IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 July 2022, accepted 9 September 2022, date of publication 16 September 2022, date of current version 29 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3207472

SURVEY

A Novel Architectural Framework on IoT Ecosystem, Security Aspects and Mechanisms: A Comprehensive Survey

MOHAMMED BOUZIDI[1], **NISHU GUPTA**[1], **(Senior Member, IEEE),**
FAOUZI ALAYA CHEIKH[2], **(Senior Member, IEEE), ANDRII SHALAGINOV**[3],
AND MOHAMMAD DERAWI[1]

[1]Department of Electronic Systems, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[2]Department of Computer Science, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, 2815 Gjøvik, Norway
[3]School of Economics, Innovation and Technology, Kristiania University College, 0107 Oslo, Norway

Corresponding author: Nishu Gupta (nishu.gupta@ntnu.no)

ABSTRACT For the past few years, the Internet of Things (IoT) technology continues to not only gain popularity and importance, but also witnesses the true realization of everything being smart. With the advent of the concept of *smart everything*, IoT has emerged as an area of great potential and incredible growth. An IoT ecosystem centers around innovation perspective which is considered as its fundamental core. Accordingly, IoT enabling technologies such as hardware and software platforms as well as standards become the core of the IoT ecosystem. However, any large-scale technological integration such as the IoT development poses the challenge to ensure secure data transmission. Perhaps, the ubiquitous and the resource-constrained nature of IoT devices and the sensitive and private data being generated by IoT systems make them highly vulnerable to physical and cyber threats. In this paper, we re-define an IoT ecosystem from the core technologies view point. We propose a modified three layer IoT architecture by dividing the perception layer into elementary blocks based on their attributed functions. Enabling technologies, attacks and security countermeasures are classified under each layer of the proposed architecture. Additionally, to give the readers a broader perspective of the research area, we discuss the role of various state-of-the-art emerging technologies in the IoT security. We present the security aspects of the most prominent standards and other recently developed technologies for IoT which might have the potential to form the yet undefined IoT architecture. Among the technologies presented in this article, we give a special interest to one recent technology in IoT domain. This technology is named IQRF that stands for Intelligent Connectivity using Radio Frequency. It is an emerging technology for wireless packet-oriented communication that operates in sub-GHz ISM band (868 MHz) and which is intended for general use where wireless connectivity is needed, either in a mesh network or point-to-point (P2P) configuration. We also highlighted the security aspects implemented in this technology and we compare it with the other already known technologies. Moreover, a detailed discussion on the possible attacks is presented. These attacks are projected on the IoT technologies presented in this article including IQRF. In addition, lightweight security solutions, implemented in these technologies, to counter these threats in the proposed IoT ecosystem architecture are also presented. Lastly, we summarize the survey by listing out some common challenges and the future research directions in this field.

INDEX TERMS Cyber attacks, IoT architecture, Internet of Things (IoT) ecosystem, IQRF, network security.

I. INTRODUCTION

Portable and smart embedded devices have become an indispensable part of our day-to-day life. They are widely used in

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

a number of applications, ranging from tiny locations trackers to large vehicles, medical instruments and buildings. Devices, thus, become standalone and smart, envisaging themselves as an integrated smart system. Additionally, the ability of these smart devices to communicate and connect to the Internet makes them the cornerstone of a new level of technological paradigm that will redefine the actual perception of the Internet of Things (IoT). The term IoT was first envisaged by Kevin Ashton in 1999 [1] to define a network that not only connects people but also 'things or devices' around them. By 2009 the number of devices (things) connected to the Internet exceeded the number of people on Earth. With over 12.3 billion active endpoints in 2021 [2], the IoT market is transforming the business and consumer world in an unforeseen manner and is set to propel a new industrial revolution. Moreover, International Data Corporation (IDC) forecasts that the number of connected devices will reach 41.6 billion in 2025 [3]. Apparently, IoT is reaching out to a diversity of technological domains such as health system, connected vehicles, traffic management, power grids, environmental monitoring, smart buildings, homes, cities, industrial, agricultural and commercial management. Therefore, IoT will unbelievably have a great impact on almost every aspect of our lives.

The growing number of applications make the significance of IoT in the future evident. This growth is due to the technological evolution with the improvement of the key techniques such as the communication bandwidth, lower operational costs, enhanced productivity, better quality control, device accessibility, low power consumption, high computation capabilities, heightened understanding and visibility into real-world activities, and high storage capacity. Additionally, integrated technologies such as Wireless Sensor Networks (WSN), Machine-to-Machine (M2M) communication, cyber-physical systems, human-machine interaction, etc. have evolved as integral components of IoT. However, security issues related to these technologies continue to disrupt IoT based data communication. Since IoT consists of a collection of networks and computational devices, it inherits the conventional security issues related to the traditional networks. Moreover, IoT devices have been susceptible to cyber attacks and various exploitation [4]. This is due to the fact that resource-constraint environment does not give flexibility to implement high-level cybersecurity measures. Therefore, the entire IoT architecture need to be secured from threats that may pose problems to confidentiality, privacy and integrity of the overall system. Since the conventional security mechanisms are heavy for IoT devices due to their resources limitations, lightweight security solutions are required.

A. MOTIVATION AND CONTRIBUTION

The main motivation behind this work is to re-define an IoT ecosystem architecture from the core technologies view point by proposing a modified three layers IoT architecture. Moreover, along with the already known security mechanisms and standards, we present the security mechanisms implemented in IQRF technology to secure its data.

Major contributions of this article can be resumed in two points:

(1) We re-define the three layered architecture comprising *Perception Layer (L_p)*, *Network Layer (L_n)* and *Application Layer (L_a)* as IoT mainly operates on these layers. In the new architecture we divide $\mathrm{L_p}$ into three blocks namely *Perception Sensor Block (PB_s)*, *Perception Application Block (PB_a)* and *Perception Network Block (PB_n)*. We also add an Edge Block *(B_e)* which is an intermediate block that acts as a bridge between the IoT device network and the Internet as illustrated in Figure 1. Few justifications behind the division of the L_p into three separate blocks are:

  (a) Adding PB_s will help in controlling the nodes and in data acquisition. At this block IoT devices measure the physical quantities of the place where they are located and convert them into digital signals to be transmitted and analyzed at upper layers.

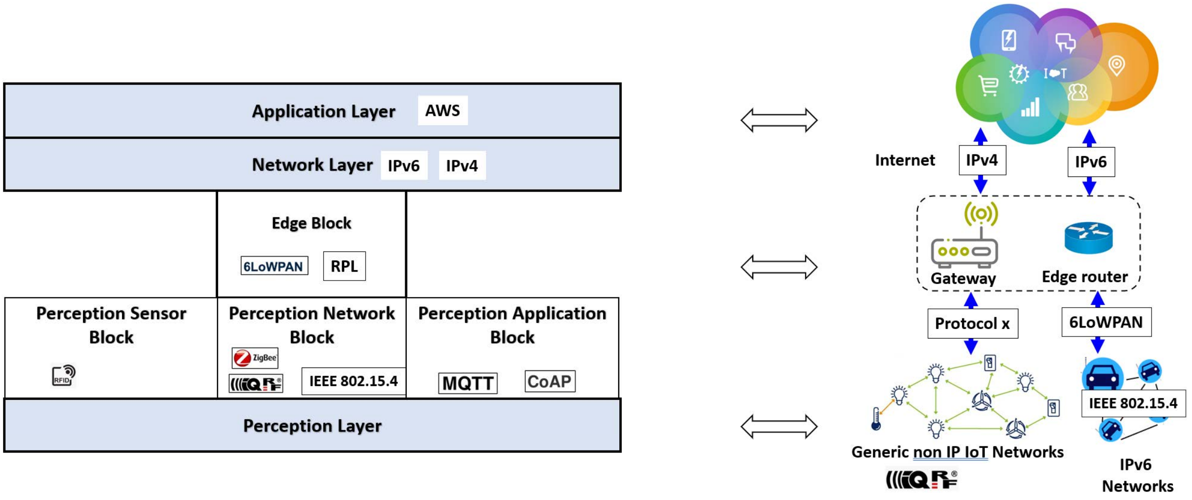
  (b) Adding PB_a will help differentiate high-level applications such as smart cities, smart transportation, smart grid etc. defined at the Application Layer of an IoT ecosystem than low-level application protocols such as Constrained Application Protocol (CoAP), Message Queuing Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP) and Advanced Message Queuing Protocol (AMQP) which are designed to be installed in resource-constrained IoT devices.

  (c) Adding PB_n will help differentiate IoT networks, for instance IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) or non-IP generic networks standing behind an IPv4 gateway such WSN from the IP based Network Layer. 6LoWPAN networks and IPv6 networks are linked to each other through B_e.

  (d) The modified architecture gives a better classification of IoT enabling technologies, IoT challenges and IoT security solutions as presented further in this paper.

The concept of dividing the L_p into blocks has been discussed before. Authors in [5] and [6] define L_p as two different parts and attempt to study their security aspects. First part is the *perception node* or device reflecting the sensing side of IoT devices such as sensors, microcontrollers and RFID tags. Second part is the *perception network* reflecting the networking side of IoT networks such as low-power and lossy networks. However, to best of our knowledge, adding PB_a and B_e to the IoT ecosystem has not been visualized yet.

(2) We give a special focus to IQRF technology by highlighting its implemented security aspects along with the other known security aspects already implemented in



(a) Layer-wise IoT Ecosystem Architecture

(b) Component-wise IoT Ecosystem Architecture

FIGURE 1. IoT ecosystem architecture.

TABLE 1. Related surveys on security aspects and mechanisms in the IoT.

Year	Author	Contributions
2019	Vikas Hassija et al. [19]	Presents a detailed review of the security-related challenges and sources of threat in the IoT applications
2020	Shapla Khanam et al. [20]	Presents an overview of IoT, its system architecture, enabling technologies, and discusses security challenges
2020	Bin Liao et al. [21]	Analyzes the security of IoT devices and provides the countermeasures in response to security problems and challenges by using mobile computing
2020	Salma et al. [22]	Presents the challenges of IoT security and the security requirements needed by IoT systems
2020	Vishal et al. [23]	Surveys the security, privacy and trust for Smart Mobile-Internet of Things
2020	Ismail et al. [24]	Presents a review of security attacks towards WSNs and IoT, along with the techniques for prevention, detection, and mitigation of those attacks
2021	Pawani et al. [25]	Surveys the security considerations with 6G enabling technologies
2021	Shalitha et al. [26]	Surveys the exploitation of Network Slicing for Internet of Things in 5G Networks
2021	Van-Linh Nguyen et al. [27]	Surveys the security and privacy issues based on prospective technologies for 6G
2021	Dinh C. Nguyen et al. [28]	Surveys wireless artificial intelligence applications in various data-driven domains
2021	Yasmine et al. [29]	Provides an up-to-date vision of the current research topics related to IoT security and propose a taxonomy of IoT attacks and analyze the security vulnerabilities of IoT at different layers
2021	Pasika et al. [30]	Analyse the security and privacy of the Multi-Access Edge Computing system
2021	Zhiyuan Yu et al. [31]	Surveys the security and privacy problems arising from the interaction of cyber world and physical world, with the context of broad cyber-physical applications
2021	Euijong Lee et al. [32]	Surveys the international standards related to interoperability and security for IoT environments
2022	Xing et al. [33]	Provides an overview of IoT equipment's physical security and safety, antitheft and antivandalism schemes along with circuit and system design, additional sensing devices, biometry and behavior analysis, and tracking methods
2022	Arup et al. [34]	Surveys the security and privacy threats for bluetooth low energy in IoT and wearable devices
2022	Lijun et al. [35]	Analyse various dimensions of trust, dynamic changes of context, privacy preserving, and cross-domain issues
2022	Jiani et al. [36]	Provides general security guidelines for IoT-enabled smart city developments, highlights common security challenges and reviews recent cryptographic security implementations for IoT-enabled smart cities
2022	Emilie et al. [37]	Provides a comprehensive overview of machine learning approaches to enable more effective and less detectable attacks and investigates cyberattacks integrating machine learning algorithms and provides future research directions, especially for jamming, side channel, false data injection and adversarial machine learning attacks
2022	This Survey	Surveys the security aspects and mechanisms in the IoT and proposes a new layer-wise IoT architecture

IoT technologies and standards presented in this article and which could be compared to IQRF. Several research papers about IQRF technology have been introduced and most of them demonstrate the utilization of IQRF technology in different cases such as wireless temperature measurement [7], monitoring system [8], smart cities [9], home automation [10], [11] and other use-cases described in [12]. However, no detailed studies have been done on the security aspects of IQRF.

B. RELATED EXISTING SURVEYS AND SCOPE OF OUR SURVEY

There is no widely accepted definition for IoT nor a single consensus on an IoT architecture. Different architectures have been presented in [13], [14], [15], [16], [17], and [18] attempting to address IoT aspects from different perspectives. A list of major survey and review works done on security aspects and mechanisms in the IoT domain in the last few years is given in Table 1.

C. ORGANIZATION OF THE PAPER

The paper is organized as follows. After the introduction in Section I, we redefine an IoT ecosystem and propose a new layer-wise IoT architecture in Section II. Section III presents some of the most prominent enabling technologies in IoT and their native security mechanisms. These technologies are categorized under each layer of the proposed architecture. Furthermore, based on the layered IoT architecture, we outline the research framework of security aspects and mechanisms in the IoT framework. In Section IV we discuss several common IoT threats and categorize them under the proposed architecture. In Section V we present security mechanisms and solutions for IoT ecosystem to overcome different threats. Section VI presents in brief some future research directions. Finally, we conclude the paper in Section VII.

II. IoT ECOSYSTEM

In business context, the concept of an ecosystem has been brought by James [38] after his studies in biological sciences of a natural life ecosystem which is defined as an interaction of organisms with each other and with the environment where they exist. According to Moor, in a business ecosystem, the company's capabilities co-evolve around innovations. Therefore, innovation is considered as the core around which the ecosystem is formed. Since IoT is built around the concept of connecting physical world to the virtual world of the Internet, IoT enabling technologies such as hardware and software platforms as well as standards may become the core of the IoT ecosystem [39]. Moreover, IoT ecosystem core may focus on three key technical domains: connected devices or perception, connectivity or network (also called transport), and applications or services [40]. Currently, there is no single consensus on one IoT architecture which is universally agreed [15]. However, different IoT architectures are proposed such as three layer architecture [13], [14], five layer architecture [15], [16], six layer architecture [17] and even seven layer architecture [18]. The most basic among these architectures is the three layer architecture [15]. This architecture defines the main idea of IoT and was introduced at its early stages of research. It consists of L_p, L_n and L_a. In this paper, we adopt the three layer architecture. We propose to divide the L_p into three blocks namely PB_s, PB_n and PB_a. We add B_e that connects the PB_n to the Network Layer of the layered IoT architecture as illustrated in Figure 1. Layers and blocks are explained further in this section. To show the relationship (mapping) between layers or blocks and the real world implementations and technologies, a component-wise IoT architecture is added besides the layer-wise IoT architecture as shown in Figure 1b.

The layer-wise IoT architecture can be seen as a generalized framework for device networking. It is based on the concept of splitting up a communication system into several abstract layers, each one stacked upon the previous one. Each layer of the architecture handles a specific task and communicates with its neighbouring layers. Therefore, the data flows vertically along the layers, from L_p up to the Application Layer and down in the opposite direction and horizontally from the PB_s, to the PB_a, and in opposite direction. Similar to the layer-wise architecture, the components-wise architecture shown in Figure 1b consists of three logical levels: *IoT devices*, *edge devices* and *infrastructure/cloud*. IoT devices (things) are nodes with direct connection to the physical world providing information or actuating on the environment in which they are placed. IoT devices may be sensors or actuators typically resource-constrained, mobile or static and connected to each other through a wired or a wireless links. Edge devices are typically part of the wired network infrastructure, most of the time static and located close to IoT devices that need a bridging to Internet. Unlike IoT devices, edge devices may have significant computational resources such as CPU, memory and communication interface. Therefore, computation tasks can be done at this level in case short delays are required or the communication with the cloud might causes a bottleneck problem. Moreover, gateways or border routers are a typical examples of edge devices. The cloud is a complete set of tools to connect, process, store, and analyze data coming from IoT devices through the edge devices. It is rich in computation power, however there may be significant delays to IoT devices due to the bottleneck problem. Moreover, using the cloud is important for aggregating data and drawing insights from that data to build up applications such as smart cities, smart homes, connected cars, smart agriculture, energy management, smart shopping, etc. On the other side, the component-wise architecture illustrated in Figure 1b shows two types of IoT networks, IPv4-based networks and IPv6-based networks. As IPv4 protocol is not originally designed for the IoT and is inherently limited to about 4 Billion addresses, most of the devices in IPv4-based IoT applications are not directly addressed with an IP address. They are rather set in groups of devices (networks) connected to each other in a mesh, star or tree topology using certain communication protocols (Protocol X) and connected to the Internet through an IPv4 gateway. In the near future, vast number of things connected to the Internet will need an IPv6 address since the IPv4 address space will be effectively consumed [41]. Accordingly, IPv6 addressing is now desirable as it provides 2^{128} unique addresses or approximately 3.4 10^{38} addressable thing. In IPv6-based and resource-constrained networks, more specifically IEEE 802.15.4 networks [42], devices have a short transmission range, low data rate and limited memory and hence, are unable to handle an IPv6 packet. Therefore, using IPv6 packets in IEEE 802.15.4 networks leads to compatibility issues. To solve these issues, a new interface protocol is required. For this purpose an adaptation layer is suggested and implemented by Internet Engineering Task Force (IETF) [43] allowing transmission of IPv6 packets over Low-power Wireless Personal Area Networks and abbreviated as 6LoWPAN [44]. The adaptation layer is defined to be on the top of MAC layer of IEEE 802.15.4 [45] and mainly made for IPv6 headers compression/decompression, fragmentation/reassembly and routing in IEEE 802.15.4-based networks. Other functions such as neighbor discovery and multicast support are also defined at this layer. In our proposed layer-wise architecture in Figure 1 the adaptation layer can be summarized in the Edge Block. At this level a 6LoWPAN border router may be installed [46]. The 6LoWPAN border router acts as a gateway between IEEE 802.15.4 networks and IPv6 Internet. Devices with intensive resources such as smart phones may connect directly with an IPv6 address to the Network Layer (Internet).

A. IoT ECOSYSTEM: PERCEPTION LAYER

The L_p is also known as the sensor layer of an IoT ecosystem. This layer is the information origin of IoT applications such as smart houses, smart grid and smart city defined at the Application Layer. It contains heterogeneous end devices, generally real time objects such as sensors and actuators. Objects collect information from the surrounding environment where they are located and transmit it to the network layer [17]. As mentioned earlier and illustrated in Figure 1, the L_p is divided into three blocks and an intermediate block that connects the Perception Network to the Network layer (Internet). The Edge Block can be seen as different installed gateways for instance the case of IPv4 networks or border routers for IPv6 networks. The three perception blocks plus the edge block are described in the following subsections.

1) PERCEPTION SENSOR BLOCK

Perception Sensor Block PB_s helps hardwired IoT sensors such as smart meters, temperature sensor, humidity sensor, etc. to acquire data to feed IoT applications. RFID tags are popular types of perception IoT nodes or sensors [5]. Moreover, sensors might be deployed at unattended remote locations. Therefore, they are exposed to physical attacks such as physical tampering, node capture, and eavesdropping. The acquired data at the PB_s is transferred to the PB_a.

2) PERCEPTION APPLICATION BLOCK

Perception Application Block PB_a comprises of application protocols that handle the communication either between gateways and the Network Layer in case of IPv4 IoT applications, or between resource-constrained devices (end nodes) and the Network Layer in case of IPv6 IoT applications. There are several application protocols at this block including, but not limited to CoAP, MQTT, XMPP and AMQP [47]. For instance, non-IP networks are connected to the Network Layer behind an IPv4 gateway and the application protocol may be installed on the gateway itself. While in networks where devices support IPv6 protocol e.g. 6LoWPAN networks, devices are addressed directly with an IPv6 address and the application protocol may be installed on the device itself. Data after being treated at this block is sent to the PB_n.

3) PERCEPTION NETWORK BLOCK

Perception Network Block PB_n comprises of the networking part of WSNs. At this block the communication is usually done in wireless mode, for instance as in IEEE 802.15.4 networks. Moreover, the PB_n forwards data from IoT devices to the Edge Block to be sent later to the Network Layer [5]. In the PB_n, routing is the key responsibility. Therefore, proactive routing protocols such as Wireless Routing Protocol (WRP), Topology Dissemination Based on Reverse-Path Forwarding Protocol (TBRPF) and reactive routing protocols such as Temporarily Ordered Routing Algorithm (TORA), Energy-aware Temporarily Ordered Routing Algorithm (E-TORA), Routing Protocol for Low-Power and Lossy Networks (RPL) are used to find and maintain optimal routing paths in IoT WSNs [48]. RPL is a promising routing protocol in IEEE 802.11.4 networks that uses 6LoWPAN protocol.

4) EDGE BLOCK

As mentioned earlier, transmission of IPv6 packets over IEEE 802.15.4 networks is not a natural fit. Therefore, and adaptation layer that makes possible the transmission of IPv6 packets in IEEE 802.15.4 networks is required. The adaptation layer is defined to be the interface between IEEE 802.15.4 MAC layer (Perception Network Block in our architecture) and the Network Layer. This layer has some basic functions such as compressing and decompressing IPv6 packets headers, fragmentation and reassembly of IPv6 packets, and mesh-under routing of IPv6 packets using one of the mentioned WSN routing protocols [49].

B. IoT ECOSYSTEM: NETWORK LAYER

The Network Layer is the core layer of IoT ecosystem architecture. This layer is also called transport layer as information routing is the main function of this layer. Hence, this layer aims to transmit the data collected from the (L_p) to any specific information processing system through Internet using technologies such as Wi-Fi, LTE, 3G/4G/5G etc. ensuring the transport of end devices information to the application layer [50].

C. IoT ECOSYSTEM: APPLICATION LAYER

IoT Application Layer covers high-level IoT applications that enable device-to-device and human-to-device interactions in a reliable and robust manner. The Application Layer helps in the processing of data and provide services requested by the end-users. After being collected by IoT devices, data is analyzed at the Application Layer for decision making in different application domains including but not limited to smart healthcare, smart cities, smart home, smart agriculture, and disaster management. Applications in IoT can be divided into five categories [5] such as personal and social applications, home applications, transportation and logistics, healthcare applications and smart environment. All mentioned applications deal with different data types, different sensors and gateways and they require different data analysis models.

The (L_p) with its three blocks plus the Edge Block, The Network Layer and The Application Layer in an IoT Ecosystem are vulnerable to different types of cyber and physical security attacks. We present these attacks in Section 4.

III. SECURITY IN IoT ECOSYSTEM ENABLING TECHNOLOGIES

IoT ecosystem represents a very flexible way of organizing smart applications and building consumer-oriented infrastructure. However, there are a number of issues that affects the security and privacy of the involved parties when it comes to low-power IoT devices. Often, there is a trade-off between implementing cybersecurity measures and maintaining operations within given tolerances. As a result, implementation of data protection and cyber defence mechanisms comes as the last priority [51]. In this section we present the native security mechanisms of today's most prominent IoT enabling technologies and standards that are classified under each layer of the proposed IoT ecosystem architecture as illustrated in Figure 1. The security mechanisms of these technologies are summarized in Table 3.

A. IoT PERCEPTION LAYER SECURITY ASPECTS

1) PERCEPTION SENSOR BLOCK SECURITY

a: SECURITY IN RFID

RFID system is made of two parts. First an RFID electronic tag, also called the transponder which contains a constrained microchip to store information, and an antenna. The RFID tag can be attached to the object for purpose of identification, tracking or monitoring. Second, an RFID reader, also called the interrogator. The reader communicates, reads or writes (interrogates) the tag through radio waves. Moreover, the tag can be either passive (therefore it is powered in wireless mode by the reader to function), or active with an on-board power supply. Passive tags are read over few centimeters while active tags can be read from farther distances depending on the application. When RFID reader is equipped with an appropriate communication protocol allowing its connectivity to the Internet, the distributed RFID readers can identify, track and monitor tagged objects globally. This is the so-called Internet of Things [52], [53], [54]. A typical use of RFID technology is in industries in order to reduce the operating costs by: better supply chain and inventory management; reducing manual processes through automated scanning; providing real-time information needed for better decision making; improving the speed and accuracy for tracking pallets, cartons, and containers; helping to control stocks levels; improving the management of inventory and so on [55]. Other benefits of RFID can also be mentioned in fields such as in agriculture, livestock's identification, health sector, airline industry, food industry, pharmaceutical industry and many more [55].

In comparison to the benefits that RFID offers, it does not cover sufficient security and privacy support due to its resource limitations. Many requirements are pointed out for RFID security in [56], [57], [58], and [59] such as protection from unauthorized access, protection from illicit tracking, protection from skimming, availability, authenticity, integrity, anonymity, forward secrecy and technology scalability. However, building an RFID security mechanism is a big concern due to fact that the RFID devices are limited in terms of computational capabilities, unreliable communication and less power [57]. Additionally, many types of attacks on RFID systems, either physical-based or software-based can be mentioned including but not limited to, eavesdropping, relay attacks, traffic analysis, spoofing, denial of service (DoS), tag removal, back-end attacks, jamming, blocking, tag destruction, malware tag content changes, replay attack and tag cloning [60]. RFID security policy to mitigate security and privacy risk relies either on (a) Physical methods such as electrostatic shielding (Faraday Cage), blocker tag where it constantly sends fake tag serial numbers to conceal the order number of other tags, reader frequency modification, tag frequency modification and kill order mechanism, (b) The code mechanism which is designing and achieving a code protocol that fits with RFID security requirements such as hash-lock schemes, or (c) Both of them [61].

2) PERCEPTION APPLICATION BLOCK SECURITY

a: SECURITY IN CoAP

CoAP is an IoT application layer protocol created by the Constrained RESTful Environments (CoRE) working group in the Internet Engineering Task Force (IETF) standardization body. This group aims to design a Representational State Transfer (REST) architecture to be supportable by the constrained devices with limited computation, storage and communication capabilities. CoAP is a UDP-based specialized web transfer protocol for use with constrained nodes and constrained networks e.g., low-power and lossy networks.

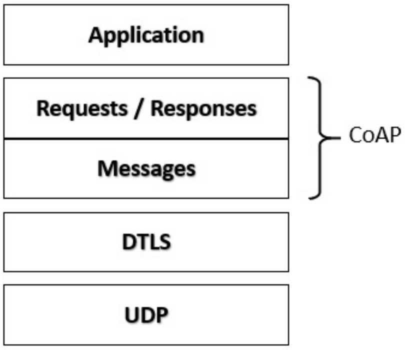


FIGURE 2. Abstract layering of DTLS-Secured CoAP [62].

Moreover, this protocol is designed to interface with Hyper Text Transfer Protocol (HTTP) allowing applications with specialized requirements such as very low overhead, multicast support and simplicity for constraint environment to interact with the web. However, CoAP does not blindly uses HTTP, instead it is designed as a subset of RESTful architecture to be optimized for M2M communication [62], [63]. As defined in [62] and illustrated in Figure 2, CoAP as single protocol can be seen as two-layer approach. The first is the Messaging layer deployed to deal with the UDP layer and its unreliable nature, and the second is the Request/Response layer where method and response codes are used. Similar to HTTP which uses Transport Layer Security (TLS) [64] over TCP to ensure data security, CoAP uses the Datagram Transport Layer Security (DTLS) [65] protocol over UDP to encrypt data as shown in Figure 2. DTLS protocol is another version of TLS protocol and basically designed to allow TLS to deal with the unreliable nature of the datagram transport protocol.

Security in CoAP protocol can be ensured in many ways. The mandatory security mechanism to implement for CoAP is the DTLS. Other applications may use another security mechanism such as IP security (IPsec). Therefore, in CoAP, devices that need authorization for certain operation are expected to run at least under one of the two previously mentioned security mechanisms, DTLS or IPsec. However, most of the experiments in securing CoAP so far have been made with DTLS. After providing the security information that a CoAP device needs at the end of the provisioning phase including the keying materials and access control lists, the CoAP device will be in one of the four security modes [62], [66]. First mode is *NoSec*, meaning that there is no protocol level security. In this mode the DTLS protocol is disabled, unlike the other three security modes. However in this mode other security alternatives can be used such as IPsec providing security at lower layer. Moreover, in this mode packets are simply sent over normal UDP-IP and the only way to secure the system is to keep attackers away from being able to send or receive packets in networks with nodes running with CoAP. Second is *Pre Shared Key* (PSK) mode, where the keys are shared in advance between the communicating parties to establish DTLS link. Depending on the deployed cipher suite, the use of PSKs is better than the use of a public key which makes DTLS useful in constrained devices networks. Additionally, in this mode there is a list of PSKs and each key may include one or more nodes that can be used to communicate with. Thus, a system selects an appropriate key and then establishes a DTLS session. Nodes in this mode must support at least the TLS_PSK_WITH_AES_128_CCM_8 cipher suite [67]. This suite provides authentication using PSK (Symmetric) and 8 byte authentication tag. Third mode is the *Raw Public Key* (RPK) where it is assumed that nodes have an asymmetric key pair installed with no certificate. The asymmetric key pair or RPK can be generated and installed during the manufacturing process. However, nodes willing to use the RPK need to support the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 [67]. Fourth mode is called *Certificate* where each node has an asymmetric key pair with a X.509 certificate that binds it to its authority name and is signed by a third party (trusted root). Nodes in this mode must support the same cipher suite as RPK mode. Moreover, in this mode, a node has also a list of trusted roots for certificate validation. However, this security mode requires the availability and usage of a security infrastructure.

In cipher suites used for RPK and Certificate modes, DTLS along with AES/CCM integrates the Elliptic Curve Cryptography (ECC) concept for device authentication using the Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman Algorithm Ephemeral keys (ECDHE) for key agreement as defined in [68].

b: SECURITY IN MESSAGE QUEUE TELEMETRY TRANSPORT MQTT

MQTT is an application layer transport protocol suitable for M2M and IoT communication. This open Client Server publish/subscribe protocol standardized by OASIS is designed to be simple and lightweight messaging protocol suited to be used by the constrained devices in low-bandwidth and unreliable networks. Moreover, MQTT protocol has been widely implemented across a variety of industries since it is has been designed. The architecture of MQTT consists of a publisher, a subscriber and a broker [69]. Publishers, for instance sensors, put the data on the broker which plays the role of an intermediary from which subscribers such as applications interested in topics take the data that has been published by the sensors. In its conception, MQTT contains some of the key characteristics: (i) Some of them can be related to the publish/subscribe pattern which provides the ability of sending a message by one publisher to many subscribers (one-to-many), (ii) MQTT supports different Quality of Service (QoS) levels viz. the first level (QoS 0) related to message's best efforts delivery. Even though some of the messages can be lost, *at most one* of them has to reach the destination, the second level (QoS 1) *at least one* message has to arrive at the destination but duplication can happen, and the third level (QoS 2) where messages have to reach the destination but *exactly once*, therefore there is no duplication (iii) Messaging transport is independent than the continent of the payload, (iv) MQTT has less transport overhead and protocol exchanges minimizing the network traffic, and (v) Notifying interested parties when an abnormal disconnection happens [70].

To keep it simple and lightweight, MQTT standard doesn't provide a specific security mechanism in its own like for instance CoAP. However, it keeps the choice open for the developer to deploy the security technology specific to their designs. Moreover, this standard recommends some security solutions that can be implemented with MQTT such as SSL/TLS [64]. It also recommends for implementations using SSL/TLS as a security option to use the TCP user port 8883 as a secured port (secure-mqtt) assigned by IANA [71] opposite to the port 1883 port which does not use TLS protocol. However, SSL/TLS is not the lightest of the protocols and does add a significant overhead to the network. MQTT also provides an authentication mechanism through the CONNECT packet. This packet supports the basic authentication of a network and it is the first packet sent by the client to the server after establishing a network connection. This packet gives the possibility for an application to integrate a username and a password in the payload fields. Therefore, applications can choose how to use the content of these fields, for instance providing their own authentication mechanisms. Another way to secure data in MQTT can be by encrypting data at the application's level that uses this protocol.

3) PERCEPTION NETWORK BLOCK SECURITY

a: SECURITY PHY AND MAC OF IEEE 802.15.4

IEEE 802.15.4 standard [72] defines the MAC and PHY layer of many networking specifications protocols including but not limited to 6LoWPAN, Zigbee, WirelessHART, WiSUN, MiWi and Thread. This standard is developed to provide a framework and the lower layers of the OSI model, the physical (PHY) layer and the medium access control (MAC) sublayer for low-cost, low-rate and low-power wireless connectivity networks. In addition to its defined features, IEEE 802.15.4 MAC sublayer provides the basic floor for designers to implement application-appropriate security mechanisms at higher layers. Therefore, four basic security services at MAC sublayer [72], [73], [74] can be requested by higher layers:

- Access control on MAC sublayer gives the legitimate nodes the ability to detect and block messages from unauthorized devices which are not part of the network.
- Message integrity allows devices in the network to detect the authenticity of an intercepted and modified message in the transit. This is realized by including in each packet the computed message integrity code (MIC) by the sender and the receiver using a shared secret cryptographic key.
- Message confidentiality, this is done through a symmetric-key encryption mechanism to keep the message abstract for the interceptor. In order to have different cipher-texts for the same message, a unique nonce is used at each packet encryption. Moreover, when the Time Slotted Channel Hopping (TSCH) mode is disabled, the nonce is generated uniquely for each re-transmission ensuring that old communications cannot be reused in replay attacks. However, the replay protection is not provided in IEEE 802.15.4 when TSCH mode is enabled.
- Replay protection means that if an adversary eavesdrops on a legitimate message, record it, and resend it to the receiver attempting a relay attack, this can be detected by the receiver using the MIC incremented by the sender for each packet.

TABLE 2. Security suites supported by IEEE 802.15.4 [73].

Name	Description
Null	No security
AES-CTR	Encryption only, CTR Mode
AES-CBC-MAC-128	128 bit MAC
AES-CBC-MAC-64	64 bit MAC
AES-CBC-MAC-32	32 bit MAC
AES-CCM-128	Encryption & 128 bit MAC
AES-CCM-64	Encryption & 64 bit MAC
AES-CCM-32	Encryption & 32 bit MAC

In IEEE 802.15.4, the security requirements must be explicitly specified by the application in which this standard is implemented by choosing one of the security suits summarized in Table. 2. Therefore, by default the security at applications using IEEE 802.15.4 is disabled as long as the application does not set any control parameters on IEEE 802.15.4 MAC sublayer. IEEE 802.15.4 sets the encryption algorithm to use when cyphering the data to transmit. However, the standard does not specify how the keys have to be managed or what kind of authentication policies have to be applied and hence, these issues are treated at upper layers. Moreover only packets of type beacon, data and control packets can optionally be secured by IEEE 802.15.4 MAC sublayer's integrity and confidentiality services. However, the security for acknowledgment packets is not supported by IEEE 802.15.4 MAC sublayer [72], [73], [74].

b: SECURITY IN ZigBee

ZigBee is an open standard owned by ZigBee Alliance that is built on top of the PHY layer and MAC sublayer of IEEE 802.15.4 standard. Moreover, ZigBee standard describes specifications for higher protocol layers, the ZigBee Network (ZNTW) layer and ZigBee Application (ZAPL) layer. ZNTW layer provides functionality to ensure correct operation of the IEEE 802.15.4 MAC sublayer and to provide a suitable service interface to the application layer. ZAPL layer consists of three main components: (i) Application Support sublayer (APS) which act as an interface between the ZAPL layer and ZNTW layer, (ii) Application Framework which is the space where ZigBee applications are situated on every ZigBee device, and (iii) ZigBee Device Objects (ZDO) which is the interface providing a class of functionalities between the application objects in the Application Framework and APS. Several responsibilities are attributed to ZDO such as initializing different blocks in ZigBee stack [75] (for instance APS, ZNTW layer and Security Service Provider (SSP) block) and assembling configuration information from the end applications to implement service discovery, security management, network management, etc.

ZigBee standard support two types of security models, centralized and distributed. The centralized security model is complex but most secure since this model involves a third logical device in addition to routers and end devices in the network. The third logical device is called the trust center or the network coordinator. From the security viewpoint, the trust center's responsibilities are: (i) Authenticating and configuring routers and end devices when they are joining the network, (ii) Generating network key for encrypted communication across the network, (iii) Switching to a new network key either periodically or when it is required limiting the life time of the network key, (iv) Establishing a unique link key for each device to securely communicate with the trust center when joining the network, and (v) Maintaining the security of the whole network. In this security model routers and end devices are not involved in establishing any of the network keys. Unlike the centralized security model, the distributed security model is simpler but less secure. In this model, only routers and end devices are involved in the network. In addition to their routing function, routers are the ones responsible for forming the distributed network and also in registering newly joint routers and end devices. Routers issue the network keys for messages encryption in the network.

All security mechanisms used in ZigBee rely on AES 128 bits encryption algorithm in Enhanced Counter with CBC-MAC (CCM*) mode of operation since initially ZigBee security complements the security services provided by IEEE 802.15.4 standard in which the same security policies are used. In ZigBee standard there are three kind of symmetric keys: (i) Master key which is a shared key used during the execution of a symmetric-key establishment protocol. The master key is the basis for long-term security between the two devices, and may be used to generate link key, (ii) Link key is a key that is shared exclusively between only two peer entities present at ZAPL layer within a ZigBee network, and (iii) Network key is used by ZigBee devices to secure outgoing ZNTW layer frames and that is available for use to process the incoming frames also. The ZNTW layer key is a temporary, unique AES 128 bits key generated by the trust center whenever it is outdated and shared with all devices in the network using the old key. Moreover, network key is necessary for any node willing to join the network [76].

c: SECURITY IN IQRF

IQRF is an emerging technology based on wireless packet-oriented communication using Direct Peripheral Access (DPA) protocol via radio frequency connectivity. This main components of this technology are a transceiver module (TR), an operating system (OS) and a gateway. The IQRF TR module is an intelligent electronic board containing a communication device, a micro-controller and other optional components. Moreover, IQRF TR modules are end devices (nodes) in every IQRF wireless network. IQRF OS provides access to the TR module resources such as processor, memory, peripherals and communication interfaces. This operating system is installed on the micro-controller of each IQRF TR module. Additionally, IQRF OS contains a large number of functions for communication and network services such as bounding, routing and devices discovery. Therefore, IQRF OS represents the network layer of the IQRF wireless networks supporting peer-to-peer and mesh networking. IQRF gateway called Gateway Daemon (GWD) is an interface to LAN and Internet connectivity (cloud). The IQRF GWD is a project that provides open-source components for building IQRF Gateways [9], [77]. Furthermore, IQRF uses in its TRs modules for communication the low-power, low-data rate RF transceiver named ST SPIRIT1 [78]. In addition to its communication capabilities, SPIRIT1 includes an AES 128-bit encryption co-processor providing the basic ground for IQRF to implement its security mechanisms.

In IQRF networks, encryption is the way to prevent unauthorized access and protect sensitive data. Hence, all encryption schemes in IQRF networks utilizes AES 128-Bit standard. IQRF technology uses three different encryption mechanisms. First, access encryption which is used to secure all sensitive wireless operations such as bounding and maintenance. Bounding is one of the most critical operations from the security point of view. I this operation, all sensitive data such as network keys (used in network encryption), node ID and node address are exchanged. Therefore this phase has to be well protected. To do so, an access key is generated from a 16 bytes user specified password. The generated access key along with AES 128-Bit in Electronic Codebook (ECB) mode is used for data access encryption. Second, network encryption which is deployed during normal network operations. Therefore, all packets circulating in IQRF network are encrypted. In this encryption mechanism, the AES 128-Bit standard with 16 bytes network encryption key and additional Cipher Block Chaining (CBC) proprietary algorithm is used. Unlike access encryption key, the network encryption key is derived from a 192 bits long, unique, and randomly generated password by the manufacturer and stored in all IQRF TRs. However, in a given IQRF network, only the password stored in the coordinator is used to generate the network encryption key. Third, user encryption mechanism which is used to increase security by encrypting the user's data. This mode is fully controlled by the user. Therefore, a 16 bytes key is manually entered. However, the user key must be the same for all nodes willing to join a given network. Similarly, to access encryption and network encryption, user encryption is also based on AES-128 with 16 bytes long key but in ECB mode [79].

4) EDGE BLOCK SECURITY

a: SECURITY IN 6LoWPAN

IP version 6 (IPv6) [80] allows every edge device of the network to be directly addressed. Hence, this flattens the addressing hierarchy, obviates the need of complex gateways and simplifies the connectivity model. Moreover, Low-Power Wireless Personal Area Network (LoWPAN) is a simple, low cost wireless communication network in applications with limited power and relaxed throughput requirements. Therefore, 6LoWPAN is a protocol definition merging the two concepts, IPv6 and LoWPAN to enable networks including constrained devices with limited computation, storage and communication capabilities to deal with IPv6 requirements [81]. More specifically, networks conform to the IEEE 802.15.4 standard which are characterized by short range, low bit rate, low power and low cost. Since IPv6 uses packets much larger in size than the largest frame defined in IEEE 802.15.4, a fragmentation and reassembly adaptation layer must be provided as it is defined in the proposed standard [44].

Often 6LowPAN applications require confidentiality and integrity. This can be realized at higher layers such as application, transport or at lower layers such as the data link layer. In this context, IEEE 802.15.4 provides link layer security based on AES with several modes of operation that can ensure the confidentiality and integrity. However IEEE 802.15.4 omits the details about for instance key management, bootstrapping and security. They are also extraneous to 6LoWPAN and not addressed in its specifications.

b: SECURITY IN IPV6 ROUTING PROTOCOL FOR LOW-POWER AND LOSSY NETWORKS (RPL)

Low-Power and Lossy Networks (LLNs) are networks comprising constrained routers and their interconnects. They are usually constrained in processing power, storage and energy sources. LLNs are also known by their high loss rates, low data rate and instability. Moreover, LLNs support point-to-point, multipoint-to-point and point-to-multipoint traffic flows. IPv6 Routing Protocol for LLNs (RPL) is a distance-vector (proactive) routing protocol. The routing in RPL is based on Destination Directed Oriented Acyclic Graphs (DODAGs). Hence, nodes in DODAG topology are connected in such a way that no cycles are present. The resulting topology is similar to a tree where all routes in each graph end at single destination (sink) called DODAG root. Moreover, the graph is built by the use of an Objective function (OF). This function defines how routing metrics are computed taking in account routing constraints such as Expected Number of Transmissions (ETX), the current amount of battery and other functions during the topology construction. Therefore, a logical topology is built over a physical infrastructure and this specifies an RPL instance defining an OF for a set of one or more DODAGs. Each node in the network has an assigned rank number (Rank). This number defines the distance in terms of hops of that node from the root node. Rank may also be seen as a function of the routing metric or it may be calculated with respect to other constraints. Moreover, a Rank of a node strictly increases or strictly decreases depending on the node's position relative to DODAG root. In addition, the rank helps the protocol to avoid routing loops by computing node's position relative to other nodes and to the DODAG root.

RPL protocol supports four control messages: (i) DODAG Information Solicitation (DIS) sent by a node requesting information about any nearby DODAGs for purpose to join an existing DODAG, (ii) DODAG Information Object (DIO), a message that shares information from an existing DODAG such as the Rank of a node, the current RPL Instance, the IPv6 address of the root, etc. DIO is a response to DIS request, (iii) Destination Advertisement Object (DAO) message that can be used by a node to report its parents to the DODAG root. The DODAG root can assemble together downward along the DODAG to a particular node using DAO parent sets from each node in the route, (iv) DAO acknowledgment (DAO-ACK), a unicast packet sent by a node parent or a DODAG root that received a DAO message as a confirmation to reception, and (v) Consistency Check (CC) message which is used for nodes to resynchronize using CC messages and ensure that message's counter value is not repeated. CC can be sent by a node to protect against replay attacks. RPL uses in it's control messages the Internet Control Message Protocol (ICMPv6) header [82] followed by a message body where the security field can be enabled. Unlike routing protocols that broadcast control messages at fixed time interval causing energy wastage and may present energy hole threat for the network, RPL adapts the DIO messages sending intervals to the frequency of changes of the network topology. Therefore, in non-mobile and stable networks, RPL control messages are rarely sent [83], [84].

RPL protocol defines a secured version of its control messages. Hence, setting the most significant bit (MSB) in the RPL message field named *Code* will identify whether or not the security is enabled for the RPL message (DIS, DIO, DAO or DAOACK). If the security is chosen to be enabled, a security field of four bytes is added to the message right after the ICMPv6 header. Moreover, RPL provides few security mechanisms to ensure network data confidentiality and integrity. In fact, RPL security mechanisms can be seen as three possible security modes, (i) unsecured mode where the exchange security relies on the security of other layers if any is implemented; (ii) pre-installed mode where nodes fully join the network with a pre-shared key and; (iii) authenticated mode where nodes join the network only as leafs waiting for an authentication authority to provide a second key to be fully connected to the network [85]. It is specified in RPL specification document [83] that the encryption for RPL messages is ensured by the AES-128-CCM cryptographic algorithm.

B. IoT NETWORK LAYER SECURITY ASPECTS

The Network Layer is the middle layer of the IoT three layer architecture. This layer is also the third layer of the OSI model. Data routing, data forwarding, logical connection setup, delivery error reporting are the main functions of this layer. Network Layer represents the backbone of systems based on the OSI model as it contains hardware devices such as routers, switches, firewalls, repeaters and bridges.

c: SECURITY IN IPV6 AND IPV4

IPv6, the new version of the Internet Protocol is developed to provide new services and the only available alternative to IPv4. It can support the expansion of Internet enabled applications and devices. The current Internet infrastructure uses the IPv4. However, due to the shortage of IPv4 addresses and the need of a next Internet protocol generation, the adoption of IPv6 is inevitable. IPv6 is expected to enhance many aspects and solve some problems within IPv4. It makes Internet more secure. Compared to IPv4, IPv6 encompasses major modifications such as the address length (128 bits instead of 32 bits), three types of addresses (unicast, anycast and multicast), headers are simplified compared to IPv4 and formerly mandatory IP security (IPSec) [86]. Moreover, IPv6 supports end-to-end communication. This allows the source and destination nodes to communicate directly without the need of intermediate systems such as Network Address Translation (NAT) as in IPv4 Internet. Another important feature in IPv6 protocol is auto-configuration. Unlike IPv4 that uses stateful protocols such as Dynamic Host Configuration Protocol (DHCP) which requires a server to store host's configuration information, IPv6 in addition to it's DHCPv6 introduces another simplified stateless auto-configuration method allowing nodes to assign themselves an IPv6 address using only the available local information with neither connecting to a server nor using a DHCPv6 [87].

IP security (IPSec) [88] is a suite of protocols designed by IETF. This protocol provides network layer (Internet) encryption and authentication of traffic at IP level. In IPv4, the use of IPSec is optional. Therefore, in IPv4 networks, the NAT is used instead. However, in IPv6 networks, the support of IPSec is mandatory as the use of NATs become unnecessary because of the expanded address space. The Authentication Header(AH) and the Encapsulation Security Payload (ESP) are used to implement the IPSec [89]. Since the security in IPv4 was not taken into consideration while designing the IPv4 protocol, some security alternatives were developed. The Secure Sockets Layer (SSL) is one of them and used to secure web browsing, data transfers and e-mails [89]. The use of IPSec in IPv6 will not make IPv6 more secure than IPv4 as this security mechanism is available for both of them. The need of Key Management Infrastructure (KMI) is vital for the use of IPSec to make the implementations of IPv4 and IPv6 more practical. In addition to that, establishing a KMI is not an easy task as it requires complicated mechanisms of trust and key management [86].

C. IoT APPLICATION LAYER SECURITY ASPECTS

The Support Layer [90] that provides support for the requirements of diversified applications via intelligent computing techniques, for instance cloud computing, middleware, service support etc. is merged with the Application Layer in the proposed IoT ecosystem architecture. Additionally, the Application Layer consists of applications and services including but not limited to intelligent transportation, healthcare, intelligent traffic, smart environment, smart home, etc., [90]. The security of IoT applications merely is not a part of this paper, but also we focus on the security of the cloud in an IoT ecosystem.

The cloud provides to companies and users various capabilities such as computing power, storage capacity, services, and running applications over the Internet. However, there are several security concerns related to cloud computing which are faced by both, the cloud providers and their customers. A number IoT cloud providers presented in [91] and [92] are emerging into the market. In this following paragraph we present the security mechanisms of Amazon Web Services cloud platform.

d: AMAZON WEB SERVICES (AWS) IoT PLATFORM

AWS is a cloud computing platform with high scalability, availability and dependability. AWS presents the necessary tools for customers to run different kind of applications. Confidentiality, Integrity, and Availability (CIA) are very important for AWS to maintain the client's confidence and trust. One of the security policies of AWS is the shared security responsibility [93]. The security responsibility is shared between the customer and the cloud service provider at the moment where the customer moves its system and data to the cloud. AWS is responsible of securing the infrastructure where the cloud is installed and the customer is responsible to put the data on the cloud or the connectivity to it. For instance, configuration of certain security features on the cloud such as user accounts and credentials, logging, and TLS/SSL for data transmission is the responsibility of the customer. Security configurations that has to be done by the customer varies also depending on the selected cloud services and the customer's data degree of sensitivity. On the other hand AWS is responsible of protecting the global infrastructure such as hardware, software, networking, and facilities where all the offered AWS services are run. Protecting the infrastructure hisas the highest priority for AWS. According to AWS, the design and management of AWS global infrastructure security is based on best practices and several security compliance standards listed in [93]. This makes AWS as one of the most secured existing cloud infrastructures.

AWS network architecture allows customer to select the desired level of security and resilience depending on the customer's need. Elements such as secure network architecture, secure access points, transmission protection, amazon corporate segregation, fault tolerant design, and network monitoring and protection make AWS as a world class network infrastructure. These elements come under the network security of AWS and are described in [93] as follow: (i) Secure network architecture includes firewall and other edge devices of the network used to control and monitor the communications. Edge devices provide the sets of rules, Access Control Lists (ACL) and other configurations controlling the information flow, (ii) Secure access points, called also secure API endpoints, is reached by limiting the number of access points to the cloud. This strategy allows a good monitoring of the network traffic. Endpoints allows the customer to establish a secure communication using HTTPs with the customers' system instances or stored data, (iii) Transmission protection is ensured by HTTPs using the Secure Sockets Layer (SSL) protocol. AWS provides also an additional layer of security such as Amazon Virtual Private Cloud (VPC) for customers who require higher level of security. VPC provides a private subnet and give the customer the possibility of using IPSec Virtual Private Network (VPN), (iv) Amazon corporate segregation is implemented by segregating the AWS production network from Amazon corporate with a set of segregation devices, (v) Fault tolerant design ensuring a high level of availability and minimizing the impact of failures on the customers, and (vi) Network monitoring and protection using automated monitoring systems in order to provide a high level of service performance and availability. Furthermore, account security features such as credentials for access, HTTPs endpoints for encryption data transmission, user activity logging, and others are also provided by AWS to keep customers' account safe from unauthorized access [92], [93].

IV. TYPES OF ATTACKS IN AN IoT ECOSYSTEM

For long time several types of attacks have been present in the traditional cyberspace including interconnected computerized networks, services, computer systems, embedded processors, and information storage or sharing [94]. However, the new threat in IoT is the scale of connected devices and relative simplicity of attacks. Therefore, millions of interconnected resource-constrained devices can be a potential victim of cyber attacks. In this section, we briefly present the most common attacks in an IoT ecosystem. From the technical viewpoint, various attacks illustrated in Figure 3 are encountered in different layers of the IoT ecosystem architecture defined in this paper. At the end of this section we show in Table 4 how the IoT enabling technologies presented in this paper may be affected by these attacks.

A. IoT PERCEPTION LAYER SECURITY ATTACKS

1) PERCEPTION SENSOR BLOCK ATTACKS

a: NODE CAPTURE/REPLICATION ATTACK

Wireless sensor networks can quickly scale to large node configurations. As the sensor nodes are low-cost, their hardware components are unprotected by a type of physical shielding that could prevent access to processing, memory, sensing or communication components. Therefore, placing unshielded sensor node in a hostile environment enables an adversary with a little effort to access the sensor's internal state and capture, replicate or insert a duplicated node in a chosen network. Such attacks may cause dramatic consequences and the network might be corrupted by the adversary or disconnects a significant part of it [95].

b: DEVICE TAMPERING ATTACK

An adversary can physically tamper with the node for example, switch off or restart and steal keys, codes, and data [5].

c: NODE PHYSICAL DAMAGE ATTACK

In this attack an adversary can physically harms or destroy a node in an IoT system and results a Denial of Service [96]

d: JAMMING ATTACK

Jamming attack belongs to one of the DoS attack class. It is an active attack, meaning that it can be responsible of modifying the data stream or a creation of false data stream. In this attack an adversary employs malicious nodes to disrupt the communication in an IoT perception network through interference. In resource-constrained network, these type of attacks affect negatively the limited resources of the devices, hence harming the network. Jamming attack can be classified into four types [97]: Constant jamming, where the attacker generates constant noise at the same frequency that the WSN operates; Deceptive jamming, where the attacker replaces the valid signals or fabricates instead of sending random bits; Random jamming, where the jammer node jams the network for a particular amount of time and turns off the radio and sleeps for the rest of time instead of being active continuously; and reactive jamming, where the jammer node stays quiet when the channel is idle and starts emitting radio signals as soon as it senses the channel activity.

e: MAN IN THE MIDDLE ATTACK (MiM)

In this type of attack, the attacker intercepts the communication between two nodes and becomes the originator of messages. The receiver node can be tricked thinking that the received messages are from a legitimate source. An example of MiM attack is in RFID systems where the attacker places two fake nodes, one close to the tag and another one close to the reader whom it wants to be deceived. After intercepting the signal from the reader, the fake node close to the reader forwards the signal to the fake node near the tag without trying to identify the content of the messages. Similarly, the fake node close to the tag forwards the signal to the tag and

TABLE 3. Security in IoT enabling technologies A: Access Encryption; N: Network Encryption; U: User Encryption; L: Link Encryption; R: Recommended.

Security Mechanisms			AES-CCM-128	AES-CCM-64	AES-CCM-32	AES-CBC-128	AES-CBC-64	AES-CBC-32	AES-CTR	AES-ECB-128	DTLS	IPSec	TLS	SSL	UID & PWD
IoT Perception Layer Enabling Technologies	Perception Sensor Block	RFID													
	Perception Application Block	CoAP									*				
		MQTT											* R		*
	Perception Network Block	IEEE 802.15.4	*	*	*	*	*	*	*						
		ZigBee	* ANL												
		IQRF				*N				*AU					
	Edge Block	6LoWPAN													
		RPL	*												
IoT Network Layer Enabling Technologies		IPv6										*			
		IPv4										* R			
IoT Application Layer Enabling Technologies		AWS										*	*	*	*

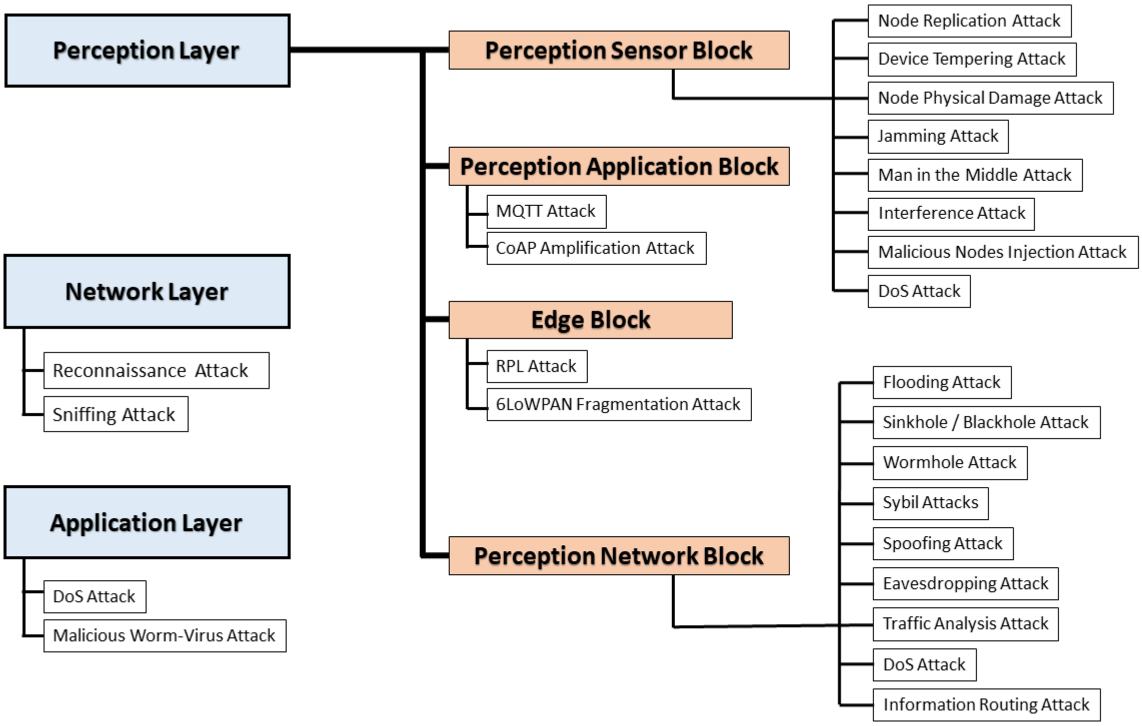


FIGURE 3. IoT ecosystem attacks.

receives a replay from it. The replay message contains the tag ID. Then the replay message is forwarded back to the reader [98].

f: INTERFERENCE ATTACK

In Interference attack, the attacker tries to find out the operating frequency that the WSN uses to transmit data and generates a RF signal at the same frequency. The generated signal can be anything random, creating a noisy environment for the sensor nodes in the network or sending packets following the same protocol used in a WSN with an aim to create collisions. When collision occurs, the back-off time increases for the collided nodes, and therefore, the stream of data changes [97].

g: MALICIOUS NODES INJECTION ATTACK

Malicious Nodes Injection Attack occurs when the adversary has the ability to compromise an arbitrary number of nodes.

In this type of attack, the attacker injects malicious nodes, generally with powerful resources such as processing, storage and transmission capabilities and make them work together in order to create a colliding attack. This attack can be realized in two consecutive phases. First, replicating a targeted legitimate node after compromising it and accessing its stored information, thus gaining full control of it. At that moment, the replicated powerful node is then injected into the network and isolates the compromised node by moving it or depleting its energy. Second, creating another malicious node or entity with a new identity including the copied information from the compromised node and injecting it in the network after synchronizing it with the first injected node. However, this last injected node is not a replica of the compromised node but it is a new node with same properties. The result is two injected malicious nodes working together to achieve desired attacks [99].

h: DoS ATTACK

From the L_p view, given the limited computation ability, a node can easily be vulnerable to DoS attack. This type of attack attempts to make a network resources unavailable to legitimate users [100].

2) PERCEPTION APPLICATION BLOCK ATTACKS

a: CoAP AMPLIFICATION ATTACK

A node with an installed CoAP replays to requests with a response packet. Moreover, a replay packet to request packets may be larger in size than the request itself. This property is know as amplification. An attacker may use this property in CoAP and send small packets requesting for larger packet replays. The misuse of this property may overload the targeted node and cause DoS to it or to the entire network [101].

b: MQTT ATTACK

MQTT can be subjected to several attacks. Disrupting or exhausting the broker by an attacker causes a DoS. Moreover, MQTT is a TCP based protocol and is vulnerable to TCP based DoS attacks. A threat model for MQTT-based IoT devices is presented in [102]. In this paper, authors present a number of attacks with different scenarios for each attack such as DoS, identity spoofing, information disclosure, elevation of privilege, and data tampering.

3) PERCEPTION NETWORK BLOCK ATTACKS

a: FLOODING ATTACK

This type of attack leads to saturating the network by generating a large amount of traffic. As a result, the links between nodes become unavailable. An example of this type of attack is HELLO flood attack [103].

b: SINKHOLE/BLACKHOLE ATTACK

In this type of attack an intruder compromises a node to attract all the traffic from neighboring nodes. The compromised node advertises falsified information data to attract a lot of traffic. Due to their communication pattern, WSNs with base station to which all nodes send data, are more vulnerable to sinkhole attacks [103], [104]. Most of the time this attack is lunched in networks using AODV routing protocol. The malicious node waits for the neighboring nodes to initiate a route request (RREQ). Once the RREQ is initiated, the malicious node receives it and sends immediately a false route replay (RREP) message with a higher sequence number convincing the node which sent the request that the route toward the destination is fresh. In this case, the requesting node ignores all the RREPs from other neighboring nodes and sends packets over the malicious node. Whenever a RREQ takes place near the malicious node, it replays with a fake RREQ and takes all routes to it creating what is called a black hole [105].

c: WORMHOLE ATTACK

Wormhole attack happens when two adversaries located in two geographically separated networks create a communication tunnel referred to as wormhole. This tunnel can be a wired link or a wireless link with sufficient range and bandwidth operating at different frequency band. Once the communication is established between adversaries, attacks such as man-in-the-middle can be performed [105].

d: SYBIL ATTACK

In Sybil attack an adversary generates multiple fake identities in the network to control legitimate nodes. In particular, a Sybil attack involves subverting the identities of nodes by creating pseudonymous identities for facilitating malicious access to a network. The distinction between a normal user and an attacker is challenging in Sybil attacks and this makes it one of the most dangerous security threats to IoT networks [106].

e: SPOOFING, REPLAY, AND MESSAGE ALTERING ATTACK

In this type of attack, the attacker injects new or an intercepted data into the network in an attempt to disrupt the network operations. This injection of data can be done either internally by using a compromised node or externally by using a malicious entity. Hence, replayed messages produces incorrect information which can be propagated in the network causing network routing or operation failures [107], [108].

f: EAVESDROPPING ATTACK

Also known as sniffing or snooping attack, it is an incursion where the adversary tries to steal information from the network. The adversary listens passively to the network for the sent, received or broadcast packets to gain access to information such as node identification numbers, sensitive data or routing updates. The intercepted data can be used by the attacker to compromise nodes, degrade application performance or disrupt routing [108].

g: TRAFFIC ANALYSIS ATTACK

This type of attack is similar to eavesdropping attack. However in traffic analysis attack, the attacker simply analyzes the traffic without compromising the data for instance to deduce the traffic pattern, determine the location of key nodes, the routing structure or the application behavior [97], [108].

h: DoS ATTACK

DoS attack in WSNs is when an adversary tries to prevent a partial or total number of legitimate nodes from accessing to network services. This attack can be carried by flooding messages in a network and make it unavailable for users [100], [105].

i: INFORMATION ROUTING ATTACK

Information routing attack is a type of attack where the adversary uses different techniques such as spoofing, altering or replaying routing information to complicate the network operations. This attack can create routing loops, dropping valid packets or partitioning the network [109].

4) EDGE BLOCK ATTACKS

a: RPL ATTACK

RPL is basically vulnerable to most of the WSN attacks presented in [109], [110], and [111] such as selective forwarding attack where the attacker disrupts routing paths; Sinkhole attack attracting nearby nodes to route traffic to the malicious node; Wormhole attack creating a special link between two malicious nodes in the same network or in two different networks and forward packets; Topology attacks for instance rank attack and local repairing attack aiming to change the internal operation of the nodes and break the optimized network topology and; Finally HELLO flood attack.

b: 6LoWPAN FRAGMENTATION ATTACK

As an adaptation layer, 6LoWPAN provides the connectivity between non resource-constrained IPv6-based networks and resource-constrained networks for instance the ones conform to IEEE 802.15.4. Due to the size of IEEE 802.15.4 MTU (127 bytes) compared to the IPv6 MTU (1280 bytes), the IPv6 frame must to be fragmented and transmitted as elementary frames [44]. However, an attacker may take advantage of this situation and either sends its own fragments especially if no authentication mechanism is used or messing the buffer order at the receiver before it is reassembled [109].

B. IoT NETWORK LAYER SECURITY ATTACKS

The implementation of IPv6 as an alternative to the dying IPv4 will not disappear the previous IPv4-based networks attacks. In this subsection we present some of the attacks related to the Network Layer of the IoT ecosystem architecture.

c: SNIFFING ATTACK

In IPv4 and IPv6 based networks, data can be captured while traveling thorough the network. Especially if the confidential transmitted data is not encrypted, the attacker can compromise it easily by running sniffing attack [112].

d: RECONNAISSANCE ATTACK IN IPV4 AND IPV6 NETWORKS

In reconnaissance attack, an intruder collects data about hosts and other network devices and also interconnections of the victim's network and use it to perform other types of attacks. There are two types of methods that are used to launch a reconnaissance attack. Active methods consist of scanning techniques and passive methods such as data mining. One of the active methods is where the intruder pings the targeted network using ping probes to determine the victim's network IP addresses. Once the pinging is done, the intruder scans the ports usually using a software that can perform both actions, pinging and port scan. Although reconnaissance procedures are the same in both IPv4 and IPv6 networks, the size of the sub network (Subnet) in IPv6 (64 bits), which is much larger than the one in IPv4, makes IPv6 networks much more resistant to reconnaissance attacks than IPv4 networks and because of this the number of probes that the intruder must introduce is (2^{64}) which is practically impossible [89]. Even though IPv6 based networks are more immune against reconnaissance attacks, the multicast addresses defined in IPv6 specification document [80] can enable the intruder to perform attacks targeting some of the network's resource.

C. IoT APPLICATION LAYER SECURITY ATTACKS

e: MALICIOUS WORM-VIRUS ATTACK

In this type of attack, an adversary can spread a malicious code using different means such as downloading files on the Internet, emails or instantaneously attached files (pictures, docs, etc.). The worm replicates itself exponentially in the system or the network where it is sent or installed. With this action, the adversary tries to create damages in the targeted system by consuming storage space or network bandwidth. While with viruses the adversary generally aims to corrupt or modify files [96].

f: DoS ATTACK

DoS attack can also be at the Application Layer where the attacker for instance blocks legitimate users from accessing IoT applications by denying the system services [96].

V. CURRENT SECURITY MECHANISMS IN IoT ECOSYSTEM

A secure and efficient implementation of an IoT ecosystem needs to take in account three primary security and privacy goals; Confidentiality, Integrity and Availability (CIA). Confidentiality, which is roughly equivalent to privacy is an important feature in an IoT ecosystem. This feature ensures the protection of data such as patient's data, private information and secret keys from unauthorized access or to be

TABLE 4. Projection of attacks on IoT ecosystem enabling technologies.

IoT Ecosystem Enabling Technologies			RFID	CoAP	MQTT	IEEE 802.15.4	ZigBee	IQRF	6LoWPAN	RPL	IPv6 and IPv4	AWS
IoT Perception Layer Attacks	Perception Sensor Block	Node Capture/Replication Attack	*				*	*				
		Device Tempering Attack	*				*	*				
		Node Physical Damage Attack	*				*	*				
		Jamming Attack					*	*				
		Man in the Middle Attack	*			*	*	*				
		Interference Attack	*			*	*	*				
		Malicious Nodes Injection Attack					*	*				
		DoS Attack	*	*	*	*	*	*	*	*	*	
	Perception Application Block	CoAP Amplification Attack		*								
		MQTT Attacks			*							
	Perception Network Block	Flooding Attack				*	*	*				
		Sinkhole / Blackhole Attack								*		
		Wormhole Attack								*		
		Sybil Attack	*				*	*				
		Spoofing, Replay, and Message Altering Attack	*			*	*	*		*		
		Eavesdropping Attack	*			*	*	*				
		Traffic Analysis Attack	*			*	*	*				
		Information Routing Attack					*	*		*		
	Edge Block	RPL Attack								*		
		6LoWPAN Fragmentation Attack							*			
IoT Network Layer Attack		Sniffing Attacks									*	
		Reconnaissance Attacks									*	
IoT Application Layer Attacks		Malicious Worm-Virus Attack										*
		DoS Attack										*

disclosed. In some scenarios, confidentiality may not be mandatory, for instance when the data is publicly presented. Integrity in an IoT ecosystem ensures the accuracy, consistency and trustworthiness of the data over its entire life cycle. Therefore, measures must be taken to ensure that data is not changed in transit or altered by unauthorized people. Integrity is a mandatory security feature in the CIA triad. The degree of integrity can be different from an IoT system to another. For instance, a patient remote monitoring system must have a high integrity check level against human or non-human caused data alteration as in the latter the consequences can be dramatic compared to an ambient temperature sensor node. A good backup system must be available in case there is a need to restore the affected data. Availability ensures that the IoT ecosystem keeps providing services despite the presence of a malfunctioning system or malicious entities. In an IoT ecosystem, availability has also different levels depending on the application domain. For instance, a fire system would have higher availability requirements. Availability can be ensured by rigorous system maintenance and upgrades. It is also ensured by providing adequate communication bandwidth for critical systems and take in account the bottlenecks problems. Redundancy and making backups are also important concepts when it comes to providing a reliable IoT ecosystem. Moreover, fast and adaptive recovery of IoT system from unusual situations such as attacks or natural disasters or another worse scenario is essential [113].

Developing a secure IoT ecosystem and taking into account possible security risks is very difficult task. Therefore, the Open Web Application Security Project (OWASP) defines the broadly agreed ten rules representing the most critical security risks to an IoT ecosystem [114]. This helps the manufacturers, developers and consumers to better understand the security risks associated with IoT. Moreover, it helps users to make better security decisions when building, deploying or assessing the technology.

Traditional security mechanisms can't be directly applied to IoT systems as it uses different standards and communication technologies. IoT systems need an appropriate protection against all possible attacks or vulnerabilities. Therefore, security is needed at each layer. Following are security mechanisms deployed in IoT at each layer to deal with security and privacy goals and the OWASP defined risks.

A. IoT PERCEPTION LAYER SECURITY MECHANISMS

1) PERCEPTION SENSOR BLOCK SECURITY MECHANISMS

a: AUTHENTICATION AND IDENTIFICATION

The pervasive and scalable nature of IoT devices make the traditional identification and authentication schemes inapplicable. Identification in IoT ecosystem is crucial for the system's and user's security and privacy. Therefore, the choice of the authentication technique is critical. We review a lot of authentication techniques presented for different scenarios. The article [115] surveys more than forty authentication protocols developed to be used in the context of the IoT. Authors in this paper categorize authentication protocols in four different sets based on the environment where they can be deployed namely M2M, Internet of Vehicles (IoV), Internet of Energy (IoE), and Internet of Sensors (IoS). Based on [115] IoT authentication can be categorized into three types: authentication that uses symmetric crypto system, authentication that uses asymmetric crypto system and authentication uses hybrid protocols. It is also mentioned in [115] that the realization process to establish an IoT authentication protocol is achieved in seven steps. First, the definition of network model for instance M2M, IoV, IoE or IoS. Second, the definition of authentication model for instance mutual authentication, perfect forward secrecy, anonymity, and untraceability. Third, the definition of threat model. Fourth, the selection of countermeasure techniques such as cryptographic methods, biometric, Bloom Filter, biometric etc. Fifth, the proposition of main phases of the protocol for instance initial setup or registration process. Sixth, analyze the security using formal security verification techniques such as ProVerif, BAN-logic, and AVISPA. Seventh, evaluation of the system performances such as storage cost, computation complexity, communication overhead, error rates etc.

Authors in [116] presented One Time Password (OTP) authentication protocol for IoT based on elliptic curves. In this paper, authors demonstrated that the proposed protocol performs better than the existing OTP ones by keeping the same security levels. A certificate-based authentication method is proposed in [117]. Authors in this investigation study tried to prove or not the practicability of running a certificate on resource-constrained devices. It is concluded that a certificate-based authentication method is heavy on resource-constrained devices and they proposed three methods, one of them is to pre-validate the certificate at the gateway as it can be more powerful in terms of computation and storage. Mahalle *et al.* [118] proposed a Threshold Cryptography-based Group Authentication (TCGA). This scheme is applied to a group of devices ensuring simultaneous authentication of all the devices in the group. This is beneficial in case a large number of devices need to be authenticated at the same time. Results show that the proposed scheme is lightweight and scalable and resistant to battery exhaustion, replay and MIM attacks. Another certificate-based authentication work for WSNs in distributed IoT applications is proposed in [119]. The proposed method comprises two phases, registration and authentication, allowing the network entities and end-users to authenticate each other and establish a secure link. A hardware based authentication technique discussed in [120] proposes an authentication technique based on Physical Unclonable Functions (PUF). This method can prevent identity theft and device cloning. Similar to [120], authors in [121] identify PUF that uses device's physical properties such as fingerprint to identify the device. Combining PUF and Physical Key Generation (PKG) serves as an encryption and authentication service. Many more identification and authentication works are surveyed and described in [16] and [122].

b: LIGHTWEIGHT ENCRYPTION

The conventional cryptographic methods might not be suitable for IoT devices due to their resource-constrained nature. Moreover, the conventional algorithms may incur too high latency or cause high power consumption for such devices. Therefore, lightweight cryptography is the required technology ensuring security of end-to-end communication, low power consumption and adaptability in resource-constrained environments. However, there are three major challenges that need to be considered when deploying cryptographic security solutions to IoT devices [123]. First is the overhead of security solutions which must be reduced to fit with the resource-constrained nature of IoT. Second is the power consumption of security solutions which must be minimal. Third is the security solution performance that should be acceptable to support application needs. The aforementioned challenges motivate researchers to find a lightweight cryptographic primitives applicable and can secure pervasive resource-constrained devices such as RFID tags and wireless sensor nodes. The National Institute of Standards and Technology (NIST) started in 2013 a lightweight cryptography project to evaluate the performance of the already approved cryptographic standards made by NIST and understand the need to have a lightweight cryptography standards [124]. Similarly, a vast number of lightweight cryptographic primitives have been proposed over the past few years offering performance advantages over the conventional cryptographic algorithms [125], [126]. Moreover, most of the proposed lightweight encryption algorithms for IoT are symmetric as the asymmetric algorithms are too complex for resource-constrained devices and energy consuming [126]. Lightweight encryption algorithms includes lightweight block ciphers, lightweight hash functions and lightweight stream ciphers.

Lightweight Bloc Ciphers: In the literature, several lightweight block ciphers have been proposed. A simpler version of the classical Data Encryption Standard (DES) called DES Lightweight (DESL) is proposed in [127]. In DESL, the round function uses a single S-box but repeats eight times instead of eight S-Boxes as in DES. In addition, DESL omits the initial and the final permutations for a better implementation. Families of simple block ciphers named SIMON and SPEAK [128] were designed specifically to ensure security on constrained devices. Unlike encryption algorithms such as AES, these block ciphers use simple round functions iterated as many times as necessary for security offering compact realizations in constrained setups. Another block cipher called PRESENT [129] is designed specifically for constrained hardware environments. This block cipher consists of 31 rounds with 64bits block size and two supported keys, 80 and 128 bits of length. The block cipher called RC5 [130] is a block cipher with different sizes, 32, 64, and 128 bits. It is a symmetric block cipher with a variable number of rounds, word size and a secret key. This block cipher is simple and lightweight and requires low memory space. Many other block ciphers are presented in the literature and a list is provided in [131]. Better performance of block ciphers lies on the small block size, small key size, number of rounds and simpler key schedules [124].

Lightweight Hash Functions: Modern hash methods such as MD5 and SHA-1 and others methods are not efficient enough for IoT devices due to their large internal state sizes and high power consumption requirements. Therefore, NIST in [124] have recommended some of the new and lightweight developed hashing methods such SPONGENT, PHOTON, Quark and Lesamnta-LW. Major differences between the conventional and lightweight hash functions are the internal state, the output size, and the message size [132].

Lightweight Stream Ciphers: The ECRYPT STREAM (eSTREAM) [133] project aimed to promote the design of an efficient and compact stream ciphers suitable for widespread adoption. Three among seven ciphers are particularly designed to be suitable for applications with restricted resources such as CPU, memory and battery. The three stream ciphers are named Grain [134], Trivium [135] and Mickey [136].

2) PERCEPTION APPLICATION BLOCK SECURITY MECHANISMS

a: CERTIFICATION AND ACCESS CONTROL

One of the methods to identify truly communication parties in a network is through the use of certifications. For instance using two ways Public Key Infrastructure (PKI), strong authentication can be achieved in an IoT system. This is necessary to prevent attacks such as Sybil attack and ensure the validity of the information. Access control is another mechanism to increase the security in an IoT systems. It limits the access of nodes or people based on their role in the IoT system [137], [138].

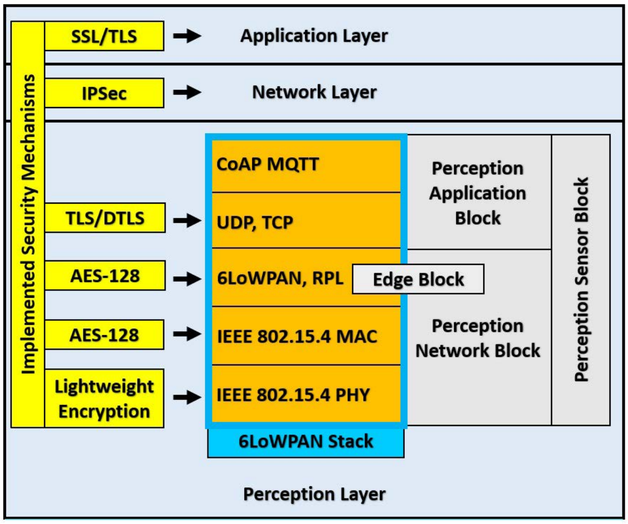


FIGURE 4. IoT ecosystem architecture with enhanced security.

3) PERCEPTION NETWORK BLOCK SECURITY MECHANISMS

a: SECURE ROUTING IN IoT

In an IoT network, a secure routing protocol is required to only guarantee message availability. However, messages integrity and confidentiality can be handled at higher layers. To prevent routing attacks, several routing protocols for WSN and Wireless Ad-hoc Networks (WANET) are proposed in the literature. Secure multi-hop routing for IoT communications (SMRP) [139] is an idea of merging the node's authentication process when joining the network with the routing process providing IoT network security without incurring significant overheads. Authors in this work deduce that SMRP produces a secure multi-hop IoT network without performance degradation when compared to the Optimized Link State Routing Protocol (OLSR). Another secure routing protocol named Two-way acknowledgment-based trust (2-ACKT) is proposed in [140]. This protocol calculates the trust based on the link layer acknowledgment (LLACK) in IEEE 802.15.4 MAC and a two hop acknowledgment from the downstream neighbor. A framework based on block-chain to identify and report malicious nodes trying to tamper a Low-power and Lossy Network (LLN) configuration information is proposed in [141]. SCOTRES scheme [142] is also proposed to be integrated with the Dynamic Source Routing (DSR) to secure routing functionality in the network layer of WSN or WANET. This protocol is proposed to be deployed in network with low mobility.

B. IoT NETWORK LAYER SECURITY MECHANISMS

b: FIREWALLS IN IPV4 AND IPV6 NETWORKS

Generally speaking, sensors are the enablers for IoT. Sensors or IoT devices send the acquired data to the cloud over the Internet. However, the data may be compromised on the way by an adversary. To prevent this threat, firewalls as one of the important security mechanisms at the Network Layer are applied in both IPv4 and IPv6 networks [87]. Firewalls check the traffic coming in or out from the local network. Usually firewalls are implemented at the edges of the Internet where the local networks are attached, for instance at gateway level. Moreover, firewalls contain a predefined set of rules used as filtering methods for the traffic. Therefore, received packets are either accepted or discarded based on the predefined rules. In IPv4 networks, firewalls are deployed using a software with predefined filtering rules for frequently used applications. Similarly, firewalls in IPv6 networks must have a built in support for the IPv6 protocol. Additionally, the IPv6 firewall must be able to recognize and process the new header format and other associated protocols introduced in IPv6 protocol such as ICMPv6 [82].

C. IoT APPLICATION LAYER SECURITY MECHANISMS

c: CLOUD COMPUTING

The cloud is one of the key technologies participating in the development of IoT offering high storage capacity and calculation with low deployment costs. The collected data from IoT devices is stored and analyzed and can finally be used in an effective way providing a meaningful insight to the users. Moreover, the cloud can play a role in securing IoT systems at minimum cost. This can be realized by the fact that the cloud space and computation power allocation depend on the user needs [137], [138].

d: MIDDLEWARE

The interoperability of heterogeneous devices need well defined standards. However this is not an easy task as application requirements are divers, therefore it is difficult to develop standards for each. One solution is the use of a middleware platform. It abstracts the details of the things to applications. The middleware also acts as a software bridge between things and their applications. Moreover it provides an Application Programming Interface for communication, data management, computation, security, and privacy [15]. However, since IoT applications are in general related to people's life or industries, the security and the privacy need to be addressed at this level. This can be done by implementing authentication and access control mechanisms.

VI. FUTURE RESEARCH DIRECTION

By stacking together the individual technologies, standards and protocols presented in this paper, one can form the 6LoWPAN protocol stack to support the realization of an inter-operable IoT as defined in [143] and [45]. The 6LoWPAN stack highlighted in Figure 4 represents the PB_a and the PB_n in our proposed architecture, while the PB_s represents the sensing part and the interface to the physical environment.

LLNs applications often require confidentiality and integrity protection. This can be ensured by providing security mechanisms at different layers of the 6LoWPAN stack. At the PB_a, DTLS can be used to secure applications running under CoAP protocol or TLS for applications using MQTT instead. IEEE 802.15.4 security primitives can also be used within the 6LoWPAN adaptation layer. Due to the limited resources on the IoT devices, a lightweight cryptography is required ensuring security to end-to-end communication and low power consumption. At higher layers such as the Network Layer and the Application Layer, IPsec and SSL/TLS are used respectively. Researchers working in this field have enormous scope in building a robust IoT ecosystem that can be trusted by the end users. Alternatively, to explore implementing ‘‘zero trust’’ approach into devices while maintaining effective security controls is another research direction. Some of the key research areas include trusted ecosystems and mutual authentication, provisioning of highly scalable device identities, and designing public key infrastructure from the production floor to the end-user.

VII. CONCLUSION

The integration of IoT devices into the Internet is challenging as they are characterized differently from the traditional internet devices, more specifically characteristics such as power consumption, computational power and storage capacity. Moreover, IoT enabling technologies and standardized protocols presented in this paper enable IoT resource-constrained devices to be integrated to IPv6 Internet.

In this paper we have proposed a modified three layer architecture of an IoT ecosystem by dividing the Perception Layer into three blocks. The reason behind this is to differentiate high-level applications from low-level application protocols both of which are often placed at the Application Layer of the IoT architecture. Another reason is to differentiate IoT LLNs with the Internet in such a way that the proposed architecture gives a better classification of the enabling technologies, threats and countermeasures.

The paper highlighted some of the key technologies, protocols and standards with their native security challenges, concerns and resolutions. By combining these technologies and standards, a secure layer-wise IoT architecture is established and a secured 6LoWPAN stack can be formed in future as extension.

REFERENCES

[1] D. Evans, ‘‘The Internet of Things: How the next evolution of the internet is changing everything,’’ Cisco, San Francisco, CA, USA, White Paper, 2011, pp. 1–11, vol. 1, no. 2011. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] S. Sinha. (Sep. 2021). *State of IoT 2021: Number of Connected IoT devices*. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[3] International Data Corporation. (2019). *The Growth in Connected IoT Devices is Expected to Generate 79.4 ZB of Data in 2025, According to a New IDC Forecast*. [Online]. Available: https://www.globaldots.com/resources/blog/41-6-billion-iot-devices-will-be-generating-79-4-zettabytes-of-data-in-2025/

[4] A. Shalaginov, I. Kotsiuba, and A. Iqbal, ‘‘Cybercrime investigations in the era of smart applications: Way forward through big data,’’ in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2019, pp. 4309–4314.

[5] 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.

[6] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[7] P. Bazydlo, S. Dabrowski, and R. Szewczyk, "Wireless temperature measurement system based on the IQRF platform," in *Mechatronics—Ideas for Industrial Application*. Cham, Switzerland: Springer, 2015, pp. 281–288.

[8] R. Hajovsky and M. Pies, "Use of IQRF technology for large monitoring systems," *IFAC-PapersOnLine*, vol. 48, no. 4, pp. 486–491, 2015.

[9] M. Bouzidi, Y. Dalveren, F. A. Cheikh, and M. Derawi, "Use of the IQRF technology in Internet-of-Things-based smart cities," *IEEE Access*, vol. 8, pp. 56615–56629, 2020.

[10] R. Kuchta, R. Vrba, and V. Sulc, "IQRF smart wireless platform for home automation: A case study," in *Proc. 5th Int. Conf. Wireless Mobile Commun.*, 2009, pp. 168–173.

[11] V. Sulc, R. Kuchta, and R. Vrba, "IQRF smart house—A case study," in *Proc. 3rd Int. Conf. Adv. Mesh Netw.*, Jul. 2010, pp. 103–108.

[12] M. Pies and R. Hajovsky, "Using the IQRF technology for the Internet of Things: Case studies," in *Proc. Int. Conf. Mobile Wireless Technol.* Singapore: Springer, 2017, pp. 274–283.

[13] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Secur.*, Dec. 2013, pp. 663–667.

[14] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 336–341.

[15] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *J. Electr. Comput. Eng.*, vol. 2017, Jan. 2017, Art. no. 9324035.

[16] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, Mar. 2019.

[17] M. Zhang, F. Sun, and X. Cheng, "Architecture of Internet of Things and its key technology integration based-on RFID," in *Proc. 5th Int. Symp. Comput. Intell. Design (ISCID)*, vol. 1, Oct. 2012, pp. 294–297.

[18] K. Gafurov and T.-M. Chung, "Comprehensive survey on Internet of Things, architecture, security aspects, applications, related technologies, economic perspective, and future directions," *J. Inf. Process. Syst.*, vol. 15, no. 4, pp. 797–819, 2019.

[19] 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.

[20] S. Khanam, I. B. Ahmedy, M. Y. I. Idris, M. H. Jaward, and A. Q. B. M. Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219709–219743, 2020.

[21] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, "Security analysis of IoT devices by using mobile computing: A systematic literature review," *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[22] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an Internet of Secure things: A survey on issues and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1372–1391, 2nd Quart., 2020.

[23] 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.

[24] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 2nd Quart., 2020.

[25] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.

[26] S. Wijethilaka and M. Liyanage, "Survey on network slicing for Internet of Things realization in 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 957–994, 2nd Quart., 2021.

[27] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[28] D. C. Nguyen, P. Cheng, M. Ding, D. Lopez-Perez, P. N. Pathirana, J. Li, A. Seneviratne, Y. Li, and H. V. Poor, "Enabling AI in future wireless networks: A data life cycle perspective," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 553–595, 1st Quart., 2021.

[29] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Recent security trends in Internet of Things: A comprehensive survey," *IEEE Access*, vol. 9, pp. 113292–113314, 2021.

[30] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021.

[31] Z. Yu, Z. Kaplan, Q. Yan, and N. Zhang, "Security and privacy in the emerging cyber-physical world: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1879–1919, 3rd Quart., 2021.

[32] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A survey on standards for interoperability and security in the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1020–1047, 2nd Quart., 2021.

[33] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag, and K. Huang, "Physical security and safety of IoT equipment: A survey of recent advances and opportunities," *IEEE Trans. Ind. Informat.*, vol. 18, no. 7, pp. 4319–4330, Jul. 2022.

[34] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and privacy threats for Bluetooth low energy in IoT and wearable devices: A comprehensive survey," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 251–281, 2022.

[35] L. Wei, Y. Yang, J. Wu, C. Long, and B. Li, "Trust management for Internet of Things: A comprehensive study," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7664–7679, Jan. 2022.

[36] J. Fan, W. Yang, Z. Liu, J. Kang, D. Niyato, K.-Y. Lam, and H. Du, "Understanding security in smart city domains from the ANT-centric perspective," 2022, *arXiv:2202.05023*.

[37] E. Bout, V. Loscri, and A. Gallais, "How machine learning changes the nature of cyberattacks on IoT networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 248–279, 1st Quart., 2022.

[38] M. James, *The Death of Competition*. New York, NY, USA: Harper Collins, 1996.

[39] S. Leminen, M. Westerlund, M. Rajahonka, and R. Siuruainen, "Towards IoT ecosystems and business models," in *Internet of Things, Smart Spaces, and Next Generation Networking*. Berlin, Germany: Springer, Aug. 2012, pp. 15–26.

[40] O. Mazhelis, E. Luoma, and H. Warma, "Defining an Internet-of-Things ecosystem," in *Internet of Things, Smart Spaces, and Next Generation Networking*. Berlin, Germany: Springer, Aug. 2012, pp. 1–14.

[41] T. Savolainen, J. Soininen, and B. Silverajan, "IPv6 addressing strategies for IoT," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3511–3519, Oct. 2013.

[42] J. Zheng and M. J. Lee, "A comprehensive performance study of IEEE 802.15. 4," *Sensor Netw. Oper.*, vol. 4, pp. 218–237, Sep. 2006.

[43] N. Kushalnagar, G. Montenegro, and C. Schumacher, *IPv6 Over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*, Network Working Group, RFC document 4919, 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4919

[44] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks," Internet Proposed Standard RFC, Tech. Rep., Sep. 2009, p. 130, vol. 4944.

[45] R. Garg and S. Sharma, "A study on need of adaptation layer in 6LoWPAN protocol stack," *Int. J. Wireless Microw. Technol.*, vol. 7, no. 3, pp. 49–57, May 2017.

[46] P. K. Kamma, C. R. Palla, U. R. Nelakuditi, and R. S. Yarrabothu, "Design and implementation of 6LoWPAN border router," in *Proc. 13th Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, Jul. 2016, pp. 1–5.

[47] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the Internet of Things," *Trans. IoT Cloud Comput.*, vol. 3, no. 1, pp. 11–17, 2015.

[48] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 551–591, May 2013.

[49] A. H. Chowdhury, M. Ikram, H.-S. Cha, H. Redwan, S. M. S. Shams, K.-H. Kim, and S.-W. Yoo, "Route-over vs mesh-under routing in 6LoWPAN," in *Proc. Int. Conf. Wireless Commun. Mobile Comput. Connecting World Wirelessly (IWCMC)*, Feb. 2009, pp. 1208–1212.

[50] 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, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 477–480.

[51] North Carolina Council of State. (2017). *#WatchOut: Analysis of Smartwatches for Children*. Accessed: Jun. 24, 2019. [Online]. Available: https://www.conpolicy.de/en/news-detail/watchout-analysis-of-smartwatches-for-children/

[52] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *Proc. 2nd Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2012, pp. 1282–1285.

[53] I. Pea-López, "ITU internet report 2005: The Internet of Things," 7th ed., Int. Telecommun. Union, Geneva, Switzerland, Tech. Rep., Nov. 2005. [Online]. Available: https://itu.tind.io/record/6354/

[54] H. Liu, M. Bolic, A. Nayak, and I. Stojmenovic, "Taxonomy and challenges of the integration of RFID and wireless sensor networks," *IEEE Netw.*, vol. 22, no. 6, pp. 26–35, Nov. 2008.

[55] T.-J. Fan, X.-Y. Chang, C.-H. Gu, J.-J. Yi, and S. Deng, "Benefits of RFID technology for reducing inventory shrinkage," *Int. J. Prod. Econ.*, vol. 147, pp. 659–665, Jan. 2014.

[56] C. C. Tan and J. Wu, "Security in RFID networks and communications," in *Wireless Network Security*. Berlin, Germany: Springer, 2013, pp. 247–267.

[57] A. K. Singh and B. Patro, "Elliptic curve signcryption based security protocol for RFID," *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 1, pp. 344–365, 2020.

[58] H. Knospe and H. Pohl, "RFID security," *Inf. Secur. Tech. Rep.*, vol. 9, no. 4, pp. 39–50, 2004.

[59] N. Dinarvand and H. Barati, "An efficient and secure RFID authentication protocol using elliptic curve cryptography," *Wireless Netw.*, vol. 25, no. 1, pp. 415–428, 2019.

[60] P. Y.-F. Lam, "Development of a multi-domain RFID security model for global supply chains, and a practical framework for model adoption," Ph.D. dissertation, Fac. Bus. Law, School Inf. Syst., Curtin Univ., Perth, WA, Australia, 2020.

[61] P. Kitsos and Y. Zhang, *RFID Security Techniques, Protocols and System-on-Chip Design* (RFID Fundamentals and Applications). Boston, MA, USA: Springer, 2008, pp. 3–27.

[62] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)(RFC 7252)," Univ. Bremen TZI, Germany, Tech. Rep. RFC 7252, Jun. 2014, doi: 10.17487/RFC7252.

[63] 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.

[64] E. Rescorla and T. Dierks, "The transport layer security (TLS) protocol version 1.3," Tech. Rep. RFC 8446, 2018.

[65] E. Rescorla and N. Modadugu, "RFC 6347: Datagram transport layer security version 1.2," IETF, Fremont, CA, USA, Tech. Rep., Jan. 2017.

[66] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, Aug. 2015, doi: 10.1109/COMST.2015.2388550.

[67] D. McGrew and D. Bailey, *AES-CCM Cipher Suites for Transport Layer Security (TLS)*, document RFC TR 6655, Jul. 2012.

[68] Y. Nir, S. Josefsson, and M. Pegourie-Gonnard, "Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS) versions 1.2 and earlier," Internet Requests Comments, Tech. Rep. RFC 8422, 2018, vol. 8422. [Online]. Available: https://www.rfc-editor.org/info/rfc8422, doi: 10.17487/RFC8422.

[69] A. Shalaginov, O. Semeniuta, and M. Alazab, "MEML: Resource-aware MQTT-based machine learning for network attacks detection on IoT edge devices," in *Proc. 12th IEEE/ACM Int. Conf. Utility Cloud Comput. Companion*, Aug. 2019, pp. 123–128.

[70] A. Banks, E. Briggs, K. Borgendale, and R. Gupta, "MQTT version 5.0," OASIS Standard, Burlington, MA, USA, Tech. Rep., Jun. 2019.

[71] M. Cotton and B. Leiba, *Guidelines for Writing an IANA Considerations Section in RFCs*, Standard RFC 8126, 2017, doi: 10.17487/RFC8126.

[72] *IEEE Standard for Low-Rate Wireless Networks*, Standard 802.15.4-2015, 2016.

[73] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15. 4 networks," in *Proc. 3rd ACM Workshop Wireless Secur.*, 2004, pp. 32–42.

[74] G. Dini and M. Tiloca, "Considerations on security in ZigBee networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput.*, 2010, pp. 58–65.

[75] P. Li, J. Li, L. Nie, and B. Wang, "Research and application of ZigBee protocol stack," in *Proc. Int. Conf. Measuring Technol. Mechatronics Autom.*, Mar. 2010, pp. 1031–1034.

[76] *ZigBee Standards Organization*, document 053474r20, Davis, CA, USA, 2012.

[77] P. Seflova, V. Sulc, J. Pos, and R. Spinar, "IQRF wireless technology utilizing IQMESH protocol," in *Proc. 35th Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2012, pp. 101–104.

[78] N. STMicroelectronics. (2015). *Spirit1 Radio*. [Online]. Available: https://www.st.com/en/partner-products-and-services/rc-spirit1-868.html

[79] IQRF. (2018). *IQRF OS Operating System. User's Guide*. [Online]. Available: https://www.iqrfalliance.org/data_files/news/user-guide-iqrf-os-403d-tr-7xd-181025.pdf

[80] S. Deering and R. Hinden. (1998). *Internet Protocol, Version 6 (IPV6) Specification—RFC2460*. [Online]. Available: https://www.ietf.org/rfc/rfc2460.txt

[81] G. Mulligan, "The 6LoWPAN architecture," in *Proc. 4th Workshop Embedded Networked Sensors (EmNets)*, 2007, pp. 78–82.

[82] A. Conta, S. Deering, and M. Gupta, "Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification," Netw. Work. Group, Tech. Rep. RFC 4443, Dec. 1998.

[83] T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, and R. K. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks," Tech. Rep. RFC 6550, 2012, pp. 1–157, vol. 6550, doi: 10.17487/RFC6550.

[84] T. Tsvetkov and A. Klein, "RPL: IPv6 routing protocol for low power and lossy networks," *Network*, vol. 59, pp. 59–66, Jul. 2011.

[85] P. O. Kamgueu, E. Nataf, and T. D. Ndie, "Survey on RPL enhancements: A focus on topology, security and mobility," *Comput. Commun.*, vol. 120, pp. 10–21, May 2018.

[86] A. R. Choudhary, "In-depth analysis of IPv6 security posture," in *Proc. 5th Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*, Nov. 2009, pp. 1–7.

[87] D. Žagar, K. Grgić, and S. Rimac-Drlje, "Security aspects in IPv6 networks—Implementation and testing," *Comput. Electr. Eng.*, vol. 33, nos. 5–6, pp. 425–437, 2007.

[88] S. Kent and R. Atkinson, "Security architecture for the internet protocol," Netw. Work. Group, Tech. Rep. RFC 4301, 1998, doi: 10.17487/RFC4301.

[89] E. Durdağ and A. Buldu, "IPv4/IPv6 security and threat comparisons," *Proc. Social Behav. Sci.*, vol. 2, no. 2, pp. 5285–5291, 2010.

[90] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018.

[91] P. P. Ray, "A survey of IoT cloud platforms," *Future Comput. Inform. J.*, vol. 1, nos. 1–2, pp. 35–46, 2017.

[92] S. Narula, A. Jain, and Prachi, "Cloud computing security: Amazon web service," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Technol.*, Feb. 2015, pp. 501–505.

[93] A. Amazon, "Amazon web services overview of security processes," Amazon Web Services, Tech. Rep., Aug. 2015.

[94] J.-S. Um, "Cyber systems," in *Drones as Cyber-Physical System*. Cham, Switzerland: Springer, 2019, pp. 59–99.

[95] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy (S&P)*, May 2005, pp. 49–63.

[96] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 32–37.

[97] S. Uke, A. Mahajan, and R. Thool, "UML modeling of physical and data link layer security attacks in WSN," *Int. J. Comput. Appl.*, vol. 70, no. 11, pp. 1–4, May 2013.

[98] L. Galluccio, G. Morabito, and M. Catania, "Facing man-in-the-middle and route diversion attacks in energy-limited RFID systems based on mobile readers," in *Proc. 10th IFIP Annu. Medit. Ad Hoc Netw. Workshop*, Jun. 2011, pp. 58–64.

[99] F. Kandah, Y. Singh, W. Zhang, and C. Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 539–547, 2013.

[100] B. Sasikala, M. Rajanarajana, and B. Geethavani, "Internet of Things: A survey on security issues analysis and countermeasures," *Int. J. Eng. Comput. Sci.*, vol. 6, no. 5, pp. 21435–21442, Jun. 2017.

[101] S. Arvind and V. A. Narayanan, "An overview of security in CoAP: Attack and analysis," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2019, pp. 655–660.

[102] S. Naeem Firdous, Z. Baig, C. Valli, and A. Ibrahim, "Modelling and evaluation of malicious attacks against the IoT MQTT protocol," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jun. 2017, pp. 748–755.

[103] A. Kamble, V. S. Malemath, and D. Patil, ''Security attacks and secure routing protocols in RPL-based Internet of Things: Survey,'' in *Proc. Int. Conf. Emerg. Trends Innov., ICT (ICEI)*, Feb. 2017, pp. 33–39.

[104] E. C. H. Ngai, J. Liu, and M. R. Lyu, ''An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks,'' *Comput. Commun.*, vol. 30, nos. 11–12, pp. 2353–2364, Sep. 2007.

[105] G. S. Mamatha and S. C. Sharma, ''Network layer attacks and defense mechanisms in MANETS—A survey,'' *Int. J. Comput. Appl.*, vol. 9, no. 9, pp. 12–17, Nov. 2010.

[106] A. Alharbi, M. Zohdy, D. Debnath, R. Olawoyin, and G. Corser, ''Sybil attacks and defenses in Internet of Things and mobile social networks,'' *Int. J. Comput. Sci. Issues*, vol. 15, no. 6, pp. 36–41, 2018.

[107] R. Sarma and F. A. Barbhuiya, ''Internet of Things: Attacks and defences,'' in *Proc. 7th Int. Conf. Smart Comput. Commun. (ICSCC)*, Jun. 2019, pp. 1–5.

[108] J. Teng, W. Gu, and D. Xuan, ''Defending against physical attacks in wireless sensor networks,'' in *Handbook on Securing Cyber-Physical Critical Infrastructure*, S. K. Das, K. Kant, and N. Zhang, Eds. Boston, MA, USA: Morgan Kaufmann, 2012, ch. 10, pp. 251–279. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780124158153000108

[109] P. Pongle and G. Chavan, ''A survey: Attacks on RPL and 6LoWPAN in IoT,'' in *Proc. Int. Conf. Pervasive Comput. (ICPC)*, Jan. 2015, pp. 1–6.

[110] L. Wallgren, S. Raza, and T. Voigt, ''Routing attacks and countermeasures in the RPL-based Internet of Things,'' *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, 2013, Art. no. 794326.

[111] C. Karlof and D. Wagner, ''Secure routing in wireless sensor networks: Attacks and countermeasures,'' *Ad Hoc Netw.*, vol. 1, nos. 2–3, pp. 293–315, Sep. 2003.

[112] A. Kulshrestha and S. K. Dubey, ''A literature reviewon sniffing attacks in computer network,'' *Int. J. Adv. Eng. Res. Sci.*, vol. 1, no. 2, pp. 1–10, 2014.

[113] M. Abomhara and G. M. Køien, ''Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks,'' *J. Cyber Secur.*, vol. 4, no. 1, pp. 65–88, 2015.

[114] P. Ferrara, A. K. Mandal, A. Cortesi, and F. Spoto, ''Static analysis for the OWASP IoT top 10 2018,'' *Proc. SPIoT*, vol. 19, 2019, pp. 1–5.

[115] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, ''Authentication protocols for Internet of Things: A comprehensive survey,'' *Secur. Commun. Netw.*, vol. 2017, Sep. 2017, Art. no. 6562953.

[116] V. L. Shivraj, M. A Rajan, M. Singh, and P. Balamuralidhar, ''One time password authentication scheme based on elliptic curves for Internet of Things (IoT),'' in *Proc. 5th Nat. Symp. Inf. Technol., Towards New Smart World (NSITNSW)*, Feb. 2015, pp. 1–6.

[117] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, ''Towards viable certificate-based authentication for the Internet of Things,'' in *Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Secur. Privacy*, 2013, pp. 37–42.

[118] P. N. Mahalle, N. R. Prasad, and R. Prasad, ''Threshold cryptography-based group authentication (TCGA) scheme for the Internet of Things (IoT),'' in *Proc. 4th Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. (VITAE)*, May 2014, pp. 1–5.

[119] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, ''Two-phase authentication protocol for wireless sensor networks in distributed IoT applications,'' in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 2728–2733.

[120] D. Mukhopadhyay, ''PUFs as promising tools for security in Internet of Things,'' *IEEE Design Test*, vol. 33, no. 3, pp. 103–115, Jun. 2016.

[121] C. Huth, J. Zibuschka, P. Duplys, and T. Guneysu, ''Securing systems on the Internet of Things via physical properties of devices and communications,'' in *Proc. Annu. IEEE Syst. Conf. (SysCon)*, Apr. 2015, pp. 8–13.

[122] Y. Atwady and M. Hammoudeh, ''A survey on authentication techniques for the Internet of Things,'' in *Proc. Int. Conf. Future Netw. Distrib. Syst.*, Jul. 2017, pp. 1–18.

[123] X. Fan, K. Mandal, and G. Gong, ''WG-8: A lightweight stream cipher for resource-constrained smart devices,'' in *Proc. Int. Conf. Heterogeneous Netw. Qual., Rel., Secur. Robustness*. Berlin, Germany: Springer, 2013, pp. 617–632.

[124] K. McKay, L. Bassham, M. S. Turan, and N. Mouha, ''Report on lightweight cryptography,'' Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. Nist Draft NISTIR 8114, 2016.

[125] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, ''Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions,'' *J. Ambient Intell. Humanized Comput.*, pp. 1–18, May 2017, doi: 10.1007/s12652-017-0494-4.

[126] A. Biryukov and L. P. Perrin, ''State of the art in lightweight symmetric cryptography,'' SnT, CSC, Univ. Luxembourg, Tech. Rep., 2017.

[127] G. Leander, C. Paar, A. Poschmann, and K. Schramm, ''New lightweight DES variants,'' in *Proc. Int. Workshop Fast Softw. Encryption*. Berlin, Germany: Springer, 2007, pp. 196–210.

[128] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, ''The Simon and speck lightweight block ciphers,'' in *Proc. 52nd Annu. Design Autom. Conf.*, 2015, pp. 1–6.

[129] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe, ''PRESENT: An ultra-lightweight block cipher,'' in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2007, pp. 450–466.

[130] S. Charbathia and S. Sharma, ''A comparative study of Rivest cipher algorithms,'' *Int. J. Inf. Comput. Technol.*, vol. 4, no. 17, pp. 0974–2239, 2014.

[131] D. Dinu, Y. Le Corre, D. Khovratovich, L. Perrin, J. Großschädl, and A. Biryukov, ''Triathlon of lightweight block ciphers for the Internet of Things,'' *J. Cryptograph. Eng.*, pp. 1–20, 2018.

[132] A. Y. Poschmann, ''Lightweight cryptography: Cryptographic engineering for a pervasive world,'' Ph.D. thesis, Embedded Secur. Group, Horst Görtz Inst. IT Secur., Fac. Elect. Eng. Inf. Technol., Ruhr-Univ. Bochum, Bochum, Germany, 2009.

[133] M. Robshaw, ''The eSTREAM project,'' in *New Stream Cipher Designs*. Boston, MA, USA: Springer, 2008, pp. 1–6.

[134] M. Hell, T. Johansson, and W. Meier, ''Grain: A stream cipher for constrained environments,'' *Int. J. Wireless Mob. Comput.*, vol. 2, no. 1, pp. 86–93, May 2007.

[135] C. De Canniere and B. Preneel, ''TRIVIUM,'' in *New Stream Cipher Designs*. Berlin, Germany: Springer, 2008, pp. 244–266.

[136] S. Babbage and M. Dodd, ''The mickey stream ciphers,'' in *New Stream Cipher Designs*. Cham, Switzerland: Springer, 2008, pp. 191–209.

[137] X. Xiaohui, ''Study on security problems and key technologies of the Internet of Things,'' in *Proc. Int. Conf. Comput. Inf. Sci.*, Jun. 2013, pp. 407–410.

[138] M. A. Bhabad and S. T. Bagade, ''Internet of Things: Architecture, security issues and countermeasures,'' *Int. J. Comput. Appl.*, vol. 125, no. 14, pp. 1–4, Sep. 2015.

[139] P. L. R. Chze and K. S. Leong, ''A secure multi-hop routing for IoT communication,'' in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 428–432.

[140] X. Anita, J. M. L. Manickam, and M. A. Bhagyaveni, ''Two-way acknowledgment-based trust framework for wireless sensor networks,'' *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 5, 2013, Art. no. 952905.

[141] R. Sahay, G. Geethakumari, and B. Mitra, ''A novel blockchain based framework to secure IoT-LLNs against routing attacks,'' *Computing*, vol. 102, pp. 2445–2470, Sep. 2020.

[142] G. Hatzivasilis, I. Papaefstathiou, and C. Manifavas, ''SCOTRES: Secure routing for IoT and CPS,'' *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2129–2141, Dec. 2017.

[143] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. V. D. Abeele, E. D. Poorter, I. Moerman, and P. Demeester, ''IETF standardization in the field of the Internet of Things (IoT): A survey,'' *J. Sensor Actuator Netw.*, vol. 2, no. 2, pp. 235–287, Apr. 2013.

MOHAMMED BOUZIDI received the B.S. degree from the University of Science and Technology of Oran, Algeria, and the M.S. degree in automation from the University of Burgundy, Dijon, France. He is currently pursuing the Ph.D. degree with the Institute of Electrical Systems, NTNU, Gjøvik, Norway. His doctoral research aims to investigate the most recent IoT technologies for reliable, sustainable, and maintainable smart cities to provide energy-efficiency and secure communication.

NISHU GUPTA (Senior Member, IEEE) received the Ph.D. degree in electronics and communication engineering from MNNIT Allahabad, India, in 2016. His Ph.D. research was devoted to the development of MAC protocols for safety applications in VANETs. He is currently a Postdoctoral Fellow (ERCIM Alain Bensoussan Fellowship) with the Department of Electronic Systems, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway. He is the author and an editor of several books and book chapters with publishers, including Springer, Taylor & Francis, Wiley, and Scrivener Publishing. His research interests include intelligent vehicles, the IoT, smart city and transportation, and augmented cyber-security. He has served as a member of the Zero Trust Architecture working group of MeitY-C-DAC-STQC Project under ''e-Governance Standards and Guidelines,'' Ministry of Electronics and Information Technology (MeitY), Government of India. He was a recipient of the Best Paper Presentation Award at NTU, Singapore, in 2019, and he serves as a reviewer for various high quality journals.

FAOUZI ALAYA CHEIKH (Senior Member, IEEE) received the Ph.D. degree in information technology from the Tampere University of Technology, Tampere, Finland, in 2004. He has been a Researcher with the Signal Processing Algorithm Group, Tampere University of Technology, since 1994. Since 2006, he has also been an Associate Professor with the Department of Computer Science and Media Technology, Gjøvik University College, Norway. Since 2016, he has also been with the Norwegian University of Science and Technology. He teaches courses on image and video processing and analysis and media security. His research interests include e-learning, 3-D imaging, image and video processing and analysis, video-based navigation, biometrics, pattern recognition, embedded systems, and content-based image retrieval. In these areas, he has published over 100 peer-reviewed journal articles and conference papers. He has been involved in several European and national projects, among them ESPRIT, NOBLESS, COST 211Quat, HyPerCept, IQ-Med, and H2020 ITN HiPerNav. He is also a member of NOBIM and Forskerforbundet (The Norwegian Association of Researchers). He is on the Editorial Board of the *IET Image Processing* and the *International Journal of Advanced Robotics and Automation*, and on the technical committees of several international conferences. He is an expert reviewer for a number of scientific journals and conferences related to the field of his research.

ANDRII SHALAGINOV received the Ph.D. degree in information security from the Norwegian University of Science and Technology, in 2018. He is currently an Associate Professor and the Head of the SmartSecLab, School of Economics, Innovation and Technology, Kristiania University College, Oslo, Norway. His work in academia and industry is widely related to the application of AI for cybersecurity, detection of computer viruses, network attacks, and the protection of IoT devices. He is currently leading ENViSEC and SecureUAV projects that were granted EU Horizon2020 cascading funding from NGI programs. He is an Affiliated Member of the Malware Lab and Digital Forensics Group, Norwegian University of Science and Technology. From before, he was involved as a cybersecurity researcher in the EUIPO framework related to malware analysis on copyright-infringing websites. He also serves as a nominated representative from Norway and a Management Committee Member of COST Action CA17124 DigForAsp—''Digital forensics: Evidence analysis via intelligent systems and practices.''

MOHAMMAD DERAWI received the Diploma degrees in computer science engineering and the B.Sc. and M.Sc. degrees from the Technical University of Denmark (DTU), Denmark, in 2007 and 2009, respectively, and the Ph.D. degree in information security from the Norwegian Information Security Laboratory (NISLab), Gjøvik University (now NTNU), Norway.

In 2009, he received the title as the Youngest Engineer of Denmark. In the beginning of his Ph.D. studies, he was a Visiting Researcher at the Center for Advanced Security Research Darmstadt (CASED, www.cased.de), Germany. He is currently having a dual-career acting as a Youngest Professor of Norway and an Extremely True Innovator. He is also the Head of the ''Smart Wireless Systems'' Research Group, Department of Electronic Systems, NTNU, Norway. Since 2009, he has been active in several European and national projects. Today he holds a professorship within electrical engineering. He has next to his academic career also been working with truly innovative projects which are also a part of his additional skills. He is a person that identifies the need within an industry, market segment or culture, and spot opportunity in it. More importantly, he has also the ability to identify needs before implemented in the market, develop and refine solutions, take chances, push the envelope, and create meaning. He is specialized within information security, e-health, autonomous systems, biometric systems, wireless communications, the IoT, and digital fundamentals microcontrollers. His Ph.D. research interests include smart mobile technologies and also biometrics with specialization on behavioral biometric recognition in mobile devices.