of devices can raise key scalability issues for security providing.

b: SOLUTIONS

To deal with the security threats that target the *confidentiality* of smart grids, several methods have been proposed [89]. For example, one can use data encryption against password theft attacks [90]. Deploying authentication mechanisms can prevent eavesdropping attacks, unauthorized access, and false data injection attacks. Moreover, using encryption protocols can prevent traffic analysis attacks. To cope with data integrity attacks, some solutions have been introduced. Cryptography techniques, algorithms, and authenticity are among the most used methods to prevent attacks on data *integrity* attacks [91]. Moreover, methods such as power fingerprinting techniques, strategies based on trusted network connect, and volt-var control algorithms have also been developed [92]. Using security gateways to encrypt the traffic can be a remedy for man-in-the-middle attacks. In addition, end-to-end encryption and authentication mechanisms are crucial to reducing the consequences of the data injection attack, spoofing attacks, and data manipulation attack. The following measures have been taken to cope with the *availability* attacks. For mitigation of DoS attacks, traffic filtering technologies, anomaly detection methods, and air gapping are promising solutions [93]. Given jamming attacks, anti-jamming techniques can be adopted, such as [94].

2) SMART HEALTHCARE

Regarding the applications of IoT in healthcare, there are serious security concerns [95]. More specifically, when it comes to security, the key requirements are confidentiality, integrity, authentication, authorization, and non-repudiation.

a: THREATS

Data *confidentiality* in smart healthcare systems can be endangered through unauthorized users and eavesdropping attacks [96]. Furthermore, adversary users and accidental communication mistakes can destroy data *integrity* in such systems during data transmission.

In the smart health systems, the *authenticity* of the users (e.g., patient and physicians) and devices (e.g., nodes and aggregators) should be ensured in order to prevent from masquerading attacks against electronic health records and patient health records [97]. Moreover, authorization ensures that the right users (e.g., patients and physicians) or devices can access electronic health records and patient health records.

Besides the challenges related to security, wearable devices in smart health systems can be used for measuring data about blood pressure, temperature, heart rate, blood sugar, etc., [98]. This data is usually stored in a cloud server as Personal Health Record (PHR) for further processing and analysis by physicians. As this data is vital and personal, privacy concern is the most critical security issue in healthcare-related IoT applications.

Some literature also refers to *data freshness* as a security requirement in smart healthcare [99]. Repeat/replay attacks are among the often mentioned challenges to data freshness.

b: SOLUTIONS

Using cipher algorithms for data encryption is a remedy to the security challenges arising from *confidentiality*. Considering the security challenges related to data *integrity*, ensuring data integrity through cryptography algorithms such as AES128/256 and SHA is a solution [58].

Different authentication mechanisms should be utilized to deal with *authentication* security challenges, such as digital signatures and key-based and certificate-based authentication. Additionally, to ensure *authorization* in a smart healthcare system, the access control mechanisms should be used to define the right access for each user in the system. Moreover, to address the privacy-related issues in smart healthcare applications, developing secure access control approaches for wearables and PHR should be considered [100]. Furthermore, as PHRs are stored in cloud servers, using cryptographic primitives to improve the authentication protocols of PHRs is possible [101]. When one accesses the information in healthcare systems, the authentication mechanisms should be human-machine authentication, while for updating the collected data in the server, machine-machine authentication works.

One of the ways to mitigate repeat/replay attacks is to assure *data freshness* by verifying the data collected from the devices (e.g., sensors). The verification can be done by looking at different factors, such as up-to-date data, non-duplication data, and the order of data.

3) SMART TRANSPORTATION SYSTEMS (ITS)

The key security requirements in ITSs are confidentiality, integrity, availability, authentication/identification, and non-repudiation [65], [102]. Indeed, the different security threats in ITSs can be classified from the point of view of the security requirements.

a: THREATS

Confidentiality protection in ITSs is challenging because there are different types of devices in an ITS, such as smartphones, vehicles, roadside stations, and IoT devices. Hence, a wide range of attacks against the involved devices can destroy confidentiality. These attacks are man-in-the-middle attacks, eavesdropping attacks, model identification attacks against machine learning techniques, and parameter inference attacks against controllers [103]. Moreover, in ITSs, it is crucially important to ensure data *integrity* regarding communication and computation between different system devices, such as vehicles, traffic controllers, and roadside infrastructures. There are various potential security risks against data integrity in ITSs, including spoofing attacks, timing attacks [104], Sybil attacks, man-in-the-middle attacks, attacks against machine learning with adversarial examples, data poisoning, and policy manipulation attacks.

To guarantee the safety of passengers, ITS's involved devices must be able to operate and communicate with each other. Different attacks can restrict the *availability* of devices in ITS, such as DoS, spoofing attack, timing attack, jamming attack, man-in-the-middle attack, policy manipulation attacks, and data poisoning [59]. Regarding *authentication/identification*, it is vital for an ITS to correctly identify and authenticate the users who want to participate in the communication and data transmission [105]. This is because many security threats are posed through different types of attacks, including spoofing, timing attack, Sybil attacks, and man-in-the-middle attack.

Non-repudiation is an essential security requirement for ITSs, especially in VANETs and V2V communications. This is mainly due to the fact that non-repudiation can protect communications from false denial activities [106]. The loss of event data can lead to security risks against non-repudiation. Last but not least, mobility is another security challenge in ITS applications [107]. The mobility of the entities in ITSs poses challenges to deploying security solutions.

b: SOLUTIONS

To alleviate *confidentiality-related* security challenges, a couple of techniques have been proposed, including symmetric cryptography, asymmetric cryptography, and a secure steganographic algorithm [108]. Each of them has its pros and cons. When considering data *integrity*, Message Authentication Code (MAC) is one of the main approaches to ensure data integrity in ITSs [109]. However, using this technique can cause additional computational overhead.

To cope with the *availability-related* security challenges, signature-based authentication techniques have been proposed [60]. The most important problem with this method is that it needs additional infrastructure. In addition, challenge-response protocols and message authentication codes are provided for security challenges related to *authentication* and *identification*. These methods can pose overhead in terms of time and computation. And finally, to tackle security issues related to *non-repudiation*, digital signatures and signature-based authentication are among the most used techniques [110].

4) SMART AGRICULTURE

One can classify the security risks in smart agriculture into five main sub-categories: threats against privacy, authentication, data confidentiality and integrity, and availability.

a: THREATS

In smart agriculture applications, many IoT sensors and smart meters collect different types of data, e.g., humidity, temperature, and water quality monitoring [61]. The collected data is sensitive as the analysis of this data can disclose valuable information (e.g., the applied nutrient solution for plants and the locations of sensors) to a third party. Hence, it is essential to preserve this *private information* from unauthorized access and security threats such as insider data leakage and cloud data leakage. As for *authentication-related* security challenges, a malicious user (or program) tries to forge an identity in order to enter the system as an authorized node [111]. To this end, the malicious actor may carry out different attacks, such as impersonation, spoofing, replay attack, and masquerade attack.

When it comes to data *confidentiality*, the main goal of an attacker is to stand in an ideal place to eavesdrop on the communication between IoT devices or IoT devices with an access point. There are different types of eavesdropping attacks in smart agriculture, including brute-force attacks, tracing attacks, known-key distinguishing attacks, and false data injection attacks [112]. As the name implies, the main goal of the attacks against *availability* is for services to become unavailable in a smart agriculture system. DoS and jamming attacks are the main types of threats in this category [113].

Smart agriculture systems are also subjected to data *integrity* attacks [114]. This attack lets unauthorized entities access and modify sensitive information, such as the pH of agricultural water. This category includes man-in-the-middle attacks, forgery attacks, biometric attacks, and Trojan attacks.

b: SOLUTIONS

Different solutions have been proposed to deal with *privacy-related* challenges, including privacy-preserving techniques during the data aggregation process in a smart agriculture system [115], location privacy solutions [116], content-oriented protection [117], data anonymization techniques, and privacy-preserving trust evaluation methods. To reduce the threats related to data *integrity*, some solutions have been proposed, such as label-based access control technique [118], content integrity verification [119], and message authentication codes [120].

To provide *authentication*, different solutions have been proposed. For example, RFID authentication methods alleviate the situation when one uses RFID tags in smart agriculture [121], delegated authentication, label-based access control, and blockchain-based access control [122].

Access control algorithms based on cipher text is one of the solutions to preserve *confidentiality* in smart agriculture [123]. Moreover, blockchain-based access control mechanisms can be adopted in smart agriculture systems.

5) INDUSTRIAL IoT (IIoT)

According to [62], the main security requirements in IIoT are authentication, data/traffic flow confidentiality, integrity, and availability.

a: THREATS

In IIoT, *authentication* is an important security requirement to preserve the legality of data access and, consequently, to guarantee data confidentiality. False data injection and spoofing attacks can be launched in an IIoT system with an ineffective authentication mechanism. These types of attacks can inject adversarial code and commands into the system [124] for different purposes, such as controlling industrial machinery and performing unsafe operations.

In the context of IIoT systems, *confidentiality* refers to ensuring data/traffic flow access only by authorized entities. The lack of confidentiality measures in an industrial system can lead to losing customers' and vendors' data and intellectual property such as trade secrets. Malware is one of the security attacks that can threaten the confidentiality of an IIoT system through the disclosure of information. Furthermore, in IIoT, there is a possibility that a malicious entity (e.g., man-in-the-middle, malware, and worms) manipulates data without detection and consequently destroys the *integrity* of data [125]. The lack of data integrity in an industrial environment can lead to damaging consequences, such as hiding and altering crucial details related to the safety parameters of industrial pieces of machinery or standards, degradation of product quality, and industrial machinery breakdown.

Security threats may also focus on the *availability* of industrial systems to make them unable to do their typical tasks through overloading [63]. Different types of physical and cyber-attacks can threaten the availability of an IIoT system, such as DoS attacks, DDoS attacks, Mirai botnet, BrickerBot, and Reaper.

b: SOLUTIONS

To deal with security challenges in IIoT systems that threaten *authentication*, different authentication techniques have been adopted, including trust-based authentication, proximity-based authentication [126], and edge-assisted device authentication [127]. Moreover, using authentication and verification methods, such as user key sets, digital signatures, and certificates, can mitigate security risks related to unauthorized access to the system [128].

Applying cryptographic techniques is one of the common countermeasures for *confidentiality*- and *integrity-related* attacks in IIoT systems [129]. Moreover, the security of cloud computing and big data components, third parties, and vendors should be considered [130].

When considering the *integrity* of IIoT systems, one of the proposed solutions is to use Manufacturing Security Enforcement Device (MSED) for encryption [64]. In addition, using control and report filters after sensors, defining secure data exchange channels between IoT devices, IoT devices authorization through digital certificates/Public Key Infrastructure (PKI), and data monitoring to identify possible unauthorized modifications.

The key measure to increase the *availability* of IIoT systems is to protect these systems against DoS attacks. To this end, various approaches have been proposed, such as Software Defined Networks (SDN)-based and distributed approaches and the real-time availability monitoring of IoT devices [131].

6) SMART CITIES

Due to the wide range of deployed sensory devices (e.g., cameras, temperature sensors, noise level sensors, flood detectors, etc.), heterogeneity, and Big Data content gathered, it is challenging to provide security for all the use cases in smart cities [132]. Indeed, different security threats may make against different architecture levels (e.g., physical, network, database, and application layers) and smart city applications (e.g., smart living, smart environment, and smart energy).

a: THREATS

As we mentioned, various security threats may occur in the smart city applications, including:

1) DoS attacks: As the name implies, the main aim of DoS attacks is to make the system resources or services unavailable to the potential users in smart city applications. DoS attacks can target the network layer or application layer [133]. Both classes of DoS attacks may have damaging effects on smart city applications that offer monitoring services in a centralized manner.
2) Malware: this type of threat refers to the attack by a software program that can perform unauthorized actions (e.g., illegal access, stealing or changing information) on the infected system [134]. In smart cities, the CCTV system is a prime example, in which malware can access the system and view privacy and security-sensitive contexts, such as an individual's home or bank.
3) Eavesdropping attack: eavesdropping is an example of a passive attack in which an attacker tries to listen to unsecured communications between two or several parties to access data. Given the smart cities, eavesdropping is a serious threat as it can compromise the integrity and confidentiality of the system [135].
4) Masquerade attack: refers to the situation where a malicious actor can get unauthorized access to the system and steal information through a fake identity (e.g., device or entity) [136]. For example, in smart

transportation, this type of attack can cause the disclosing of restricted information and, consequently, destroy the integrity of the system or change the information in the system.

5) Disinformation attack: In this type of attack, the attacker intentionally disseminates false data (e.g., sensor reading data) intending to affect the result or mislead the behavior of the system's users. In smart cities, disinformation attacks can lead to consequences ranging from delays to unnecessary congestion [137].
6) Message modification attack: In this attack, an intruder tries to change the message header (e.g., changing the message destination) or data (e.g., putting malicious content) in order to cause unexpected behaviors in system performance [138]. Message modification attacks may also lead to delays and congestion in the system and compromise data integrity in smart city applications.
7) Traffic analysis attack: In a traffic analysis attack, a malicious may monitor and analyze the network traffic in order to find the existing patterns (e.g., when a specific user sleeps/wakes up), metadata (e.g., when/how packets were transmitted) and useful information [139]. Traffic analysis is a passive type of attack which can threaten information confidentiality in smart cities.
8) Privacy-related issues: Smart city applications can raise several privacy concerns, including information on lifestyle and routine extracted from CCTV systems and identity and location of the passengers derived from smart transportation systems.

b: SOLUTIONS

Given the security threats facing smart city applications, multiple solutions and technologies have been proposed, including Blockchain [140], cryptography techniques [141], biometrics, machine learning-based techniques [142], and the introduction of regulations for IoT systems. In addition, to cope with privacy-related threats in smart cities, a couple of approaches can be used, such as access control techniques [143], encryption algorithms [144], and anonymization [145]. Nevertheless, most of these countermeasures are adopted to overcome outsider intruders. However, some potential insider intruders (e.g., in a monitoring system, an employee who accesses the captured videos) also need to be considered.

B. FOCUSING ON THE PROTOCOLS OF THE IoT APPLICATION LAYER

Broadly speaking, there are two major classes of IoT application layer protocols: 1) message passing protocols and 2) service discovery protocols [48]. More specifically, by messaging, we mean data sharing and data exchange among devices, while service discovery refers to the process such as device detection and services being offered on the network. Messaging protocols usually provide standard and custom security services, such as encryption mechanisms (e.g., data confidentiality is supported through TLS and DTLS cryptographic protocols, Simple Authentication and Security Layer (SASL) framework has been used as a basis for authentication and authorization mechanisms) [146], while built-in security services are not offered in service discovery protocols.

Despite these security mechanisms, security shortcomings in the design of the application layer protocols need to be investigated. Moreover, it is worth mentioning that security services are not mandatory and must be explicitly enabled by protocol developers. Furthermore, we explore each application protocol's security challenges and related solutions. In the following, we discuss the security aspects of the most essential IoT application layer protocols identified during the study of the associated papers.

1) MESSAGE QUEUING TELEMETRY TRANSPORT (MQTT)

MQTT is a lightweight message passing protocol developed to let many devices send data in a network [147]. MQTT uses a publish/subscribe mechanism and a server (also called the broker). This makes it feasible to reliably publish messages over networks with low bandwidth. MQTT is a de facto standard protocol for IoT messaging. In the first years of its release, MQTT was used as a proprietary protocol by the oil and gas industries to facilitate communication in SCADA systems. Nowadays, MQTT has become a popular open source protocol for connecting millions of IoT and industrial IoT devices used in different applications, such as remote monitoring, health parameters monitoring, and motion detection.

MQTT protocol provides different authentication mechanisms and encryption techniques based on TLS. However, these security services cannot adequately protect the security of the devices that use the MQTT protocol and the MQTT broker [148]. Accordingly, the following security vulnerabilities can be defined in the MQTT-enabled clients.

a: THREATS

1) Authentication vulnerabilities: If the MQTT broker does not conduct a proper examination of the identity of the publisher/subscriber and does not block multiple authentication attempts, the attackers can take advantage of these vulnerabilities to access MQTT-devices or run DoS attacks against the broker [149].
2) Authorization vulnerabilities: The MQTT broker may not appropriately assign publishing and subscribing permissions for clients (i.e., devices). Due to this vulnerability, a malicious agent can take control of the data and functions of MQTT-enabled devices.
3) Message delivery failures: The messages have been sent by a publisher and not delivered due to the lack of subscribers. This failure can significantly affect the proper performance of the broker.
4) Message integrity: The integrity of messages sent by a publisher cannot be properly checked by the broker and

subscribers [150]. Attackers can utilize this security exposure to launch many attacks.

b: SOLUTIONS
To alleviate security challenges related to the MQTT protocol, some approaches have been proposed, including [151]:

1) Client (i.e., devices) authentication.
2) Authorization client's access to the server resources.
3) Privacy-preserving mechanisms for MQTT control packets and application messages.
4) Integrity checking mechanisms for MQTT control packets and application messages.

2) CONSTRAINED APPLICATION PROTOCOL (CoAP)
CoAP is designed to work with constrained nodes (e.g., IoT devices) and networks (e.g., building automation). CoAP is a client-server protocol in which a CoAP-enabled node (or client) can command another client by transmitting a CoAP packet [54]. One of the biggest advantages of CoAP is the ability to allow resource-constrained devices to join an IoT network, even via networks with constrained resources such as low bandwidth and low network availability. CoAP has been mainly adopted in Machine-to-Machine (M2M) use cases, such as smart homes, smart energy, and building automation.

a: THREATS
CoAP gives the possibility to use DTLS as a separate layer, providing some security capabilities. DTLS for CoAP provides four different security modes that developers can select on the basis of different factors, such as security requirements, energy consumption, and performance. Despite using a security protocol (i.e., DTLS) on another layer, the lack of proper security mechanisms can lead to security risks for the CoAP-enabled devices, such as man-in-the-middle attacks. Accordingly, the following security vulnerabilities could be defined in the CoAP environments:

1) IP spoofing: An attacker can send a spoofed response message or a flood of messages with a spoofed IP address in the CoAP environment if the IP addresses of CoAP nodes have been forgotten.
2) Vulnerabilities related to caching and proxying: If the access control approaches for caching and proxying are not precisely developed, their content can be compromised [152].
3) Block attack: An on-path attacker can be placed between a device (e.g., sensor or actuator) and the server to block the delivery of the messages (requests and responses). When a block attack occurs against an actuator, it can lead to a situation where the client loses the server's status information and consequently does not work properly.
4) Parsing attacks: The root of this type of attack is that the incoming messages have not been properly processed/handled by client and server parsers. Consequently, the CoAP node can be crashed under attack due to running an arbitrary remote code.

b: SOLUTIONS
To tackle the aforementioned security challenges in CoAP protocol, the following remedies can be taken:

1) Adopting the DTLS security modes to secure CoAP-enabled nodes.
2) Providing effective access control mechanisms.
3) Providing secure communication.
4) A remedy for block attacks in the IoT systems is to use confirmable messages. Moreover, when a response message is not received, the client should take appropriate actions.

3) EXTENSIBLE MESSAGING AND PRESENCE PROTOCOL (XMPP)
XMPP is an open XML communication protocol that provides a broad range of services such as multi-party chat, instant messaging, presence technology, voice and video calls, and collaboration [153]. The main advantages of XMPP are that it is open, secure, standard, proven, decentralized, extensible, flexible, and diverse. XMPP has been effectively utilized for communication in IoT embedded networking, pub/sub messaging systems, etc. XMPP is especially an ideal communication protocol for use within IoT applications. Different real-world projects use XMPP for IoT, including Google Cloud Print, Firebase Cloud Messaging, and Logitech Harmony Hub.

a: THREATS
Regarding security, the XMPP protocol supports authentication mechanisms through SASL and data confidentiality/integrity through TLS by default [154]. Despite providing these security services, the protocol can face different security risks (e.g., unauthorized access to a server by attackers or stanza modification/deletion/replaying by attackers) due to the deficiency of end-to-end encryption.

b: SOLUTIONS
Some extensions of this protocol have been proposed to deal with the security vulnerabilities in the XMPP protocol. For example, in [155], special measures have been adopted to prevent DoS attacks, while [156] has focused on the SASL authentication-related vulnerabilities.

4) MULTICAST DOMAIN NAME SYSTEM (mDNS)
mDNS as a service discovery protocol is an extension of the DNS protocol [157]. More specifically, mDNS protocol is a multicast design of DNS. mDNS can be employed for locating the devices/services in a local network by name and without using any DNS server. In other words, mDNS is capable of handling domains. One can refer to factory floor networks or industrial networking as an example of using mDNS. The service discovery of mDNS is a very

interesting characteristic for IoT devices because it enables them to establish self-organizing networks on top of the fundamental network infrastructure.

The interested reader is directed to [45] for more information on the mDNS protocol.

a: THREATS

Compared to the messaging protocols, no built-in security feature is offered by the mDNS protocol. Hence, the protocol is vulnerable to several security risks. These risks are as follows:

1) DoS attacks
2) Poisoning attacks
3) Remote attacks

Moreover, given the lack of encryption approaches and the multicast type of communications in mDNS, security threats may appear, and often stay hidden and unrecognized in mDNS-enabled environments [158].

b: SOLUTIONS

As mDNS does not offer any built-in security mechanism, providing efficient security services is crucially important. These security services mainly focus on DoS attacks mitigation, including:

1) The mitigation of security risk through cutting mDNS services each time not needed.
2) Closing port number 5353 in order to block the mDNS UDP (User Datagram Protocol) traffic from/to outside the local link.

Regarding privacy issues, some techniques have been proposed by researchers. For example, encryption of all data in multicast communications or imposing limitations on using multicast [159]. In addition, to deal with the shortage of built-in authentication techniques, some authentication mechanisms have been proposed by researchers [160].

5) SIMPLE SERVICE DISCOVERY PROTOCOL (SSDP)

SSDP is also a service discovery protocol that can be used in small networks, e.g., home networking, to discover network services and advertise services [161]. SSDP is designed based on HTTPU. To exchange messages, this protocol utilizes UDP as the transport layer protocol. In an IoT network, SSDP allows devices to find each other on the network, set up communication, and coordinate operations across the network. For example, when an IoT node aims to discover local devices on the network, it can send an SSDP discovery message and wait for reply messages from any node that gets it.

a: THREATS

Similar to mDNS, SSDP protocol also does not offer any built-in security service. As a consequence, this protocol becomes vulnerable to various security attacks. These attacks seriously compromised the multicast and service discovery of SSDP protocol. One of the most referred attacks is reflection/amplification DDoS attack, which can overwhelm the target device [162]. Moreover, passive attacks can affect SSDP-enabled devices, in which an attacker can exploit the multicast messages for eavesdropping purposes, e.g., discovering sensitive information and, consequently, violating privacy and confidentiality. In addition to the aforementioned security risks, SSDP-enabled devices may also face poisoning attacks and device misconfiguration attacks.

b: SOLUTIONS

As SSDP services are activated by default on the majority of devices, to mitigate DDoS attacks at the level of the individual device, these services should be inactivated each time not needed. Moreover, due to the potentially malicious usage of M-SEARCH messages, these request messages should be monitored appropriately and possibly blocked. Furthermore, deploying encryption techniques on top of SSDP protocol can preserve the authenticity and confidentiality of content transmission [45].

Tables 2 and 3 summarise the security requirements, threats, and solutions for IoT application layer that are discussed in Section V.

VI. OPEN ISSUES AND FUTURE RESEARCH DIRECTIONS

This section provides a few potential open issues and future research lines identified from our findings.

A. THE LACK OF COMPREHENSIVE SECURITY- and/OR PRIVACY-PROTECTING FRAMEWORKS

We have reviewed and analyzed several papers related to IoT security, especially application layer security [6], [8], [23], [56], [70], [84], [94], etc. However, in all of these papers, there is no thorough framework that guarantees security in IoT for a wide range of use cases. To fill this gap, there is a growing need to establish a comprehensive, lightweight framework to ensure security in IoT environments.

B. INSECURE INTERFACES

IoT devices, as smart-physical objects, are capable of communicating, collecting, pre-processing, and sharing this data to achieve their defined objectives, such as environmental monitoring, smart home, and smart grids. To this end, an IoT device may use several interfaces. These include interfaces for communication (wireless or wired), web interfaces, storage interfaces, Internet connectivity interfaces, storage/memory interfaces, and input/output interfaces for sensors. The users may use these interfaces to do different control, management, and configuration tasks, such as query the IoT devices, monitor their status and control them from anywhere.

Multiple IoT security threats arise from insecure interfaces. These security vulnerabilities include the lack of device authentication/identification and weak encryption. For example, in a home automation use case, an internal or external intruder may exploit the web interface to launch attacks.

TABLE 2. Summary of the key security requirements, threats, and potential solutions in the IoT application use cases.

Use case	Key requirements	Threats	Solutions
Smart grids	Confidentiality	Password-pilfering, Traffic analysis Eavesdropping, Unauthorized access False data injection, Password theft	Data encryption, Authentication Encryption protocols
	Integrity	Data tampering, Wormhole, Spoofing Data injection, Data manipulation Man-in-the-middle, Masquerading	Cryptography, Authenticity Power fingerprinting, Volt-var control Security gateways End-to-end encryption
	Availability	Jamming attacks, Wormhole/DoS Buffer overflow, Masquerading Spoofing	Traffic filtering, Anomaly detection Air gapping, Anti-jamming
Smart healthcare	Confidentiality	Unauthorized users, Eavesdropping	Data encryption, algorithms
	Integrity	Adversary users and accidental communication mistakes	Cryptography algorithms e.g., AES128/256 and SHA
	Authentication	Masquerading	Authentication mechanisms, Digital signatures, key-based authentication, Certificate-based authentication
	Authorization	N/A	Access control mechanisms
	Non-repudiation	N/A	N/A
	Privacy	Privacy is the most concern in this application.	Secure access control, Cryptographic, Authentication
ITSs	Confidentiality	Man-in-the-middle, Eavesdropping Model identification Parameter inference	Symmetric cryptography Asymmetric cryptography Steganographic algorithm
	Integrity	Spoofing, Timing/ Sybil, Man-in-the-middle, Data poisoning Policy manipulation	Message Authentication Code
	Availability	DoS/Timing, Spoofing, Jamming attacks, Man-in-the-middle Policy manipulation	Signature-based authentication
	Authentication/ identification	Spoofing, Timing, Sybil Man-in-the-middle	Protocols and message authentication codes
	Non-repudiation	Loss of event data	Digital signatures, Signature-based authentication
Smart agriculture	Confidentiality	Eavesdropping, Brute-force attacks Tracing, Known-key distinguishing False data injection	Access control, based on cipher text, Blockchain-based access control

TABLE 2. *(Continued.)* Summary of the key security requirements, threats, and potential solutions in the IoT application use cases.

Use case	Key requirements	Threats	Solutions
	Integrity	Man-in-the-middle Biometric attacks, Trojan Forgery attacks	Label-based access control Content integrity verification Message authentication codes
	Availability	DoS, Jamming attacks	N/A
	Authentication	Impersonation, Spoofing, Reply attack, Masquerade	RFID authentication, Delegated authentication, Label-based access control, Blockchain-based access control,
	Privacy	Unauthorized access Insider data leakage Cloud data leakage	Privacy-preserving during the data aggregation, Location privacy solutions, Content-oriented protection, Data anonymization, Privacy-preserving trust evaluation methods
Industrial IoT	Confidentiality	Malware Lack of confidentiality measures Worms	Cryptographic techniques Security of cloud computing Security of big data components
	Integrity	Man-in-the-middle, Malware, Worms	Cryptographic techniques Control and report filters MSED encryption , Secure data exchange Data monitoring
	Availability	DoS/DDoS, Mirai botnet BrickerBot, Reaper	SDN-based approaches Distributed approaches Real-time availability monitoring
	Authentication	Ineffective authentication mechanism False data injection Spoofing attacks	Trust-based authentication Proximity-based authentication Edge-assisted device authentication Digital signatures and certificates
Smart cities	Security	DoS attacks, Malware, Eavesdropping attack, Masquerade attack, Disinformation attack, Message modification attack, Traffic analysis attack	Blockchain, Cryptography techniques, Biometrics, Machine learning
	Privacy	Privacy-related issues	Anonymization, Access control techniques, Encryption

Hence, guaranteeing the proper precautions and safety steps to secure the interfaces is crucial.

C. SCALABILITY-RELATED SECURITY CHALLENGES

As mentioned in Section V-A1, the IoT systems are usually large in the number and heterogeneity of the deployed devices. The large scale of these systems can raise key scalability-related security challenges [163]. The first challenge is low processing capability and storage capacity in large-scale IoT networks. More specifically, many IoT devices, e.g., smart sensors for fine-grain sensing, have a very limited process and storage capability. This becomes them almost incapable of implementing and executing resource-demanding security techniques, such as anti-malware and security protocols. The second challenge is the physical protection of IoT devices. Most current IoT security approaches are focused on defense against distant adversaries and are assumed that the devices are not physically available to the adversaries. However, this is mostly not true for large-scale IoT networks, consisting of many scattered devices in and outside buildings, industrial environments, cities, etc. In most cases, it is possible for attackers to easily get physical access to IoT devices and do destructive actions, such as retrieving data and reflashing the devices. The last but not least challenge is the long-running sessions of IoT devices. Usually, IoT devices have long-running sessions which may length for days, weeks, and months. Meanwhile, most current communication protection solutions (i.e., channel protection) are designed for short-running sessions. Hence, this can become problematic for IoT communication with long-running sessions. For example, attackers can learn much by only wiretapping the communication channel.

Regarding the above-mentioned discussion, one who designs security solutions for IoT should consider the security issues arising from IoT networks' scalability characteristics.

D. BLOCKCHAIN

IoT systems are usually large-scale and distributed in nature. These features turn security into a critical challenge in such systems. In other words, IoT environments call for scalable, decentralized, and lightweight security protection. At the same time, blockchain technology has the ability to respond to the above-mentioned challenges by providing distributed, secure, and private mechanisms [164]. In addition, Ethereum blockchain developed a new feature, named smart contracts, that can perform a crucial function in managing, controlling, and securing IoT devices. Generally speaking, based on our understanding of blockchain technology and IoT security, we can refer to the following items as the roles that this technology can fulfill for IoT security: 1) Data integrity and authentication, 2) Access control and privacy, and 3) Secure communications.

Despite these decisive advantages, blockchain-based solutions suffer from challenges, such as delay, computational overhead, and energy hunger [165].

E. NETWORK VIRTUALIZATION FOR IoT

As mentioned, IoT use cases range from smart grids to smart agriculture. Due to the wide range of IoT applications, the infrastructures of IoT become increasingly complicated and call for highly dynamic and effective management and configuration techniques. SDN and Network Function Virtualization (NFV) in working together under the umbrella of Network Softwarization have been considerably investigated for IoT recently [166]. Following this trend, IoT management solutions based on softwarization techniques have been one of the focuses in recent years. More specifically, considering the large scale of IoT networks, it is nearly impossible to configure remote devices manually. SDN is capable of enabling effective configuration and management solutions across IoT networks. These solutions can be adapted for IoT application deployment, network slicing, device configuration and discovery, and management of edge/cloud.

Besides SDN, management solutions based on NFV also have been adopted for IoT networks. These solutions may be related to different aspects of IoT, including security, reducing costs in IoT, load balancing, on-demand management, etc. Moreover, virtualization-based solutions can be explicitly adopted for IoT security purposes. For example, as we mentioned in Section V-A1, large-scale IoT networks can present challenges to the security of the networks. The single-point programmability feature of SDN technology can bring many advantages in terms of security functions, resource optimization, network policy, etc. Moreover, virtualizing IoT devices' functions can enforce security procedures on physical devices.

F. MACHINE LEARNING FOR IoT SECURITY

Considering the number of IoT attacks is increasing at an exponential rate, it is necessary to provide solutions that combine state-of-the-art methods and technologies from machine learning and Big Data. Machine learning-based solutions can provide Embedded Intelligence (EI) in IoT systems and can be used to deal with various security issues, such as intrusion and anomaly detection. For several reasons, machine learning-based algorithms are promising solutions for different aspects of IoT systems, especially security. The first reason is that IoT systems produce massive data that machine learning models can use for training purposes and bring intelligence to IoT networks. Furthermore, the IoT data utilized by machine learning techniques allow IoT networks to arrive at more intelligent and informed decisions. Machine learning models are widely adopted in IoT networks to deal with various security issues, including attacks and malware detection, malicious code detection, DDoS attack detection, and facial recognition and authentication.

However, for designing machine learning-based solutions, one should consider the following points: 1) The scalability of the solution, 2) Selecting the right datasets for training, 3) Continuous model training and data labeling, and 4) The computational complexity of the model.

TABLE 3. Summary of the main security threats and potential solutions in the IoT application layer protocols.

Protocol	Threats	Solutions
MQTT	Authentication issues Authorization issues Message delivery failures Message integrity	Client/device authentication Authorization client's access to servers Message privacy-preserving mechanisms Message integrity checking mechanisms
CoAP	IP spoofng Caching and proxying vulnerabilities Block attack Parsing attacks	Adopting DTLS security modes Access control mechanisms Secure communication Confrimable messages
XMPP	Unauthorized access Stanza modification Stanza deletion/replaying	Protocol improvement SASL authentication
mDNS	DoS attacks Poisoning attacks Remote attacks	Limitation on mDNS services Closing port
SSDP	Reflection/amplifcation attacks Passive attacksEavesdropping attacksPoisoning attacks	Limitation on SSDP services Message monitoring and blocking Encryption techniques

VII. DISCUSSION AND CONCLUSION

As our paper indicates, the IoT application layer security is paramount. A strong body of literature has investigated IoT security from different points of view. However, few studies have been conducted to individually review the security aspects of the IoT application layer. Providing a precise classification of the critical security requirements, threats, and existing solutions in the IoT application layer will facilitate the development of novel IoT use cases and the IoT application layer protocols and improve the security of the existing IoT-based solutions.

In this paper, we studied the IoT application layer's security. We first provided background on IoT and its security and then discussed some related papers to emphasize their differences and our work. Afterward, we categorized and discussed the key security requirements of the IoT application layer, threats, and potential solutions. To take the right direction and conduct an extensive review, our study is based primarily on two perspectives: IoT use cases and IoT application layer protocols.

Given the IoT application layer, we identified six key security requirements - confidentiality, integrity, availability, authentication/authorization, non-repudiation, and privacy. Satisfying these security requirements can lead to the proper operation of the IoT systems and prevent security vulnerabilities and threats. Based on these requirements, we investigated the security aspects of the six key IoT use cases - smart grids, smart healthcare, ITs, smart agriculture, industrial IoT, and smart cities. Furthermore, we discussed the security challenges and potential solutions of the leading IoT application layer protocols, including MQTT, CoAP, XMPP, mDNS, and SSDP. Given future research lines, as we mentioned, many studies have been conducted on using blockchain technologies and machine learning to guarantee security in IoT settings.

REFERENCES

[1] L. Atzori, I. A. Iera, and M. Giacomo, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, May 2010.

[2] A. Shahraki, M. Abbasi, A. Taherkordi, and A. D. Jurcut, "A comparative study on online machine learning techniques for network traffic streams analysis," *Comput. Netw.*, vol. 207, Apr. 2022, Art. no. 108836.

[3] McKinsey Global Institute. *The Internet of Things: Mapping the Value Beyond the Hype*. Accessed: Jun. 20, 2022. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/Industries/Technology

[4] M. Plaza-Hernandez, I. Sittón-Candanedo, R. S. Alonso, L. C. M.-D. Iturrate, J. Prieto, K. Kravari, T. Kosmanis, G. Katranas, M. P. Silva, and J. M. Corchado, "Edge computing and Internet of Things based platform to improve the quality of life of the silver economy on leisure cruise ships," in *Proc. Int. Symp. Comput. Sci. Intell. Controls (ISCSIC)*, Nov. 2021, pp. 159–163.

[5] F. J. Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A survey," *IEEE Access*, vol. 8, pp. 69200–69211, 2020.

[6] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.

[7] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[8] D. Swessi and H. Idoudi, "A survey on Internet-of-Things security: Threats and emerging countermeasures," *Wireless Pers. Commun.*, vol. 124, pp. 1557–1592, Jan. 2022.

[9] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on Internet of Things security: Requirements, challenges, and solutions," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100129.

[10] A. Shahraki, M. Abbasi, and Ø. Haugen, "Boosting algorithms for network intrusion detection: A comparative evaluation of real AdaBoost, gentle AdaBoost and modest AdaBoost," *Eng. Appl. Artif. Intell.*, vol. 94, Sep. 2020, Art. no. 103770.

[11] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[12] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, p. e3677, Mar. 2022.

[13] N. Mazhar, R. Salleh, M. Zeeshan, and M. M. Hameed, "Role of device identification and manufacturer usage description in IoT security: A survey," *IEEE Access*, vol. 9, pp. 41757–41786, 2021.

[14] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[15] G. Katranas, A. Riel, J. M. Corchado-Rodríguez, and M. Plaza-Hernández, "The SMARTSEA education approach to leveraging the Internet of Things in the maritime industry," in *Proc. Eur. Conf. Softw. Process Improvement*. Cham, Switzerland: Springer, 2020, pp. 247–258.

[16] C. C. Sobin, "A survey on architecture, protocols and challenges in IoT," *Wireless Pers. Commun.*, vol. 112, no. 3, pp. 1383–1429, Jun. 2020.
[17] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, 2018.
[18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.
[19] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria, M. K. Afzal, and S. W. Kim, "Multimedia Internet of Things: A comprehensive survey," *IEEE Access*, vol. 8, pp. 8202–8250, 2020.
[20] J. Chen, C. Touati, and Q. Zhu, "Optimal secure two-layer IoT network design," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 1, pp. 398–409, Mar. 2020.
[21] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.
[22] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.
[23] A. E. Omolara, A. Alabdulatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, W. H. Alshoura, and H. Arshad, "The Internet of Things security: A survey encompassing unexplored areas and new insights," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102494.
[24] A. Canito, K. Aleid, I. Praça, J. Corchado, and G. Marreiros, "An ontology to promote interoperability between cyber-physical security systems in critical infrastructures," in *Proc. IEEE 6th Int. Conf. Comput. Commun. (ICCC)*, Dec. 2020, pp. 553–560.
[25] S. Zhu, S. Yang, X. Gou, Y. Xu, T. Zhang, and Y. Wan, "Survey of testing methods and testbed development concerning Internet of Things," *Wireless Pers. Commun.*, vol. 123, no. 1, pp. 165–194, 2022.
[26] S. A. Haider, M. N. Adil, and M. Zhao, "Optimization of secure wireless communications for IoT networks in the presence of eavesdroppers," *Comput. Commun.*, vol. 154, pp. 119–128, Mar. 2020.
[27] M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained IoT networks," *Internet Things*, vol. 11, Sep. 2020, Art. no. 100212.
[28] X. Luo, L. Yin, C. Li, C. Wang, F. Fang, C. Zhu, and Z. Tian, "A lightweight privacy-preserving communication protocol for heterogeneous IoT environment," *IEEE Access*, vol. 8, pp. 67192–67204, 2020.
[29] Z. Xiong, Y. Zhang, N. C. Luong, D. Niyato, P. Wang, and N. Guizani, "The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things," *IEEE Netw.*, vol. 34, no. 1, pp. 166–173, Jan. 2020.
[30] T. A. Ahanger, A. Aljumah, and M. Atiquzzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108771.
[31] I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, "Survey on IoT: Security threats and applications," *J. Robot. Control*, vol. 2, no. 1, pp. 42–46, 2021.
[32] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.
[33] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018.
[34] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Gener. Comput. Syst.*, vol. 100, pp. 144–164, Nov. 2019.
[35] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the Internet of Things," *Proc. Comput. Sci.*, vol. 175, pp. 591–596, Jan. 2020.
[36] B. Balamurugan and D. Biswas, "Security in network layer of IoT: Possible measures to preclude," in *Security Breaches and Threat Prevention in the Internet of Things*. Hershey, PA, USA: IGI Global, 2017, pp. 46–75.
[37] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, May/Jun. 2016.
[38] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet Things*, vols. 1–2, pp. 1–13, Sep. 2018.
[39] A. Abdelmaboud, A. I. A. Ahmed, M. Abaker, T. A. E. Eisa, H. Albasheer, S. A. Ghorashi, and F. K. Karim, "Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions," *Electronics*, vol. 11, no. 4, p. 630, Feb. 2022.
[40] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) security intelligence: A comprehensive overview, machine learning solutions and research directions," *Mobile Netw. Appl.*, vol. 27, pp. 1–17, Mar. 2022.
[41] I. Kotenko, K. Izrailov, and M. Buinevich, "Static analysis of information systems for IoT cyber security: A survey of machine learning approaches," *Sensors*, vol. 22, no. 4, p. 1335, Feb. 2022.
[42] R. Kanagavelu and K. M. M. Aung, "A survey on SDN based security in Internet of Things," in *Proc. Future Inf. Commun. Conf.* Cham, Switzerland: Springer, 2018, pp. 563–577.
[43] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving Internet of Things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, p. 8, Feb. 2020.
[44] K. S. Sudha and N. Jeyanthi, "A review on privacy requirements and application layer security in Internet of Things (IoT)," *Cybern. Inf. Technol.*, vol. 21, no. 3, pp. 50–72, Sep. 2021.
[45] G. Nebbione and M. C. Calzarossa, "Security of IoT application layer protocols: Challenges and findings," *Future Internet*, vol. 12, no. 3, p. 55, Mar. 2020.
[46] L. Nastase, "Security in the Internet of Things: A survey on application layer protocols," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci. (CSCS)*, May 2017, pp. 659–666.
[47] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in IoT applications," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Feb. 2017, pp. 477–480.
[48] D. Johnson and M. Ketel, "IoT: Application protocols and security," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 4, pp. 1–8, Apr. 2019.
[49] J. Ferdows, S. T. Mehedi, A. S. M. D. Hossain, A. A. M. Shamim, and G. M. R. I. Rasiq, "A comprehensive study of IoT application layer security management," in *Proc. IEEE Int. Conf. for Innov. Technol. (INOCON)*, Nov. 2020, pp. 1–7.
[50] P. K. Donta, S. N. Srirama, T. Amgoth, and C. S. R. Annavarapu, "Survey on recent advances in IoT application layer protocols and machine learning scope for research directions," *Digit. Commun. Netw.*, Oct. 2021.
[51] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors*, vol. 20, no. 13, p. 3625, Jun. 2020.
[52] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of Things (IoT): A security taxonomy for IoT," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 163–168.
[53] N. Tripathi and N. Hubballi, "Application layer denial-of-service attacks and defense mechanisms: A survey," *ACM Comput. Surv.*, vol. 54, no. 4, pp. 1–33, 2021.
[54] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," in *Proc. 3rd MEC Int. Conf. Big Data Smart City (ICBDSC)*, Mar. 2016, pp. 1–7.
[55] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020.
[56] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.
[57] M. B. Gough, S. F. Santos, T. AlSkaif, M. S. Javadi, R. Castro, and J. P. S. Catalão, "Preserving privacy of smart meter data in a smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 707–718, Jan. 2022.
[58] F. Alshehri and G. Muhammad, "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare," *IEEE Access*, vol. 9, pp. 3660–3678, 2021.
[59] R. H. et. al., "A survey: Security challenges of vanet and their current solution," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 2, pp. 1239–1244, Apr. 2021.
[60] I. Ali, Y. Chen, M. Faisal, and M. Li, "Certificateless signature-based authentication scheme for vehicle-to-infrastructure communications using bilinear pairing," in *Efficient and Provably Secure Schemes for Vehicular Ad-Hoc Networks*. Singapore: Springer, 2022, pp. 91–119.
[61] X. Yang, L. Shu, J. Chen, M. A. Ferrag, J. Wu, E. Nurellari, and K. Huang, "A survey on smart agriculture: Development modes, technologies, and security and privacy challenges," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 2, pp. 273–302, Feb. 2021.

[62] T. Gebremichael, L. P. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg, ''Security and privacy in the industrial Internet of Things: Current standards and future challenges,'' *IEEE Access*, vol. 8, pp. 152351–152366, 2020.
[63] N. Agrawal and R. Kumar, ''Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey,'' *ISA Trans.*, Mar. 2022.
[64] L. L. Dhirani, E. Armstrong, and T. Newe, ''Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap,'' *Sensors*, vol. 21, no. 11, p. 3901, Jun. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/11/3901
[65] D. A. Hahn, A. Munir, and V. Behzadan, ''Security and privacy issues in intelligent transportation systems: Classification and challenges,'' *IEEE Intell. Transp. Syst. Mag.*, vol. 13, no. 1, pp. 181–196, Spring 2021.
[66] F. Al-Turjman and S. Alturjman, ''Confidential smart-sensing framework in the IoT era,'' *J. Supercomput.*, vol. 74, no. 10, pp. 5187–5198, Oct. 2018.
[67] S.-X. Wang, H.-W. Chen, Q.-Y. Zhao, L.-Y. Guo, X.-Y. Deng, W.-G. Si, and Z.-Q. Sun, ''Preserving scheme for user's confidential information in smart grid based on digital watermark and asymmetric encryption,'' *J. Central South Univ.*, vol. 29, no. 2, pp. 726–740, Feb. 2022.
[68] A. Sharma, K. Gautam, and T. K. Koirala, ''Comparison of IoT application layer protocols on soft computing paradigms: A survey,'' in *Advances in Communication, Devices and Networking*. Singapore: Springer, 2022, pp. 307–317.
[69] P. Li, J. Su, and X. Wang, ''ITLS: Lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy,'' *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6828–6841, Aug. 2020.
[70] C. Machado and A. A. M. Fröhlich, ''IoT data integrity verification for cyber-physical systems using blockchain,'' in *Proc. IEEE 21st Int. Symp. Real-Time Distrib. Comput. (ISORC)*, May 2018, pp. 83–90.
[71] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, ''Internet of Things for the future of smart agriculture: A comprehensive survey of emerging technologies,'' *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 4, pp. 718–752, Apr. 2021.
[72] S. Madhawa, P. Balakrishnan, and U. Arumugam, ''Roll forward validation based decision tree classification for detecting data integrity attacks in industrial Internet of Things,'' *J. Intell. Fuzzy Syst.*, vol. 36, no. 3, pp. 2355–2366, 2019.
[73] T. Sultana and K. A. Wahid, ''Choice of application layer protocols for next generation video surveillance using internet of video things,'' *IEEE Access*, vol. 7, pp. 41607–41624, 2019.
[74] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, ''Security requirements for the Internet of Things: A systematic approach,'' *Sensors*, vol. 20, no. 20, p. 5897, Oct. 2020.
[75] J. Yan, J. Liu, and F.-M. Tseng, ''An evaluation system based on the self-organizing system framework of smart cities: A case study of smart transportation systems in China,'' *Technol. Forecasting Social Change*, vol. 153, Apr. 2020, Art. no. 119371.
[76] M. T. Ahvanooey, M. X. Zhu, Q. Li, W. Mazurczyk, K.-K.-R. Choo, B. B. Gupta, and M. Conti, ''Modern authentication schemes in smartphones and IoT devices: An empirical survey,'' *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7639–7663, May 2022.
[77] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, ''VANET security surveys,'' *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[78] P. Gupta and M. I. O. Prabha, ''A survey of application layer protocols for Internet of Things,'' in *Proc. Int. Conf. Commun. Inf. Comput. Technol. (ICCICT)*, Jun. 2021, pp. 1–6.
[79] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, ''Cross-layer privacy enhancement and non-repudiation in vehicular communication,'' in *Proc. Commun. Distrib. Syst., ITG/GI Symp.* Frankfurt, Germany: VDE, 2007, pp. 1–12.
[80] C.-L. Chen, Y.-Y. Deng, C.-T. Li, S. Zhu, Y.-J. Chiu, and P.-Z. Chen, ''An IoT-based traceable drug anti-counterfeiting management system,'' *IEEE Access*, vol. 8, pp. 224532–224548, 2020.
[81] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ''VANet security challenges and solutions: A survey,'' *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[82] A. A. A. Sen, F. A. Eassa, K. Jambi, and M. Yamin, ''Preserving privacy in Internet of Things: A survey,'' *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 189–200, Jun. 2018.
[83] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, ''Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey,'' *IEEE Access*, vol. 8, pp. 167123–167163, 2020.
[84] T. Salman and R. Jain, ''A survey of protocols and standards for Internet of Things,'' 2019, *arXiv:1903.11549*.
[85] F. Nizzi, T. Pecorella, F. Esposito, L. Pierucci, and R. Fantacci, ''IoT security via address shuffling: The easy way,'' *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3764–3774, Apr. 2019.
[86] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, ''A survey on cyber security for smart grid communications,'' *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.
[87] A. D. Jurcut, P. Ranaweera, and L. Xu, ''Introduction to IoT security,'' in *IoT Security: Advances in Authentication*. Hoboken, NJ, USA: Wiley, 2020, pp. 27–64.
[88] H. Zhang, B. Liu, and H. Wu, ''Smart grid cyber-physical attack and defense: A review,'' *IEEE Access*, vol. 9, pp. 29641–29659, 2021.
[89] S. Sengan, V. Subramaniyaswamy, V. Indragandhi, and L. Ravi, ''Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning,'' *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107211.
[90] Y. Li, P. Zhang, and R. Huang, ''Lightweight quantum encryption for secure transmission of power data in smart grid,'' *IEEE Access*, vol. 7, pp. 36285–36293, 2019.
[91] J. Zavala-Díaz, E. Reyes-Archundia, J. C. Olivares-Rojas, M. V. Chávez-Báez, J. A. Gutiérrez-Gnecchi, and A. Méndez-Patiño, ''Study of public key cryptography techniques for authentication in embedded devices for smart grids,'' in *Proc. IEEE Int. Autumn Meeting Power, Electron. Comput. (ROPEC)*, Nov. 2021, pp. 1–5.
[92] S. Singh, V. B. Pamshetti, A. K. Thakur, and S. P. Singh, ''Multistage multiobjective Volt/VAR control for smart grid-enabled CVR with solar PV penetration,'' *IEEE Syst. J.*, vol. 15, no. 2, pp. 2767–2778, Jun. 2021.
[93] A. Huseinović, S. Mrdović, K. Bicakci, and S. Uludag, ''A survey of denial-of-service attacks and solutions in the smart grid,'' *IEEE Access*, vol. 8, pp. 177447–177470, 2020.
[94] H. Pirayesh and H. Zeng, ''Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,'' *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.
[95] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, ''Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure,'' *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–23, Nov. 2018.
[96] H. Ghayvat, S. Pandya, P. Bhattacharya, M. Zuhair, M. Rashid, S. Hakak, and K. Dev, ''CP-BDHCA: Blockchain-based confidentiality-privacy preserving big data scheme for healthcare clouds and applications,'' *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1937–1948, May 2022.
[97] K. Renuka, S. Kumari, and X. Li, ''Design of a secure three-factor authentication scheme for smart healthcare,'' *J. Med. Syst.*, vol. 43, no. 5, pp. 1–12, May 2019.
[98] D. He, R. Ye, S. Chan, M. Guizani, and Y. Xu, ''Privacy in the Internet of Things for smart healthcare,'' *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 38–44, Apr. 2018.
[99] C. Xu, H. H. Yang, X. Wang, and T. Q. S. Quek, ''Optimizing information freshness in computing-enabled IoT networks,'' *IEEE Internet Things J.*, vol. 7, no. 2, pp. 971–985, Feb. 2020.
[100] S. M. Ahmed and A. Rajput, ''Threats to patients' privacy in smart healthcare environment,'' in *Innovation in Health Informatics*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 375–393.
[101] A. Algarni, ''A survey and classification of security and privacy research in smart healthcare systems,'' *IEEE Access*, vol. 7, pp. 101879–101894, 2019.
[102] A. Maimaris and G. Papageorgiou, ''A review of intelligent transportation systems from a communications technology perspective,'' in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 54–59.
[103] V. Behzadan and A. Munir, ''Models and framework for adversarial attacks on complex adaptive systems,'' 2017, *arXiv:1709.04137*.
[104] F. Azam, S. Kumar, K. P. Yadav, N. Priyadarshi, and S. Padmanaban, ''An outline of the security challenges in VANET,'' in *Proc. IEEE 7th Uttar Pradesh Sect. Int. Conf. Electr., Electron. Comput. Eng. (UPCON)*, Nov. 2020, pp. 1–6.
[105] M. Wazid, B. Bera, A. K. Das, S. P. Mohanty, and M. Jo, ''Fortifying smart transportation security through public blockchain,'' *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16532–16545, Sep. 2022.
[106] M. Gayathri and C. Gomathy, ''An overview of security services and trust-based authentication schemes in VANET,'' in *Micro-Electronics and Telecommunication Engineering*. Basel, Switzerland: MDPI, 2022, pp. 193–205.

[107] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.
[108] Y. Sun, K. Yu, A. K. Bashir, and X. Liao, "Bl-IEA: A bit-level image encryption algorithm for cognitive services in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 30, 2021, doi: 10.1109/TITS.2021.3129598.
[109] X. Shen, Y. Lu, Y. Zhang, X. Liu, and L. Zhang, "An innovative data integrity verification scheme in the Internet of Things assisted information exchange in transportation systems," *Cluster Comput.*, vol. 25, pp. 1791–1803, Jan. 2022.
[110] E. F. Cahyadi and M.-S. Hwang, "A comprehensive survey on certificateless aggregate signature in vehicular ad hoc networks," *IETE Tech. Rev.*, pp. 1–12, Jan. 2022.
[111] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and privacy in smart farming: Challenges and opportunities," *IEEE Access*, vol. 8, pp. 34564–34584, 2020.
[112] S. Salamatian, W. Huleihel, A. Beirami, A. Cohen, and M. Médard, "Why botnets work: Distributed brute-force attacks need no synchronization," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2288–2299, Sep. 2019.
[113] M. A. Ferrag, L. Shu, H. Djallel, and K.-K.-R. Choo, "Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0," *Electronics*, vol. 10, no. 11, p. 1257, May 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/11/1257
[114] S. Sontowski, M. Gupta, S. S. Laya Chukkapalli, M. Abdelsalam, S. Mittal, A. Joshi, and R. Sandhu, "Cyber attacks on smart farming infrastructure," in *Proc. IEEE 6th Int. Conf. Collaboration Internet Comput. (CIC)*, Dec. 2020, pp. 135–143.
[115] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.
[116] P. Appavoo, M. C. Chan, A. Bhojan, and E.-C. Chang, "Efficient and privacy-preserving access to sensor data for Internet of Things (IoT) based services," in *Proc. 8th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2016, pp. 1–8.
[117] K. Gai, K.-K. R. Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in Internet-of-Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3059–3067, Aug. 2018.
[118] Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, "LACS: A lightweight label-based access control scheme in IoT-based 5G caching context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.
[119] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, "LIVE: Lightweight integrity verification and content access control for named data networking," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 308–320, Feb. 2015.
[120] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.
[121] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Gener. Comput. Syst.*, vol. 83, pp. 629–637, Jun. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17313043
[122] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.
[123] S. I. Hassan, M. M. Alam, U. Illahi, M. A. Al Ghamdi, S. H. Almotiri, and M. M. Su'ud, "A systematic review on monitoring and advanced control strategies in smart agriculture," *IEEE Access*, vol. 9, pp. 32517–32548, 2021.
[124] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, Apr. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0278612518300463
[125] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A survey on the usage of blockchain technology for cyber-threats in the context of industry 4.0," *Sustainability*, vol. 12, no. 21, p. 9179, 2020.
[126] U. M. Qureshi, G. P. Hancke, T. Gebremichael, U. Jennehag, S. Forsström, and M. Gidlund, "Survey of proximity based authentication mechanisms for the industrial Internet of Things," in *Proc. 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2018, pp. 5246–5251.
[127] Y. Lu, D. Wang, M. S. Obaidat, and P. Vijayakumar, "Edge-assisted intelligent device authentication in cyber-physical systems," *IEEE Internet Things J.*, early access, Feb. 16, 2022, doi: 10.1109/JIOT.2022.3151828.
[128] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudhary, "SELAMAT: A new secure and lightweight multi-factor authentication scheme for cross-platform industrial IoT systems," *Sensors*, vol. 21, no. 4, p. 1428, 2021.
[129] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3567–3569, Aug. 2018.
[130] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. A. Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2017, pp. 1039–1046.
[131] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial Internet of Things: A software-defined networking approach," *Comput. Ind.*, vol. 104, pp. 47–58, Jan. 2019.
[132] P. M. Rao and B. Deebak, "Security and privacy issues in smart cities/industries: Technologies, applications, and challenges," *J. Ambient Intell. Hum. Comput.*, vol. 13, no. 1, pp. 1–37, Feb. 2022.
[133] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2046–2069, 4th Quart., 2013.
[134] D. Popescul and L. D. Radu, "Data security in smart cities: Challenges and solutions," *Inf. Economică*, vol. 20, no. 1, pp. 29–38, Mar. 2016.
[135] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, Oct. 2019, Art. no. 101660.
[136] S. Abbas, M. Faisal, H. U. Rahman, M. Z. Khan, M. Merabti, and A. U. R. Khan, "Masquerading attacks detection in mobile ad hoc networks," *IEEE Access*, vol. 6, pp. 55013–55025, 2018.
[137] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: A survey, research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1718–1743, 2nd Quart., 2019.
[138] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent advances in VANET security: A survey," in *Proc. IEEE 82nd Veh. Technol. Conf. (VTC-Fall)*, Sep. 2015, pp. 1–7.
[139] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep learning for network traffic monitoring and analysis (NTMA): A survey," *Comput. Commun.*, vol. 170, pp. 19–41, Feb. 2021.
[140] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, "Blockchain for smart cities: A review of architectures, integration trends and future research directions," *Sustain. Cities Soc.*, vol. 61, Oct. 2020, Art. no. 102360.
[141] T. K. Dang, C. D. M. Pham, and T. L. P. Nguyen, "A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities," *Sustain. Cities Soc.*, vol. 56, May 2020, Art. no. 102097.
[142] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Comput. Commun.*, vol. 154, pp. 313–323, Mar. 2020.
[143] M. Drozdowicz, M. Ganzha, and M. Paprzycki, "Semantic access control for privacy management of personal sensing in smart cities," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 1, pp. 199–210, Jan. 2022.
[144] M. Rasori, P. Perazzo, and G. Dini, "A lightweight and scalable attribute-based encryption system for smart cities," *Comput. Commun.*, vol. 149, pp. 78–89, Jan. 2020.
[145] Y. Lin, Z. Shen, and X. Teng, "Review on data sharing in smart city planning based on mobile phone signaling big data: From the perspective of China experience: Anonymization VS de-anonymization," *Int. Rev. Spatial Planning Sustain. Develop.*, vol. 9, no. 2, pp. 76–93, 2021.
[146] J. Myers, *Simple Authentication and Security Layer (SASL)*, document RFC 2222, Kanazawa, Japan, 1997.
[147] E. B. Sanjuan, I. A. Cardiel, J. A. Cerrada, and C. Cerrada, "Message queuing telemetry transport (MQTT) security: A cryptographic smart card approach," *IEEE Access*, vol. 8, pp. 115051–115062, 2020.
[148] D. Dinculeană and X. Cheng, "Vulnerabilities and limitations of MQTT protocol used between IoT devices," *Appl. Sci.*, vol. 9, no. 5, p. 848, 2019.
[149] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, and S. Karuppayah, "MQTT vulnerabilities, attack vectors and solutions in the Internet of Things (IoT)," *IETE J. Res.*, vol. 68, pp. 1–30, 2022.
[150] F. Chen, Y. Huo, J. Zhu, and D. Fan, "A review on the study on MQTT security challenge," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2020, pp. 128–133.
[151] M. S. Harsha, B. M. Bhavani, and K. R. Kundhavai, "Analysis of vulnerabilities in MQTT security using Shodan API and implementation of its countermeasures via authentication and ACLs," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 2244–2250.

[152] J. Mišić and V. B. Mišić, "Proxy cache maintenance using multicasting in CoAP IoT domains," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1967–1976, Jun. 2018.
[153] P. Saint-Andre, *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*, RFC 3921, Oct. 2004.
[154] M. B. Yassein, M. Q. Shatnawi, and D. Al-Zoubi, "Application layer protocols for the Internet of Things: A survey," in *Proc. Int. Conf. Eng. MIS (ICEMIS)*, Sep. 2016, pp. 1–4.
[155] P. Saint-Andre. *XEP-0205: Best Practices to Discourage Denial of Service Attacks*. Accessed: Jun. 23, 2022. [Online]. Available: https://xmpp.org/extensions/xep-0205.html
[156] P. S.-A. Millard. *XEP-0178: Best Practices for Use of SASL External With Certificates*. Accessed: Jun. 23, 2022. [Online]. Available: https://xmpp.org/extensions/xep-0178.html
[157] S. Cheshire and M. Krochmal, *Multicast DNS*, RFC 6762, Feb. 2013.
[158] I. Dolnák, A. Jantošová, and J. Litvik, "An overview of DNS security in V2X networks," in *Proc. 17th Int. Conf. Emerg. eLearn. Technol. Appl. (ICETA)*, Nov. 2019, pp. 156–159.
[159] A. R. Kang, J. Spaulding, and A. Mohaisen, "Domain name system security and privacy: Old problems and new challenges," 2016, *arXiv:1606.07080*.
[160] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, discovery, and authentication for the Internet of Things," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2016, pp. 301–319.
[161] G. Singh and B. Singh, "Simple service discovery protocol based distributed reflective denial of service attack," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 12, pp. 143–150, 2017.
[162] M. Asim, "A survey on application layer protocols for Internet of Things (IoT)," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 3, pp. 996–1000, 2017.
[163] S. N. Swamy and S. R. Kota, "An empirical study on system level aspects of Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 188082–188134, 2020.
[164] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A survey of IoT and blockchain integration: Security perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021.
[165] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021.
[166] I. Alam, K. Sharif, F. Li, Z. Latif, M. M. Karim, S. Biswas, B. Nour, and Y. Wang, "A survey of network virtualization techniques for Internet of Things using SDN and NFV," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–40, Mar. 2021.

MAHMOUD ABBASI (Member, IEEE) received the B.Eng. degree from the Department of Computer Engineering, Islamic Azad University of Birjand, and the M.Sc. degree from the Department of Computer Engineering, Islamic Azad University of Mashad. He is currently pursuing the Ph.D. degree in the IoTalentum with the BISITE Research Group, University of Salamanca. His current research interests include the general area of communication systems and networks and ML, the Internet of Things, and blockchain.

MARTA PLAZA-HERNÁNDEZ received the Graduate degree in physics from the University of Salamanca, the master's degree in environmental management from Brunel University London, and the master's degree in smart cities and intelligent buildings from the University of Salamanca. She has worked as a Research Fellow at the Institute of Science and Technology Studies (ECYT, USAL) and the Institute of Environment, Health, and Societies (Brunel University London). She currently combines her Ph.D. studies in intelligent applications to industrial and environmental problems with her research and teaching work with the BISITE Group. She manages European projects, such as SMARTSEA, TECTONIC, IoTalentum, and QFORTE. She is also involved in the organization of international conferences (PAAMS and co-events, SSCTIC, Globecom, and ICCBR). She is also responsible for generating and delivering content in different international master's and courses.

JAVIER PRIETO (Senior Member, IEEE) received the degree in telecommunication engineering, the degree in marketing research and techniques, and the Ph.D. degree in information and communication technologies from the University of Valladolid, in 2008, 2010, and 2012, respectively. Since 2007, he has been working in different public and private research centers, such as the Foundation Center for the Development of Telecommunications of Castilla y León (CEDETEL), the University of Valladolid, Spain, and the Massachusetts Institute of Technology (MIT), Cambridge, MA as a Visiting Researcher. He was a Distinguished Researcher at the Department of Computer Science and Automation, University of Salamanca. He is currently an Associate Professor at the Bioinformatics, Intelligent Systems and Educational Technology (BISITE) Research Group, University of Salamanca. He is a member of the Institute of Biomedical Research of Salamanca (IBSAL), the Editor-in-Chief of the *Internet of Things Section of the Smart Cities* journal, and a Senior Editor of the IEEE COMMUNICATIONS LETTERS. He has received the Extraordinary Performance Award for Doctorate Studies from the University of Valladolid.

JUAN M. CORCHADO received the Ph.D. degree in computer science from the University of Salamanca, and the Ph.D. degree in artificial intelligence from the University of the West of Scotland. He is currently a Professor at the University of Salamanca. He was the Vice-Rector for Research, from 2013 to 2017, and the Director of the Science Park with the University of Salamanca. He was elected twice as the Dean of the Faculty of Sciences. He directs the Recognized Research Group Bioinformatics, Intelligent Systems and Educational Technology (BISITE), in 2000.