IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 31 October 2022, accepted 29 November 2022, date of publication 7 December 2022,
date of current version 21 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3227449

SURVEY

Analysis on Security and Privacy Guidelines: RFID-Based IoT Applications

HEZAM AKRAM ABDULGHANI, NIELS ALEXANDER NIJDAM, AND DIMITRI KONSTANTAS
Geneva School of Economics and Management, Geneva University, 1211 Geneva, Switzerland

Corresponding author: Hezam Akram Abdulghani (mohammed.akram@unige.ch)

This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme through AVENUE Project (https://h2020-avenue.eu/) under Grant 769033, in part by the nIoVe Project (https://www.niove.eu/) under Grant 833742, and in part by the SHOW Project (https://show-project.eu/) under Grant 875530.

ABSTRACT The Internet of Things (IoT) comprises many technologies, among them is Radio Frequency Identification (RFID), which can be used to track single or multiple objects. This technology has been widely used in healthcare, supply chain, logistics, and asset tracking. However, such applications require a high level of security and privacy and are unfortunately vulnerable to various attacks and threats that need to be addressed in order for RFID-based IoT applications to reach their full potential. To this end, we propose a set of security and privacy guidelines for RFID, supported by modelling guidelines, mitigations, and the attack vectors cohesively. We compare to the state of the art and point out their shortcomings on known guidelines and reason to address these in our model. The overall methodology is as follows: (i) identify the security and privacy guideline features, (ii) highlight the security goals for RFID-based IoT applications, (iii) analyze the features in relation to RFID industrial standards, and relate them to security goals, (iv) summarize attacks and threats against RFID applications and correlate them with violated security goals, (v) derive a set of security and privacy guidelines for RFID applications in accordance with security and privacy by design frameworks. We also describe our derived guidelines in connection with the involved stakeholders, and (vi) outline the existing mitigation strategies to implement our proposed guidelines. Finally, we describe the main limitations of our work that should be investigated in the future and identify the multiple challenges that concern current security strategies.

INDEX TERMS Internet of Things, RFID, security guidelines, privacy guidelines, countermeasures, security goals, privacy and security by design, attacks.

I. INTRODUCTION

Radio Frequency Identification (RFID) has been around for decades [1]. Ever since its first application, the number of RFID enabled objects has been steadily growing. It can be considered as a sensor technology that can reduce the cost and complexity of data collection. Especially with the concept of Internet of Things (IoT), its market growth is expected to reach 'USD 35.6 billion by 2030 [2]. In fact, IoT improves the communication between applications and humans with the aim of making physical objects easily integrated into it. Furthermore, IoT can be seen as a universal network that provides communication between objects-and-objects, human-to-human, and human-to-object by assigning each physical object a unique digital identity [3], [4]. Therefore, every object in the world must be associated with a unique identity to achieve the ultimate goal of IoT. For this purpose, the RFID technology can be considered as a candidate platform to address this problem [5]. This is because each RFID tag contains a unique identification that can be embedded or attached to an object. Its popularity for IoT stems from one of the main requirements, namely providing any digital asset with a unique identity, which in turn makes them addressable for exchanging information. Integrating RFID tags into IoT applications will support the unique identification of billions of objects estimated to be connected to Internet. This type of object connectivity can be achieved using the Internet Protocol version 6 (IPv6) addressing

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

scheme, which can be used in a number of applications and can be assigned hundreds of billion addresses [6].

RFID enabled solutions have found their way into almost any environment where digital assets need some kind of identification, tracking, and control, e.g., retail, smart homes, health care, smart traffic/city, industry 4.0, agriculture, electricity. However, with it comes a plethora of security risks, which have been an ongoing challenge since its inception [7]. While various solutions have been provided to specific problems and risks, a well-defined set of guidelines on cybersecurity and RFID enabled devices remains highly demanded by RFID stakeholders, such as developers, customers, and manufacturers.

To date, a few research efforts in the state-of-the-art have been conducted toward this objective, all of which, however, have some limitations, described below.

In [8], Ann Cavoukian proposes a set of privacy guidelines for RFID such as protecting critical information, preventing physical tempering, and preventing tracking. Manufacturers and providers can use these guidelines when designing and implementing RFID applications. The main goal of these guidelines is to allow RFID technology to reach its full potential by addressing some of its privacy concerns (e.g., tracking and monitoring). However, she does not provide a comprehensive set of security and privacy guidelines (e.g., secure kill command) or identify the mitigation strategies necessary to implement the privacy guidelines. Furthermore, attackers and threats against RFID applications remain untouched.

In [9], National Institute of Standards and Technology (NIST) proposes a set of security and privacy guidelines for RFID systems, such as encrypting tags data, secure tags disposal, preventing tracking, and minimizing interference. NIST also discusses some of the RFID standards and their security approaches. NIST, however, does not identify RFID stakeholders who may benefit from its guidelines, nor does it discuss mitigation techniques that can be used to implement its guidelines. Furthermore, NIST does not address all known attacks and threats against RFID systems, nor does it investigate their violations of security goals, such as confidentiality, integrity, availability, and others.

In [10], the authors highlight some of the RFID applications suitable for smart home environments. More importantly, they identify some of the security and privacy requirements, such as secure kill command, using strong authentication, and preventing tracking. These requirements are suitable for smart home environments. However, the authors propose only a few security and privacy requirements mentioned above and develop a security framework to fulfill their suggested requirements. Furthermore, they neither identify attacks and threats against RFID, nor state their violations of security goals. In addition, they do not specify these requirements based on what they propose.

In [11], Smart Border Alliance (SBA) conducted a study on RFID security and privacy, the main objectives of which are: (i) investigating privacy and security issues that may arise from the use of such technology, (ii) offering some recommendations that could be used to achieve its security and privacy requirements, (iii) highlighting only four security goals related to RFID applications, namely confidentiality, integrity, availability, and non-repudiation, and (iv) identifying some attacks on RFID.

However, SBA does not provide a comprehensive set of security and privacy guidelines for RFID, nor does it discuss all of their corresponding implementation approaches. For example, some RFID guidelines, such as supporting distance-based information, verifying all readers' requests to tags, using unique security parameters, and secure disposal of tags, are not investigated, along with their appropriate countermeasures. Furthermore, SBA does not identify the RFID stakeholders who can use its guidelines, nor does it define based on what it states its guidelines.

In [12], the authors suggest some of the security and privacy requirements for RFID-based IoT applications, such as the secure kill command, preventing tracking, and separating personal information from the tag identifier. The authors also highlight and discuss some of the security goals of RFID-based IoT applications. These security goals include confidentiality, integrity, authenticity, availability, and reliability. However, the authors do not discuss attacks and threats against RFID applications or identify their breached security goals. Furthermore, the authors identify neither the RFID stockholders who may use their requirements, nor state the principles under which they derive their requirements.

In our previous work in [13], published in the Sensor and Actuator Network Journal, in which we proposed a comprehensive set of security and privacy guidelines for IoT, covering computing nodes, protocols, and RFID. The main contribution of our previous work was to reinforce IoT security and privacy by design by shifting the mind set of IoT stakeholders (e.g., developers and manufacturers) to properly integrate our derived guidelines into their applications from the start, along with their corresponding mitigation techniques.

However, this work will focus only on addressing these limitations as follows. (i) provides a rationale under which each derived RFID guideline is stated, (ii) provides a reasoning under which RFID attacks can violate certain security goals, (iii) identifies security by design or privacy by design principles, (iv) discusses industrial standards for RFID and their recommended security mechanisms, (v) states all RFID guidelines (e.g., encrypt data on tags), and (vi) identifies all mitigation techniques (e.g., physical security controls).

A. MOTIVATION AND OBJECTIVES

Table 1 shows a summary of previous research efforts in RFID and our intended objectives represented as ''addressed features'', of which the most obvious can be classified as follows: (i) investigating the vast landscape of RFID along with its common attacks, (ii) identifying required security goals to protect RFID, (iii) suggesting a set of security and

TABLE 1. Comparison of research efforts presented in the literature.

Addressed Features		State-of-the Art Work						
		[8]	[9]	[12]	[10]	[13]	[11]	This Work
RFID security and privacy Guidelines	(G1) Minimize interference	✓	✗	✓	✗	✓	✓	✓
	(G2) Protect critical information	✓	✗	✓	✗	✓	✗	✓
	(G3) Prevent reverse engineering	✗	✗	✓	✗	✓	✗	✓
	(G4) Support distance-based information	✗	✗	✓	✗	✓	✗	✓
	(G5) Verify all readers' request to tags	✗	✗	✗	✗	✗	✗	✓
	(G6) Change the anonymous ID frequently	✗	✓	✓	✗	✓	✓	✓
	(G7) Secure kill command	✗	✓	✗	✓	✓	✓	✓
	(G8) Prevent physical tampering	✓	✗	✗	✗	✓	✓	✓
	(G9) Implement hardware trust	✓	✗	✗	✗	✓	✗	✓
	(G10) Avoid untrusted manufacturers	✗	✗	✗	✗	✓	✗	✓
	(G11) Use unique security parameters	✗	✗	✗	✗	✓	✗	✓
	(G12) Separate personal information from the tag identifier	✓	✓	✗	✗	✗	✗	✓
	(G13) Prevent tag Counterfeiting	✗	✓	✗	✗	✓	✓	✓
	(G14) Prevent tracking	✓	✓	✓	✓	✓	✓	✓
	(G15) Secure disposal of tags	✗	✗	✓	✗	✗	✗	✓
	(G16) Encrypt the data on tags	✓	✗	✗	✗	✗	✗	✓
	(G17) Use strong authentication	✗	✗	✗	✓	✗	✓	✓
	(G18) Minimize distance between reader and tag	✗	✗	✗	✗	✗	✗	✓
Types of Guidelines	Privacy	✓	✓	✓	✓	✓	✓	✓
	Security	✗	✓	✓	✓	✓	✓	✓
Guidelines intended for	(MAN) Manufacturer	✓	✗	✓	✗	✓	✗	✓
	(DEV) Developer	✓	✗	✓	✗	✓	✓	✓
	(CNS) Customer	✗	✗	✓	✗	✓	✗	✓
	(PRV) Provider	✗	✗	✗	✗	✓	∼	✓
Threats mitigated by guidelines		✗	✗	✗	∼	∼	✗	✓
Security goals violated by attacks		✗	✗	✗	∼	✗	✗	✓
Technique to implement Guidelines		✗	∼	✗	✗	∼	∼	✓

Note: ∼ Partial Support; ✓ Support; ✗ No Support.

privacy guidelines for RFID applications, and (iv) discussing existing mitigation strategies to implement the proposed guidelines.

It is not hard to observe many limitations (see Table 1) as you go through them. Therefore, our research is devoted to overcome those drawbacks that can be categorized as follows.

1) The lack of a complete list of security and privacy guidelines, followed by to whom such guidelines are targeted for use in practice.
2) The need to identify appropriate mitigation strategies to implement guidelines.
3) The need to investigate attacks associated with RFID and their violation of security goals.

B. CONTRIBUTION

A contribution breakdown of this work can be summarized as follows.

1) Highlight the security goals for RFID-based IoT applications and briefly discuss two widely known security and privacy by design frameworks.
2) Summarize possible threats and attacks against RFIDs and correlate them with violated security goals.
3) Define the following concepts in the scope of RFID-based IoT applications, namely security attack, secure device/application, security guideline, and privacy guidelines.
4) Review and analyze the security mechanisms recommended by RFID industrial standards.
5) Propose a set of security and privacy guidelines for RFID-based IoT applications and provide 'reasoning through which each guideline is derived based on one or two principles of security by design or privacy by design frameworks
6) Discuss the main limitation of our work and identify the many problems and challenges that current security strategies face.

C. RESEARCH QUESTIONS

This article addresses the following questions:

1) **RQ1:** What are the key security goals required for RFID-based IoT applications? Can such security goals

help define a secure device and a security attack within the scope of RFID-based IoT?
2) **RQ2:** What are the main current RFID industrial standards and their recommended security features? Are these recommended security features adequate to protect RFID systems?
3) **RQ3:** What are the main principles of security and privacy by design of RFID-based IoT systems? Can such principles help define a security guideline and a privacy guideline for such systems?
4) **RQ4:** What are common attacks against RFID applications and their violation of security goals such as confidentiality, integrity, availability, and so on?
5) **RQ5:** What are the mitigation strategies suggested for RFID applications? Can these mitigation techniques be attributed to identified attacks?
6) **RQ6** What are the security and privacy guidelines suggested for RFID-based IoT? Is it possible to develop an RFID-based IoT security framework that links these mitigation techniques, guidelines, and attacks?

D. MANUSCRIPT ORGANIZATION

The remainder of the work is organized as follows. In Section II, we give an overview of RFID in terms of its components, business model in the scope of IoT, applications, and key security challenges. In Section III, we outline RFID security goals and stakeholders in the IoT scope. In Section IV, we describe some of the RFID standards and analyze their recommended security mechanisms. In Section V, we present current research on security and privacy by design frameworks in the scope of RFID-based IoT applications. In Section VI, we recognize attacks on RFID applications, as well as their violation of security goals. In Section VII, we discuss all countermeasures available to prevent possible attacks against RFID. In Section VIII, we propose guidelines for RFID-based IoT applications in association with interested stakeholders. In Section IX, we explain the main drawback of this paper and discuss the open issues and challenges facing current security mechanisms. Finally, we describe our conclusion in Section X.

II. RFID BACKGROUND

This section first discusses the primary components of RFID technology and then describes the business model of RFID-based IoT applications. It also identifies the scope of RFID-based IoT applications and the key challenges of RFID security.

A. RFID SYSTEM COMPONENTS

Applications using RFID technology typically consist of four main elements (see Figure 1), described below.

1) AN RFID TAG

Sometimes it is called a transponder, which holds data for object identification. In general, a tag is a small electronic object attached to an antenna designed specifically for wireless data transmission. A tag is embedded or assigned to an object and transmits data over the air in response to a reader request [14]. Each tag contains a unique identifier and may also contain other features, such as environmental sensors, security features, and memory to store additional data. The market of RFID tags consists of several types of tags, each type of tag having its own size, security mechanisms, cost, and performance [15].

Although some tags are designed to meet certain standards, they are often customized according to specific application requirements. Identifying the key aspects of a tag can help those responsible for RFID applications recognize the key aspects of the tag needed in their application and environment. The main aspects of tags include the format of the identifier, the operational frequencies, the power source and the functionality [16].

The format of tag identifier used in different industries is Electronic Product Code (EPC) developed by the EPCglobal industry group [17]. The tag identifier format includes four data fields. (i) The header uses to specify the type of EPC. (ii) The EPC manager ID, which uniquely recognizes the organization responsible for assigning the serial number bits and object class. (iii) The object class uses to identify the class of objects (e.g., a particular model of television set). (iv) Serial numbers, which uniquely define the item of that class of objects, such as a certain television set [18].

Tags require a power source to execute their operations, such as storing and retrieving data, sending radio waves to a reader, and executing other computations (e.g., security mechanisms). Tags can be powered by electromagnetic signals sent by readers or by an on-board battery. Tags can be classified into four categories (passive, active, semi-active and semi-passive) based on their power sources [19].

Passive tags utilize the electromagnetic energy received from the reader's transmission to respond to the reader. The response signal of a passive tag, called the backscattered signal, contains only a small portion of the power of the reader's signal, which significantly limits the operating range of the tag and only backs data processing in a simple manner.

Active tags depend on internal batteries, which are used to power broad circuits, interact with the reader, and perform other operations. Unlike passive tags, these tags can communicate over a wider range and are expensive. However, they have a predefined battery life [20].

Semi-active tags are active tags that remain inactive or dormant until they receive the reader's wake-up signals. Similarly to active tags, they can use their batteries to communicate with readers over longer distances. Unlike active tags, the battery life of semi-active tags can last longer. However, in some instances (for example, when a tag passes quickly from a reader), the awakening method can result in undesirable time delays.

Semi-passive tags are passive tags that use batteries to power on-board circuitry. However, such tags cannot generate return signals. These tags are often known as sensor tags because they can use their own batteries to power

FIGURE 1. Components of RFID.

sensors. Unlike passive tags, they are expensive and larger. However, semi-passive tags possess more functions than passive tags [21].

2) AN RFID TAG READER

It writes and reads tag data, and a tag and a reader must follow the same standard so they can communicate with each other. In some cases, if a tag is based on a proprietary protocol, the reader also has to implement the same protocol to communicate with that tag. Despite this, it should be noted that the reader does have some characteristics that are independent of a tag. Such aspects include: (i) duty cycle and power output, (ii) mobility, and (iii) antenna design.

The reader's duty cycle is most often determined by standard and regulation. The duty cycle can be described as the percentage of time that a RFID reader emits energy over a given period of time. For example, a reader that sends radio waves for 30 seconds every minute will have 50% duty cycle. Readers require more energy power when communicating with passive tags compared to when communicating with active tags. This is because the signal should be strong enough to get the tag and allow the backscatter to return to the reader.

The reader's mobility depends on a back-end database interface, which could be wireless or wired. In most cases, wired readers are placed in fixed locations, whereas wireless readers can be placed in different environments, and more importantly, they can support different applications as they move.

3) AN RFID ANTENNA

Readers can use a wide variety of antenna types, and the coverage pattern can differ from tag to tag depending on the type of antenna. To minimize the risk of eavesdropping and, at the same time, to reduce interference, it is recommended to limit the reader's coverage area to only reach the intended tags. Antennas may be embedded in an object or detachable [22].

4) A BACK-END DATABASE

It holds records associated with the tag content. Generally, a reader decodes the tag data and passes them to local applications through a middleware that acts as an interface between RFID applications and the reader [22]. This part is beyond the scope of this article as we do not intend to propose guidelines for RFID data at rest. Therefore, we are not going to discuss this in detail.

B. BUSINESS MODEL OF RFID-IoT

The emerging RFID technology has inspired IoT to connect physical objects to wireless networks to exchange raw data on object status, movement, position, and process [23]. The IoT is described as a large dynamic global network where each physical and digital asset is individually recognized by its unique identifier that is used to quickly track its status [24]. IoT has allowed devices to be remotely accessible to users. As a result of the IoT, the technologies of RFID and sensor networks will lead to new challenges where information and communication systems are becoming integrated into our daily lives.Interactions between objects and machines allow them to autonomously respond to certain situations. One of these is that the device can intelligently make decisions through other machine inputs. In general, the IoT ecosystem consists of three main layers: a perception layer, a network layer, and an application layer [25]. According to a study by [26], RFID-IoT systems should have five types of layered architecture to integrate RFID-IoT into business models. The five-layer architecture includes the perception, network, middleware, application, and business layers as shown in Figure 2.

The aspects of each layer are described below.

1) Perception layer: It is commonly known as the object layer, which consists of physical objects and sensor devices. According to object identification techniques, sensor objects may be infrared sensors, RFID, or bar-codes. The main purpose of this layer is to collect and identify information from various IoT objects attached to an item and other IoT sensors such as proximity sensors, gyroscopes, and optical sensors. The information collected is then passed over to the network layer to be encrypted and transmitted to the information processing system.
2) Network layer: The network layer can also be referred to as a 'transmission layer.' It helps to transfer sensor object information to an information processing system

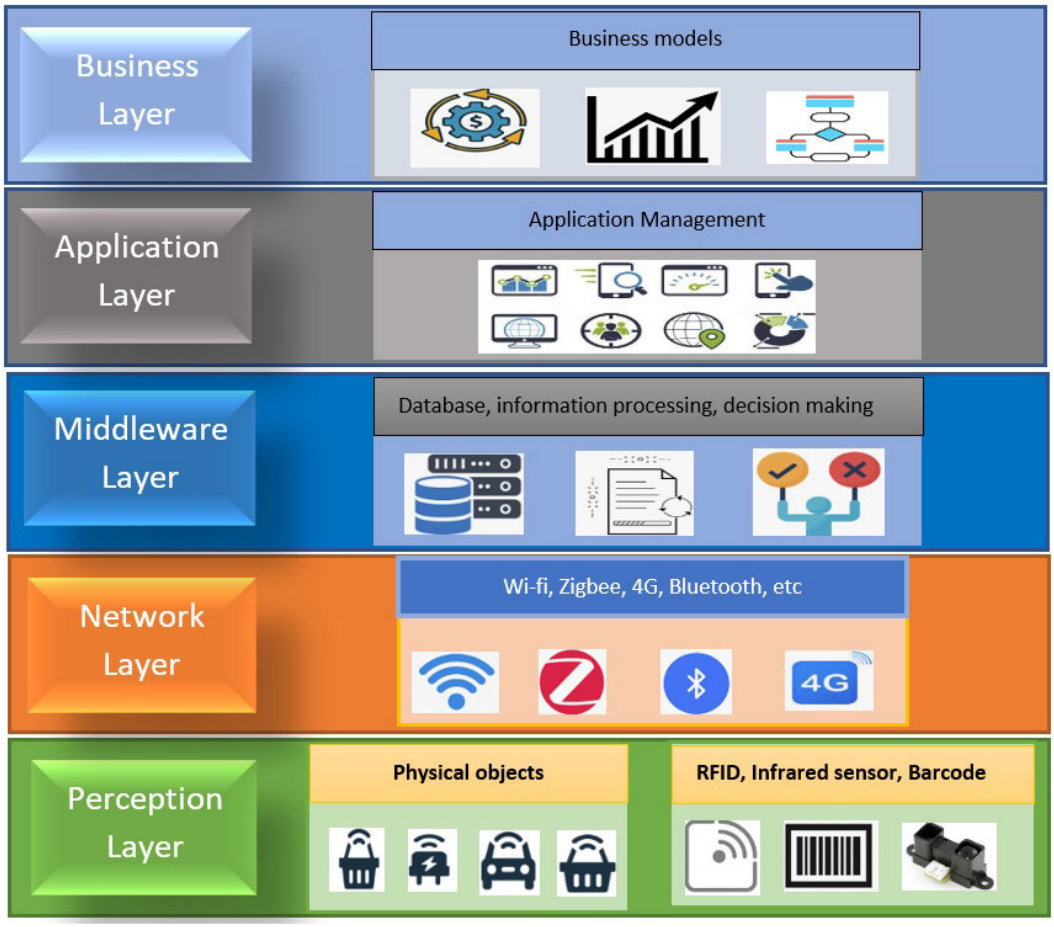

FIGURE 2. RFID-based IoT business model architecture.

in a secure environment. Depending on the sensor devices, the transmission medium can be wireless (e.g., WiFi, infrared, Bluetooth) or wired. It transmits information from the perceptual layer to the middleware layer.

3) Middleware Layer: IoT objects implement various types of service. Each object communicates and connects only to the other objects that implement the same service type. It is responsible for managing services and has a connection to the database. It obtains information from the network layer and stores it in the database. It processes the information and performs ubiquitous calculations. More importantly, it automatically makes decisions based on the results.
4) Application layer: This layer offers global application management based on information about objects that are being handled within the middleware layer. IoT-adopted applications can be smart home, smart agriculture, smart agriculture, etc.
5) Business layer: It is responsible for managing the entire IoT ecosystem, including applications and services. Based on the data received from the application layer, this layer constructs business models, graphs, flowcharts, and more. A good business model determines the real success of IoT technologies. In particular, the determination of future actions and business plans depends on the analysis of results.

C. RFID-BASED IoT APPLICATIONS

RFID-based IoT applications can generally be classified into three categories: (i) supervising, (ii) monitoring, and (iii) tracking. Supervising evaluates and monitors the activities and behaviors of objects or users that are generally achieved without their knowledge [58], for example, by recording objects' movements in the database. Monitoring observes the current state of the object by periodically examining it and provides a warning in the event of a change. For example, hospitals can use this technique to detect suspicious activities in objects and report them immediately [15]. Tracking identifies where moving objects are. Recent published studies related to RFID-based IoT applications can be found in [59], [60], [61], [62], [63], and [64].

Table 2 classifies and summarizes RFID-based IoT applications according to their identification goals, abbreviations, and recently published articles.

TABLE 2. RFID-based IoT applications types.

The goal of Identification	Application Type	Abbreviations	References
Identifying the existence of an object	Asset management	ASM	[27]–[29]
Identifying the location of an object	Tracking	TRA	[30]–[32]
Identifying the source of an object	Authenticity verification	AUV	[33]–[35]
Linking data with the object for decision making	Process control	PRC	[36]–[43]
Identifying the authorized users holding tags	Access control	ACC	[44]–[46]
Identifying affiliated objects	Matching	MAT	[47], [48]
Performing a financial transaction	Contact-less payment	COP	[49]–[51]
Monitoring and control of objects during their lifetime	Supply chain management	SCM	[52]–[57]

D. RFID-BASED IoT CHALLENGES

Although RFID-based IoT applications appear promising, their technical and operational aspects also present a range of challenges, as discussed below.

1) SECURITY ISSUES

Due to their limited cost, the tags themselves do not have the ability to adequately ensure security. According to [65], this can lead to unauthorized users using the legal reader or the purchased reader to communicate directly with the tag. After discovering tags with their information, they can use the RFID system without permission through illegal means, such as counterfeits. In addition, the tags can be encoded and copied. For read-write tags, they may face the risk of data rewriting. Several researchers have participated in the implementation of low-cost privacy and security protocols to increase their applicability [66], [67]. Many lightweight RFID solutions have been proposed, but they are still expensive, vulnerable to security risks, and do not fully address security issues [58]. To this point, the author of [68] states that security concerns related to RFID tags can have major implications for individuals and organizations. Tags that are not properly protected are always easy targets for eavesdropping, DoS attacks, traffic analysis, and other things.

2) COLLISION PROBLEMS

The communication link between the tags and the readers is wireless and therefore can be exposed to electromagnetic interference. Simultaneous transmission over RFID can lead to collisions, as readers and tags usually connect to the same wireless channel. Therefore, when building large-scale RFID applications, it is very important to use efficient collision detection protocols that simultaneously identify multiple tags [69]. Many anticollision protocols have been proposed to identify RFID tags, such as the query tree (QT) [70], binary tree (BT) [71], frame-slotted ALOHA protocol (FSA) [72]. Despite this, most protocols have an overall detection efficiency of less than 50% [73].The development of new and better protocols requires the best characteristics of the identification protocol.

3) PRIVACY CONCERNS

As the connection between objects becomes closer and the connection between people and objects becomes even closer, the privacy of large amounts of data and users becomes an urgent task in RFID-based IoT applications. The ability to read personally correlated information without consent poses serious privacy concerns such as tracking, as tags can be embedded or inserted into anything or any living being. In addition to this, unauthorized readers could even violate privacy by accessing tags without adequate access controls. Although the content of the tag is secure, privacy issues, such as tracking, are possible due to predictable tag responses. For example, a traffic analysis attack can affect location privacy. RFID applications still require privacy policies that take into account the total cost [68].

4) DESIGN AND INTEGRATION CHALLENGES

Two other problems have also been the main hurdles to the widespread adoption of RFID. The first problem is the design, since RFID technology still requires tags and readers designed to ensure a very reliable identification. The second challenge of RFID is its integration with existing applications. To do this, efficient RFID middleware should be developed to connect new RFID systems to existing infrastructure back-ends [74]. For interested readers, the authors of [75] provide an overview of the most well-known technologies, as well as applications that have recently been integrated with RFID.

III. DEFINITION OF SECURITY GOALS AND STAKEHOLDERS IN THE SCOPE OF RFID

To answer RQ1, the following section outlines RFID security goals, stakeholder, and, above all, defines a secure object and a security attack.

The literature divides traditional security goals into three main groups. (i) Confidentiality, (ii) Integrity and (iii) Availability, referred to as CIA-triad. Confidentiality guarantees that sensitive data can only be obtained from legitimate users or objects. The confidentiality of RFID sensitive data, such as credit cards and medical records, must be protected. The authors of [77], stated that the detrimental consequences of fraudulent access to medical objects can range from the disclosure of personal data to life-threatening situations. The integrity of RFID enabled devices is also an essential requirement for providing reliable services, as it ensures that such devices always receive authorized commands and data. However, lack of data integrity in any RFID application can cause undesirable effects, such as attacks on insulin pumps [78]. The availability of RFID applications is also

TABLE 3. RFID-based IoT security goals [76].

Security goals	Definition	Abbreviations
Confidentiality	A capacity of RFID-based IoT applications to restrict data access only to authorized users	CONF
Integrity	A capacity of RFID-based IoT applications to maintain completeness and accuracy of their data	INTG
Non-repudiation	A capacity of RFID-based IoT applications to validate the incidence of any event	NREP
Availability	A capacity of RFID-based IoT applications to provide accessibility of its services	AVAL
Privacy	A capacity of RFID-based IoT applications to sustain privacy rules or policies	PRIV
Auditability	A capacity of RFID-based IoT applications to monitor all events taking place	AUDI
Accountability	A capacity of RFID-based IoT applications to hold users accountable for their actions	ACNT
Trustworthiness	A capacity of RFID-based IoT applications to verify an object identity	TRST

TABLE 4. RFID-based IoT stakeholders [13].

Stakeholders	Roles	Abbreviations
Manufacturer	Building RFID-based IoT hardware	MAN
Developer	Developing RFID-based IoT solutions or services	DEV
Provider	Providing RFID-based IoT products or services to customers	PRV
Consumer	Using RFID-based IoT objects in different aspects of their daily lives	CNS

fundamental, as it ensures that their data is always available and accessible to their valid users.

Although Confidentiality, Integrity and Availability triad (CIA-triad) is well known, it is not efficient to investigate new threats that may appear in a cooperative environment such as IoT or RFID, according to [79]. To address this issue, the authors in [79] suggest a complete set of security goals, known as Information, Assurance, and Security octave (IAS), by studying a huge amount of current information in terms of security.

Table 3 summarizes the security goals suggested by the IAS octave, along with their abbreviations and definitions in connection with RFID-based IoT applications.

According to Table 3, we define:

Security attack: An attack that violates at least one of the security goals of the RFID applications.

Secure object/application: An object/application that achieves all of the RFID-based IoT security goals.

To build a framework of security and privacy guidelines that reflects all aspects of the life cycle of RFID-based IoT applications, we first propose a classification of identified RFID stakeholders into four groups, depicted in Table 4. We then relate key stakeholders to their respective roles to determine the degree to which the guidelines are adapted and the impact on stakeholders.

IV. RFID STANDARDS

To answer RQ2, the following section provides an overview of some of the RFID standards, analyzes their recommended security mechanisms, and links them to the security goals shown in Table 3.

A. INDUSTRY STANDARDS FOR RFID AND THEIR SECURITY MECHANISMS

The interoperability of RFID-based IoT applications can only be achieved when tags and readers follow the same standard, which facilitates, for example, object updates and communications. EPCglobal standards and specifications, suggested for patient safety and supply chain systems, are the most popular industry standards. EPCglobal proposes several specifications, such as the Class-0 Ultrahigh Frequency (UHF), Class-1 Generation -1 High Frequency (HF) and Class-1 Generation-2 UHF specifications. The class-1 Generation-2 was selected as the standard by EPCglobal [9].

1) (EPC0) CLASS-0 UHF

EPCglobal initially developed it for the supply chain. The main objective of this class was to build an inexpensive identification tag, and it offers two basic security aspects. A self-destructive feature, and a 16-bit cyclic redundancy check (CRC). The self-destructive aspect is known as the kill command (a 24-bit password) issued by a reader to permanently deactivate a tag. In this case, the tag no longer responds to commands.

2) (EPC1) CLASS-1 GENERATION-1

This class has two specifications. One is for HF operations and the other is for UHF operations. For example, the HF specification identifies a tag operated at 13.56 MHz and is equipped with two security features: a 16 bit CRC and a self-destruct feature, which is 24 bits.

3) (EPC1S) CLASS-1 GENERATION-2 VERSION 1 STANDARD

EPCglobal selects this specification as a standard and includes two basic security mechanisms, the kill command and cover coding method. The number of bits used in the kill command and the access password is 32 bits [80]. Cover coding obscures the data transmitted from the reader to the tag and works as follows. (i) A reader sends the message to a tag asking for a key, (ii) the tag creates a random 16 bit number and sends it back to the reader, (iii) the reader generates the ciphertext by implementing an exclusive-OR (XOR) function on the plain text and the key, (iv) the reader transmits the ciphertext to the tag, and (v) the tag implements the XOR

function that uses the key and the ciphertext to obtain the plain text. Moreover, this standard comes with an optional password-protected access control, the main objective of which is to temporarily or permanently make some parts of a tag memory read-and-write protected or write-safeguarded.

4) (EPC1S2) CLASS-1 GENERATION-2 VERSION 2 STANDARD

In 2013, EPCglobal released EPC1S2 to address some security issues found in EPC1S and supports backward compatibility with EPC1S [81]. This standard offers a novel framework that facilitates the design and implementation of secure applications and protocols. EPC1S2 provides new commands for untraceable file management and privacy and security protection. EPC1S2 also comes with several optional commands, such as SecureComm, ReadBuffer, TagPrivilege, ReadBuffer, Authenticate, Challenge, and KeyUpdate. Authcomm can be used to build authenticated messages and tagprivilege can be used to set appropriate tag privileges. SecureComm can be used to encrypt messages. Untraceable and new File-management commands (e.g., FileOpen, FilePrivilege, FileSetup, FileList) can be used to protect privacy, since user memory can be divided into one or more files. Maximum files cannot exceed 1023 and maximum file size cannot exceed 2044 kilobytes each. Readers can allow access to certain or all files. Memory partitioning can be used to store product life cycle data on a tag. The assignment of data to certain files will grant access to some of those data, which will be limited to certain users [82].

B. ANALYSIS ON RFID STANDARDS

1) THE SECURITY ANALYSIS ON EPC0 AND EPC1

The implementation of these specifications into RFID-based IoT applications will, for sure, violate all the security goals suggested in Table 3. For example, CONF is violated, as the communication link between tags and a reader is not encrypted at all. Therefore, if the attacker is in close proximity, eavesdropping may be possible. Not only that, the memory of writable tags can be easily modified as it lacks access controls. INTG is also violated, as the unique identifier of a tag can be altered and spoofed. The CRC feature of this class protects only against random failures. Typically, tags do not have tamper-proof technology.

Although this specification comes with a self-destructive function called the kill command, it can be used to violate AVAl by disabling a tag for all, since it lacks an access control technique and a key management infrastructure. Last but not least, PRIV is not respected, as an attacker may use the unique identifier to track objects or individuals holding tags.

2) THE SECURITY ANALYSIS ON EPC1S

Due to its security features, some of the security goals can be achieved. For example, CONF and PRIV can be achieved using a cover coding method that obscures passwords and data written to tags using a write command. If security mechanisms- lock commands to protect all memory and CRC error detection commands- to send with parity bits- are properly implemented, then INTG can also be achieved.

It should be noted that managing and creating random numbers in EPC1S is a necessary requirement to ensure CONF, PRIV, and INTG of RFID applications. This is because EPC1S does not specifically define a random number generator method. Using a less secure method from the reader, an attacker can break the cover coding process and then easily eavesdrop on the communication link [83].

Furthermore, EPC1S is vulnerable to various threats and attacks, and its level of security needs to be improved according to many studies [84], [85], [86], [87]. These vulnerabilities arise from the lack of explicit authentication techniques and security functionalities [88]. For example, EPC1S does not support heavy weight symmetric and asymmetric algorithms, nor does it support even hash functions [89]. Therefore, complex cryptographic encryption mechanisms cannot be implemented on an EPC tag for security reasons. EPC1S is also not explicitly integrated into anti-cloning mechanisms and does not have a mechanism by which the reader can verify the identification of scanned tags. Furthermore, EPC1S does not support flexible file management, according to [82].

Due to the limitations mentioned above, preventing multiple threats, such as eavesdropping, impersonation, and cloning, can be very challenging. However, several research efforts [90], [91], [92], [93], [94], [95], [96], [97], [98] have been conducted to improve the security and privacy of EPC1S. However, other studies such as [99] and [100] have shown that EPC1S cannot provide good security without changing its air protocol.

3) THE SECURITY ANALYSIS ON EPC1S2

Like EPC1S1, this standard supports the use of a CRC function, a pseudo random number generator (PRNG), and XOR function. Furthermore, EPC1S2 offers a new architecture that simplifies the creation and implementation of secure applications and protocols by providing several optional commands (e.g., AuthComm, and KeyUpdate).

The authors in [82] and [101] stated that although this architecture is very flexible and powerful, both industry and academia are currently not familiar with its features and have had some difficulties integrating these optional functions into promising applications. To date, several research efforts have been conducted to do so. For example, many research studies [102], [103], [104], [105], [106], [107] have been conducted to develop different authentication protocols that meet the EPC1S2 standard.

V. SECURITY AND PRIVACY BY DESIGN PRINCIPLES FOR RFID-BASED IoT

To answer RQ3, the following section highlights security and privacy by design principles for RFID in the scope of IoT and, above all, defines a security guideline and a privacy guideline.

TABLE 5. Privacy by design principles for RFID-based IoT applications.

Privacy principles	Definition	Abbreviations
Minimization	Data and assets of RFID-based IoT applications must be trimmed to a minimal level	MIN
Hide	Sensitive data and assets of RFID-based IoT applications must be ensconced	HID
Separation	Data life cycle of RFID-based IoT applications must be handled in a distributed approach	SEP
Aggregation	Data life cycle of RFID-based IoT applications must be processed in an abstract method	AGG
Notification	RFID-based IoT applications must inform users before storing or sharing their data	NOT
Control	RFID-based IoT applications must always give users the control over their data	CON
Enforcement	RFID-based IoT applications must always respect users' privacy over their operations	ENF
Demonstration	RFID-based IoT applications must always comply with privacy regulations	DEM

TABLE 6. Security by design principles for RFID-based IoT applications.

Privacy principles	Definition	Abbreviations
Minimise attack surface	Reduce the complexity of RFID-based IoT applications and assets	MAS
Establish secure defaults	High-security level by default for RFID-based IoT components	ESD
Least privilege	Users get the minimum levels of access to RFID-based IoT functions	LP
Defence in depth	Security must be applied in different layers of RFID-based IoT applications	DD
Fail securely	Take secure precautions in case of RFID-based IoT applications failures	FS
Don't trust services	Restrict third-party services permissions to RFID-based IoT applications	DTS
Separation of duties	Restrict users' privileges to access RFID-based IoT resources	SD
Avoid security by obscurity	RFID-based IoT applications rely on strong standard security mechanisms	ASO
Keep security simple	RFID-based IoT applications avoid using very complex security architectures	KSS
Fix security issues correctly	RFID-based IoT applications identify the root cause of problems	FSI

A. DEFINITION OF PRIVACY PRINCIPLES IN THE SCOPE OF RFID-BASED IoT

In the literature, several frameworks have been suggested to facilitate the process of eliciting privacy requirements and integrating privacy capabilities into applications. In [8], Ann Cavoukian, proposed the original privacy by design framework. The framework provides seven principles, and developers should follow these principles when developing privacy-sensitive applications. These principles are as follows: (i) privacy as the default setting, (ii) privacy embedded into design, (iii) respect for user privacy, (iv) proactive not reactive, (v) full life-cycle protection, (vi) full functionality positive-sum, and (vii) visibility. However, these principles are commonly suggested for computer systems, and software engineering that develops IoT applications may find it difficult to adopt such principles into their applications, as they are given at high abstraction levels and do not provide enough information to implement them.

In [108], Hoepman proposes eight simple principles of privacy by design that traditional software developers can use to improve their applications from the start. Due to its simplicity and clarity for the real use cases given, this work will depend on this framework to state our derived privacy guidelines for RFID-based IoT applications,

Table 5 summarizes the privacy by design principles proposed by Hoepman and provides their definitions in the context of RFID-based IoT applications and abbreviations.

According to Table 5, we define:

Privacy guideline: A guideline that derives at least from one of the principles of privacy by design.

B. DEFINITION OF SECURITY BY DESIGN PRINCIPLES IN THE SCOPE OF RFID-BASED IoT

In [109], European Union Agency for Network and Information Security (ENISA) indicates that attacks and threats against the IoT ecosystem stem from the complexity and heterogeneity of its enabling technologies. Indeed, ENISA emphasizes the importance of incorporating security best practices or security requirements to secure applications from the ground up. To this end, Open Web Application Security (OWASP) in [110] proposes security by design principles that developers can use to build secure applications. This work relies on these principles to state our derived security guidelines for RFID-based IoT applications.

Table 6 summarizes the security by design principles proposed by OWASP and provides their definitions in the context of RFID-based IoT applications and abbreviations.

According to Table 6, we define:

Security guideline: A guideline that derives at least from one of the security by design principles.

VI. POSSIBLE ATTACKS AGAINST RFID TAGS

To answer RQ4, the following section describes attacks and threats applicable for RFID and correlates them with RFID security goals, identified in Table 3. More specifically, it annotates with '⚠' when the security goal in question is violated by the described attack. An overview of RFID attacks and their violations of security goals can be found in Table 7.

A. (AT1) PHYSICAL ATTACK

RFID tags are susceptible to physical attacks, as some RFID enabled objects can be deployed in uncontrolled

environments and, more importantly, may have poor physical security. In such scenarios, an adversary may have full physical access to such objects and could bring them to their laboratory for modification. Various attacks and threats on RFID tags have been investigated in the literature [111]. The most well-known are listed below.

- Tag removal: Some RFID tags attached to items can be easily removed due to lack of physical security. This prohibits all legitimate readers from interacting with vandalized tags [112].
- Tag switching: In this scenario, attackers target tags associated with valuable objects, such as products in stores. Due to the lack of physical protection, tags that are not protected against outside invaders can be easily captured, removed, altered, or swapped. In this attack, attackers replace the tags on expensive RFID products with cheaper items, allowing them to reduce prices at checkout. Such attacks are possible because some back-end servers cannot ensure and create accurate associations between tags and items. Therefore, it poses an important security concern and such attacks cannot be massively scaled [113].
- Tag destruction: Due to lack of physical security, tags can be physically destroyed by attackers, even if they do not receive a specific benefit. An RFID destroyer with the purpose of embarrassing people or disrupting operations can easily damage the RFID tag with inadequate physical protection. This action can involve applying pressure, chemical exposure, or even removing all visible antennas [113].
- Tag modification: Most RFID tags utilize writable memory, so attackers can exploit this functionality to alter or delete valuable data from the tag's memory [114].
- Reverse engineering: To save costs, most of the RFID tags in the estimate do not have a tamper-resistant mechanism for long periods of time. In this case, attackers could take the tags apart, copy them, or physically inspect them to extract valuable information [115]. An example of such attacks is the shoplifting attack. Several retail locations have installed Electronic Article Surveillance (EAS) systems at the main entrance of the store. The main purpose of the system is to differentiate EAS-tagged products that are purchased from a retail store and are not disabled. For example, EAS alerts are activated if a product is accidentally or intentionally taken from the store without paying its price. Shoplifting is treated as an RFID attack, not related to the theft of an item from a store, but rather the theft of the RFID tag for further reverse engineering [116].
- Distance fraud: This attack enables tags to function outside the legitimate zone by convincing the reader that they are within the legal range. Tags use malicious antennas or begin sending out replies before challenges are received to minimize delays caused by being outside the legitimate range. This attack can be mitigated by sending several challenges with strict conditions under which responses should depend on the challenges.This attack has a greater impact on RFID applications where access permissions can vary depending on location [116].

This attack directly violates all security goals (see Table 7), as the attacker has full control and access to the physical object.

B. (AT2) DOS ATTACK

This is a type of attack that can affect communication between authorized readers and the tags. This attack occurs when the attacker simultaneously sends different signals to the server as responses, preventing a system from communicating further. Dos attacks on RFID systems can be classified into four categories:

- Kill command attack: This is a command that authorized readers can use to disable tags when they are not needed to perform their functions. However, an attacker may use this feature to launch more commands that permanently deactivate tags [117].
- Jamming: With RFID tags that listen to each radio within their coverage range, adversaries can transmit electromagnetic waves in the form of noise to interrupt their communication and block tags from communicating with readers [118].
- Tag data modification: This type of Dos attack occurs when an adversary has the ability to alter the EPC data on a tag to a meaningless number that the reader does not recognize anymore [117].
- Desynchronization attack: The main goal of this type of Dos attack is to block the update of secret keys transferred between the tag and the reader. A scenario occurs when an attacker can sabotage the synchronous state between the tag and the reader by preventing the message updates, causing the tag and the reader to store different values [119].

AT2 affects the AVAL, as implied by the attack definition. ACNT is no longer guaranteed due to the low response times of the system. For INTG, the guaranteed transmission can be compromised, especially for real-time applications. The AUDI is also violated because the system cannot continuously monitor objects' activities. Table 7 represents the security goals violated by *AT2*.

C. (AT3) EAVESDROPPING

Although eavesdropping attacks are typically linked to communication protocols, they can be explicitly carried out for the RFID tags. The main objective of this type of attack is to intercept, read, and even modify RFID application messages. Threats posed by eavesdropping on RFID tags have been considered in many published reports (e.g. [11]). In addition to these reports, several published surveys can be found in [16] and [120]. In [120], the authors discussed some practical attacks and their experimental settings.

AT3 violates CONF and PRIV, as the attacker indirectly intercepts and reveals the private data generated and processed by the RFID enabled objects. Additionally, NREP is

affected, as the attacker can drop some packets, preventing the system from validating the incidence of its events. Table 7 represents the security goals violated by *AT3*.

D. (AT4) TAG COUNTERFEITING

In such attacks, attackers can change the object's identity with tag-modifying methods. Unlike cloning attacks that require more information to be initiated, counterfeit attacks require less information to be lunched. In such attack, a tag is partially modified [111]. *AT4* violates all security goals (see Table 7), as the attacker operates directly on the RFID tag by modifying its identity.

E. (AT5) TAG CLONING

This type of attack occurs when attackers read data from authorized RFID tags, then design tags or objects to mimic the behaviors of authorized tags. Such attacks are very valuable for hackers and, at the same time, too risky for the company's reputation. By cloning tags, attackers gain access to sensitive data and closed areas [121]. An example of this attack is found in [122], where the authors demonstrate their technical abilities in attacking the Texas Instruments Digital Signature Transponder (DST) system. In fact, they can obtain a secret cryptographic key from a DST object by collecting only two pairs of challenge-response. Since they were able to recover the key, they simply used a low-cost RFID object to copy the target DST so that it simulates its radio output to fool the reader.

Similar to tag counterfeiting attacks, *AT5* violates all security goals (see Table 7) since the attacker operates directly on the RFID tag by cloning its functions.

F. (AT6) TAG TRACKING

This is one of the most common threats against RFID tags, since each tag has a unique identifier that is transmitted to nearby readers. A malicious reader could simply read a tag attached to a person or object, leading to strong tacking information [121], [123], [124]. This tracking approach is possible even if the tag identifier is random and does not contain identifiable data. The simplest form of such attacks can be achieved by using malicious readers to read the identifiers of fixed tags. This attack could be amplified if the identification of the tag was combined with personal data. For example, according to [18], when a customer purchases some products with his credit card, a merchant can associate his identity with a tag. In this case, the merchant could use the networks of RFID readers installed inside or outside the store to identify and profile customers. This attack violates PRIV as the attacker is indirectly capable of attributing the private data to specific identities. Additionally, NREP is violated because an attacker can change the identity of a tag, making it difficult for the system to verify the frequency of their events. Table 7 represents the security goals violated by *AT6*

G. (AT7) TAG INVENTORYING

Several types of tags that contain sensitive information are easily integrated into multiple objects. For this purpose, the EPC tag consists of two fields: the product code and the manufacturer code. Therefore, individuals with the EPC tag are susceptible to inventorying [125]. For example, by identifying which type of medical object is attached to a patient (such as an insulin pump), an attacker can guess his/her medical condition. Like the tag tracking attack, PRIV and NREP (see Table 7) are affected by *AT7*.

H. (AT8) SIDE CHANNEL ATTACK

With RFID technology, a side-channel attack can even occur when the communication link between the tags and the reader is encrypted. In this scenario, an attacker can use a ready-to-use tool to intercept messages between tags and readers to extract information from various patterns. For example, an attacker could estimate the number of people living in a house after reading the tags at the entrance of that house [126].

Similar to eavesdropping attacks, a set of security goals (see Table 7), namely CONF, NREP, and PRIV are violated by *AT8*.

I. (AT9) REPLAY ATTACK

Replay attacks are one of the most significant threats facing RFID systems. This type of attack, depending on the system configuration, is possible when the data is transmitted from one component to another. This kind of attack can be achieved by interrupting the communication route and manipulating the information between different RFID components [127]. For example, an attacker can copy valid RFID communication responses in such attacks and then send them to one or more parties, trying to impersonate another. Typically, copied packets are retrieved by the adversary by eavesdropping or creating sessions. A good example of such attacks is the broadcast of correct copies of radio signals transmitted by valid tags to readers that allow access via authentic tags. An RFID application is particularly susceptible to replay attacks due to the small and inexpensive tags, leading to a lack of in-depth security measures [115], [128].

AT9 could violate all security goals (see Table 7), if the packets exchanged between a tag and a reader lack any fresh nonces. In this case, an adversary could reuse or modify the old packets and replay the old ones again in order to obtain similar privileges or access.

J. (AT10) SPOOFING

This attack is a kind of fraudulent attack in which an adversary installs a vicious device on a communication link. Since an attacker impersonates a real tag, the attacker can gain all privileges and information about that tag. This information is then stored by the adversary on the malicious node [129].

TABLE 7. The violated security goals by RFID attacks.

Attacks	Security goals							
	CONF	INTG	NREP	AVAL	PRIV	AUDI	ACNT	TRST
AT1	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
AT2	⚠	⚠		⚠		⚠	⚠	
AT3	⚠		⚠		⚠			
AT4	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
AT5	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
AT6			⚠		⚠			
AT7			⚠	⚠				
AT8	⚠		⚠		⚠			
AT9	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
AT10	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
AT11	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
AT12	⚠	⚠	⚠	⚠	⚠	⚠	⚠	⚠
AT13	⚠		⚠		⚠			

Because attackers can impersonate a legitimate tag and store its sensitive information, *AT10* could violate all security goals (see Table 7).

K. (AT11) RELAY ATTACK

This type of attack can be viewed as a man-in-the-middle attack, in which an illegal tag attempts to interact with a legitimate reader and persuades the reader to believe that it is a valid tag; it is authentic to communicate with it. In this scenario, the security mechanism of the system is violated, and the main parties do not know about the breach. This attack becomes more dangerous if RFID tags are not equipped with cryptographic algorithms [130].

If the tags are not protected by encryption mechanisms, then *AT11* can violate all security goals (see Table 7).

L. (AT12) DISCLOSURE ATTACK

In this type of attack, an attacker can guess secret information (e.g., shared keys, IDs and other secret data) from RFID applications. Identity disclosure and full disclosure attacks are two different types of such attacks on RFID applications. In a full disclosure attack, the attacker can recover all the information stored in the tag, while in an identity disclosure attack, the attacker can steal the tag's identity [131]. Typically, the disclosure attack is carried out through two methods, namely a recursive linear attack and a recursive differential attack. Recursive differential attacks consist of probabilistic attacks and require multiple authentication sessions to carry out such attacks. Recursive linear attacks are passive attacks that require only one authentication session to carry out such attacks [132].

AT12 can violate all security goals (see Table 7) as an attacker can guess secret information, such as shared keys.

M. (AT13) JAMMING

In a jamming attack, an attacker can block communication between legitimate tags and readers to prevent nodes from interacting with readers.Attackers build signals that are identical to readers, making tags unreadable for readers [21].

AT13 violates AVAL as the attacker could prevent the tags from communicating with a reader. It also violates NREP, AUDI, ACNT, and RFID because the RFID system fails to validate and monitor its incidents, hold objects responsible for their actions, and verify the identities of objects. The violations of the security goals can be found in Table 7.

VII. MITIGATION TECHNIQUES FOR PROTECTING RFID TAGS

To answer RQ5, this section reviews the mitigation techniques in the RFID tags and attributes them for the attack vectors, identified in Section VI. An overview of the countermeasures proposed for RFID applications is presented in Table 8.

A. (MT1) CRYPTOGRAPHIC SCHEMES

Attributed to attack *AT2*, *AT3*, *AT4*, *AT5* and *AT6*. In RFID tags, a straightforward implementation of full encryption algorithms is not possible due to the need for low-cost tags (e.g., 10 cents), which limits their computing power and memory. It should be noted that the implementation of Advanced Encryption Standard (AES) algorithms requires 5000 to 10000 gates, while RFID tags can support 1000 to 2000 gates [133]. Nevertheless, Jung et al. [134] suggest a novel AES implementation that only requires 3595 gates. The recently proposed RFID encryption technique is described in [135]. However, in RFID tags, there is no fully implemented version of AES. Cryptographic schemes can be divided broadly into various categories:

1) LIGHTWEIGHT HASH FUNCTION

Being widely used to address security concerns of RFID applications, different solutions have been proposed in the literature [135], [136], [137], [138]. The most common lightweight hash functions available for RFID applications are SPONGENT [139], L-CAHASH [140], Quark [141], and Hash-One [142]. Aumasson et al. proposed a lightweight hash function, known as Quark, in 2013. In fact, the authors proposed three types of quarks: D-Quark, T-Quark, and U-Quark. D-Quark has 80 bits of security and T-Quark has 112 bits of security, so it requires 2296 gates. U-Quark supports 64-bit security and requires 1379 gates.

2) LIGHTWEIGHT PROTOCOLS

Low-cost tag requirement is essential for RFID technology, making it difficult to implement traditional cryptographic algorithms. However, several lightweight cryptographic protocols have been proposed [145], [146]. For example, the authors of [125] suggest a lightweight mutual authentication protocol for the tags RFID, which requires only 300 gates. More importantly, the authors argue that this protocol provides an accepted level of security for certain applications.

3) KEY MANAGEMENT

Symmetric cryptography has been used in most RFID applications (e.g., 3 Data Encryption Standard (DES) in epassport). Key management techniques are used in such situations. The reason is that tags and readers share a unique tag-specific secret key that no one of the two parties can begin to identify with the other. It should be noted that secret key sharing is a problem with RFID applications. If a tag, on the one hand, begins to distinguish and express its identity in plain text, then all other readers working at the same frequency can read and track this identity. If a reader, on the other hand, begins verifying itself with the tag without knowing which tag to interrogate, it cannot identify the secret key to use. To this end, several mechanisms have been proposed in the literature to solve this paradox [165], [166], [167], [168], [169].

4) LIGHTWEIGHT BLOCK CIPHER

Unlike stream ciphers, which encrypt only a single bit, block ciphers encrypt the entire block. Depending on the block cipher structure, researchers identify various types of structure such as the generalized Feistel network (GFN), substitution permutation networks (SPN), and Feistel networks. In the literature, multiple lightweight block ciphers have been proposed, the most notable of which are RECHANGLE [170], LILLIPUT [171], LRBC [172], SFN [35], BORON [173] and LICI [174].

5) LIGHTWEIGHT STREAM CIPHER

A light stream cipher consumes minimal computational effort, but provides high levels of security by creating a cipher text based on a given plaintext. This merges a pseudo-random shared key with the plaintext to enable plaintext encryption. Depending on its structure, there are a variety of stream ciphers, such as Shift Register with Carry Feedback (FCSR), linear Feedback Shift Register (LFSR), addition/rotation/XOR (ARX), Nonlinear Feedback Shift Register (NFSR), and random shuffle [175]. In the literature, several lightweight stream ciphers have been proposed, of which the most notable are Fruit-80 [176], SVH [177], ALE [178], and WG-8 [179].

6) AUTHENTICATION

For authentication, RFID applications use challenge-response based authentication protocols. The symmetric key is initially shared between a tag and a reader. The tag ensures that the reader knows that the key belongs to them without revealing it. This process involves transferring a reader's challenge to a tag. Then the tag uses the shared key to perform some cryptographic functions to generate a response and send it back to the reader. The reader runs the same cryptographic functions with the shared key to verify if the results of its calculations match those received from the tag. Having the same results, the reader authenticates the tag. Note that this process is performed in reverse when mutual authentication is needed. Symmetric cryptography was used in existing authentication protocols [180], [181], [182], while asymmetric cryptography was less adopted [183].

7) DISTANCE-BOUNDING PROTOCOL

It is a lightweight authentication protocol that not only verifies that a communication entity (e.g., tag or reader) has the correct key, but also determines whether the distance between readers and tags is below a certain threshold [184]. Measurement of this distance can be achieved using RTT (round trip time), which measures the time it takes for a reader to send a challenge and receive a reply from a tag, or using signal strength RSSI (Receiving Signal Strength Indicator) [185]. Generally, a distance-bounding protocol works in three stages. (i) This stage is called the initial setting, where session parameters (eg, nonces) are defined by readers and tags. (ii) This phase is called the time phase, in which the challenge-response cycles take place, and the round trips are measured by the reader. (iii) This stage is called the final authentication stage, and in this stage, the reader is ensured that the second stage has been faithfully carried out so that the reader can utilize RTT to determine the distance. This is accomplished by verifying the accuracy of all round trip times and proving that the tag signature is valid.

B. (MT2) KILL COMMAND

Attributed to attack *AT2*, *AT4*, *AT5*, *AT6*, *AT7* and *AT8*. It is one of the simplest mechanisms proposed by the Auto-ID Center and EPCglobal to safeguard the client's privacy [80]. During the manufacturing process, some of the RFID tags may be equipped with a kill command, which

TABLE 8. A summary of the mitigation strategies proposed for RFID tags.

Implementation Techniques	References	Year	Mechanism used
MT1	[137]	2022	Proposes a set of enhancements to mitigate security threats found in a popular lightweight encryption approach known as Extended Tiny Encryption Algorithm (XTEA) to achieve mutual authentication for RFID and Green Wireless Sensor Network Applications.
	[138]	2021	Suggests a Cryptographic solution-based secure ECC-enabled RFID authentication protocol for the Internet of Vehicle. This solution is made up of three lightweight stages: Setup stage, Server Authentication stage, and Tag authentication stage.
	[143]	2019	Suggests a lightweight protocol to securely authenticate RFID tags and a reader based on one assumption, that is, each tag preshares a secret key with the reader.
	[135]	2018	Proposes symmetric encryption technique for RFID applications based on dynamic key generation
	[144]	2022	Proposes a novel RFID authentication protocol which depends on a lightweight block cipher algorithm
	[145]	2022	Proposes three lightweight protocols that can be used to authenticate inexpensive tags
	[146]	2022	Suggests a safe and effective mutual authentication protocol using bitwise operations.
	[147]	2022	Suggests a new lightweight RFID authentication protocol that can resist several attacks
MT2	[80]	2006	Tag deactivation was proposed by EPCglobal
MT3	[148]	2008	Suggests an isolated container made of a metal mesh to protect the privacy of tags
	[149]	2005	Suggests a new approach to enhance isolation between receivers and transmitters for passive RFID applications
	[150]	2019	Proposes a new carrier leakage cancelation technique that is needed in UHF RFID reader circuit
	[151]	2002	Suggests jamming all neighboring radio channels by an active RF jammer that frequently hinders particular RF channels
MT5	[152]	2009	Suggests a look-up mapping mechanism to achieve the goal of location privacy by converting the genuine ID of RFID into an anonymous one.
	[67]	2022	Proposes an anonymous and secure highlight RFID protocol used specifically for the Internet of Vehicles.
	[153]	2022	Suggests a lightweight anonymous RFID authentication protocol using XOR and pseudorandom function (PRF) operations
	[125]	2006	Proposes a novel technique to change an anonymous ID frequently to prevent some privacy issues (e.g., tracking attack)
MT6	[154]	2013	Proposes an Physically Unclonable Function (PUF)-based authentication protocol which utilizes a pair of item-level tags to prevent cloning attacks
	[155]	2020	Proposes a lightweight PUF-based authentication protocol that is used to secure communications between smart meters and neighborhood gateways
	[156]	2021	Proposes a secure authentication protocol developed based on PUF and AES
	[157]	2014	Proposes an PUF-based authentication protocol to prevent memory leakage
MT7	[158]	2005	Suggests a personal RFID firewall in which all requests from readers to tags must be verified
	[159]	2006	Proposes a novel idea for a personal RFID-privacy object known as RFID Enhancer Proxy (REP) that operates as a proxy for RFID tags
	[160]	2008	Proposes a framework which can be used to enhance RFID security by using a proxy. The proxy has control over a user's tags and interacts with them.
	[161]	2006	Suggests and implements the RFID Guardian in which people will be able to monitor and control access to their tags by merging unique RFID tag simulation capabilities with a RFID reader
MT8	[121]	2003	Suggests the use of blocker tags as a technique for preserving users' privacy as result of integrating RFID tags into their products
	[162]	2004	Proposes a new version of the blocker concept called soft blocking that provides flexible privacy policies
MT9	[163]	2021	Suggests an approach that could be used to protect passive RFID tags from eavesdroppers by localizing attackers and kicking them out
	[164]	2018	Suggests a new approach that can guess the indoor distance of UHF tags.
	[18]	2006	Suggests a metric using the signal-noise ratio which can be used to identify the distance between a tag and a reader

is a distinct Personal Identification Number (PIN) (e.g., a 32-bit password). Having received the correct PIN from the reader, the RFID tags can be deactivated forever. In this case, such a tag cannot send further information. This process is irreversible. An alternative mechanism known as a sleep command can be used to make the RFID tags inactive for a period of time. To design and implement such approaches, a complex and secure PIN management technique is required. The author in [12] states that killing the RFID tags is not feasible for various IoT based applications, as it could violate one of the IoT security goals, which is AVAL.

C. (MT3) ISOLATION

Attributed to attack *AT3*, *AT5*, *AT6*, *AT7* and *AT8*. One of the most efficient approaches to safeguard the privacy of RFID tags is to isolate them from electromagnetic waves. One way is to build and use separation rooms. However, this approach is highly expensive [148]. An alternative technique is suggested in which an isolation container made of metal is utilized to impede electromagnetic waves. This container is called the Faraday cage [151]. Another approach of blocking specific radio channels using an active radio frequency jammer is proposed.

D. (MT4) CUSTOMER RESPONSIBILITIES

Attributed to attack *AT1*. Customers have a basic rule to prevent some attacks on the RFID tags. For example, customers are responsible for not buying RFID tags from non-reputable manufacturers. Another example is the prevention of the RFID-Tag switch attack in retail stores. In this scenario, the cashiers need to know the approximate supermarket prices for the items to determine whether the tag is turned on or not [116].

E. (MT5) ANONYMOUS TAG

Attributed to attack *AT6* and *AT7*. In [152], the authors suggest a new technique based on table lookup mapping to protect the privacy of RFID tags. The main goal of this technique is to store a mapping between an anonymous ID and a genuine ID to prevent an adversary from revealing the mapping schema to recognize a genuine ID from the anonymous one. Despite emitting anonymous IDs through tags, attackers can still track an RFID tag if its ID does not change over time. Therefore, anonymous ID must be frequently altered to avoid the tacking problem [125].

F. (MT6) HARDWARE-BASED SOLUTIONS

Attributed to attack *AT1* and *AT2*. It can be achieved by integrating PUF into the circuit. The process of adding noise functions to integrated circuits is known as PUF. Having queried with a challenge z, a PUF generates a reply x that depends on both z and the unique intrinsic physical feature of the object [186]. PUFs should be physically unclonable, and tamper-proof [187]. Furthermore, PUFs offers unique object identification and authentication [157], [187].

G. (MT7) PERSONAL FIREWALL

Attributed to attack *AT2*, *AT3*, *AT4*, and *AT6*. A personal RFID firewall can be utilized to monitor all incoming reader requests and can be implemented in an RFID object that has powerful hardware capabilities in terms of storage capacity and computational power (e.g., mobile phones) [158]. Such a firewall provides highly complex rules or policies that need to be implemented; an example of such policies is given in [188], indicating that ''my tag should not release my personal information when I am not within 50 meters of my workplace''.

H. (MT8) BLOCKING

Attributed to attack *AT3*, *AT4*, *AT5*, *AT6*, *AT7* and *AT8*. In [121], the authors propose an effective approach, called blocking, to preserve the privacy of tags RFID. In such a method, a modifiable bit, called a privacy bit, is attached to each tag. Changing a privacy bit to '0' indicates that the tag will be exposed to public scanning, while changing the privacy bit to '1' means that the tag is private. This approach requires a specific type of tag, called a blocker tag. Another approach called soft blocking has been suggested in [162]. It largely depends on the configuration of the reader to force a group of policies to be implemented in an RFID application. This group of policies ensures that readers only read public tags. A reader's violation of the tag policy can be detected using a monitoring object.

I. (MT9) DISTANCE ESTIMATION

Attributed to attack *AT5*. The authors in [88] suggest a method to determine the distance between a tag and a reader based on the signal-to-noise ratio. They claim to be able to infer a metric in which the distance between readers trying to read a tag is predicted. This allows the tag to provide only distance-based information. For example, upon scanning at 10 meters, the tag will publish only public data, but it will provide its unique identifier at 1 meter.

J. (MT10) PHYSICAL ACCESS CONTROLS

Attributed to attack *AT1*, *AT3*, and *AT5*. Attackers, in some cases, need to be close enough to some of RFID enabled devices to perform destructive activities to compromise its data INTG and AVAL by damaging and modifying its components. Therefore, it is imperative to prevent, or at least limit, an attacker's ability to have a direct physical access to such devices. Physical security controls such as walls, gates, surveillance cameras and locked doors must therefore be applied to all RFID devices.

According to [9], the implementation of physical access controls could mitigate several threats, such as physical destruction of RFID tags and readers, denial of service due to illegal commands or radio interference, and cloning tags. However, it should be noted that physical access controls, within a perimeter, do not prevent radio interference emitted by legitimate tags and readers, nor do they alleviate threats triggered by an insider attacker.

VIII. ANALYSIS ON SECURITY AND PRIVACY GUIDELINES FOR RFID

To answer RQ6, the following section describes our derived guidelines, some of which have been suggested in our earlier work [13], for RFID in relation to the stakeholders involved. Table 9 determines the degree of adoption of guidelines and their impact on stakeholders. This section also provides the 'reason' used to formally state each guidance. Consecutively, the overall structure of the guidelines is presented with links between the guidelines, mitigation techniques, and attacks, as shown in Figure 3.

A. (G1) MINIMIZE INTERFERENCE

This guideline suggests minimizing interference between the RFID tags and a reader as much as possible. The deployment of RFID tags far from other objects generated radio frequency noise (e.g., microwaves) can mitigate such interference. In addition, interference may occur due to the high duty cycle of the RFID reader, which depends on regulations and standards. According to [9], readers with more power and duty cycles can read tags more precisely, more quickly, and at greater distances. However, the use of high-energy power

will increase the risks of eavesdropping. This guideline can be achieved by *MT4*, *MT3*, and *MT8*.

Reasoning: This guideline is formulated according to the MAS principle proposed in the security by design framework.

Table 9 represents the stakeholders who might use this guideline. For instance, CNS, DEV and PRV could conduct pilot installations that evaluate the performance of RFID applications in planned environments. Also MAN could implement RFID Anti-Collision Protocols (e.g., Abramson's Logic of Hiring Access (ALOHA) protocol or tree-based algorithms) [72]. For interested readers, all types of RFID collisions can be found in [189].

B. (G2) PROTECT CRITICAL INFORMATION

This guideline suggests that each RFID tag must be equipped with specific mechanisms (e.g., a side-channel analysis) to inhibit fraudulent attempts to obtain its vital information. Several patterns, such as power analysis, can be utilized by an adversary to reveal sensitive information about an object, even if its communication link is encrypted. For example, if an attacker, using any technique, could read the tags at the entrance of a home, the attacker could guess the number of people in the home at any time by computing the number of communications [190]. This guideline requires that different mitigation techniques (*MT5*, *MT2*, *MT3*, and *MT8*) to be implemented in RFID applications.

Reasoning: This guideline is derived in accordance with two principles *DD* and *HID* proposed in the security by design framework and the privacy by design framework, respectively. Table 9 represents the stakeholders who may utilize this guideline. This guideline is not applicable to CNSs, as they cannot equip their RFID enabled objects with special countermeasures, such as side channel analysis, to prevent illegal attempts to obtain their personal information.

C. (G3) PREVENT REVERSE ENGINEERING

Since some RFID-based IoT objects may be deployed in remote environments (e.g., gas and oil industry), such objects are prone to physical attacks such as reverse engineering. An adversary, for example, could gain access to an object and then the attacker could take it apart to uncover its key security parameters and components. Therefore, this guideline suggests that each RFID-based IoT object should be equipped with a tamperproof mechanism to prevent reverse engineering attacks [191]. It can be implemented by *MT6*.

Reasoning: This guideline is derived in accordance with the DD principle proposed in the security by design framework. Table 9 represents the stakeholders who may utilize this guideline. This guideline is not applicable for Provider (PRV) and Consumer (CNS) as they cannot equip their RFID objects with a tamper-proofing mechanism.

D. (G4) PROVIDE DISTANCE-BASED INFORMATION

This guideline indicates that an RFID tag must provide its information to a reader if and only if it is located within its predefined range. For example, a tag could only publish public data if it is scanned at 10meter, while it could offer its unique identifier if it is scanned within 1meter [18]. This guideline can be implemented by *MT9*.

Reasoning: This guideline is stated in accordance with the HID principle and the MAS principle proposed in the privacy by design framework and the security by design framework, respectively. Table 9 shows the stakeholders that may benefit from this guideline.

E. (G5) CHECK ALL READERS' REQUEST TO TAGS

To prevent unwanted scanning of RFID tags, the authors in [158] indicated the importance of examining all the requests from the readers. For this purpose, an object with high hardware capacity in terms of memory, computing power, and storage capacity can be used. It can be implemented by *MT7*.

Reasoning: This guideline is stated in accordance with the DD principle proposed in the security by design framework. Table 9 identifies the stakeholders who may utilize this guideline.

F. (G6) CHANGE ANONYMOUS ID FREQUENTLY

In [192], a technique based on a lookup table was proposed to inhibit attackers from revealing real IDs of tags after changing them to anonymous ones. Nevertheless, adversaries could still track RFID applications as long as anonymous IDs are not replaced over time. Two mitigation approaches (*MT5* and *MT1*) can be used to achieve this guideline.

Reasoning: This guideline is derived in accordance with the HID principle proposed in privacy by design framework. Table 9 identifies the stakeholders who may utilize this guideline.

G. (G7) SECURE KILL COMMAND

During the manufacturing process, the tags are designed with a kill command, which is unique PIN (e.g., a 23-bit password). Due to this feature, the tags can be permanently killed or disabled by the reader if they receive a valid PINs. For instance, a tag on a supermarket product might be killed or deactivated by the supermarket employer upon the sale of the product, protecting client privacy and preventing tracking [193]. This guideline therefore suggests that the kill command in each RFID tag should be secured and cannot be killed by unauthorized readers. Isolation of tags, as well as blocking, can be considered as direct ways to protect a secure kill command, as attackers cannot reach such tags. The authors in [159], indicated the importance of using a personal RFID firewall to make kill commands more secure. This guideline can be implemented by *MT3*, *MT7*, and *MT8*.

Reasoning: This guideline is formulated in accordance with the CON principle proposed in the privacy design framework. Table 9 recognizes the stakeholders who may utilize this guideline.

TABLE 9. The involved stakeholders in our proposed guidelines.

Guidelines	The involved IoT stakeholders			
	MAN	DEV	PRV	CNS
G1	✓	✓	✓	✓
G2	✓	✓	✓	✗
G3	✓	✓	✗	✗
G4	✗	✓	✓	✓
G5	✗	✓	✓	✗
G6	✓	✓	✗	✗
G7	✓	✓	✗	✗
G8	✓	✓	✗	✗
G9	✓	✗	✗	✗
G10	✗	✓	✓	✓
G11	✓	✓	✗	✗
G12	✓	✓	✓	✗
G13	✓	✓	✗	✗
G14	✓	✓	✓	✓
G15	✓	✓	✓	✓
G16	✓	✓	✓	✗
G17	✓	✓	✓	✗
G18	✓	✓	✓	✓

H. (G8) PREVENT PHYSICAL TAMPERING

In some cases, RFID enabled objects can be installed and operated in remote or hostile environments in which direct access to such objects can be possible, making them susceptible to hardware/software attacks [194]. Therefore, this guideline suggests that each IoT object should be equipped with a suitable tamper-resistant measure. It can be implemented by *MT6*

Reasoning: This guideline is stated according to the DD principle proposed in the security by design framework, as well as the HID principle proposed in the privacy by design framework. Table 9 recognizes stakeholders who can use this guideline.

I. (G9) IMPLEMENT HARDWARE TRUST

Trust data in RFID-based IoT applications is of paramount importance, as such applications are developed to communicate with each other to accomplish certain tasks. If the data INTEG of a single sensor has been compromised, the entire RFID-based IoT application may be considered insecure. For example, a humidity sensor could be modified to always give a certain inattentive value of the real one [195]. Therefore, this guideline suggests the use of hardware trust in each object, such as PUF. It can be implemented by *MT6* and *MT1*.

Reasoning: This guideline is formulated according to the DD principle proposed in security by design framework. Table 9 shows the stakeholders who may utilize this guideline.

J. (G10) AVOID UNTRUSTED MANUFACTURER

The growing demand for RFID applications and services led to the development of various manufacturers, some of which (untrusted ones) may develop some products to perform malicious activities from the ground up. Such products can later be used by attackers to compromise the applications where these products are being deployed. Thus, this guideline suggests that customers and developers are advised to avoid purchasing RFID components or products from untrustworthy manufacturers [191]. This guideline can be implemented by *MT4*.

Reasoning: This guideline is formulated according to the DTS principle proposed in the security by design framework. Table 9 presents the stakeholders who may utilize this guideline.

K. (G11) USE UNIQUE SECURITY PARAMETERS

This guideline indicates that security parameters, such as a kill command for each tag, should be unique. The main advantage of this guideline comes from the fact that the disclosure of security parameters on an RFID object cannot be used to compromise other objects. This guideline can be achieved by *MT1*

Reasoning: This guideline is derived in accordance with the ESD principle proposed in security by design framework. Table 9 identifies the stakeholders who may utilize this guideline.

L. (G12) SEPARATE PERSONAL INFORMATION FROM TAG IDENTIFIER

There are some types of tags that can contain valuable or sensitive data on the board about objects and people attached to them. This tag is known as an EPC tag, consisting of two components: a manufacturer code and a product code. As a consequence, people or objects equipped with the EPC tag

are vulnerable to inventory attacks [88]. In [196], the authors stated that threats and attacks on RFID systems can increase exponentially if the tags' identifiers are combined with personal information. Therefore, this guideline recommends that personal information (e.g., credit card and personal profile) should be separated from tag identifiers. The main goal of this guideline is to mitigate privacy issues while increasing the acceptance and transparency associated with RFID systems. Therefore, the security of this type of tag is essential. Two mitigation techniques, namely *MT5*, and *MT1* can be used to carry out this guideline.

Reasoning: This guideline is stated based on HID, SEP and ENF principles proposed in the privacy by design framework. Table 9 presents the stakeholders who may this guideline.

M. (G13) PREVENT TAGS COUNTERFEITING

In [125], the authors showed that the only scenario in which an adversary could counterfeit a tag in RFID applications is by modifying the identity of the tag using tag manipulation techniques (e.g., side channel analysis and eavesdropping). Therefore, this guideline suggests that each RFID tag should be equipped with a lightweight anti-counterfeit technique to protect its identity. It can be implemented by *MT1* and *MT8*.

Reasoning: This guideline is formulated in accordance with the DD principle proposed in the security by design framework. Table 9 recognizes the stakeholders involved in this guideline.

N. (G14) PREVENT TRACKING

Since most RFID tags contain unique identifiers related to people or physical objects, attackers can track their information. Thus, this guideline suggests that tags' identifiers should not be read by unauthorized readers [196]. Four countermeasures, namely *MT5*, *MT8*, *MT3* and *MT2* can be used to carry out this guideline.

Reasoning: This guideline is stated in accordance with the HID principle proposed in the privacy by design framework. This guideline can be used by all IoT stakeholders (see Table 9).

O. (G15) SECURE DISPOSAL OF TAGS

Discarding RFID tags when they are no longer required to perform their desired functions could pose several privacy risks. For example, an attacker could utilize the existence of tags to track people or products, and, more importantly, the attacker could obtain access to sensitive data stored on the tag. The secure disposal of RFID components physically or electronically is an indispensable requirement to prevent such threats. When a tag supports an electronic disabling technique, a tag's kill command or a strong electromagnetic field could be used to achieve physical destruction. In this case, the tag circuitry is permanently unusable. Shredding or manual tearing could also be used to perform physical destruction. Disabling tags before disposal is recommended, as it can be achieved without physical access to each tag. This guideline can be achieved using *MT4*, *MT2*, and *MT10*.

Reasoning: This guideline is derived in accordance with the CON principle and the DD principle proposed in the privacy by design framework and the security by design framework, respectively. This guideline can be used by all IoT stakeholders (see Table 9).

P. (G16) ENCRYPT THE DATA ON TAGS

Encrypting sensitive data stored on tags is essential to prevent attackers and unauthorized persons from reading or misuse of such data. Data encryption process does not have to be accomplished by tags; it can be achieved by either a reader or a middleware, instead. This is because data encryption necessitates a key management approach, which is very complicated to implement and manage by the tag. When encryption/ decryption is carried out by the reader or middleware, network access is required to read data content stored on the tag. This technique is not suitable for dynamic readers whose real-time access to the network is missing. Furthermore, sending tag data to network components to be encrypted/decrypted will lead to network delay in RFID applications that require fast writing and reading transactions. This guideline can be implemented by *MT1*

Reasoning: This guideline is developed on the basis of the ENF and AGG principles proposed in the privacy by design framework. Also it is stated based on the DD principle proposed by the security by design framework. Table 9 presents the stakeholders who may utilize this guideline.

Q. (G17) USE STRONG AUTHENTICATION

This guideline is very important to separate fake tags from legitimate ones by a tag reader. Note that standard EPC tags lack any access control mechanisms. To this end, an attacker could use an RFID simulator to emulate certain tags to fool a tag reader. However, mutual authentication, which is the procedure by which the identity of the tag and the reader is verified by each other, can be used to enhance the security of RFID applications. Due to the limitations of the RFID tags in terms of computational power and memory, heavy-weight encryption techniques cannot be implemented on the RFID tags to accomplish the security goals [143]. To contribute to this objective, a set of lightweight encryption approaches, such as straightforward one-way hash function and pseudorandom number generator for RFID tags, has been proposed. Currently, there are ongoing efforts to develop a lightweight protocol to securely authenticate RFID tags and a reader, which can be found in Table 8.

Reasoning: This guideline is stated based on the DD principle proposed in the security by design framework. Table 9 identifies the stakeholders who may utilize this guideline.

R. (G18) MINIMIZE DISTANCE BETWEEN READER AND TAG

In RFID applications, distance requirements play an important role in determining the type of tag to be deployed. The distance requirement between the tag and the read may also

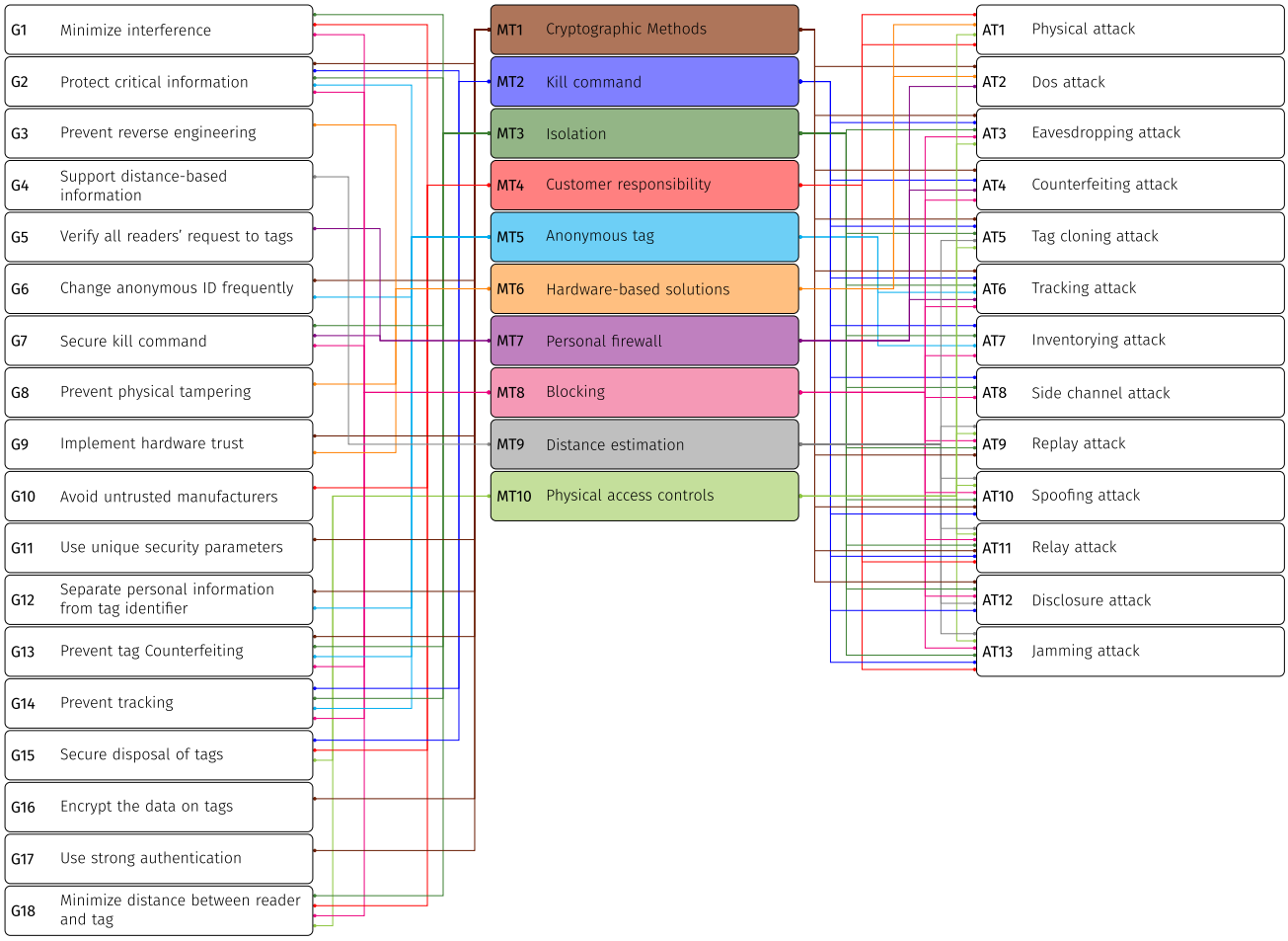

FIGURE 3. A summary of guidelines, attacks and countermeasures for RFID tags.

have some security implications. For example, an attacker could easily eavesdrop on their communications due to the longer distances between them. Furthermore, long distances give attackers the chance to use their own readers to perform illegal transactions more simply and efficiently. In some RFID applications, setting the correct distance between the tag and the reader requires considerable effort from the developers. For example, the authors of [197] state that an RFID application that authorizes access to a garage may require drivers to install an RFID-enable card within inches of the reader or may need a proximity of several feet to the RFID-enabled transponder within the car. This choice needs to consider various factors such as price and convenience. This guideline requires that different mitigation techniques (*MT10*, *MT4*, *MT3*, and *MT8*) to be implemented in RFID systems.

Reasoning: This guideline is formulated according to the MAS principle proposed in the security by design framework. Table 9 identifies the stakeholders who may use this guideline.

Figure 3 summarizes the connection between our proposed guidelines for RFID tags, followed by their appropriate mitigation techniques and associated attack vectors.

IX. DISCUSSION AND FUTURE WORK

A. THE ABSENCE OF AWARENESS AMONG RFID STAKEHOLDERS

The lack of awareness of the security benefits of RFID-based IoT objects is widespread among all stakeholders. This is because some of them do not have enough knowledge about attacks and threats they may face in the future, nor do they know the mitigation strategies required to prevent them. For example, most customers do not only lack a basic understanding of their objects, but also do not comprehend the impact of such objects on their environments in the event of being hacked or misused [198]. As a consequence, several objects may not be patched and therefore may be subjected to different attacks and threats. Manufacturers also must educate and inspire their employees to adopt security best practices [199]. Therefore, it is necessary to raise awareness among RFID stakeholders of the consequences of existing RFID attacks and threats, the use of appropriate mitigation techniques, and more importantly, the advantages of leveraging security and privacy guidelines in the early stages of RFID development.

B. LACK OF GUIDELINES FOR RFID DATA AT REST

The main objective of this work is to suggest a set of security and privacy guidelines and their mitigation techniques for RFID-based IoT applications. However, these guidelines are specifically designed to protect tags, readers, and their communications. Protecting data at rest of RFID-based IoT applications, either in the back-end database or in the cloud, is a major limitation of our work and is beyond the scope of this paper. Data protection at rest is absolutely necessary, as different applications can collaborate to perform certain tasks and services. In this case, if data INTG of a single application at rest has been compromised, then there is a very high risk of working with a cascading effect of data breach. For example, the authors in [188] indicate that thermostats operated in smart homes depend entirely on smoke detectors data to turn off heating systems in case of emergency. However, if an attacker could access these data, he/she might expose the entire smart home to danger.

Furthermore, once RFID-based IoT applications store their data in the cloud, there is no guarantee that only legitimate objects or users will have access to these data. The ENISA (https://www.enisa.europa.eu/) gives an example, where an employee (adversary) due to given access rights at the Sharplocks company was able to push a malicious update from the client's server to all of its connected objects.

To mitigate individual privacy violations and unauthorized access associated with IoT data at rest, we proposed, in our previous work in [76], a set of security and privacy guidelines for IoT data at rest. Such guidelines can be used by IoT stakeholders to develop secure IoT applications from the outset, and thus reinforce security and privacy by design. However, our framework was specifically designed for IoT applications. Theoretically, our framework could also be used to partially protect RFID-based IoT applications. This is due to some of our derived guidelines, such as minimizing data storage, encrypting data storage, and minimizing data retention, could be utilized to protect data at rest of any applications, let alone RFID-based IoT applications. However, a list of security and privacy guidelines must be explicitly derived to protect RFID data at rest in the future.

C. OPEN ISSUES AND CHALLENGES

Researchers and scientists have developed various security measures in recent decades to make RFID applications resistant to a variety of threats and attacks. However, currently there is no fully tested mechanism to protect RFID applications against all possible attacks. As soon as a new security technique is introduced by some scientists, attackers change their approach to attack a system. Thus, existing security mechanisms are always open to improvement and, at the same time, many issues need to be addressed. Therefore, researchers are motivated to work in this critical area of implementing complete solutions for the RFID system. This subsection presents several problems and challenges facing current security strategies.

1) NEED OF ULTRA-LIGHTWEIGHT SECURITY TECHNIQUES

Due to RFID-enabled devices' limitations, such as small battery sizes and small memory capacity, it is always a challenge to develop ultra-lightweight security solutions that can cope with these constraints and at the same time provide security against all types of RFID attacks. Section VII introduces multiple lightweight security methods for RFID objects that utilize OR and XOR operations. However, such security approaches do not ensure security against a variety of attacks (e.g., desynchronization and tracking attacks) [200], [201]. Therefore, developing an approach that can withstand a variety of attacks remains an open challenge. Furthermore, researchers can constantly work to minimize the battery and memory requirements of RFID-enabled devices.

2) NEED OF SECURE AUTHENTICATION TECHNIQUE

Verifying the identity of communication objects in RFID applications is a mandatory requirement.To date, researchers have used several mechanisms [202], [203], [204] to ensure authentication for RFID applications, such as elliptic curve cryptography, symmetric key cryptography, and others. However, the development of a single mechanism that takes into account all types of authentication problems remains an open challenge for researchers to come up with.

3) NEED OF HASH FUNCTIONS WITH LESS COMPUTATION OVERHEAD

Hash functions are widespread in some of the RFID security methods proposed by scientists to implement the authentication and integrity of the RFID system. However, hash functions are computationally intensive, while the computing power of RFID objects is limited, making it difficult to provide protection against a variety of security threats [200]. This means that the hash function must be smaller in output size and communicate securely with low computational costs. Therefore, the development of hash functions with fewer computational complexity is another research challenge.

4) NEED OF LIGHTWEIGHT CIPHER WITH OPTIMAL KEY SIZE

To develop lightweight ciphers, it is necessary to take into account key size and block size. The size of keys and blocks amplifies the overall computing power demands of RFID objects. However, as the size of the key or block decreases, an attacker can easily break a cipher by quickly guessing its security key. For this reason, the block cipher size must be optimized so that attackers cannot easily break through the cipher [205]. The new approach must be hardware efficient, consume minimal computing power, and resist all types of security attack.

5) NEED OF SECURE AND EFFICIENT STREAM CIPHERS

The design of stream ciphers in the present situation is based on round functions, operations, components, and structures.The main structure of the stream cipher is a

permutation of the fixed hash function. Many existing stream ciphers have been presented by different researchers [206], [207], [208]. However, such stream ciphers have many limitations [175], [209]: they are vulnerable to an associated key attack, for example. Therefore, researchers working in the area of creating secure and effective RFID applications find it challenging to build a stream cipher capable of addressing all of these shortcomings. To contribute to this goal, the development of new solutions requires taking into account various matrices such as power consumption, throughput, interface, etc., as well as several security issues.

X. CONCLUSION

The article starts out with mentioning the growth and influence of IoT in various domains, and a crucial component based on RFID-technology being responsible for its success in a large part. However, while guidelines, known mitigations, and attacks identification exist and have been researched over the past years, security and privacy threats and attacks are not well addressed as a whole. Therefore, the major contribution of this work lies in providing the first review and modelling of its kind that analyzes the vast landscape of RFID-based IoT, its existing threats, mitigations, and common security and privacy practices, bringing it together into a singular security framework (Figure 3).

To fully accomplish this contribution, a set of research questions are introduced, which serve as the road map for this study. In RQ1 and RQ3, we outline security goals and discuss security and privacy by design frameworks for RFID-based IoT applications. From there, we define several concepts in the scope of RFID-based IoT applications: (i) a security attack, (ii) a secure object/application, (iii) a privacy guideline, and (iv) a security guideline.

In RQ2, we highlight the relevant RFID standards, analyze their recommended security features, and link them to security goals. This research question illustrates that many studies have been conducted to develop various authentication protocols that meet the EPC1S2 standard.

In RQ4 and RQ5, we provide the reader with the opportunity to explore which attacks against RFID-based IoT applications have been initiated and which security goals such as CONF, INTG, and AVAL have been violated, and more importantly, how they have been mitigated. Furthermore, these two research questions show that researchers have worked hard to develop effective and secure RFID systems. However, there is room for improvement in some areas. Therefore, this article also provides some open issues and challenges that researchers working in this important area should address in the future.

In RQ6, we aim to improve security and privacy by design for RFID-enabled devices with a number of guidelines. Each of the presented guidelines is analysed and provided with a reasoning on why we think a certain guideline is appropriate for issuing one or more mitigations for certain attacks. As a whole this synthesizes and structures the security framework into a helpful tool for the security and privacy by design concept.

As pointed out in the previous section, providing guidelines for RFID data at rest would be an extension of this work and future work. It was deemed out of scope for this work as we focus on the communication technology RFID itself and thus not the data within the IoT device.

REFERENCES

[1] D. Ward. (2009). *A Brief History of RFID*. [Online]. Available: http://www.u.arizona.edu/~obaca/rfid/home.html

[2] Market and Market. (2022). *RFID Market by Offering (Tags, Readers, Software & Services), Tag Type (Passive, Active), Wafer Size, Frequency, Form Factor (Card, Implant, Key Fob, Label, Paper Ticket, Band), Material, Application & Region—Global Forecast to 2030*. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/rfid-market-446.html

[3] R. Anggarwal and M. L. Das, "RFID security in the context of 'Internet of Things,'" in *Proc. 1st Int. Conf. Secur. Internet Things*, 2012, pp. 51–56.

[4] F. Azzedin and M. Ghaleb, "Internet-of-Things and information fusion: Trust perspective survey," *Sensors*, vol. 19, no. 8, p. 1929, Apr. 2019.

[5] L. Yan, Y. Zhang, L. T. Yang, and H. Ning, *The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems*. Seattle, WA, USA: Amazon, 2008.

[6] *The IPv6 Challenge—Part 1*, Incognito Softw., Vancouver, BC, Canada, 2011.

[7] G. P. Hancke, K. Markantonakis, and K. E. Mayes, "Security challenges for user-oriented RFID applications within the 'Internet of Things,'" *J. Internet Technol.*, vol. 11, no. 3, pp. 307–314, 2010.

[8] A. Cavoukian, "Privacy guidelines for RFID information systems (RFID privacy guidelines)," Office Inf. Privacy Commissioner, Toronto, ON, Canada, Jun. 2006.

[9] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, Standard NIST SP 800-98, 2007. [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Guidelines+for+Securing+Radio+Frequency+Identification+(RFID)+Systems#0

[10] D. M. Konidala, D.-Y. Kim, C.-Y. Yeun, and B.-C. Lee, "Security framework for RFID-based applications in smart home environment," *J. Inf. Process. Syst.*, vol. 7, no. 1, pp. 111–120, 2011.

[11] *RFID Feasibility Study Final Report: RFID Security and Privacy, Strategies*, Smart Border Alliance, Rosslyn, VA, USA, 2006, pp. 1–22.

[12] M. Chamekh, M. Hamdi, S. El Asmi, and T.-H. Kim, "Security of RFID based Internet of Things applications: Requirements and open issues," in *Proc. 15th Int. Multi-Conf. Syst., Signals Devices (SSD)*, Mar. 2018, pp. 699–703.

[13] H. A. Abdul-Ghani and D. Konstantas, "A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective," *J. Sens. Actuator Netw.*, vol. 8, no. 2, p. 38, Apr. 2019. [Online]. Available: https://www.mdpi.com/2224-2708/8/2/22

[14] A. A. A. Ibrahim, K. Nisar, Y. K. Hzou, and I. Welch, "Review and analyzing RFID technology tags and applications," in *Proc. IEEE 13th Int. Conf. Appl. Inf. Commun. Technol. (AICT)*, Oct. 2019, pp. 1–4.

[15] Z. Y. M. Yusoff, M. K. Ishak, and K. A. Alezabi, "The role of RFID in green IoT: A survey on technologies, challenges and a way forward," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 6, no. 1, pp. 17–35, Jan. 2021.

[16] *RFID Security Issues & Challenges*, Mandai's Polytech., Pune, India, 2014.

[17] J. I. Aguirre, "EPCglobal: A universal standard," Ph.D. dissertation, System Des. Manag. Program, Brown Univ., Providence, RI, USA, 2007. [Online]. Available: http://web.mit.edu/smadnick/www/wp/2007-01.pdf

[18] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[19] M. A. Baballe, "A Study on the Components used in RFID System and its Challenges," *Global J. Res. Eng. Comput. Sci.*, vol. 1, no. 1, pp. 1–7, Oct. 2021.

[20] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, 2004, pp. 210–219.

[21] A. Kumar, A. K. Jain, and M. Dua, "A comprehensive taxonomy of security and privacy issues in RFID," *Complex Intell. Syst.*, vol. 7, no. 3, pp. 1327–1347, Jun. 2021, doi: 10.1007/s40747-021-00280-6.
[22] K. Ahsan, "RFID components, applications and system integration with healthcare perspective," *Deploying RFID: Challenges, Solutions, and Open Issues*. London, U.K.: IntechOpen, Aug. 2011.
[23] A. Alwadi, A. Gawanmeh, S. Parvin, and J. N. Al-Karaki, "Smart solutions for RFID based inventory management systems: A survey," *Scalable Comput., Pract. Exp.*, vol. 18, no. 4, pp. 347–360, Nov. 2017.
[24] Y. D. Santos and E. Dias Canedo, "On the design and implementation of an IoT based architecture for reading ultra high frequency tags," *Information*, vol. 10, no. 2, p. 41, Jan. 2019.
[25] L. Tan and N. Wang, "Future internet: The Internet of Things," *McKinsey Quart.*, vol. 2, no. 2, pp. 70–79, 2010.
[26] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. Frontiers Inf. Technol.*, Dec. 2012, pp. 257–260.
[27] V. K. Shukla and B. Singh, "Conceptual framework of smart device for smart home management based on RFID and IoT," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 787–791.
[28] R. Kulkarni and S. Kulkarni, "Hospital asset management using IoT and RFID," *Int. J. Res. Eng. Sci.*, vol. 9, no. 8, pp. 1–6, 2021. [Online]. Available: https://www.ijres.org
[29] G. Wenjun, "Design and implementation of asset management system based on RFID," in *Proc. IEEE Int. Conf. Power, Intell. Comput. Syst. (ICPICS)*, Jul. 2021, pp. 579–583.
[30] F. J. Valente and A. C. Neto, "Intelligent steel inventory tracking with IoT/RFID," in *Proc. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA)*, Sep. 2017, pp. 158–163.
[31] B. Khoo, "RFID-from tracking to the Internet of Things: A review of developments," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.*, Dec. 2010, pp. 533–538.
[32] P. A. Kamble and R. A. Vatti, "Bus tracking and monitoring using RFID," in *Proc. 4th Int. Conf. Image Inf. Process. (ICIIP)*, Dec. 2017, pp. 400–405.
[33] F. M. Belenguer, A. Martínez-Millana, A. M. Salcedo, and J. H. A. Nunez, "Vehicle identification by means of Radio-Frequency-Identification cards and magnetic loops," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 12, pp. 5051–5059, Dec. 2020.
[34] A. Kliem and O. Kao, "Cooperative device cloud: A resource management framework for the Internet of Things," in *Connectivity Frameworks for Smart Devices*. Cham, Switzerland: Springer, 2016.
[35] L. Li, B. Liu, Y. Zhou, and Y. Zou, "SFN: A new lightweight block cipher," *Microprocessors Microsystems*, vol. 60, pp. 138–150, Jul. 2018.
[36] K.-P. Gao, G.-C. Shen, N. Zhao, C.-P. Jiang, B. Yang, and J.-Q. Liu, "Wearable multifunction sensor for the detection of forehead EEG signal and sweat rate on skin simultaneously," *IEEE Sensors J.*, vol. 20, no. 18, pp. 10393–10404, Sep. 2020.
[37] M. Tanaka, "Improving obesity and blood pressure," *Hypertension Res.*, vol. 43, no. 2, pp. 79–89, Feb. 2020, doi: 10.1038/s41440-019-0348-x.
[38] H. Koshimizu, R. Kojima, K. Kario, and Y. Okuno, "Prediction of blood pressure variability using deep neural networks," *Int. J. Med. Informat.*, vol. 136, Apr. 2020, Art. no. 104067, doi: 10.1016/j.ijmedinf.2019.104067.
[39] T. K. Dhiman, G. B. V. S. Lakshmi, R. Kumar, K. Asokan, and P. R. Solanki, "Non-enzymatic detection of glucose using a capacitive nanobiosensor based on PVA capped CuO synthesized via co-precipitation route," *IEEE Sensors J.*, vol. 20, no. 18, pp. 10415–10423, Sep. 2020.
[40] B. Man, "Noninvasive spectroscopic detection of blood glucose and analysis of clinical research status," *J. Healthcare Eng.*, vol. 2022, pp. 1–5, Feb. 2022.
[41] M. Dautta, M. Alshetaiwi, J. Escobar, and P. Tseng, "Passive and wireless, implantable glucose sensing with phenylboronic acid hydrogel-interlayer RF resonators," *Biosensors Bioelectron.*, vol. 151, Mar. 2020, Art. no. 112004, doi: 10.1016/j.bios.2020.112004.
[42] T. Arikawa, T. Nakajima, H. Yazawa, H. Kaneda, A. Haruyama, S. Obi, H. Amano, M. Sakuma, S. Toyoda, S. Abe, T. Tsutsumi, T. Matsui, A. Nakata, R. Shinozaki, M. Miyamoto, and T. Inoue, "Clinical usefulness of new R-R interval analysis using the wearable heart rate sensor WHS-1 to identify obstructive sleep apnea: OSA and RRI analysis using a wearable heartbeat sensor," *J. Clin. Med.*, vol. 9, no. 10, pp. 1–16, 2020.
[43] V. Mazzaracchio, L. Fiore, S. Nappi, G. Marrocco, and F. Arduini, "Medium-distance affordable, flexible and wireless epidermal sensor for pH monitoring in sweat," *Talanta*, vol. 222, Jan. 2021, Art. no. 121502, doi: 10.1016/j.talanta.2020.121502.
[44] M. M. Bahgat, "Enhanced IoT-based online access control system for vehicles in truck-loading fuels terminals," in *Proc. IEEE 6th Int. Conf. Ind. Eng. Appl. (ICIEA)*, Apr. 2019, pp. 765–769.
[45] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in Internet-of-Things: A survey," *J. Netw. Comput. Appl.*, vol. 144, pp. 79–101, Oct. 2019.
[46] S. Trab, E. Bajic, A. Zouinkhi, M. N. Abdelkrim, and H. Chekir, "RFID IoT-enabled warehouse for safety management using product class-based storage and potential fields methods," *Int. J. Embedded Syst.*, vol. 10, no. 1, p. 71, 2018.
[47] C. Corches, M. Daraban, and L. Miclea, "Availability of an RFID object-identification system in IoT environments," *Sensors*, vol. 21, no. 18, p. 6220, Sep. 2021.
[48] C. Z. Li, R. Y. Zhong, F. Xue, G. Xu, K. Chen, G. G. Huang, and G. Q. Shen, "Integrating RFID and BIM technologies for mitigating risks and improving schedule performance of prefabricated house construction," *J. Cleaner Prod.*, vol. 165, pp. 1048–1062, Nov. 2017, doi: 10.1016/j.jclepro.2017.07.156.
[49] P. M. Akshay, K. Murugesh, and Y. Patra, "IoT based automated paid parking using electromagnetic RFID tag," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, May 2019, pp. 1451–1452.
[50] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, K. Jambi, and M. Alrasheedi, "A novel and secure smart parking management system (SPMS) based on integration of WSN, RFID, and IoT," in *Proc. 15th Learn. Technol. Conf. (LT)*, Feb. 2018, pp. 102–106.
[51] Y. Agarwal, P. Ratnani, U. Shah, and P. Jain, "IoT based smart parking system," in *Proc. 5th Int. Conf. Internet Things Appl. (IOTA)*, Jan. 2016, pp. 464–470.
[52] C. Gu, "Fast discrepancy identification for RFID-enabled IoT networks," *IEEE Access*, vol. 6, pp. 6194–6204, 2018.
[53] O. Urbano, A. Perles, C. Pedraza, S. Rubio-Arraez, M. L. Castelló,M. D. Ortola, and R. Mercado, "Cost-effective implementation of a temperature traceability system based on smart RFID tags and IoT services," *Sensors*, vol. 20, no. 4, p. 1163, Feb. 2020.
[54] M. Nabeel M, M. Srinivasan, E. Prince, and R. Padmanabhan, "IoT architecture for advanced manufacturing technologies," *Mater. Today: Proc.*, vol. 22, pp. 2359–2365, Jan. 2020, doi: 10.1016/j.matpr.2020.03.358.
[55] K. Fan, Q. Luo, K. Zhang, and Y. Yang, "Cloud-based lightweight secure RFID mutual authentication protocol in IoT," *Inf. Sci.*, vol. 527, pp. 329–340, Jul. 2020.
[56] B. Chakraborty and S. Das, "Introducing a new supply chain management concept by hybridizing TOPSIS, IoT and cloud computing," *J. Inst. Eng. India C*, vol. 102, no. 1, pp. 109–119, Feb. 2021, doi: 10.1007/s40032-020-00619-x.
[57] G. Alfian, M. Syafrudin, U. Farooq, M. R. Ma'arif, M. A. Syaekhoni, N. L. Fitriyani, J. Lee, and J. Rhee, "Improving efficiency of RFID-based traceability system for perishable food by utilizing IoT sensors and machine learning model," *Food Control*, vol. 110, Apr. 2020, Art. no. 107016.
[58] 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.
[59] T. V. Anagnostopoulos and A. Zaslavsky, "Effective waste collection with shortest path semi-static and dynamic routing," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Cham, Switzerland: Springer, 2014.
[60] B. S. Malapur and V. R. Pattanshetti, "IoT based waste management: An application to smart city," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Aug. 2017, pp. 2476–2479.
[61] T. Anagnostopoulos, A. Zaslavsky, and A. Medvedev, "Robust waste collection exploiting cost efficiency of IoT potentiality in smart cities," in *Proc. Int. Conf. Recent Adv. Internet Things (RIoT)*, Apr. 2015, pp. 1–6.
[62] S. Jisha and M. Philip, "RFID based security platform for Internet of Things in health care environment," in *Proc. Online Int. Conf. Green Eng. Technol. (IC-GET)*, Nov. 2016, pp. 10–12.
[63] D. He and S. Zeadally, "An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, Feb. 2015.

[64] C. Occhiuzzi, G. Contri, and G. Marrocco, "Design of implanted RFID tags for passive sensing of human body: The STENTag," *IEEE Trans. Antennas Propag.*, vol. 60, no. 7, pp. 3146–3154, Jul. 2012.

[65] S. Xiwen, "Study on security issue of Internet of Things based on RFID," in *Proc. 4th Int. Conf. Comput. Inf. Sci. (ICCIS)*, Aug. 2012, pp. 566–569.

[66] S. Sundaresan, R. Doss, S. Piramuthu, and W. Zhou, "A secure search protocol for low cost passive RFID tags," *Comput. Netw.*, vol. 122, pp. 70–82, Jul. 2017.

[67] M. Shariq, K. Singh, P. K. Maurya, A. Ahmadian, and D. Taniar, "AnonSURP: An anonymous and secure ultralightweight RFID protocol for deployment in Internet of vehicles systems," *J. Supercomput.*, vol. 78, no. 6, pp. 8577–8602, Apr. 2022, doi: 10.1007/s11227-021-04232-2.

[68] A. Ullah, "IoT: Applications of RFID and Issues," *Int. J. Internet Things Web Services*, vol. 3, pp. 1–5, Jan. 2018.

[69] X. Jia, Q. Feng, and C. Ma, "An efficient anti-collision protocol for RFID tag identification," *IEEE Commun. Lett.*, vol. 14, no. 11, pp. 1014–1016, Nov. 2010.

[70] Y. C. Lai, S. Y. Chen, Z. L. Hailemariam, and C. C. Lin, "A bit-tracking knowledge-based query tree for RFID tag identification in IoT systems," *Sensors*, vol. 22, no. 9, pp. 1–17, 2022.

[71] Y.-H. Chen, Y.-A. Chen, and S.-R. Huang, "A mobility aware binary tree algorithm to resolve RFID jam and bottleneck problems in a next generation specimen management system," *Micromachines*, vol. 11, no. 8, p. 755, Aug. 2020.

[72] D. Benedetti, G. Maselli, C. Petrioli, and M. Piva, "The impact of external interference on RFID anti-collision protocols," *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 76–79, Jun. 2019.

[73] M. A. Bonuccelli, F. Lonetti, and F. Martelli, "Instant collision resolution for tag identification in RFID networks," *Ad Hoc Netw.*, vol. 5, no. 8, pp. 1220–1232, Nov. 2007.

[74] H. Jabbar and T. Ted, "RFID system integration," in *Radio Frequency Identification Fundamentals and Applications, Bringing Research to Practice*. London, U.K.: IntechOpen, May 2010.

[75] E. Valero and A. Adán, "Integration of RFID with other technologies in construction," *Measurement*, vol. 94, pp. 614–620, Dec. 2016, doi: 10.1016/j.measurement.2016.08.037.

[76] H. A. Abdulghani, N. A. Nijdam, A. Collen, and D. Konstantas, "A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective," *Symmetry*, vol. 11, no. 6, pp. 1–36, 2019.

[77] M. Zhang, A. Raghunathan, and N. K. Jha, "Trustworthiness of medical devices and body area networks," *Proc. IEEE*, vol. 102, no. 8, pp. 1174–1188, Aug. 2014.

[78] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th Int. Conf. e-Health Netw., Appl. Services (HEALTHCOM)*, Jun. 2011, pp. 150–156.

[79] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *Proc. 18th Int. Conf. Availability, Rel. Secur. (ARES)*, 2013, pp. 1–11.

[80] *Specification for RFID Air Interface EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz*, Intellectual Property, EPCglobal, San Francisco, CA, USA, Oct. 2006.

[81] *Specification for RFID Air Interface Protocol for Communications at EPC™ Radio-Frequency Identity Protocols Generation-2 UHF RFID Specification for RFID Air Interface*, GS1, Brussels, Belgium, 2013, pp. 1–152.

[82] T. Y. Huang and H.-Y. Chien, "Gen2v2-security-and-privacy-features-leveraged application designs," in *Proc. 9th Asia Joint Conf. Inf. Secur. (AsiaJCIS)*, vol. 2, Sep. 2014, pp. 141–147.

[83] A. Razaq, W. T. Luk, K. M. Shum, L. M. Cheng, and K. N. Yung, "Second-generation RFID," *IEEE Security Privacy*, vol. 6, no. 4, pp. 21–27, Jul./Aug. 2008.

[84] J. H. Khor, W. Ismail, M. I. Younis, M. K. Sulaiman, and M. G. Rahman, "Security problems in an RFID system," *Wireless Pers. Commun.*, vol. 59, no. 1, pp. 17–26, 2011.

[85] D. Trček and P. Jäppinen, "RFID security," in *RFID and Sensor Networks: Architectures, Protocols, Security, and Integrations*. London, U.K.: Taylor & Francis, 2009, pp. 147–168.

[86] T. Phillips, T. Karygiannis, and R. Kuhn, "Security standards for the RFID market," *IEEE Security Privacy*, vol. 3, no. 6, pp. 85–89, Nov./Dec. 2005.

[87] J. Ertl, T. Plos, M. Feldhofer, N. Felber, and L. Henzen, "A security-enhanced UHF RFID tag chip," in *Proc. 16th Euromicro Conf. Digit. Syst. Design*, Sep. 2013, pp. 705–712.

[88] A. Juels, "Minimalist cryptography for low-cost RFID tags (extended abstract)," in *Proc. Int. Conf. Secur. Commun. Netw.*, in Lecture Notes in Computer Science, vol. 3352, 2005, pp. 149–164. [Online]. Available: http://link.springer.com/10.1007/978-3-540-30598-9_11

[89] H.-Y. Chien and C.-H. Chen, "Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards," *Comput. Standards Interfaces*, vol. 29, no. 2, pp. 254–259, Feb. 2007.

[90] D. Duc, J. Park, H. Lee, and K. Kim, "Enhancing security of EPCglobal gen-2 RFID tag against traceability and cloning," in *Proc. Symp. Cryptogr. Inf. Secur.*, Jan. 2015, pp. 97–102. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.5163&rep=rep1&type=pdf

[91] B. Alomair, L. Lazos, and R. Poovendran, "Securing low-cost RFID systems: An unconditionally secure approach," *Cryptol. Inf. Secur. Ser.*, vol. 4, pp. 1–17, Mar. 2010.

[92] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to 'privacy-friendly' tags," *Int. J. Inf. Secur. Privacy*, vol. 20, no. 4, p. 18, 2003.

[93] B. Song and C. J. Mitchell, "RFID authentication protocol for low-cost tags," in *Proc. 1st ACM Conf. Wireless Netw. Secur.*, Jan. 2008, pp. 140–147.

[94] K. H. Kim, E. Y. Choi, S. M. Lee, and D. H. Lee, "Secure EPCglobal class-1 gen-2 RFID system against security and privacy problems," in *Proc. OTM Confederated Int. Conferences Move Meaningful Internet Syst.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 4277, 2006, pp. 362–371. [Online]. Available: http://link.springer.com/10.1007/11915034_60

[95] A. Yamamoto, S. Suzuki, H. Hada, J. Mitsugi, F. Teraoka, and O. Nakamura, "A tamper detection method for RFID tag data," in *Proc. IEEE Int. Conf. RFID*, Apr. 2008, pp. 51–57.

[96] E. Y. Choi, D. H. Lee, and J. I. Lim, "Anti-cloning protocol suitable to EPCglobal class-1 generation-2 RFID systems," *Comput. Standards Interfaces*, vol. 31, no. 6, pp. 1124–1130, Nov. 2009, doi: 10.1016/j.csi.2008.12.002.

[97] J. Park, J. Na, and M. Kim, "A practical approach for enhancing security of EPCglobal RFID Gen2 tag," in *Proc. Future Gener. Commun. Netw. (FGCN)*, 2007, pp. 436–441.

[98] J. Melia-Segui, J. Garcia-Alfaro, and J. Herrera-Joancomarti, "Analysis and improvement of a pseudorandom number generator for EPC Gen2 tags," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 2010, pp. 34–46.

[99] C.-F. Lee, H.-Y. Chien, C.-S. Laih, and C.-S. Chen, "On the security of several Gen2-based protocols without modifying the standards," *J. Chin. Inst. Eng., Trans. Chin. Inst. Eng. A*, vol. 35, no. 4, pp. 391–399, Jun. 2012.

[100] M. Aigner, T. Plos, M. Feldhofer, C. Floerkemeier, Y. Na, and T. Burbridge, "Report on first part of the security WP: Anti-cloning tag (D4.3.1)," Building Radio frequency Identificat. Global Environ., Eur. Commission, D4.3.1, Brussels, Belgium, Tech. Rep. Feb. 2008. [Online]. Available: http://www.bridge-project.eu/data/File/BRIDGE_WP04_Anti_clone_prototype.pdf

[101] H.-H. Huang, L.-Y. Yeh, and W.-J. Tsaur, "Ultra-lightweight mutual authentication and ownership transfer protocol with PUF for Gen2 v2 RFID systems," *Lect. Notes Eng. Comput. Sci.*, vol. 2, pp. 16–19, Mar. 2016.

[102] G. Jin, J. Jin, B. Li, J. Mou, P. Li, and X. Zhao, "A secure mutual authentication protocol to maintain synchrony conforming to EPC Gen2V2 standard," *DEStech Trans. Eng. Technol. Res.*, vol. 1, pp. 165–171, May 2017.

[103] N. X. Hieu, V. N. Nguyen, D. Park, D. Chung, H. Lee, and J.-W. Lee, "A power efficient secure mutual authentication protocol for EPC Gen2v2 standard," in *Proc. Int. SoC Design Conf. (ISOCC), SoC Internet Everything (IoE)*, Nov. 2015, pp. 325–326.

[104] E. Taqieddin, H. Al-Dahoud, M. Mowafi, and O. Banimelhem, "An enhanced EPC Gen2v2 RFID authentication and ownership management protocol," in *Proc. IEEE 42nd Conf. Local Comput. Netw. (LCN)*, Oct. 2017, pp. 683–689.

[105] H. Niu, E. Taqieddin, and S. Jagannathan, "EPC Gen2v2 RFID standard authentication and ownership management protocol," *IEEE Trans. Mobile Comput.*, vol. 15, no. 1, pp. 137–149, Jan. 2016.
[106] Z. Liu, D. Liu, L. Li, H. Lin, and Z. Yong, "Implementation of a new RFID authentication protocol for EPC Gen2 standard," *IEEE Sensors J.*, vol. 15, no. 2, pp. 1003–1011, Feb. 2015.
[107] K. Toyoda and I. Sasase, "Secret sharing based unidirectional key distribution with dummy tags in Gen2v2 RFID-enabled supply chains," in *Proc. IEEE Int. Conf. RFID (RFID)*, Apr. 2015, pp. 63–69.
[108] J.-H. Hoepman, "Privacy design strategies," in *Proc. Int. Inf. Secur. Conf. (SEC)*, 2016, pp. 446–459. [Online]. Available: https://hal.inria.fr/hal-01370395
[109] *Good Practices for Security of IoT*, Eur. Union Agency Netw. Inf. Secur., ENISA, Athens, Greece, Nov. 2019.
[110] D. Sveikauskas. (2021). *Security by Design Principles According to OWASP*. [Online]. Available: https://www.owasp.org/index.php/Security_by_Design_Principles and https://patchstack.com/security-design-principles-owasp/
[111] H. Akram, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 1–19, 2018. [Online]. Available: https://www.ijacsa.thesai.org
[112] M. N. Zahid, J. Jiang, H. Lu, S. Rizvi, D. Eric, S. Khan, and H. Zhang, "Security issues and challenges in RFID, wireless sensor network and optical communication networks and solutions," in *Proc. IEEE 3rd Int. Conf. Safe Prod. Inf. (IICSPI)*, Nov. 2020, pp. 592–599.
[113] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Inf. Syst. Frontiers*, vol. 12, no. 5, pp. 491–505, Nov. 2010.
[114] S. F. Lorenzo, J. A. Benito, P. G. Cardarelli, J. A. Garaia, and S. A. Juaristi, "A comprehensive review of RFID and Bluetooth security: Practical analysis," *Technologies*, vol. 7, no. 1, p. 15, Jan. 2019.
[115] H. Li, Y. Chen, and Z. He, "The survey of RFID attacks and defenses," in *Proc. 8th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2012, pp. 1–4.
[116] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for IoT," *IEEE Access*, vol. 8, pp. 88892–88932, 2020.
[117] D. Tagra, M. Rahman, and S. Sampalli, "Technique for preventing DoS attacks on RFID systems," in *Proc. Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, 2010, pp. 6–10.
[118] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.
[119] S. Gabsi, V. Beroulle, Y. Kieffer, H. M. Dao, Y. Kortli, and B. Hamdi, "Survey: Vulnerability analysis of low-cost ECC-based RFID protocols against wireless and side-channel attacks," *Sensors*, vol. 21, no. 17, p. 5824, Aug. 2021.
[120] G. P. Hancke, "Eavesdropping attacks on high-frequency RFID tokens," in *Proc. 4th Workshop RFID Secur.*, 2008, pp. 259–288.
[121] A. Juels, R. L. Rivest, and M. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in *Proc. 10th ACM Conf. Comput. Commun. Secur. (CCS)*, 2003, p. 103.
[122] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in *Proc. 14th USENIX Secur. Symp.*, 2005, pp. 1–15.
[123] X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 373–384, Aug. 2021, doi: 10.1016/j.dcan.2020.09.001.
[124] A. A. Hezam, "A reference model for securing IoT," Ph.D. dissertation, Faculty Econ. Manage./Inf. Sci. Inst., Geneva Univ., Geneva, Switzerland, 2019.
[125] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in *Personal Wireless Communications*. Cham, Switzerland: Springer, 2006, pp. 159–170. [Online]. Available: http://link.springer.com/10.1007/11872153_14
[126] A. M. Nia, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Physiological information leakage: A new frontier in health information security," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 3, pp. 321–334, Jul. 2016.
[127] X. Shi, J. Cao, T. Lu, and V. Chang, "A survey on RFID security and privacy in smart medical: Threats and protections," in *Proc. 4th Int. Conf. Internet Things, Big Data Secur. (IoTBDS)*, 2019, pp. 278–285.
[128] G. A. Kulkarni and M. Mitra, "RFID security issues," *Int. J. Eng. Res. Technol.*, vol. 2, no. 9, Sep. 2014.
[129] T. Alshammri, M. Albakheet, and I. Kateeb, "Survey on radio frequency identification security and attacks," in *Proc. 5th Int. Conf. Future Netw. Distrib. Syst.*, Dec. 2021, pp. 138–143.
[130] M. Alizadeh, M. Zamani, A. R. Shahemabadi, J. Shayan, and A. Azarnik, "A survey on attacks in RFID networks," *Open Int. J. Informat.*, vol. 1, pp. 15–24, Jun. 2012. [Online]. Available: http://publication.ais.utm.my/ojs/index.php/oiji/article/view/57
[131] M. Safkhani and M. Shariat, "Implementation of secret disclosure attack against two IoT lightweight authentication protocols," *J. Supercomput.*, vol. 74, no. 11, pp. 6220–6235, Nov. 2018, doi: 10.1007/s11227-018-2538-8.
[132] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Recursive linear and differential cryptanalysis of ultralightweight authentication protocols," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1140–1151, Jul. 2013.
[133] P. Peris-lopez, J. C. Hernandez-castro, J. M. Estevez-Tapiador, and A. Ribagorda, "M^2AP: A minimalist mutual-authentication protocol for low-cost RFID tags," in *Proc. Int. Conf. Ubiquitous Intell. Comput.*, Aug. 2011, pp. 912–923.
[134] M. Jung, H. Fiedler, and R. Lerch, "8-bit microcontroller system with area efficient AES coprocessor for transponder applications," in *Proc. Workshop RFID Lightweight Crypto Conf.*, 2005, pp. 32–43.
[135] Z. Labbi, M. Senhadji, A. Maarof, and M. Belkasmi, "Symmetric encryption algorithm for RFID systems using a dynamic generation of key," *Int. J. Comput. Sci. Issues*, vol. 15, no. 1, pp. 25–33, 2018.
[136] S. M. Lee, Y. J. Hwang, D. H. Lee, and J. I. Lim, "Efficient authentication for low-cost RFID systems," in *Proc. Int. Conf. Comput. Sci. Appl.* Berlin, Germany: Springer, 2005, pp. 619–627.
[137] M. Nagarajan, M. Rajappa, Y. Teekaraman, R. Kuppusamy, and A. R. Thelkar, "Renovated XTEA encoder architecture-based lightweight mutual authentication protocol for RFID and green wireless sensor network applications," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–12, Mar. 2022.
[138] S. Sharma, B. Kaushik, M. K. I. Rahmani, and M. E. Ahmed, "Cryptographic solution-based secure elliptic curve cryptography enabled radio frequency identification mutual authentication protocol for internet of vehicles," *IEEE Access*, vol. 9, pp. 147114–147128, 2021.
[139] A. Bogdanov, M. Kneć, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, "SPONGENT: A lightweight hash function," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2011, pp. 312–325.
[140] C. Hanin, B. Echandouri, F. Omary, and S. E. Bernoussi, "L-CAHASH: A novel lightweight hash function based on cellular automata for RFID," in *Proc. Int. Symp. Ubiquitous Netw.*, 2017, pp. 287–298.
[141] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "QUARK: A lightweight hash," *J. Cryptol.*, vol. 26, no. 2, pp. 313–339, 2013.
[142] P. M. Mukundan, S. Manayankath, C. Srinivasan, and M. Sethumadhavan, "Hash-one: A lightweight cryptographic hash function," *IET Inf. Secur.*, vol. 10, no. 5, pp. 225–231, Sep. 2016.
[143] S. Azad and B. Ray, "A lightweight protocol for RFID authentication," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2019, pp. 2–7.
[144] L. Xiao, H. Xu, F. Zhu, R. Wang, and P. Li, "SKINNY-based RFID lightweight authentication protocol," *Sensors*, vol. 20, no. 5, p. 1366, Mar. 2020.
[145] A. A. Khorasgani, M. Sajadieh, and M. R. Yazdani, "Novel lightweight RFID authentication protocols for inexpensive tags," *J. Inf. Secur. Appl.*, vol. 67, Jun. 2022, Art. no. 103191, doi: 10.1016/j.jisa.2022.103191.
[146] M. Gao and Y. Lu, "A new ultra-lightweight RFID authentication," *J. Supercomput.*, vol. 78, no. 8, pp. 10893–10905, 2022.
[147] G.-H. Wei, Y.-L. Qin, and W. Fu, "An improved security authentication protocol for lightweight RFID based on ECC," *J. Sensors*, vol. 2022, pp. 1–6, Feb. 2022.
[148] I. Syamsuddin, T. Dillon, E. Chang, and S. Han, "A survey of RFID authentication protocols based on hash-chain method," in *Proc. 3rd Int. Conf. Converg. Hybrid Inf. Technol. (ICCIT)*, Nov. 2008, pp. 559–564.
[149] J. Kim, H. Yoon, J. Park, and J. Burm, "A method to improve isolation for RFID applications," in *Proc. 8th Eur. Conf. Wireless Technol.*, 2005, pp. 447–450.
[150] M. Zhonghua and J. Yanfeng, "Carrier extraction cancellation circuit in RFID reader for improving the Tx-to-Rx isolation," *IET Circuits, Devices Syst.*, vol. 13, no. 5, pp. 622–629, Aug. 2019.

[151] J.-J. Q. Samyde and D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smart card," in *Proc. Int. Conf. Res. Smart Cards*. Cham, Switzerland: Springer, 2002, pp. 200–210.
[152] Y.-Y. Chen, J.-C. Lu, S.-I. Chen, and J.-K. Jan, "A low-cost RFID authentication protocol with location privacy protection," in *Proc. IAS*, vol. 2, Aug. 2009, pp. 109–113.
[153] Y. An, Y. Zhang, W. Cao, Z. Tong, and Z. He, "A lightweight and practical anonymous authentication protocol based on bit-self-Test PUF," *Electronics*, vol. 11, no. 5, p. 772, Mar. 2022.
[154] S. Mauw and S. Piramuthu, "A PUF-based authentication protocol to address ticket-switching of RFID-tagged items," in *Proc. Int. Workshop Secur. Trust Manag.*, in Lecture Notes in Computer Science, vol. 7783. Cham, Switzerland: Springer, 2013, pp. 209–224.
[155] M. Kaveh and M. R. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4535–4544, Sep. 2020.
[156] H. Xu, X. Chen, F. Zhu, and P. Li, "A novel security authentication protocol based on physical unclonable function for RFID healthcare systems," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–14, Jul. 2021.
[157] D. Moriyama, I. Matsuo, and M. Yung, "PUF-based RFID authentication secure and private under memory leakage," *IACR Cryptol. ePrint Arch.*, 2013, pp. 61–83, vol. 3.
[158] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID guardian: A battery-powered mobile device for RFID privacy management," in *Proc. Australas. Conf. Inf. Secur. Privacy*, in Lecture Notes in Computer Science, vol. 3574, 2005, pp. 184–194.
[159] A. Juels, P. Syverson, and D. Bailey, "High-power proxies for enhancing RFID privacy and utility," in *Proc. Int. Workshop Privacy Enhancing Technol.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 3856, 2006, pp. 210–226. [Online]. Available: http://link.springer.com/10.1007/11767831_14
[160] T. Dimitriou and M. Ave, "Proxy framework for enhanced RFID security and privacy," in *Proc. 5th IEEE Consum. Commun. Netw. Conf.*, Jan. 2008, pp. 843–847.
[161] M. R. Rieback, G. N. Gaydadjiev, B. Crispo, R. F. Hofman, and A. S. Tanenbaum, "A platform for RFID security and privacy administration," in *Proc. 20th Large Installation Syst. Admin. Conf. (LISA)*, 2006, pp. 89–102.
[162] A. Juels and J. Brainard, "Soft blocking: Flexible blocker tags on the cheap," in *Proc. ACM Workshop Privacy Electron. Soc. (WPES)*, 2004, pp. 1–7.
[163] W. Sun, "Taguard: Exposing the location of active eavesdropper in passive RFID system," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops Affiliated Events (PerCom Workshops)*, Mar. 2021, pp. 360–363.
[164] M. Omer and G. Y. Tian, "Indoor distance estimation for passive UHF RFID tag based on RSSI and RCS," *Meas., J. Int. Meas. Confederation*, vol. 127, pp. 425–430, Oct. 2018, doi: 10.1016/j.measurement.2018.05.116.
[165] T. Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," in *Proc. 1st Int. Conf. Secur. Privacy Emerg. Areas Commun. Netw. (SECURECOMM)*, 2005, pp. 59–66.
[166] S. E. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in Pervasive Computing*. Cham, Switzerland: Springer, Dec. 2013.
[167] D. Molnar and D. Wagner, "Privacy and security in library RFID," in *Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS)*, Jan. 2004, p. 210.
[168] D. Henrici and P. Müller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," in *Proc. IEEE Annu. Conf. Pervasive Comput. Commun. Workshops (PerCom)*, Mar. 2004, pp. 149–153.
[169] V. Dixit, H. K. Verma, and A. K. Singh, "Enhanced hash chain based scheme for security and privacy in RFID systems," *Int. J. Comput. Appl.*, vol. 28, no. 9, pp. 26–30, Aug. 2011.
[170] W. Zhang, Z. Bao, D. Lin, V. Rijmen, B. Yang, and I. Verbauwhede, "RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms," *Sci. China Inf. Sci.*, vol. 58, no. 12, pp. 1–15, Dec. 2015.
[171] T. P. Berger, J. Francq, M. Minier, and G. Thomas, "Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput," *IEEE Trans. Comput.*, vol. 65, no. 7, pp. 2074–2089, Jul. 2016.
[172] A. Biswas, A. Majumdar, S. Nath, A. Dutta, and K. L. Baishnab, "LRBC: A lightweight block cipher design for resource constrained IoT devices," *J. Ambient Intell. Hum. Comput.*, vol. 9, pp. 1–15, Jan. 2020, doi: 10.1007/s12652-020-01694-9.
[173] G. Bansod, N. Pisharoty, and A. Patil, "BORON: An ultra-lightweight and low power encryption design for pervasive computing," *Frontiers Inf. Technol. Electron. Eng.*, vol. 18, no. 3, pp. 317–331, Mar. 2017.
[174] J. Patil, G. Bansod, and K. S. Kant, "LiCi: A new ultra-lightweight block cipher," in *Proc. Int. Conf. Emerg. Trends Innov. ICT (ICEI)*, Feb. 2017, pp. 40–45.
[175] L. Jiao, Y. Hao, and D. Feng, "Stream cipher designs: A review," *Sci. China Inf. Sci.*, vol. 63, no. 3, pp. 1–25, Mar. 2020.
[176] V. A. Ghafari and H. Hu, "Fruit-80: A secure ultra-lightweight stream cipher for constrained environments," *Entropy*, vol. 20, no. 3, p. 180, Mar. 2018.
[177] X. Dai, Y. Huang, L. Chen, T. Lu, and S. Zhao, "SVH : A lightweight stream cipher based on dual pseudo-random transformation and OFB," in *Proc. 4th Int. Conf. Mechatronics, Mater., Chem. Comput. Eng.*, 2015, pp. 2–7.
[178] A. Bogdanov, F. Mendel, F. Regazzoni, V. Rijmen, and E. Tischhauser, "ALE: AES-based lightweight authenticated encryption," in *Proc. Int. Workshop Fast Softw. Encryption*, Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 8424, 2014, pp. 447–466.
[179] X. Fan, K. Mandal, and G. Gong, "*WG-8*: A lightweight stream cipher for resource-constrained smart devices," in *Proc. Int. Conf. Heterogeneous Netw. Quality, Rel., Secur. Robustness*, 2013, pp. 617–632.
[180] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Cham, Switzerland: Springer, 2004, pp. 357–370.
[181] S. Piramuthu, "HB and related lightweight authentication protocols for secure RFID tag/reader authentication," in *Proc. Collaborative Electron. Commerce Technol. Res. (CollECTeR)*, Jun. 2006, pp. 9–10.
[182] P. Dass and H. Om, "A secure authentication scheme for RFID systems," *Proc. Comput. Sci.*, vol. 78, pp. 100–106, Jan. 2016, doi: 10.1016/j.procs.2016.02.017.
[183] M. Girault, L. Juniot, and M. Robshaw, "The feasibility of on-the-tag public key cryptography," in *Proc. Conf. RFID Secur.*, 2007, p. 68.
[184] S. Brands and D. Chaum, "Distance-bounding protocols," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, 1993, pp. 344–359.
[185] K. P. Fishkin and S. Roy, "Enhancing RFID privacy via antenna energy analysis," in *Proc. MIT RFID Privacy Worksho*, Boston, MA, USA, Nov. 2003, pp. 1–3.
[186] K. Rosenfeld, E. Gavas, and R. Karri, "Sensor physical unclonable functions," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2010, pp. 112–117.
[187] U. Guin, D. Dimase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *J. Electron. Test.*, vol. 30, pp. 9–23, Feb. 2014.
[188] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct. 2017.
[189] G. Khadka and S. S. Hwang, "Tag-to-tag interference suppression technique based on time division for RFID," *Sensors*, vol. 17, no. 1, pp. 1–18, 2017.
[190] J. Dofe, J. Frey, and Q. Yu, "Hardware security assurance in emerging IoT applications," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2016, pp. 2050–2053.
[191] *IoT Security Compliance Framework*, IoTSF, Livingston, U.K., 2016.
[192] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward secure privacy protection scheme for low-cost RFID," in *Proc. Symp. Cryptogr. Inf. Secur., Scand. Conf. Inf. Syst.*, 2004, pp. 719–724.
[193] C. Bolan, "The Lazarus effect: Resurrecting killed RFID tags," in *Proc. 4th Austral. Inf. Secur. Manag. Conf.*, 2006, pp. 1–10.
[194] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of Internet of Things," in *Proc. ACM Workshop Security, Privacy Dependability Cyber Vehicles*, Berlin, Germany, Nov. 2013, pp. 61–64.
[195] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of Internet of Things," in *Proc. CyCAR*, 2013, pp. 61–64.
[196] L. Sun, "Security and privacy on low-cost radio frequency identification systems," *Int. J. Secur. Netw.*, vol. 5, nos. 2–3, pp. 128–134, 2010.

[197] H. Damghani, H. Hosseinian, and L. Damghani, "Investigating attacks to improve security and privacy in RFID systems using the security bit method," in *Proc. 5th Conf. Knowl. Based Eng. Innov. (KBEI)*, Feb. 2019, pp. 833–838.
[198] Department of Homeland Security. (Nov. 2016). *Strategic Principles for Securing the IoT (Version 1.0)*. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/IoTfactsheet_11162016.pdf
[199] *Baseline Security Recommendations for IoT*, ENISA, Athens, Greece, Nov. 2017.
[200] R. C.-W. Phan, "Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI," *IEEE Trans. Depend. Sec. Comput.*, vol. 6, no. 4, pp. 316–320, Oct. 2009.
[201] M. Khalid, U. Mujahid, and N.-U.-I. Muhammad, "Ultralightweight RFID authentication protocols for low-cost passive RFID tags," *Secur. Commun. Netw.*, vol. 2019, pp. 1–25, Jul. 2019.
[202] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 38, no. 5, pp. 1–7, May 2014.
[203] G. Gódor and S. Imre, "Elliptic curve cryptography based authentication protocol for low-cost RFID tags," in *Proc. IEEE Int. Conf. RFID-Technol. Appl. (RFID-TA)*, Sep. 2011, pp. 386–393.
[204] E.-K. Ryu, D.-S. Kim, and K.-Y. Yoo, "On elliptic curve based untraceable RFID authentication protocols," in *Proc. 3rd ACM Workshop Inf. Hiding Multimedia Secur.*, Jun. 2015, pp. 147–153.
[205] 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. Hum. Comput.*, vol. 4, pp. 1–18, May 2017.
[206] X. Fan, N. Zidaric, M. Aagaard, and G. Gong, "Efficient hardware implementation of the stream cipher WG-16 with composite field arithmetic," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2013, pp. 21–33.
[207] N. Zidaric, M. Aagaard, and G. Gong, "Hardware optimizations and analysis for the WG-16 cipher with tower field arithmetic," *IEEE Trans. Comput.*, vol. 68, no. 1, pp. 67–82, Jan. 2019.
[208] X. Fan, K. Mandal, and G. Gong, "WG-8: A lightweight stream cipher for resource-constrained smart devices," in *Proc. Int. Conf. Heterogeneous Netw. Quality, Rel., Secur. Robustness*, 2013, pp. 1–16.
[209] M. U. Bokhari, S. Alam, and F. Syeed Masoodi, "Cryptanalysis techniques for stream cipher: A survey," *Int. J. Comput. Appl.*, vol. 60, no. 9, pp. 29–33, Dec. 2012.

HEZAM AKRAM ABDULGHANI received the M.S. degree in software engineering from KFUPM University (KSA) and the M.Sc. degree in software engineering from Geneva University, Switzerland, in 2019. His research interests include the Internet of Things (IoT), security and privacy by design for IoT, cyber security, and use and misuse models, and more importantly, security and privacy guidelines for IoT. In addition to his educational background and having published many articles in peer-reviewed journals, he has more than four years of experience in teaching and more specifically in software engineering.

NIELS ALEXANDER NIJDAM received the Ph.D. degree in computer science from the MIRALaboratory, University of Geneva. His research topics included collaborative systems, distributed networking, remote simulations and rendering, and programmable graphics with the University of Geneva. He is currently a Computer Scientist and a Senior Researcher and is leading the Information Security Group (I-Sec Laboratory). Beyond that, he has been active in the medical domain (MRI imaging), avatar systems, cyber security, the Internet of Things, and more recently on autonomous shuttles and smart cities (with a focus on cyber security and privacy).

DIMITRI KONSTANTAS is currently a Professor at the Geneva School of Economics and Management (GSEM), University of Geneva (CH), and the Director of the Information Science Institute (ISI) and a member of the Information Service Science Institute, University Center of Computer Science (CUI), having served for seven years as the Vice Dean of the Faculty of Social and Economic Sciences, CH. He has been active, since 1987, in research in the areas of object oriented systems, e-commerce services, information security, mobile services, e-health and m-health services of elderly, and recently in shared mobility solutions. He has more than 150 publications in international conferences, journals, books, and book chapters, a long participation and leadership in numerous European projects, many nominations as a consultant and a scientific expert for several international companies and governments, and has launched three start-ups and acted as coach to numerous university start-ups. Since May 2018, he has been coordinating the H2020 European Project AVENUE, which targets in the validation of autonomous vehicles for public transportation.