A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities

Koen Tange, *Graduate Student Member, IEEE*, Michele De Donno, *Student Member, IEEE*, Xenofon Fafoutis, *Senior Member, IEEE*, and Nicola Dragoni

***Abstract*—A key application of the Internet of Things (IoT) paradigm lies within industrial contexts. Indeed, the emerging Industrial Internet of Things (IIoT), commonly referred to as Industry 4.0, promises to revolutionize production and manufacturing through the use of large numbers of networked embedded sensing devices, and the combination of emerging computing technologies, such as Fog/Cloud Computing and Artificial Intelligence. The IIoT is characterized by an increased degree of inter-connectivity, which not only creates opportunities for the industries that adopt it, but also for cyber-criminals. Indeed, IoT security currently represents one of the major obstacles that prevent the widespread adoption of IIoT technology. Unsurprisingly, such concerns led to an exponential growth of published research over the last few years. To get an overview of the field, we deem it important to systematically survey the academic literature so far, and distill from it various security requirements as well as their popularity. This paper consists of two contributions: our primary contribution is a systematic review of the literature over the period 2011-2019 on IIoT Security, focusing in particular on the security requirements of the IIoT. Our secondary contribution is a reflection on how the relatively new paradigm of Fog computing can be leveraged to address these requirements, and thus improve the security of the IIoT.**

***Index Terms*—Industrial Internet of Things, cyber-security, security requirements, fog computing.**

Acronyms

3GPP	The 3rd Generation Partnership Project
5G	Fifth generation cellular network technology
ABS	Attribute Based Signatures
AC	Access Control
ACL	Access Control List
BYOK	Bring Your Own Key
CIA	Confidentiality, Integrity, Availability
CI	Critical Infrastructure
DDoS	Distributed Denial of Service
DHT	Distributed Hash Table
DID	Decentralized Identifier
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation
ICS	Industrial Internet Consortium
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
LLN	Low-power Lossy network
LPWAN	Low Power Wide Area Network
M2M	Machine-to-Machine
MQTT	Message Queue Telemetry Transport
NB-IoT	Narrow Band IoT
NFC	Near Field Communication
NFV	Network Function Virtualization
OPC UA	The OPC Unified Architecture
OT	Operational Technology
OWASP	Open Web Application Security Project
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PUF	Physically Uncloneable Function
SCADA	Supervisory Control And Data Acquisition
SDN	Software Defined Networking
SSI	Self Sovereign Identity
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSN	Time Sensitive Networking
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Networks
ZTN	Zero Trust Networking.

I. Introduction

INDUSTRY 4.0, also referred to as 4^{th} industrial revolution, represents a new industrial era, whereby due to the

Manuscript received July 5, 2019; revised June 5, 2020; accepted July 13, 2020. Date of publication July 22, 2020; date of current version November 20, 2020. This work was supported in part by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant under Agreement 764785, FORA–Fog Computing for Robotics and Industrial Automation; and in part by the Poul V. Andersen Fund. *(Corresponding author: Nicola Dragoni.)*

Koen Tange, Michele De Donno, and Xenofon Fafoutis are with the Embedded Systems Engineering section, DTU Compute, Technical University of Denmark, 2800 Lyngby, Denmark (e-mail: kpta@dtu.dk; mido@dtu.dk; xefa@dtu.dk).

Nicola Dragoni is with the Embedded Systems Engineering section, DTU Compute, Technical University of Denmark, 2800 Lyngby, Denmark, and also with the Center for Applied Autonomous Sensor Systems, Örebro University, 702 81 Örebro, Sweden (e-mail: ndra@dtu.dk).

Digital Object Identifier 10.1109/COMST.2020.3011208

TABLE I
"INDICATIVE DIFFERENCES IN TERMS OF SELECTED ASPECTS BETWEEN IOT AND IIOT" (TAKEN FROM [9])

Selected Characteristics	**Internet of Things**	**Industrial Internet of Things**
Focus	Protection of personal data and assets	Prevention of process interruption, safety
Priorities	Confidentiality, Integrity, Availability	Availability, Integrity, Confidentiality
Device Failure Implications	No critical consequences	Interruption of processes, impact on production, potential physical threats
Reaction to threat	Possible shut down and remediation	Maintenance of operation
Upgrades and Patch Management	Possible during operation time, no reasons for significant delays	Need to be scheduled and performed during down time, which may postpone the upgrade for a considerable amount of time.
Lifecycle of the device	Relatively frequent upgrades of equipment	Long lifespan of the devices (over 15 years)
Conditions of deployment	Regular environment	Harsh environment (temperature, vibration, etc)

increasing availability, affordability, and capability of sensors, processors, and communication technologies, the number of embedded devices used in industrial applications is rapidly increasing. This leads to a growth in the interest for the IIoT: a large network of devices, systems, and applications communicating and sharing intelligence with each other, the external environment, and with humans [1]. According to Accenture [1], the IIoT could be worth 7.1 trillion U.S. dollars to the United States and more than 1.2 trillion to Europe by 2030.

In this wave of excitement, IoT security represents one of the biggest weak points holding back the adoption of the IIoT. As a matter of fact, IoT devices are often poorly secured [2] and thus easy targets for malware taking advantage of them to run devastating cyber-attacks, such as Distributed Denial of Service (DDoS) [3] (e.g., Mirai [4] affected consumer IoT) or sabotage attacks. Threats are not limited to the consumer IoT. In fact, traditional industrial environments have been subject to attacks in the past, sometimes with devastating results (e.g., StuxNet [5] or CrashOverride/Industroyer [6]). It is thus apparent that without security, IIoT will never be able to deliver its full potential. As a result, recent years have seen an unprecedented growth of research in IIoT security.

In this landscape, a relatively new computing paradigm has attracted attention: Fog computing [7]. Fog computing is a system-level architecture born from the necessity of bridging the gap between IoT and Cloud computing, by distributing resources and services along the continuum from Cloud to IoT [8]. Among others, one of the promises of Fog computing is to present a possible solution to the (I)IoT security problem.

A. Contribution

In this article, we present a systematic survey on the security requirements of the IIoT. As we quantitatively demonstrate in Section VI, the field of IIoT security has grown rapidly over the last few years, and this momentum motivates this article and the need for an up-to-date systematic survey.

In particular, as our primary contribution, we survey the literature on IIoT security over the period 2011-2019, which corresponds to more than 200 papers. In turn, we identify, categorize, and discuss the IIoT security requirements that have been identified by the research community, highlighting the research interest attracted by each of them over the target period. In addition, we provide statistics with regard to the geographical distribution and the publication venue of the surveyed papers.

As a secondary contribution, in the final part of the article, we discuss how the Fog computing paradigm can be used to address these requirements. Our reflection identifies numerous research opportunities at the intersection of Fog computing and IIoT security, along with open challenges and limitations still (partially) unsolved.

B. Outline

The paper is organized as follows. We first establish common ground by discussing the difference between IoT and IIoT, and providing a glimpse into recent IoT security surveys. Section III briefly mentions related work and motivates the need for a systematic literature review. Section IV describes the research method used in the review and formalizes the research questions. Section V surveys the security requirements resulting from the systematic review. Section VI presents a quantitative analysis of the results obtained during the research phase. Section VII discusses the role that Fog computing might play in meeting the IIoT security requirements. Finally, Section VIII concludes the paper.

II. IOT AND IIOT

Before we discuss the results of our systematic survey in depth, it is helpful to establish a common understanding of how IoT and IIoT differ. In this section, we first explore this difference, then, we provide an overview of recent IoT security surveys.

We find Table I, taken from the ENISA "Good practices for Security of Internet of Things in the context of Smart Manufacturing" [9] report, to be helpful in outlining the differences between IoT and IIoT, and use this as a guideline throughout our work. That said, the difference is not a precise, clear-cut one, and we sometimes do deviate from these guidelines, when it is abundantly clear that a scenario concerns the IIoT without meeting relevant criteria from that table.

In general, it is accepted that IIoT is a subset of IoT: IoT typically covers consumer devices in retail and lifestyle, IIoT focuses mainly on Operational Technology (OT), the smart manufacturing process, smart logistics, and smart cities.

It should not be surprising that the safety and security requirements in IIoT are generally stricter than those found in a typical IoT scenario. Even so, we find significant overlap in used terminology in the literature, and IIoT having stricter requirements does not necessarily mean that any proposed security solution for the IoT is not applicable to the IIoT. This is echoed by Yu and Guo [10], who, in a short survey on the differences between IIoT and IoT security, find that for the most part, the challenges overlap. At the same time, as will become evident throughout this study, the field is broad, and scenarios covered in the literature differ wildly. Often, one can imagine a more general IoT cousin to a specific IIoT scenario quite easily. The security requirements distilled from said IIoT scenario would thus often also apply to its IoT cousin. Vice-versa, it is likely that works are covering the IoT scenario, these would identify requirements that have not been covered in the available literature for the IIoT. This is especially true for requirements derived out of common challenges such as resource constraints and key distribution. Therefore, we recommend readers with an interest in any given IIoT scenario to also search the available literature for the more general IoT case, and consider if the requirements found in those works uncover security liabilities that have not been addressed in existing IIoT work.

A. IoT Security Surveys

There exist ample surveys investigating the state of IoT security, and we will briefly look at several relatively recent surveys, discussing how their identified security requirements might relate to the IIoT.

In [11], the authors survey the literature for real IoT attacks and present a taxonomy. They also identify integrity, anonymity, confidentiality, privacy, access control and authorization, authentication, resilience, and self-organization as security requirements for IoT systems in general. These are all represented in the requirements collected in this work as well, and reiterate that generic IoT solutions can work for IIoT systems, if they do not violate scenario-specific constraints. Neshenko *et al.* [12] provide a much more thorough study of IoT vulnerabilities and attacks, but do not relate these to security requirements. Nevertheless, we can see that the familiar topics of authentication and access control, assurance, and confidentiality return implicitly throughout the text. The threats described by the authors include problems such as false data injection, improper patch management, and improper encryption. Many of these can be directly connected to the security requirements listed in this work.

In [13], the authors provide a top-down survey of IoT security. They discuss security requirements for healthcare, smart grids, manufacturing, smart homes, transport, and smart cities. Some of these are also considered to be in the IIoT domain [9], and indeed the security requirements identified in these sections overlap with the ones collected in this survey, albeit on a higher level of abstraction. In each investigated domain, they list a subset of these as requirements. For smart grids, they identify availability, confidentiality, integrity, non-repudiation, and privacy, and additionally list challenges we also identify in our work: heterogeneity, scalability, privacy, and so on. What is apparent through their work, is that the main way in which the requirements for the various domains differ is in their priority, for instance, privacy and confidentiality weigh higher in healthcare than in transport. Further, the authors make the insightful observation that one specific challenge for the IIoT that is not as apparent in general IoT networks, is that its crucial safety requirements often compete with security in terms of resources. It is perhaps the balance that must be found between these two aspects that sets the IIoT apart from normal IoT systems. Indeed, whenever resource constraints are not an issue, or when safety constraints are less strict, standard IoT solutions often suffice.

III. Related Work

To the best of our knowledge, the most recent works focused on reviewing IIoT security are [14] and [15]. The former focuses primarily on threats characterization by looking at existing attacks, while the latter mainly reviews the differences between information technology and operational technology in an Industry 4.0 setting, and discusses the challenges. However, neither of these works explicitly discuss security requirements, opting to leave them as implied by the described threats and challenges. Another recent study [16] focuses on Industry 4.0 system architecture as a whole and observes that there is an increase in security-focused architectural proposals, but does not discuss security in depth. Some older surveys dated back to 2015 and 2016 mention IIoT security requirements [17], [18], but they also refrain from an in-depth discussion.

Recently, Hansch *et al.* [19] published a study identifying and mapping security requirements to an OPC UA model, allowing easier machine-based verification. While they provide many security requirements, they are based on a limited set of use cases, and no thorough explanation for their derivation is given. Moreover, they are of a less abstract level than the ones we attempt to derive in this work.

As a result, we deem it necessary to provide an up-to-date, systematic survey that specifically addresses IIoT security requirements.

IV. Research Method

In this section, we present the research method that is used in this systematic literature review on security requirements for the IIoT.

We adopt the research method detailed by Petersen *et al.* [20] and utilize the suggested template for describing our approach. In the next subsections, we elaborate on research questions, search strategy, study selection, and validity concerns.

A. Research Questions

The main aim of this work is to identify security requirements for the IIoT. This can then guide us in identifying which of these show potential to be solved by Fog computing. In addition, we want to provide an overview of the research activity in the field: how research activity has developed throughout the years, how this research was published, and what its geographical distribution is.

Thus, our research questions can be formulated as follows:

- **RQ1:** what are the security requirements of the IIoT?
- **RQ2:** how are publications related to IIoT security spread throughout the years?

TABLE II
QUERIES USED FOR OUR SEARCH, EXPRESSED IN PSEUDO-CODE

Query	Description
Q1	*in title:* IIoT OR “Industrial Internet of Things" OR "Industry 4.0"
Q2	(*in title:* IIoT OR “Industrial Internet of Things" OR "Industry 4.0") AND *in abstract:* security

TABLE III
NUMBER OF PAPERS OBTAINED

Source	Q1	Q2
ACM	60	12
IEEE Xplore	2702	323
ScienceDirect	369	21
Total	*3158*	*356*

- **RQ3:** how is IIoT security research activity geographically distributed?
- **RQ4:** what are the most popular publication venues for IIoT security research?

Answering these questions will aid in getting a better understanding of the current security landscape for the IIoT, while at the same time identifying various concrete research opportunities related to Fog computing. Each of these can then be traced back to concrete security requirements relevant to the Industry 4.0 paradigm.

B. Search Strategy

We utilize the adjusted PICOC criteria for software engineering [21] in order to identify relevant keywords. In particular:

- **Population:** we consider the IIoT as the application area in which our research is conducted. However, this is a very broad population, therefore, we take into account only studies addressing IIoT security.
- **Intervention:** this criterion does not apply to our research questions, as we are interested in *any* work in the IIoT domain that describes security requirements.
- **Comparison:** we compare the security requirements identified by different studies by taking into account such factors as the number of studies that mention them, related threats, and proposed solutions.
- **Outcomes:** we present the identified security requirements as well as the properties of their mitigation, allowing us to discuss which requirements call for further research.
- **Context:** as we do not empirically compare the available works, this criterion does not apply to our study.

With these criteria in mind, we have formulated the following keywords: *IIoT, Industrial Internet of Things, Industry 4.0,* and *Security*.

We considered as sources the following databases: ACM Digital Library, IEEE Xplore, Elsevier/ScienceDirect. In this domain, we believe that the combination of these three sources provides an accurate representation of the research that has been conducted globally.

We divided the search into two stages. First, we queried the databases for articles related to IIoT/Industry 4.0 in general, based on their titles. This provided an overview of the amount of research conducted in this field. After that, we narrowed down our search to only include works related to security, by excluding articles not containing the word “security” in their abstract. The queries are summarized in Table II. The search results for both queries are listed in Table III. The queries have been executed in March 2020.

C. Study Selection

Starting from 356 papers resulting from our queries, we further filtered the studies with multiple phases.

Firstly, the JabRef[1] reference management software was used to identify and delete duplicates. Five duplicates were found, leaving the number of considered papers for the subsequent phases at 351.

Subsequently, we independently reviewed the titles and abstracts of each article in order to reduce selection bias. Each article was marked as being relevant, not relevant, or of doubtful relevance. Articles were voted for inclusion when the work covered cyber-security challenges and/or solutions for Industry 4.0, and it was published before 2020, since that is the year in which this study is conducted. We do not believe that filtering on a minimum publication date is necessary at this time, due to the relatively young age of this field. Articles were voted for exclusion when the work was not related to Industry 4.0 security, contained duplicate content, or was not presented in legible English.

The following rules were used for filtering out articles based on title and abstract review (this has been done jointly by two authors of the paper):

- when both authors considered an article relevant, the article was included for the next phase;
- when one author expressed doubt and the other author considered an article relevant, the article was included for the next phase;
- when both authors expressed doubt, a joint review was done considering also other sections of the article (e.g., introduction, outline, conclusion) to determine its relevance. If this review did not clear up doubts for either of the authors, the article was given the benefit of the doubt and included for the next phase;
- when one author considered an article relevant, while the other considered it to not be relevant, the article was marked for joint review as described in the previous rule;
- when one author considered an article not relevant, while the other considered it to be doubtful, the article was marked for joint review as with the previous rules;
- when both authors considered an article not relevant, the article was excluded.

[1] https://www.jabref.org

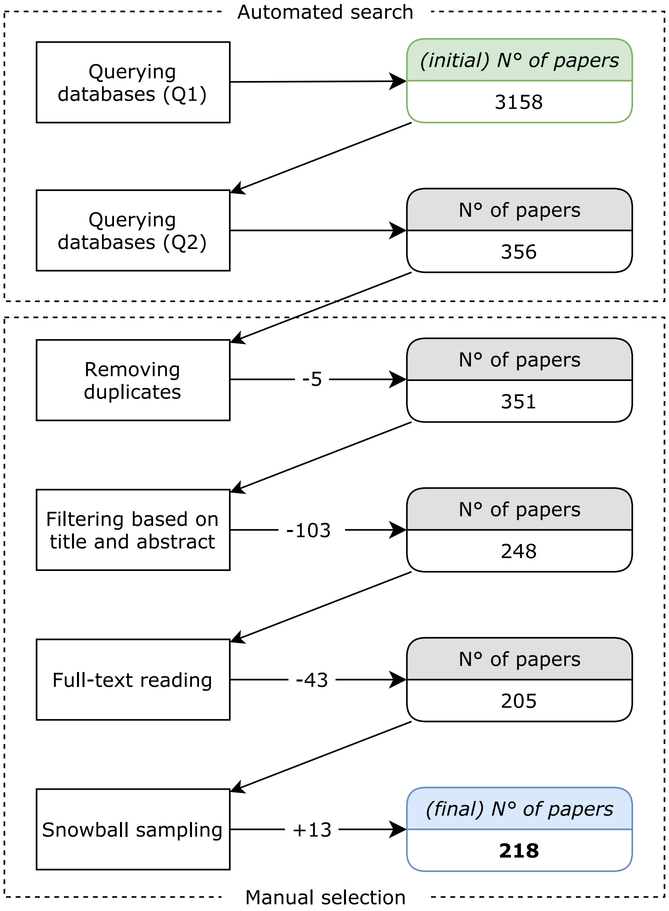

Fig. 1. A schematic representation of the entire study selection process.

After the individual title and abstract reviews, 68 articles were excluded and 69 were marked as doubtful entries requiring a joint review. These were then jointly reviewed, leading to an additional 35 exclusions. The remaining 248 papers were considered for full-text reading, overall reducing the number of papers to analyse by 92% compared to results of Q1 and 30% compared to Q2.

In the full-reading phase, we extracted information relevant to the stated research questions, as well as identifying the challenges discussed in the papers. We then used this data to provide a comprehensive picture of the security challenges and corresponding requirements for the IIoT. In this phase, it became clear that a number of papers were not relevant to our work, resulting in the discarding of other 43 papers. Additionally, we identified 13 papers of interest through reverse snowball sampling and added these to the selection. This brings the final number of papers considered in this survey to 218.

The entire study selection process and related numbers are summarized in Figure 1.

D. Validity Evaluation

Every study that is subject to manual selection is vulnerable to researcher bias in the filtering process. In order to reduce this issue, we performed the filtering process twice: two authors of this paper selected studies independently, and the results of the filtering process were based on a systematic approach combining the selections of both authors, and in some cases a joint review.

Also, to mitigate possible selection bias, we have performed reverse snowball sampling, allowing for the introduction of papers originally not considered due to not being captured by our search queries.

Furthermore, we have described our research process in detail, and have taken care to list the criteria by which we filtered studies. This is done to increase the repeatability of this work.

Finally, it is worth mentioning that our approach does not suffer from the Matthew's effect, as opposed to querying databases that rank papers based on citation count [22].

V. IIoT Security Requirements (RQ1)

In this section, we present the security requirements that we found to have been discussed in the selected literature. We describe why these requirements are deemed relevant and summarize some of the proposed solutions. We also discuss why these requirements are difficult to satisfy for Industry 4.0 applications, which gives the insight needed to see why the discussed security requirements are hard to meet with conventional solutions. Furthermore, they provide a set of motivational factors for why the research discussed in this section is necessary.

We observed that the focus of the investigated literature is mainly on Industry 4.0, even if in this field highly varying scenarios are considered. For example, some articles discuss petrochemical plant management [246], while others focus on drones [177], [192], [199], and so on. Each of these scenarios has its own threat model and will thus also differ in terms of security requirements from the others, to a certain degree. However, we note that the majority of them show considerable overlap, and that even the ones that are unique to one particular scenario, might still translate into a research opportunity, or might be possibly addressed with Fog computing. Therefore, we have attempted to include all such requirements in this section, and mention their relevance to particular scenarios, to provide context.

In the rest of this section, we discuss all IIoT security requirements found in this study, grouped by the overarching categories to which they belong. Figure 2[2] depicts a hierarchical structure of the various subsections, together with all the works related to each subsection. References were picked and positioned using the following heuristics: firstly, if a work is mentioned in a subsection (be it in a table or the text itself), it is included in the level 1 node representing that subsection (e.g., Authentication); secondly, if a work is mentioned in a topic *within* a subsection (e.g., Key Distribution), it is included in the level 2 node representing that subsubsection in the mind-map. Additionally, in order to minimize redundancy in the mind-map, the following rule was followed: when a reference is included for both a subsection (e.g., Network Security) and

[2] In electronic versions of this work, nodes and references in this map are clickable, allowing for easier navigation through the document.

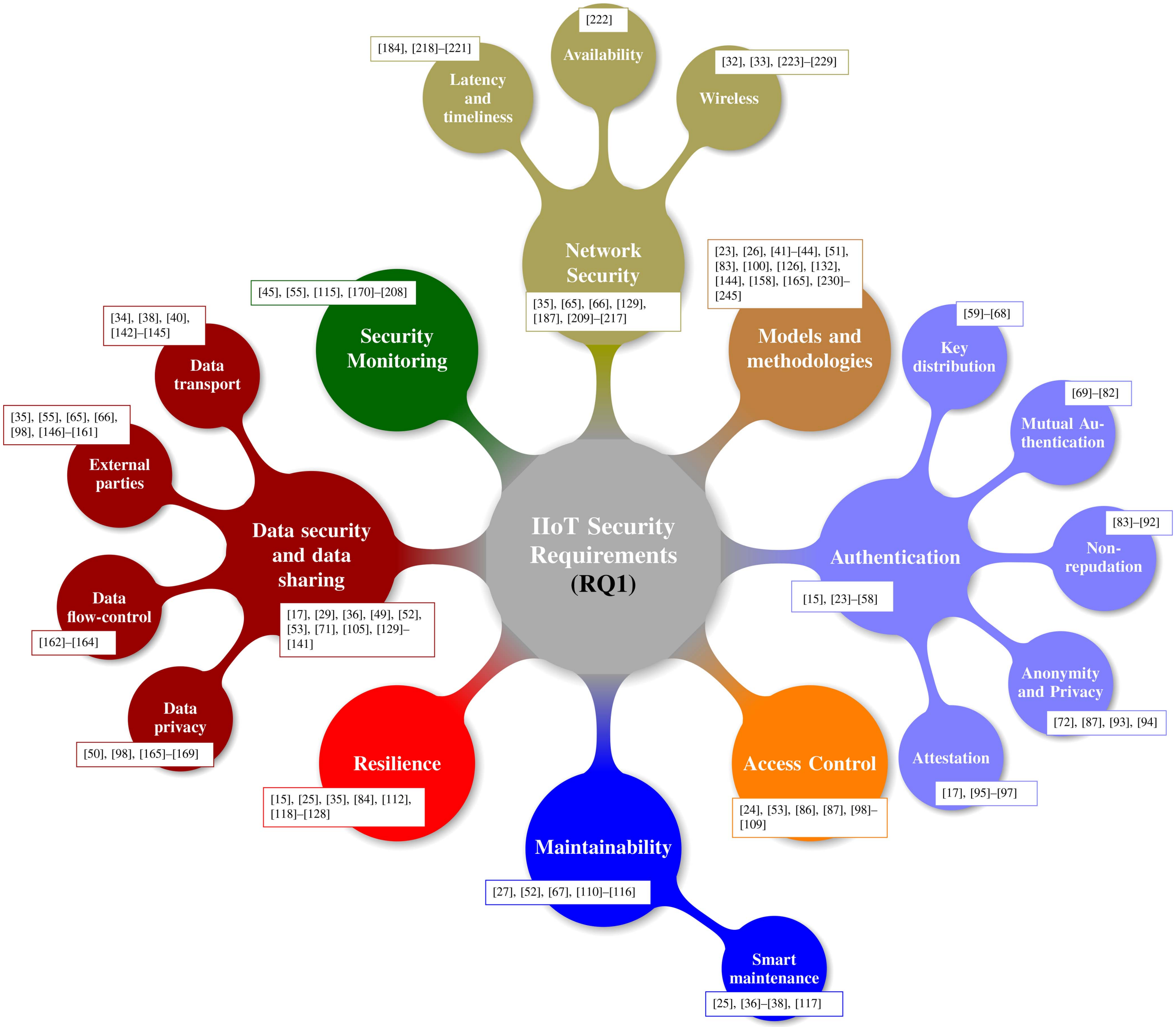

Fig. 2. A clickable mind-map giving an overview of the categories (subsections) and specific topics (subsubsections) discussed in Section V. References in this mind-map were chosen for inclusion when explicitly mentioned in the portion of text represented by each node, or when deemed relevant to the category, based on a full-text review.

one or more of its subsubsections (e.g., Wireless), then preference is given to the latter, and the reference is removed from the subsection itself. This does *not* eliminate redundancy between nodes of the same level (e.g., a reference can still be included for both Key Distribution and Mutual Authentication), but it does allow for a representative overview of works relevant to any topic.

Finally, in Section V-J, we close this section with a summary and an analysis of the obtained results.

Except for Section V-A and Section V-J, every section contains a table relating the most important security requirements of that category to a collection of works that we deemed the most relevant to these topics. Additionally, every table shows the research interest (low, medium, high, very high) of the scientific community for each security requirement in that category. This interest is inferred from the percentage of works identifying or addressing the specific security requirement compared to all the (unique) papers related to that category. The number of papers addressing a specific category is taken from Figure 2 as the number of papers appearing in the corresponding level 1 (i.e., subsection) and all level 2 (i.e., subsubsections) nodes, but removing duplicates. For instance, the total number of papers discussing Network Security is given by the count of the references appearing in Figure 2 for the nodes Network Security, Latency and timeliness, Availability, and Wireless, without duplicates. It is important to note that a number of works identify multiple security requirements, thus, appear in multiple subsections; as such, the calculated percentages do not represent disjoint partitions of the set of investigated works, thus their sum will not result in 100%. The range of percentages assigned to each interest level are shown in Table IV and have been chosen based on the distribution of

TABLE IV
INTEREST LEVELS ASSIGNED TO EACH SECURITY REQUIREMENT IN RELATION TO ITS CATEGORY

Relative interest	Range (x)
Low	0% ≤ x ≤ 7%
Medium	7% < x ≤25%
High	25% < x ≤45%
Very High	45% < x ≤100%

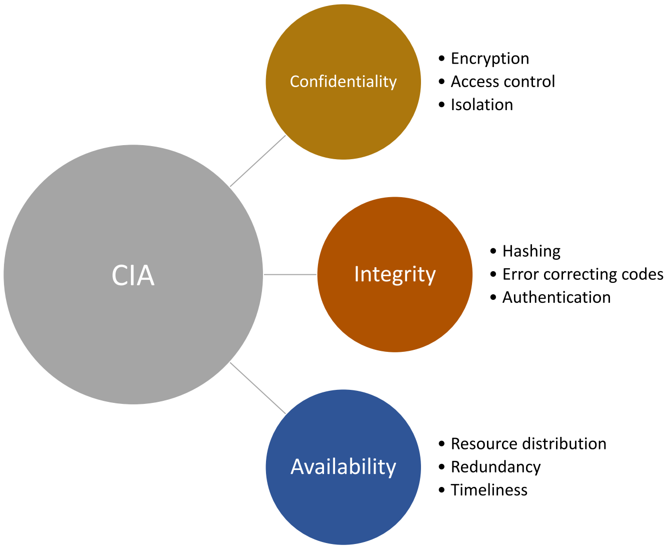

Fig. 3. The CIA triad, with some examples for each property.

percentages assigned to security requirements across all categories. As an example of the interest level, consider a category AB discussed by 50 papers, and a security requirement AB-01 identified by 5 of these 50 papers, the research interest for the requirement AB-01 will be *medium*, with a percentage of 10%.

The aim of these tables is to give the interested reader a stepping stone to more in-depth works for each requirement, but also the topics itself.

A. The CIA Triad

The Confidentiality, Integrity, Availability (CIA) triad is a well-known information security model, and can be considered as a set of extremely abstract security goals or requirements. A subset of these lie at the root of every other security requirement. Figure 3 provides a graphical representation of the triad and shows some examples of solutions related to each property. We briefly describe the three properties as they are described by [130] below:

- **Confidentiality** pertains to protecting information in all its forms. This includes data encryption, access control, network isolation, but also privacy aspects.
- **Integrity** concerns consistency, accuracy, authenticity, and more generally the overall trustworthiness of entities.
- **Availability** concerns operational guarantees of the system. This covers topics such as redundancy and decentralization, but also guarantees that tasks will be performed within hard deadlines.

Typically, the CIA triad is used in information security, meaning that the three properties relate to information only. However, it is equally applicable in other domains, such as cyber-physical systems [132]. Indeed, many of the works we investigated explicitly mention the triad (e.g., [25], [63], [89], [97]). Traditionally the focus in industrial environments has been first on availability, second on integrity, and last on confidentiality. However, with Internet-connected systems, this requires reconsideration, and all three aspects should be brought up to an acceptable level. Thus, with the development of new IIoT and Industry 4.0 solutions, confidentiality and integrity should be weighed equally to availability.

While these three aspects are a very good starting point and are certainly important to keep in mind when specifying the security goals for any system, it is not always useful to reduce concrete requirements back to elements of the CIA triad, if one already has more (e.g., contextual) information that might help with deriving an unambiguous security goal. For example, it is easy to state that data at rest should be kept confidential, but such a requirement does not convey the conditions that a confidentiality mechanism should satisfy. Moreover, it leaves a lot of room for interpretation (e.g.,, confidential to which parties?). On the other end of the spectrum, very fine-grained requirements are only possible if one is developing for a specific scenario.

In the next subsections, we strive to find a middle ground where we describe security requirements at a high enough level to see where the challenges in achieving them lie, but at the same time refrain from going too deep into any scenario, although we might refer to them as anecdotal evidence supporting the legitimacy of a requirement.

B. Authentication

Authentication of remote entities (both humans and machines, or even applications) is a key concern for many forms of IoT communication [31]. Within the context provided by IoT and IIoT applications, this brings some extra challenges [15], [17], [49]. There is a need for extremely lightweight authentication schemes, with little overhead in terms of computation time and transfer size, among other things.

A second but very important concern is verifying the integrity and authenticity of data, e.g., to ensure that a configuration file was created by an authorized party, and not modified since. Also here, the IIoT domain has special requirements that prevent the adoption of commonly used authentication mechanisms. Many topics in this section therefore also concern integrity, albeit not explicitly mentioned in every instance.

Wang and Wang [82] name some other typical challenges (mainly aimed at wireless industrial communication) that need to be taken into account when investigating authentication and integrity methods. They consider extreme resource constraints, the open broadcast nature of wireless communications (i.e., anyone can read and send messages on certain frequencies), extremely large network sizes, and lack of infrastructure support.

As an example of authentication challenges in existing systems, we consider the Message Queue Telemetry Transport (MQTT) protocol. This is a widely deployed protocol for data

TABLE V
AUTHENTICATION-RELATED SECURITY REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
A-01	multi-factor authentication	[24], [26], [72], [73], [77], [78], [82]	Medium	9%
A-02	key distribution	[29], [53], [55], [59]–[63], [67], [85]	Medium	13%
A-03	node addition, revocation, rekeying	[29], [30], [63], [67], [82]	Low	6%
A-04	decentralized key management	[24], [53], [55], [62], [67]	Low	6%
A-05	transitive authentication	[62]	Low	1%
A-06	mutual authentication	[28], [48], [52], [70]–[74], [76]–[78], [81], [87]	Medium	17%
A-07	privacy-preserving authentication	[72], [77], [78], [87], [93], [94]	Medium	8%
A-08	minimization of user interaction	[70]–[72], [76]–[80]	Medium	10%
A-09	non-repudiation	[84], [86], [89]	Low	4%
A-10	attestation	[17], [39], [95], [97]	Low	5%

exchange in the industrial domain, and features some very basic and insecure authentication methods [57]. According to Katsikeas *et al.* [34], the protocol allows authentication through a simple username and password combination, which are communicated in plaintext. A second authentication method sometimes used is through a unique client identifier, which is easily spoofable. While it is possible to secure these methods by complementing MQTT with Transport Layer Security (TLS) or IPSec, those two protocols are too resource-intensive for many IIoT applications, and lighter alternatives are necessary, such as TinyTLS [56] or DTLS [58]. Now that industrial networks are becoming increasingly connected to the Internet, this becomes more and more important.

The importance of sufficiently secure authentication mechanisms is reflected by the fact that positions 2 and 3 in the Open Web Application Security Project (OWASP) IoT Top 10 [47] on IoT vulnerabilities concern attack vectors where (a lack of) authentication is an important aspect. Its importance is also underlined by the popularity of this topic with recent research efforts, with many papers addressing or identifying the above issues (see Table V). These works identify several authenticity properties that can be considered requirements in various use-cases in the IIoT domain. We describe these in more detail in the following subsections.

For a comprehensive survey on IoT authentication algorithms, we refer the interested reader to Ferrag *et al.* [31]. The authors cover many authentication algorithms and compare them based on computational efficiency, threat protection, and more. Kail *et al.* [33] provide another survey covering multiple industrial protocols aimed specifically at Low Power Wide Area Network (LPWAN) technologies.

Next, we discuss a number of authentication-related topics in the following subsections. First, we look at key distribution, after which we discuss mutual authentication and multi-factor authentication. Then, we address non-repudiation as a requirement, followed by anonymous authentication and privacy preservation in authentication algorithms. As a final topic, we discuss attestation techniques through trusted hardware.

1) Key Distribution: Key distribution is a challenging requirement for many applications in the IoT [68], and naturally extends to the IIoT. With devices being set up and used in hostile environments, possibly being very mobile, dynamically joining and leaving networks, and possibly being very constrained in resources, there is a pressing need for efficient, flexible, and dynamic key management mechanisms. Airehrour *et al.* [59] argue that traditional Public Key Infrastructure (PKI) is outdated, stating that "it was at no time designed to handle the complications of managing industrial-scale networks of 50 billion devices that IoT promises to usher in.". This raises the question of whether all IoT devices should exist in the same authentication domain, and if centralized authentication authorities such as PKIs are even a sensible choice for that many devices. We will not attempt to answer these questions here.

In order to deal with dynamic environments, some naturally implied requirements for key management solutions are that they can handle node addition, revocation, as well as rekeying [63]. Resource-constrained devices will have issues with key generation, computationally intensive algorithms, and transmission of large/many messages. Moreover, in an industrial setting, device owners might not trust the manufacturer to generate keys for them, and will want to do this themselves [67]. Availability can be an issue as well. In Critical Infrastructure (CI) environments, an authentication authority has to be reachable at all times. Because of this, Blanch-Torne *et al.* [62] state that it is not sufficient to rely on one central authority for authentication. Additionally, they also identify transitive authentication (if A knows B and B knows C, B can introduce A to C) as a requirement in some scenarios.

In [63], the authors propose a key management solution that aims for little transmission overhead by requiring only one transmitted message for one-way-authentication. While this makes for an energy-efficient protocol, it appears to not be very scalable or dynamic, since all nodes need to be known beforehand, and addition, revocation and rekeying are not thoroughly discussed.

Ulz *et al.* [67] propose a Bring Your Own Key (BYOK) approach, to address the trust issue between device owners and manufacturers. However, it does require devices to have Near Field Communication (NFC) capabilities, and key distribution requires a human to physically move between a central server and the device.

Another approach is suggested by [62], where there is no centralized authority, but a Distributed Hash Table (DHT) that takes care of identity propagation and lookups. Their solution is a distributed one, and also provides transitive authentication. It is scalable and dynamic, but the protocol is not designed with energy-efficiency in mind, and can require a considerable number of messages at times.

While the above-mentioned sources address the identified requirements to some extent, none of them addresses multiple at once. Clearly, there is still plenty of opportunity for novel research in this area. One potential solution to several key distribution challenges that might become viable in the future, is quantum key distribution [65], [66]. In such a system, it is impossible to eavesdrop on a transmission without altering its payload, meaning that any eavesdropping attempt can be detected.

Blockchain technologies are another promising candidate, showing potential to overcome several key challenges. Bartolomeu *et al.* [61] discuss Self Sovereign Identity (SSI) techniques for IIoT, which build on top of blockchains to provide Decentralized Identifiers (DIDs). These systems have as a property that all entities carry their own identification data, eliminating the need for a centralized root of trust. They discuss the challenges faced by several frameworks capable of providing DIDs, some of the most prevalent being the need for a common data model for interaction between parties, and a lack of research in their application to Machine-to-Machine (M2M) authentication. A different approach is taken in [60], where the blockchain-based BCTrust protocol is extended with key management functionality. One challenge with blockchain is that due to the immutability of blockchains, revocation or alteration of data is impossible. The standard solution is to add append modifications at the end of the chain, but there exist some early results showing that small scale changes are possible using Chameleon hashing schemes. This comes at the cost of some security [64], but further research is needed.

2) Mutual Authentication: In [82], mutual authentication is identified as one of the requirements for any practical authentication scheme, and Kolluru *et al.* [76] state that mutual authentication between any two IoT devices is necessary, as many of them are exposed to external environments. Moreover, because of this many-to-many requirement, a user/password system is neither user-friendly nor flexible enough. It is also difficult to handle in dynamic environments. They thus identify the need for authentication mechanisms that can be used between any pair of devices, with minimal user interaction. Autenrieth *et al.* [71] even state that fully automated mutual authentication is a requirement. Some recent work that aims to facilitate this is done in [74], and uses trusted components such as Physically Uncloneable Functions (PUFs). PUFs are functions implemented in hardware in a way that aims to make them very hard to copy, thus being able to act as a device “fingerprint”. Another way to facilitate M2M authentication in settings where the participating devices are geographically nearby, is by using physical context such as luminosity or temperature. Loske *et al.* [79] survey the available literature on this so-called context-aware authentication. If the transmissions are wireless, devices can also be identified through their radio frequency fingerprint [81].

One way of minimizing interaction is by relying on biometrics for identification and authentication (although one should be careful to not use biometrics for authorization). One property of biometric-based authentication schemes is that they cannot be used for M2M authentication, as biometrics are always derived from living beings. Therefore, these types of protocols might not be feasible in every industrial context, although they adapt well to some (e.g., smart healthcare [73]). In [72], a two-factor mutual authentication method is proposed, combining smart cards and biometrics, although recent work shows that their protocol is not secure against various attacks [75]. Li *et al.* [77], [78] use a combination of user/password and biometrics instead as a two-factor approach, while Deebak *et al.* [73] combine smart cards, passwords, and biometrics. The proposed methods claim to be very lightweight – but reliance on biometrics by itself requires specialized hardware (or some non-trivial computational capacity to process, e.g., audio or video signals), which might not always be an option. Further, it typically requires physical proximity, although recent work [80] shows that remote biometric authentication is a possibility.

Another way to minimize user interaction is by deriving identities through analysis of behavioral patterns. This shares the property that it cannot be used for M2M authentication with biometric-based methods. The Fifth generation cellular network technology (5G) authentication scheme for smart devices proposed in [70] uses Cloud-based learning to dynamically identify and authenticate users based on behavioral patterns, showing another approach for minimizing user interaction. This concept has also been used in the field of intelligent vehicles whereby drivers are identified by their driving behavior [69].

3) Non-Repudation: Non-repudation is a message property, ensuring that the author of a message is not able to later repudiate (i.e., deny) their authorship of that message. Non-repudiation can also extend to concepts other than messages (e.g., an entity cannot repudiate their accountability for an action that was started/requested by them).

Fraile *et al.* [84] provide some concrete examples showing why non-repudiation can be considered a security requirement. Firstly, users might perform illegal actions, and the system needs a way to track these actions. If these actions are reputable, the system becomes susceptible to log injection attacks, an observation echoed by Ankele *et al.* [83]. Another example mentioned is the situation where a manufacturer finds out that their configuration files on some hardware have been deleted, after the hardware vendor has performed updates to this system. Without a non-repudiation mechanism in place, the deletion of these configuration files cannot be unambiguously traced back to the software update. Another example can be found in [89], where the challenges in applying the Assurance Case methodology for the IIoT are laid out. Assurance Cases are structured arguments, for use during, e.g., software development, that show that certain properties of a system hold. The authors of this work identify non-repudation as a requirement for the assurance of security properties of a system. The blockchain-based authentication and access control scheme described in [87] also states that non-repudiation is an essential property.

Li *et al.* [86] propose a certificateless authentication scheme for Wireless Sensor Networks (WSN) environments. The advantage of their approach is that, because some of the heavier computations can be moved to third parties (e.g., a gateway), the computational requirements on sensor nodes themselves can remain low. Their protocol achieves non-repudiation by ensuring that messages are publicly verifiable. Certificateless schemes are a fairly popular topic in this domain. More recent examples of work on similar schemes for IIoT are [85], [88], [92] (broken in [91]), and [90].

4) Anonymity and Privacy: Anonymous authentication is verifying the authenticity of an entity without disclosing that entity's identity. This is necessary in situations where one wants to protect the privacy of users. Lin *et al.* [87] identify the need to protect users from being identifiable when an adversary has access to the authentication service. Cui *et al.* [93] also mention privacy-preserving access control. One example of a threat due to lack of anonymous authentication is provided by [72]: an adversary could conduct traffic analysis to create profiles on sensitive assets in an industrial environment, and possibly derive sensitive data from those profiles. Paliwal [94] proposes a hash-based privacy preserving authentication scheme specialized for WSNs scenarios. In this work, a variety of requirements are identified for schemes for WSNs, although these mostly relate to low-level properties that generalize to any secure authentication scheme, such as resistance against replay attacks. Because of this, we consider these to be too low-level to be included in our analysis as is, but rather as implied by other requirements.

In [87], a public blockchain-backed authentication mechanism is proposed, thereby turning user anonymity into a hard requirement. The work in [93] does not rely on a blockchain, but relies on a server to provide computational aid (in a secure manner). While both proposed schemes use Attribute Based Signatures (ABS) as cryptographic constructs, the two approaches cater to different goals: blockchains are widely considered to be resilient and highly available systems, which can be useful in scenarios that require these aspects, while server-aided encryption schemes target low-power devices with very limited computational ability or battery life.

5) Attestation: Attestation is a method for detection of unintended and malicious changes to software [17]. Doing this remotely can provide guarantees on the integrity and authenticity of a piece of software that is being run on a remote system, and therefore allows one to place more trust in a remote system than is possible in a scenario without remote attestation.

Because attestation aims to enable these higher levels of trust, it poses very strong security requirements on hardware. At the same time, remote attestation methods implemented purely in software typically have to rely on very strong assumptions that are hard to achieve in practice [17]. Attestation can be done in a practical setting through the use of Trusted Execution Environment (TEE)s provided by trusted hardware, such as ARM TrustZone [247], Intel SGX [248], or implementations of the Trusted Platform Module (TPM) standards [249]. Not all of these might run on low-end hardware, but some recent embedded controllers contain trusted hardware components [250] that also enable attestation to some extent.

References [17], [95], and [97] all identify the need for remote attestation, in order to increase the system's resilience against intruders. Especially in contexts where parts of an overall system are deployed in hostile environments, where it is important that the correct functioning of the software is continuously verified. Additionally, Laaki *et al.* [96] also identify the possibility for hardware attestation to protect the digital twin representation of proprietary hardware setups.

As mentioned in [17], there has not been a lot of activity on trusted hardware in this domain as of yet, with most of the available attestation protocols proposed so far aiming for a more general-purpose scenario, not taking into account aspects that make integrity and authentication protocols for the IIoT a challenging domain.

C. Access Control

Access Control (AC) is necessary in a wide variety of situations; already when a device allows for two modes of interaction, one for normal user behavior and one for system administrators to deploy updates, a rudimentary form of access control is needed. Furthermore, a lack of adequate privilege separation has been identified as one of the most severe shortcomings in existing systems, such as the Supervisory Control And Data Acquisition (SCADA) protocol [100].

AC invariably relies on authentication methods, as one needs to authenticate users in order to enforce access policies. It is therefore not surprising that AC mechanisms inherit many of the authentication requirements described in Section V-B. The challenges in access control relate to resource consumption, but also availability. In highly distributed scenarios, it should not happen that AC policies are unavailable due to a connection failure.

Aiming to minimize energy consumption for lightweight devices, Li *et al.* [86] propose a certificateless signature scheme as well as an AC framework for WSNs. This is made possible by relying on a (collection of) trusted systems in the network that are powerful enough to perform a part of needed cryptographic operations. The lightweight devices then cooperate with the trusted systems to create cryptographic signatures. Some natural security requirements are mentioned, such as the CIA triad and non-repudiation. Beltrán *et al.* [24] also target low-power devices, but they explore a setting in which these resource-constrained systems interact with Cloud services. In this scenario, they identify the need for identification, authentication, authorization, and accounting mechanisms. Furthermore, they state that depending on the particular application, fine-grained authorization control might be needed, or the ability to handle dynamically changing privileges. In some other situations, they state it is useful to manage access policies centrally. However, in order to be compatible with many systems from different developers, some form of federation is needed too. In order to address these issues, they propose a token-based federated authentication scheme that makes use of PUFs to meet the energy constraints of low-power devices. The resulting authentication scheme is flexible enough to act as a building block for many types of authorization mechanisms.

The blockchain-based authentication protocol proposed in [87] also contains an AC framework, and tackles the availability and single point of failure challenges through use of a blockchain, and a DHT containing AC policies. An additional feature of this work is that it respects the privacy of

TABLE VI
ACCESS CONTROL-RELATED SECURITY REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
AC-01	handle dynamic changes	[24], [99], [104], [108]	Medium	25%
AC-02	fine-grained AC	[24], [53], [99], [104], [106]	High	31%
AC-03	centralized AC	[24], [86]	Medium	12%
AC-04	decentralized AC	[24], [87], [99], [102]–[104], [107], [109]	Very High	50%
AC-05	privacy-preserving AC	[87], [102]	Medium	12%
AC-06	transparency	[86], [87], [103]	Medium	19%
AC-07	compatibility	[107]	Low	6%

users through the use of ABS techniques. A different approach is taken by He *et al.* [102]. In this work, ring signatures are used to construct a distributed lightweight AC framework. This framework specifically targets WSNs and achieves user anonymity by grouping users with similar rights, ensuring that AC authorities cannot differentiate between signatures from users in the same group. Lahbib *et al.* [104] also propose a blockchain system, identifying the need for dynamic access control and distributed governance. They utilize smart contracts and leverage the non-repudiation and integrity inherent to blockchain systems to propose a resource management framework, with fine-grained AC built in. Yao *et al.* [109] share the sentiment that distributed AC is needed, but propose a Fog solution based on attribute credentials.

Kim *et al.* [103] consider a scenario where nodes in multihop Low-power Lossy network (LLN)s want to communicate with each other. They also identify the need for federation, but from a reliability perspective. In order to guarantee the availability of a system, it cannot rely on a single point of failure for access control enforcement. At the same time, they identify the need for a transparent scheme, that is also scalable. Decentralized protocols such as the one proposed in their work, can increase scalability, as changes are propagated much more organically through the network, than with a centralized structure, avoiding congestion issues.

In the work presented by Chen and Ng [99], AC and authorization are also identified as one of the major challenges for the IIoT. They propose an access control framework for a scenario where the owner of an IIoT device has the right to control the AC policies of their device, and wants to set up fine-grained policies. At the same time, a large number of IIoT devices are shared by multiple entities that can interact with them based on these policies.

Preuveneers *et al.* [107] argue that identity management is crucial for AC purposes, and propose a framework handling identities, authentication, and authorization in a networked production scenario. They also raise the point of compatibility with legacy devices, which is worth considering in any IoT environment.

Vanickis *et al.* [108] make the observation that due to the increase in frequency and sophistication of security attacks in recent years, there is a need to include risk assessment in the process of specifying AC policies, and that as a result of these trends there is a growing interest in Zero Trust Networking (ZTN) protocols as opposed to perimeter-based security. The principle behind ZTN is to treat the intranet with the same level of trust as the Internet. Their proposed policy enforcement framework is built upon this principle, and is able to provision firewalls across different segments of a network.

D. Maintainability

Maintainability concerns the ability to configure, reconfigure, and update (parts of) a system. In Industry 4.0, these concepts become crucial as the software and configuration of IIoT systems must have the ability to be changed, in order to provide protection against previously unknown security threats [116]. Updateability can be considered a countermeasure against security attacks, since it allows for continuous changes to firewall configurations as threats are identified, as well as software patches for newly discovered software vulnerabilities. As we will see in this section, the challenges relating to maintenance are again related to resource constraints and the dynamism of IIoT environments, making traditional maintenance solutions insufficient to adequately address the needs in this domain.

In [110], George and Thampi state that the availability of security updates is a critical concern for IIoT devices, but that due to some IIoT systems being so lightweight and the infrastructure not being fixed, it is extremely difficult to always patch all devices in a network. To mitigate this, they describe an approach that ensures update deployment on high-risk vulnerabilities, to reduce the risk of serious attacks on the infrastructure. For this, they propose a number of risk mitigation strategies that can be used to help identify the devices most in need of updates. Yadav and Paul [114] also identify the timely application of patches to all vulnerable systems in a network as a problem, and propose a patch prioritization method to mitigate this.

In addition, some IIoT systems require the ability to be updated without any disturbance to the service they provide. Mugarza *et al.* [111] propose a secure updating mechanism for mixed-criticality systems. However, their approach requires the ability to run and monitor updated binaries in a sandboxed mode. Not every device has the resources for this. They follow up on this research with an application of their system to a smart city scenario [112]. The proposed update process is in accordance with several safety standards, a requirement identified in Section V-E.

According to Seitz *et al.* [113], updating IIoT systems is often complex and cumbersome, and requires an expert technician to perform the update, which can be a lengthy process. This does not scale with the increase in connected devices,

TABLE VII
MAINTAINABILITY-RELATED SECURITY REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
M-01	software updateability	[52], [111]–[113]	High	27%
M-02	configuration updateability	[52], [67], [111]	Medium	20%
M-03	disturbance-free updates	[38], [111]	Medium	20%
M-04	usability of update process	[113]	Low	7%
M-05	traceability	[36], [113]	Medium	13%
M-06	compatibility	[36], [113]	Medium	13%
M-07	transparency	[113]	Low	7%
M-08	secure status transfer	[36]–[38], [117]	High	27%

and therefore the update process must be streamlined and simplified, with minimal possibilities for errors due to human behavior. Their suggestion is a marketplace, not unlike those seen on smartphones. In addition to usability, they state that update management of devices should be possible both on-site and remotely, and updates and installations must be logged so that they are traceable, for transparency and in case of problems. While their proposed solution appears as a global and decentralized marketplace, this might not be a good fit for every type of device, especially when the functionality of such a device is secret. Moreover, it raises questions about how much power can be given to app developers and where the trust in a system should lie, which are topics that can be highly dependant on a specific scenario, and are worthy of further investigation on their own.

Another problem is mentioned by Ulz *et al.* in [67], wherein they state that cryptographic keys also require the possibility to be updated securely. This can be interpreted as a requirement relating to the maintainability of a system's configuration, and is an argument against the deployment of hardcoded keys at manufacturing time, which sometimes happens in production environments. In a later work, they take this notion further, and propose a hardware device, that can be temporarily attached to a system to allow for secure updating and reconfiguration [52]. The updates are verified and installed in an isolated environment provided by the special hardware, for increased security and traceability, but still allows for remote queuing and deployment of updates, to some extent. However, this approach might not be practical in environments where it is hard to physically reach all deployed systems.

1) Smart Maintenance: Industry 4.0 enables smart maintenance, which is essentially predictive maintenance of (parts of) devices based on remote data collection about their usage. This allows for a more streamlined production line where system downtime and maintenance costs are reduced to a minimum. Its relevancy is underlined by the inclusion of continuous maintenance and maintenance frequency being used as measurable safety indicators in a meta-model proposal for automated security dependability detection within IIoT systems [25]. Priller *et al.* [117] provide a case study on this subject detailing a number of smart maintenance security requirements, notably the ability to update as well as secure communication channels themselves.

Lesjak *et al.* [36] reason that smart maintenance requires secure communication channels, as status information of machines is sensitive data. Moreover, the maintainer needs the ability to verify the validity of this data. They argue that there are systems for which it is essential that they are exposed to the Internet as little as possible, and propose solutions using NFC to permit secure transmission of data to the maintainer, as well as identity provisioning over NFC [37]. The specific requirements identified in this work are the need to support legacy devices, prevent data leakage, protect against Internet access, protect the validity of the maintenance data (towards the maintainer), and protect transparency of the communicated data (towards the customer). In a later study, Lesjak *et al.* [38] propose an MQTT-based approach where they add a further requirement that data transmission must not cause safety-critical interference, so that operational functionality remains unaffected.

E. Resilience

The Industrial Internet Consortium (ICS) has published an IIoT security framework [123] in which they define resilience as "the emergent property of a system that behaves in a manner to avoid, absorb and manage dynamic adversarial conditions while completing the assigned missions, and reconstitute the operational capabilities after causalities". This definition overlaps with several aspects of system trustworthiness such as safety and reliability, but also security. Indeed, [15] and [118] identify resilience as an important security challenge for the IIoT. The implication that resilience requirements bring to the security domain are that security technologies should provide the capability to continue normal system operations if parts of the system are considered compromised. This could for example be done by rerouting tasks to other capable components, or through other means, often belonging to one of three canonical approaches identified by Laszka *et al.* [126]: redundancy, diversity, and hardening.

The manner in which this requirement should be satisfied, depends heavily on the scenario. In a WSN, it might be acceptable to simply deploy enough sensors to guarantee some redundancy, meaning that a small number of compromised sensors can be kept contained and their output discarded until the issue has been addressed. In a power plant however, it might be catastrophic to disable one generator entirely if one of its components has been compromised. Instead, it might be possible to provide the compromised components' functionality in some other way, or temporarily reroute energy from other generators to guarantee some level of operations.

TABLE VIII
RESILIENCE-RELATED SECURITY REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
R-01	continuation of operation with compromised subsystems	[15], [84], [118], [121], [126]	High	31%
R-02	operation with intermittent connectivity	[84], [125]	Medium	12%
R-03	standards compliance	[25], [112], [119], [120], [127]	High	31%

Fraile *et al.* discuss device driver security in a connected virtualized factory environment [84]. They identify multiple resilience-related issues, one being that intermittent connectivity might cause loss of history if status information should be continuously sent to a centralized database or the Cloud. Their proposed solution is to keep local databases that keep a short-term history that can be synchronized with a back-end once connectivity is restored. Another identified issue is to avoid system failure, in case of a compromised device driver. The authors propose redundancy and smart fallback mechanisms to adapt to possible threats. The difficulty in a fallback mechanism is that it requires the exact same configuration and as much as possible of the current system state of the normal system, in order to allow for rapid recovery. This is not only difficult because state replication can introduce considerable overhead, but it also means that the fallback system is vulnerable to the same threats as the normal system. To mitigate this issue, the authors propose introducing some diversity in the fallback system. The proposed solutions in this work are all rather specific to the considered scenario and architecture, but use elements that are common in resiliency mechanisms in general.

When looking at low-energy devices, WSNs have been identified as a way to increase the robustness of SCADA systems against network failures, due to their distributed and self-organizing nature [125]. However, major concerns exist regarding their ability to communicate securely, and the ability to interface with some proprietary SCADA protocols. The authors also identify a number of challenges relating to the security of WSNs and propose a decentralized multi-agent architecture to remedy a number of these.

In [25] and [120], a number of measurable indicator points are identified, among which those relating to resiliency. In the latter, they then use these indicator points to propose a method for automated standard compliance testing in the Industry 4.0 domain. Standard compliance is a powerful aid in verifying the resilience, reliability, and safety of a system, and can be applied to a wide spectrum of devices. Related to standards compliance, Bauer *et al.* [119] investigate European Union Agency for Network and Information Security (ENISA) guidelines on secure Cloud services, and extract a number of measurable security metrics that relate service level agreement objectives between Cloud providers and their (industrial) customers to concrete responsibilities. These metrics could also be used in compliance testing. In this work, reliability and redundancy are also identified as measurable indicators. Similarly, Leander *et al.* [127] investigate the applicability of the IEC 62443 cybersecurity standards [124] in Industry 4.0 applications. For a short survey on the security standards relevant to Industry 4.0, we refer to [122].

F. Data Security and Data Sharing

In today's world, data security is critical in nearly any digital environment, and the IIoT is no different. Many of the works investigated in this survey identify confidentiality of data as a security requirement in some form (e.g., [17], [36], [49], [71], [133], [136]). Traditionally however, availability and integrity are considered more favorable than confidentiality for industrial environments [129], [132], as they have a measurable economic impact. This is not a sustainable viewpoint in an era of connected devices, and is changing fast now that companies seek to connect their systems to the Internet.

In a survey among companies, Autenrieth *et al.* [71] found that they too consider data security to be one of the critical factors for migration to Industry 4.0, a finding confirmed by another study conducted by Moyne *et al.* [136]. In this work, the authors additionally state that companies are hesitant to adopt data-sharing based technologies (Cloud, smart maintenance, fault detection and prevention, etc.) as there is no evidence of these technologies being safe or secure when it comes to protecting intellectual property, as a result of which they identify the need for a standardized way to achieve intellectual property protection in the presence of data sharing mechanisms. The sentiment that companies are reluctant to rely on Cloud providers for data storage and sharing is shared by Esposito *et al.* [29]. However, they also note that most data breaches come from within companies, and not Cloud providers. They propose a cloud storage solution that aims to minimize the attack surface both in the Cloud and within the company. They identify data loss mitigation as another requirement, identifying four key elements for an effective solution: prevention, identification, notification, documentation.

The challenges in this domain relate to three colliding factors: Firstly, due to the heterogeneity of devices, data security mechanisms need to be able to operate with extremely few resources. Secondly, due to the criticality of some IIoT applications, the data security requirements are very high. Thirdly, many smart capabilities are enabled by the sharing of data, but in industrial contexts, data is often sensitive and confidentiality is of utmost concern, which poses a dilemma.

Data security covers a wider area than just encryption techniques. One of the vital aspects of the Industry 4.0 paradigm is making smart use of available data. This inevitably involves sharing data with other entities, that can be anywhere from a part of the system to being outside the organization boundaries. As an example, consider the discussion on the sharing of device usage metrics in Section V-D1. Even if no other data

TABLE IX

DATA SECURITY AND DATA SHARING RELATED SECURITY REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
DSS-01	data loss mitigation	[29]	Low	2%
DSS-02	data confidentiality	[36], [50], [52], [53], [55], [98], [105], [130], [135], [139], [149]	Medium	19%
DSS-03	standardization	[136]	Low	2%
DSS-04	secure data transport	[34], [38], [40], [137], [142], [143], [145]	Low	7%
DSS-05	secure external data storage	[29], [65], [66], [98], [131], [139], [141], [146]–[156], [159], [161]	High	34%
DSS-06	data flow control	[162]–[164]	Low	5%
DSS-07	data protection legislation compliance	[50], [98], [165]	Low	5%

is shared, usage metrics will have to be sent to the device manufacturer to enable smart maintenance, but might also be used to deduce sensitive information such as production volume. A similar example would be data analysis for anomaly detection (Section V-G). While encryption techniques do offer ways to aid with partial sharing of data, we will also discuss other ways of keeping data confidential.

1) Data Transport: The MQTT protocol is widely used for data sharing between industrial systems, but by itself only supports user/password authentication, and provides no security measures on the network or application layer. This becomes problematic especially in the context of the IIoT. In order to remedy this, Lesjak *et al.* [38] propose using TLS as a secure layer upon which MQTT can function. While this provides all the security benefits of TLS, it does add considerable overhead to the edge devices that will now have to manage TLS contexts. In their work, the authors propose using a trusted hardware extension at the edge devices that can store keys and also manage the TLS context. While modern devices might have access to cheap trusted hardware, this is not always possible with legacy devices, therefore, other solutions will need to be investigated. Katsikeas *et al.* [34] also observe that TLS can be used to secure MQTT communication, but note that this will not work well in WSNs due to severe resource constraints. Therefore, they try to minimize the overhead by encrypting messages at the link layer. In a later work, Lesjak *et al.* [40] observe that an often-needed requirement is communication with other stakeholders, e.g., equipment manufacturers (for smart maintenance) or nearby links in a supply-chain. To enable authenticated, secure data communication between these, the authors propose a hybrid multi-stakeholder protocol on top of MQTT that allows end-to-end encryption of payloads that need to be transmitted to external parties.

Alternatively, more modern protocols such as The OPC Unified Architecture (OPC UA) [145] have authentication and encryption support [34], [143], and hardware acceleration for the cryptographic primitives used in these is starting to appear in lightweight products [251]. Adoption of the OPC UA could thus help in meeting some of these constraints. One recent experimental deployment combines this with trusted hardware to facilitate secure connections [142], but acknowledges that further research is needed. Finally, it is worth noting that regardless of the security protocol used, from an energy and efficiency standpoint, there is a case to be made for selectively encrypting only those messages that might harm the system if tampered with. In [144], the authors propose a symbolic analysis model that can identify such messages.

2) External Parties: Data confidentiality when at rest or in transit, is often realized through cryptographic means. The challenges in finding suitable ciphers for the very diverse IIoT environment are described by Zhou *et al.* in [55]. Again, the main challenges appear to concern energy and other resource constraints. Irrespective of the cipher used, the authors also identify the key distribution and management problem, as previously discussed in Section V-B1. More generic challenges are described by Yu *et al.* [160]. They argue that Reliable storage, convenient usage, efficient search, and trustworthy data deletion are some of the major issues for Cloud and Fog scenarios.

As the Cloud promises a large amount of storage and computational resources, Cloud connectivity is often necessary for Industry 4.0 applications. With a suitable encryption scheme, data might be stored securely in the Cloud [98], but even then it is not possible to interact with it in any way other than retrieving it for decryption. Seeking to remedy this, there has been a recent increase in research efforts in modern cryptographic techniques such as homomorphic encryption, allowing for computation on encrypted data ([65], [66]), and searchable encryption, enabling search operations on encrypted data ([146], [161]). Specific to the IIoT data sharing scenario, Deng [147] proposes an anonymous aggregate encryption system that allows IIoT devices to encrypt data into one ciphertext that can be decrypted by multiple recipients with their individual keys, while retaining their relative anonymity.

Fu *et al.* [149] propose one way of ensuring confidentiality in the Cloud, while maintaining the ability to search through data sets, through a privacy-preserving encryption scheme. Deployed IIoT devices transmit their data to special (on-site) servers which aggregate the data, remove redundant entries and prepare it for storage in a Cloud-backed database by indexing and encrypting it. Users can then search this database through trapdoor queries, meaning that the search process can be performed on the encrypted data. In order to obtain the searched data, users can download the encrypted results, and use their private keys to decrypt them. As a result, the Cloud environment will never have any access to the unencrypted data. Xu *et al.* [159] propose a similar solution, also relying on trapdoors to perform search queries on encrypted data sets in the Cloud. The difference is that in this solution, the used encryption techniques aim to be lightweight enough to allow for decryption by the IIoT devices (specifically sensor nodes) themselves, without requiring an intermediate server. This approach only targets data storage, search, and retrieval. Other use cases for Cloud environments, such as big data analysis in the Cloud itself, cannot be solved using this method. Miao *et al.* [155] also propose a Cloud-assisted method in the context of an e-health scenario, while attempting to minimize intensive tasks such as decryption and decryption at the Edge side, to computation requirements and power consumption

With the advent of blockchain technology, there has been an increase in interest in data sharing solutions based on decentralized ledgers. Sani *et al.* [157] propose a privacy preserving blockchain using mutually authenticated encryption for confidential data exchange, while others propose things such as energy trading [150] and big data markets [152]. Huang *et al.* [151] list three main challenges in blockchain technology: the trade-off between efficiency and security, coexistence of transparency and privacy, and conflicts between concurrency and throughput. These concerns are shared by Nikander *et al.* [156], who discuss throughput, latency, and resource requirements more in-depth. Further, they identify four models of operation for lightweight devices to participate in blockchains. Another proposed solution is to integrate devices with multiple ledgers, although the authors state that this is an active field of research. The aforementioned concerns are also identified in [148], where the authors further state that while blockchain promises enhanced data security and availability, for the IIoT domain there remain challenges regarding data privacy, integrity, and identify certification. They also list interoperability, standardization, and regulatory aspects as more general blockchain challenges. Other blockchain-based proposals in this domain are [153] and [154]. For a more thorough discussion on security requirements and challenges for blockchain in the IIoT, we refer the interested reader to [35], and for a discussion on risky characteristics common to blockchain technologies we point to [158].

3) Data Flow-Control: Through data flow control, data access policies can be enforced on a higher-level than encryption techniques, which provides a way to address security- and privacy requirements relating to the processing of data as it moves in a system.

Al-Ali *et al.* [162] describe a real-world use case for data flow monitoring, where certain data on machine error rates is shared within the company itself, and across organization boundaries based on a set of privacy policies. Some of these policies cannot be statically enforced because they depend on dynamically changing processes or coordinated interaction between different entities. They conclude that the ability to capture dynamic situations is a challenge that has yet to be overcome.

Identifying data security as a design requirement, Bloom *et al.* [163] investigated input-output patterns in existing IIoT applications in order to gain a better understanding of ways to secure information related to IIoT operations. Based on their observations, they propose some design patterns that can help protect data flow already in the design stage. Schütte and Brost [164] state that data flow enforcement is a requirement in certain contexts, and propose a policy-controlled data flow control framework capable of monitoring messages between entities both statically and at run-time. This allows users to not just specify access policies, but also to state how data elements are allowed to be processed by the system. Whether dynamic monitoring with this solution is possible in time-critical systems, is still a subject for further study.

4) Data Privacy: Data privacy and ownership is an important topic for many companies and governments, and with the recent popularity of Cloud storage services, these issues require careful consideration [98]. With the amount of data that is generated by modern devices, it becomes possible to create detailed profiles of users, putting their privacy at risk [168]. In an attempt to mitigate this, an anonymous data collection framework is proposed in [169].

With recent legislation in the European Union (the General Data Protection Regulation (GDPR) [166]) effectively requiring privacy-by-design for all products, data privacy should be taken seriously by manufacturers as well. Preuveneers *et al.* [50] discuss the implications of the GDPR in Industry 4.0 and smart factory environments. For example, some requirements derived from this legislation are that (in general) customers of a service have the right to retrieve their personal information, the right to be forgotten, and the right to erasure of their personal information. This should be taken into account when designing systems that interact with humans and might collect such information. Acknowledging this need for integration, Conzon *et al.* [165] describe a model-based framework for IoT, the security and privacy principles of which are derived from the GDPR.

Privacy does not only concern data collection and Cloud storage, but also requires the obfuscation or omission of metadata and other properties that can be leveraged by adversaries. For example, in WSN networks, sensor nodes are often spread over a geographically wide area, and an adversary might attempt to locate the source node of specific traffic based on message flow. To remedy this, source location privacy schemes should be deployed such as the one proposed in [167].

G. Security Monitoring

Dynamic monitoring of behavior in a system is an effective way to detect and respond to malicious activity, and systems that provide these capabilities are commonly known as Intrusion Detection Systems (IDSs). In the IIoT domain, two commonly identified security requirements are the ability to monitor infrastructure, and respond to known and unknown threats when necessary [55], [193], [198], [206]. The reason these are deemed particularly important for the IIoT comes from the fact that older, less secure devices are likely to be connected to the network as well [208]. These devices cannot always be patched to protect against known vulnerabilities, and therefore require continuous monitoring. An example of this is the IDS proposed by Kim and Kang [189], which specifically targets the Modbus protocol, a widely used industrial

TABLE X
SECURITY MONITORING REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
SM-01	infrastructure monitoring	[55], [115], [170], [171], [173], [176], [178], [181], [184], [185], [189]–[195], [197]–[199], [201]–[204], [206]–[208]	Very High	64%
SM-02	threat response	[55], [115], [175], [184], [187], [193], [198], [204]–[206]	Medium	24%
SM-03	handle heterogeneous sources	[193]	Low	2%
SM-04	security policy enforcement	[191], [199], [204]	Low	7%

control protocol, and a good example of an existing protocol severely lacking in security mechanisms. Similarly, the MQTT protocol has been covered like this [178]. A second reason can be found in providing protection against Denial of Service (DoS) attacks [115] and improving congestion control in general [187].

Hasan and Mouftah [184] state that latency is one of the major challenges for security monitoring systems, due to the geographical distance between devices in certain Industry 4.0 networks, network latency can become too high for acceptable response times to intrusions, especially when using Cloud security services.

Another identified challenge for security monitoring in the IIoT is the imbalance of data sets. Due to the sheer amount of data generated by IIoT devices and the low attack frequency, obtained data sets that can be used for machine learning approaches to intrusion detection tend to be very imbalanced [206].

Many proposed IDS solutions exist that are designed to work in the general IT domain. However, it becomes harder to monitor threats when taking into account the extreme environments in which some IIoT appliances are deployed, resource constraints, and data privacy requirements. On the other hand, as IIoT system activity is largely the result of automated processes, the traffic patterns tend to be fairly static and periodic, making it easier to perform accurate anomaly detection [180], [208]. Additionally, this predictability introduces the possibility for utilizing these patterns against the system through stealthy injection attacks [196], or to establish covert communication channels, as demonstrated in [172], and should be monitored against. In [176], Bernieri *et al.* show that this predictability can be used against attackers by developing a honeypot for a water distribution system. It simulates physical processes, and is able to detect attacks that aim to modify the system's behavior. A machine learning based IDS capable of detecting these types of attacks proposed in [181]. However, Genge *et al.* [183] note that when monitoring the output of physical processes, care has to be taken to take the gradual decay of processes (e.g., the wear on equipment) into account. They show that this can be done through statistical analysis. As the authors observed, there is very little work done in this area, and more research is needed to develop sophisticated measures that incorporate for process aging.

Settanni *et al.* [198] propose a self-adapting IDS that detects anomalies in the range of certain control values. Their solution requires the continuous collection of logs of all connected devices to a central control system, which is acceptable in environments with reasonably powerful machines, but not in WSNs or other sparse environments with lightweight nodes. The anomaly detection algorithm for physical quantities proposed by Zugasti *et al.* [208] similarly looks at observed quantities. However, in this work, no attention is given to the resource overhead of this approach, nor where it should be deployed in an IIoT system.

Very recently, there has been a surge in interest in machine learning techniques for anomaly detection in IIoT. For example, [200] and [203] provide a performance comparison of various machine learning algorithms for detecting anomalies in IIoT, in [171], Al-Hawawreh *et al.* propose a deep neural network approach for use in brownfield installations, in [170] the authors propose a similar system for ransomware detection, and in [197], the authors employ machine learning to detect time synchronization attacks. In [173], Alem *et al.* acknowledge the power of machine learning, but warn against high potentially false-positive rates. To mitigate this, they propose a hybrid system, that derives a semantic model from the ISA95 standard. Then, using a neural network for anomaly detection, they can filter out false positives and categorize anomalies based as being malicious or just dysfunction. Deep learning IDSs do not come without risk. In [186], the authors show that one can reliably create adversarial samples that defeat deep learning based systems. The findings in [188] agree with this, as also there the authors manage to bypass machine learning systems. Additionally, they show two methods of increasing resilience through retraining of the networks. Robustness against adversarial samples is something that needs to be taken into account when using machine learning for security monitoring. For a more thorough overview of the state machine learning for industrial IDSs, we refer the interested reader to [207].

Moustafa *et al.* [193] identify the requirement for IIoT monitoring services to handle a large amount of heterogeneous data sources. Their proposed solution uses Markov models and a central processing system (with parts running both in the Cloud and Fog). The data collection itself happens through middleware, thereby minimizing the overhead on resource-constrained devices.

Threat response is a requirement identified by many works in this area, e.g., [55], [198], [205]. While this is usually in the form of notifying security personnel and mitigating the threat by stopping the service, Babiceanu and Seker [175] use the flexibility provided by Software Defined Networkings (SDNs) to let the network operate in multiple modes, increasingly trading quality of service for security.

Whereas some approaches focus on intrusion detection in one layer in the Edge-Cloud spectrum, Yan *et al.* [115] propose a monitoring framework that contains systems operating in the Edge, Fog, and Cloud layers. This way, resource overhead for extremely lightweight Edge devices is kept to a minimum, while at the same time allowing localized management and response through the Fog layer. The Cloud layer uses data analysis approaches to intelligently detect attacks. This is similar to the DDoS mitigation approach proposed by Zhou *et al.* [205], where local virtual network functions, Fog, and Cloud work together to respond to DDoS attacks.

Another aspect of security monitoring concerns the continuous monitoring of network traffic ensuring that network security policies are not violated. This type of monitoring is to help maintain the integrity required of Industry 4.0 network infrastructure, and as such does not target devices themselves, but rather SDN controllers and routing devices. Melis *et al.* [191] propose a live monitoring solution of flow permission controls, as well as a proactive formal verification mechanism of the security policies in SDN systems.

That security monitoring can also be proactive, can be seen by looking at the fuzzing frameworks proposed by Flores and Mugarza [182] and Niedermaier *et al.* [45]. The authors of the latter propose a fuzzing framework, that continuously tries to "attack" networked services with randomized data streams. It is lightweight, and is able to identify vulnerabilities due to common software bugs such as buffer overflows. However, with an approach such as this, care has to be taken that system performance is not affected, and that critical services remain available. As such, fuzzers might mainly be a tool for security researchers, and developers aiming to create a highly secure product. But when deployed carefully, production systems can also utilize them to detect configuration errors and vulnerabilities.

That IIoT environments can benefit from specialized monitoring approaches can also be seen when looking at drone scenarios. In their behavior and vulnerability assessment, Sharma *et al.* [199] identify a number of security requirements that are specific to this scenario, as well as several requirements that are more generally applicable. Specifically, they identify the need for: identification mechanisms; continuous monitoring; predictive and highly accurate vulnerability assessments; and the ability for anomalous drones to be marked by the monitoring service, so that this information can be shared with all drones in a swarm. Their solution utilizes Petri Nets to monitor behavior. Some other proposed monitoring solutions aimed at drone scenarios are based on behavior rule specifications [192] and recursive parameter estimation [177]. Another example of specialized security monitoring is provided by Deshpande *et al.* [179] propose a heartbeat protocol catering specifically to WSNs, ensuring that overhead on the sensor level is minimal.

H. Network Security

Achieving adequate network security consists of many things, including authentication, secure transport, reliable and secure routing, and more. In previous sections we already discussed some of these, and will therefore focus on network infrastructure security.

With industrial networks becoming increasingly complex due to a large number of connected devices, we are faced with problems similar to those that occurred during the rapid expansion of the World Wide Web [187]. Because of this, many performance and scalability issues need to be addressed, such as bandwidth and latency contention. According to [212], many configuration, traffic control, and security systems rely on proprietary software which make integration in generic management frameworks impossible. At the same time, they state that network infrastructure is required to be flexible, to handle dynamic environments. To solve this challenge, two paradigms aimed at separating configuration and control from data transfer itself have been gaining traction: SDN and Network Function Virtualization (NFV). SDN concerns configuration and management, while NFV concerns virtual environments to run network and security functions on a layer that is abstracted the devices on which it runs. The authors propose an architecture using these paradigms to enforce security policies on switches with SDN and NFV capabilities, and move away from, e.g., firewalls. They essentially attempt to address four security requirements through this approach: the ability to specify and enforce network security policies, to minimize management and configuration overhead, to allow for dynamic reconfiguration of the network and its security policies, and to minimize the overhead caused by enforcement of security policies. Other points where SDNs can improve system security are discussed in [217].

1) Latency and Timeliness: Marchetto *et al.* [221] state that additionally connectivity and isolation between endpoints are network security requirements, although these can possibly be interpreted as security policies by themselves. While they identify these security requirements, their work addresses a slightly different matter: the Virtual Network Embedding problem, which concerns the placement of virtual network functions so that they are optimized and can be verified to correctly enforce the desired security policies. This can potentially be utilized by other works to keep overhead to a minimum and minimize network latency. Hu [218] also identifies latency as a challenge and states that the controllability and configurability of network architectures and applications are key elements in reducing latency. The implied requirement is thus that IIoT environments must be controllable and configurable at every level. This network latency issue is also relevant to security monitoring (previously discussed in Section V-G), as keeping latency to a minimum is a large issue in network monitoring services, and possible solutions include alteration of the network architecture [184].

For time-critical applications, there exist specialized standards such as the Time Sensitive Networking (TSN) standards to provide deterministic and timely networking capabilities between systems. These applications often require remote access to sensors, actuators, and Programmable Logic Controller (PLC)s driving industrial devices. These connections must fulfill the same requirements as when those devices would be directly connected on the machine level [219]. For

TABLE XI
NETWORK SECURITY REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
NS-01	dynamicity of configuration	[212], [218], [219]	Medium	10%
NS-02	security policy enforcement	[221]	Low	3%
NS-03	management overhead minimization	[212], [224]	Low	7%
NS-04	network isolation	[129], [210], [211], [217], [220], [221], [224]	Medium	24%
NS-05	timeliness	[187], [213], [218]–[221]	Medium	21%
NS-06	availability (DoS, jamming, etc.)	[187], [214], [219], [221], [222], [226]	Medium	21%
NS-07	wireless transmission security	[32], [33], [209], [215], [216], [223]–[227]	High	34%

this, safety and security measures must be present in the network architecture to correctly prioritize such traffic.

With a gradual movement towards an IIoT enabled industrial process, it is expected that many legacy devices will remain operational for some time in parallel with new technologies, in a sunset phase. These legacy devices must thus be isolated from the Internet, but care must be taken in the isolation technologies, as to not provide too much overhead in time-critical processes. To that end, Lackorzynski *et al.* [220] compare multiple readily available VPN solutions on metrics important to industrial appliances.

2) Availability: Latency is not the only issue. From a dependability perspective, single points of failure should be eliminated. However, with modern Cloud infrastructures, often the network virtualization solutions proposed by Cloud providers constrain customers to that one Cloud service provider [222]. To allow critical applications to utilize the Cloud for enhanced functionality, without sacrificing availability, the authors propose a platform to allow virtualized networks spanning multiple Cloud providers as well as private networks, while also solving the Virtual Network Embedding problem. This way, they are able to explore the flexibility of combining on-premises systems with Cloud systems, and satisfy privacy requirements by creating security policies limiting the mapping of sensitive NFV applications to specific classes of networks.

3) Wireless: Many smart devices make use of wireless technologies for data transmission. These wireless communication standards work on a lower level than the data transport technologies discussed in Section V-F1. However, the security requirements for wireless transmission that we found in the investigated literature largely overlap with those of data transport security. A common type of wireless communication technologies aimed at long-range low-power IoT devices are LPWAN technologies [229].

Chen *et al.* [223] list a number of security requirements in a review of the Narrow Band IoT (NB-IoT) standard. This standard was developed by the The 3rd Generation Partnership Project (3GPP) [252] and focuses on extremely low-power devices and indoor connections. The authors identify DoS as a much more apparent threat than in traditional networks, as low-power mobile devices will be easily drained from battery power. Another requirement is to prevent eavesdropping of transmissions, as information leakage can lead to devastating results. The authors also identify the need for devices to sign and encrypt their transmissions, in order to mitigate the potential impact of a compromised base station (they identify this as more likely than with traditional wireless technologies). Mutual authentication between devices and the base station is also mentioned, in order to prevent spoofing attacks. Recently, an exploratory investigation has shown that properties derived from the relative distance and direction between transmitters can help in identifying these types of attacks [32]. As the NB-IoT standard supports a large number of devices (100,000) being connected to one terminal, it is challenging to create sufficiently lightweight and efficient authentication and access control mechanisms for these.

Kail *et al.* [33] compare the security properties of several LPWAN technologies in the unlicensed bands. This comparison is done through the inspection of a number of capabilities that are to be expected of a secure standard, and therefore we consider them as sensible security requirements for wireless technologies: authentication, message integrity, confidentiality, Over-the-Air firmware upgrade capabilities, reliable communication, and key exchange capabilities. Note that these requirements are also already covered in other sections, so we do not list them in Table XI. Additionally, they identify the need for protection against common attacks against wireless technologies, such as wide-band jamming, selective jamming, eavesdropping, traffic analysis, replay attacks, and wormhole attacks. Their conclusion is that further research on security and privacy-related features for low-power wireless communication standards is needed. Wang *et al.* [226] argue that in order to satisfy the confidentiality requirement, encryption techniques are not sufficient, and propose a friendly jamming scheme, making it harder for eavesdroppers to distinguish communication from noise.

6TiSCH [228] is a standardization effort by the Internet Engineering Task Force (IETF), aimed at low-power deterministic IPv6 communication for WSN technologies and industrial IIoT networks, by building on the IEEE 802.15.4 standard for low-rate Wireless Personal Area Network (WPAN)s, thus supporting a different category of devices than LPWAN technologies. Although timeliness is one of the major goals of 6TiSCH, it also aims to incorporate a variety of security properties. For example, the authors state that support for Datagram Transport Layer Security (DTLS) and TLS is taken into consideration. A further discussion of 6TiSCH security is given in [227]. Related to WPAN technology, Ulz *et al.* [225] propose a secure communication framework utilizing NFC, aimed at providing a reliable solution for mobile robots that need to communicate with machines. Due to the short-range nature, this naturally helps remedy eavesdropping and interference issues

The 5G standard also addresses IoT scenarios, and provides support for virtualization of network resources. This enables the creation of isolated network partitions with different demand profiles. Two key scenarios that 5G targets are massively deployed low-bandwidth IoT devices, and critical latency-sensitive applications. Both of these map very well to common IIoT and Industry 4.0 scenarios. Kurtz *et al.* [224] elaborate on network slicing, and how it can be realized through use of SDN and NFV technologies. The security requirements identified in their work concern strict isolation of network traffic, and the ability to provide hard service guarantees, such as on latency, data rate, and reliability. Additionally, they mention the need for manageability in this environment, as misconfiguration of systems can have a negative impact on the capabilities of the overall network. Their results show that 5G technologies can be used for real-time, critical applications.

I. Models and Methodologies

In this subsection, we discuss proposed security models and methodologies in the investigated literature. As the security issues that these address are relatively high-level, the security requirements are relatively abstract and encompass multiple aspects of IIoT systems. Therefore, the security requirements listed in table XII are to be interpreted as recommendations and tools to improve the degree to which other security requirements can be satisfied, as well as easing the process of doing so.

Shaabany and Anderl [51] states that software and hardware should be designed carefully, with security in mind, in order to reduce the attack surface as much as possible during design time. Among some less-security related requirements, they argue that specialized functions should be standardized for reuse as much as possible (across manufacturers as well), that all components should be uniquely identifiable and that this identifier should be used in communication with other components, and that security guarantees should be given on every hierarchical level. To aid in addressing these needs, the authors propose a security-by-design approach encompassing both hardware and software. It is thus clear that security should be considered at every step of the development lifecycle of a system, and in [234], Eckhart *et al.* propose 14 security activities spread across multiple phases in the development process that have shown to be effective for cyber-physical systems. Maksuti *et al.* [42] take a more flexible stance than Shaabany, observing that security and business process performance will always come at the cost of each other. They state that one possible solution is to create a self-adapting system that can flexibly provide end-to-end security. To this end, they propose the investigation of self-adapting models and describe a relevant meta-model. As an example, they suggest that TLS sessions can be re-used for intermittent communication in situations where the threat is deemed to be low, but the rate at which they should be renewed can be dynamically scaled up and down to accommodate for differences in threat levels. Another security-by-design approach recommends the usage of security control assignment matrices to determine the types of security controls that should be present in various parts of a system [132].

It is often easier and more effective to create more specific architectural frameworks rather than generic ones, and the investigated literature contains specialized models and methods for various scenarios. The security-by-design approach in [165] specializes in actuating and sensing scenarios, while in [231], the authors introduce an integrated model aimed specifically at mobile e-health applications. Their approach also considers security issues at design time and can be integrated into more generic architectures. Craggs *et al.* [233] target research scenarios, and describe a reference architecture for research testbeds, making the accurate observation that real IIoT scenarios are likely to have a mixture of legacy and new technologies and that security solutions should account for this. In [237], a method for arriving at a security capability-model for IIoT supply-chains is described, as the authors identified that businesses generally lack insight in their own supply chains, which is a security liability. In a comprehensive work, McGinthy and Michaels [242] describe secure architectural frameworks for IIoT and WSN sensor nodes, with security features grouped by energy class. They address many security requirements that should be satisfied for these classes, including data confidentiality, attestable boot procedures, and key management. Bécue *et al.* [23] state that it is necessary to improve the prevention, detection, investigation, and response to adversarial machine learning attempts on AI-powered modules. At the same time, humans and machines should aid in the surveillance of each other; if a human behaves anomalously, machines should be able to detect and report this, and vice versa. They propose using a "cyber-range" approach where digital twins of physical devices are modeled by a team of engineers using feedback from the operators, as well as common design techniques such as risk assessments. These digital twins are then used to simulate more optimized usage scenarios, and red/blue teams perform attack and response scenarios, that help the digital twin learn about how to protect and respond to attacks by itself. Once a digital twin is deemed sufficiently secure it can be used in production settings. This approach requires decisions that steer towards such a model early on in the architectural design process. This is also necessary for the model described by Condry and Nielson [26]. In this model, the authors leverage capabilities of gateways between control systems and the Internet to allow for direct communication between control systems and client devices. Kondeva *et al.* [240] observe that the fields of safety and security engineering are closely related but have their own techniques and methods. They consider that safety and security requirements should not clash with each other and that these should be integrated more tightly. To this end, they introduce a method to generate attack trees from fault tree analysis.

Risk assessment for the IIoT is another field that has seen activity in recent years. In [44] and [126] two risk assessment models for the IIoT are presented. The first is mainly focused on water sewage systems, but has aspects that can be generalized, while the second aims to be general, and utilizes use cases as its input. The authors of [44] state that it

TABLE XII
MODELS AND METHODOLOGIES SECURITY REQUIREMENTS, SOURCES THAT IDENTIFY THESE, AND THEIR INTEREST LEVEL RELATIVE TO THE CATEGORY. THE RELATIVE INTEREST LEVEL IS BASED ON THE PERCENTAGE OF WORKS ADDRESSING THE SPECIFIC SECURITY REQUIREMENT COMPARED TO THE TOTAL NUMBER OF PAPERS FOR THAT CATEGORY

ID	Security requirement	Related sources	Relative interest	% within category
MM-01	adequate risk/threat assessment	[43], [44], [83], [100], [126], [232], [235], [236], [241], [244]	High	33%
MM-02	minimization of overall attack surface	[51]	Low	3%
MM-03	security by design	[23], [26], [41], [42], [51], [132], [230], [231], [234], [240], [242], [243], [245]	High	43%

is not possible to protect against threats without a proper risk assessment. The reason that traditional risk assessment methods are not adequate due to the complexity of integrating all the aspects of an IIoT system, and due to the increased impact factor in IoT environments because of the increased amount of physical assets and ways it can affect human lives. To this end, they propose a 10-phase comprehensive risk assessment method, that is able to capture many relevant aspects. Mouratidis and Diamantopoulu [43] take things even further by proposing a more formal security analysis method for the IIoT. In their method they build on the Secure Tropos language to allow for precise modeling of industrial environments, their security constraints, and relevant threats. They then use graph analysis to trace possible attack paths and identify which devices should satisfy certain security requirements. A more manual approach is taken by Boyes *et al.* [232]. They propose a multidimensional categorization framework, that can help with a better analysis of threats, aside from being useful as a more general categorization framework. They envision that a proper categorization of devices will help with identifying similar threats across different aspects of the IIoT domain.

As resource constraints are often a bottleneck for IIoT systems, it is perhaps surprising that there has not been a lot of work on modeling the overhead these bring. The only such work that was found in the literature is by Ivkic *et al.* [238], and describes an onion layer model that enables one to sum all overhead introduced by security functions.

J. Summary and Discussion

In our survey of the literature on security in the IIoT domain, we have extracted 49 security requirements covered by the investigated works, spread across 8 categories: Authentication, Access Control, Maintainability, Resilience, Data security and data sharing, Security Monitoring, Network Security, and Models and Methodologies. Additionally, we have made an effort to summarize the literature in our discussion.

In this subsection, we summarize the findings discussed in this section in two ways. Firstly, in Table XIII, we lay out the number of works per category, providing a measure of the distribution of the papers across categories. As detailed in Section V, the number of papers addressing each category is taken from Figure 2 as the number of papers appearing in the corresponding level 1 (i.e., subsection) and all level 2 (i.e., subsubsections) nodes, but removing duplicates. Secondly, we summarize all the identified research requirements in Table XIV, listed in reverse order by their popularity based on the total number of investigated works. Note that the overall interest for this table is computed based on the total number of works covered in this survey, and is thus different from earlier tables in this section where it was computed based on the numbers within each category. Table XV lists these new thresholds.

TABLE XIII
DISTRIBUTION OF THE INVESTIGATED PAPERS ACROSS THE CATEGORIES DISCUSSED IN THIS WORK

ID	Category	Papers (N°)	%
A	Authentication	77	27%
AC	Access Control	16	6%
M	Maintainability	15	5%
R	Resilience	16	6%
DSS	Data Security and Data Sharing	58	20%
SM	Security Monitoring	42	15%
NS	Network Security	29	10%
MM	Models and Methodologies	30	11%

A few observations can be made when looking at the popularity of the categories, which are laid out in Table XIII.

Firstly, research interest in Authentication, together with Data Security and Data Sharing appears significantly higher than the other categories. This is interesting because these intuitively also have the most in common with standard IoT scenarios. At the same time, the very IIoT-centered categories of Maintainability and Resilience are some of the least active. We believe that this exposes a promising area for new research.

Access Control has seemingly been of the least interest, perhaps because many of its security requirements and works are already implicitly treated in the Authentication section, and various works present frameworks that provide both, but are discussed in the Authentication category.

Security Monitoring is also fairly popular, with 41 works discussing it in various ways. What stands out about this category is that considering its popularity, there are relatively few (4) different requirements covered in the literature. This stands out even more when looking at Table XIV, where requirement SM-01 is the most popular of all. Further, both SM-01 and DSS-05 have seen significantly more interest than any other requirement. This is perhaps because these requirements are the most open-ended out of all identified requirements, thereby collecting a large variety of works that discuss them.

Finally, the observant eye might notice that in Table XIV the percentages sum up to 92.6%. This is because, throughout the study, roughly 7.4% of the investigated works identify some categories as requirements, meaning they have been included in this work, but do not identify any of the specific security requirements. Therefore, they are included in the category count, but not in the requirement count.

TABLE XIV
POPULARITY OF THE INDIVIDUAL REQUIREMENTS, TAKEN AS A PERCENTAGE OF THE TOTAL NUMBER OF UNIQUE WORKS COVERED IN THIS SURVEY

Overall interest	**ID**	**Security Requirement**	**Category**	**Overall %**
Very High	SM-01	infrastructure monitoring	Security Monitoring	9.5%
	DSS-05	secure external data storage	Data Security and Data Sharing	7.1%
	A-06	mutual authentication	Authentication	4.6%
	MM-03	security by design	Models and Methodologies	4.6%
High	DSS-02	data confidentiality	Data Security and Data Sharing	3.9%
	A-02	key distribution	Authentication	3.5%
	SM-02	threat response	Security Monitoring	3.5%
	NS-07	wireless transmission security	Network Security	3.5%
	MM-01	adequate risk/threat assessment	Models and Methodologies	3.5%
	A-08	minimization of user interaction	Authentication	2.8%
	AC-04	decentralized AC	Access Control	2.8%
Medium	A-01	multi-factor authentication	Authentication	2.5%
	NS-04	network isolation	Network Security	2.5%
	A-07	privacy-preserving authentication	Authentication	2.1%
	NS-05	timeliness	Network Security	2.1%
	NS-06	availability (DoS, jamming, etc.)	Network Security	2.1%
	A-03	node addition, revocation, rekeying	Authentication	1.8%
	A-04	decentralized key management	Authentication	1.8%
	AC-02	fine-grained AC	Access Control	1.8%
	R-01	continuation of operation with compromised subsystems	Resilience	1.8%
	R-03	standards compliance	Resilience	1.8%
	A-10	attestation	Authentication	1.4%
	AC-01	handle dynamic changes	Access Control	1.4%
	M-01	software updateability	Maintainability	1.4%
	M-08	secure status transfer	Maintainability	1.4%
	DSS-04	secure data transport	Data Security and Data Sharing	1.4%
	A-09	non-repudation	Authentication	1.1%
	AC-06	transparency	Access Control	1.1%
	M-02	configuration updateability	Maintainability	1.1%
	M-03	disturbance-free updates	Maintainability	1.1%
	DSS-06	data flow control	Data Security and Data Sharing	1.1%
	DSS-07	data protection legislation compliance	Data Security and Data Sharing	1.1%
	SM-04	security policy enforcement	Security Monitoring	1.1%
	NS-01	dynamicity of configuration	Network Security	1.1%
Low	AC-03	centralized AC	Access Control	0.7%
	AC-05	privacy-preserving AC	Access Control	0.7%
	M-05	traceability	Maintainability	0.7%
	M-06	compatibility	Maintainability	0.7%
	R-02	operation with intermittent connectivity	Resilience	0.7%
	NS-03	management overhead minimization	Network Security	0.7%
	A-05	transitive authentication	Authentication	0.3%
	AC-07	compatibility	Access Control	0.3%
	M-04	usability of update process	Maintainability	0.3%
	M-07	transparency	Maintainability	0.3%
	DSS-01	data loss mitigation	Data Security and Data Sharing	0.3%
	DSS-03	standardization	Data Security and Data Sharing	0.3%
	SM-03	handle heterogeneous sources	Security Monitoring	0.3%
	NS-02	security policy enforcement	Network Security	0.3%
	MM-02	minimization of overall attack surface	Models and Methodologies	0.3%

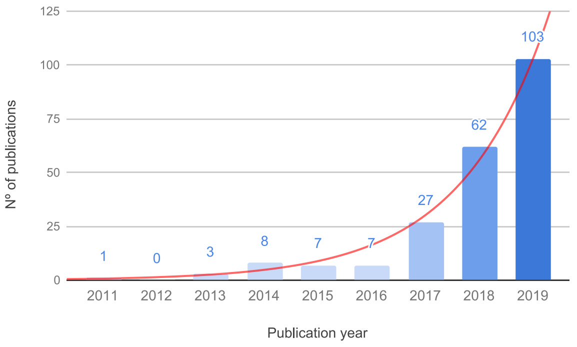

Fig. 4. Number of publications per year.

VI. Quantitative Results

In this section, we provide a quantitative analysis of the set of studies resulting from the presented research.

In particular, we address research questions (RQ2)-(RQ4) by analyzing the number of publications related to IIoT security over the years, the geographical distribution of these studies, and the favorite publication venues.

TABLE XV
INTEREST LEVELS ASSIGNED TO SECURITY REQUIREMENTS AND WEIGHTED ON THE COVERAGE OF EACH CATEGORY, APPLICABLE TO TABLE XIV

Weighted interest	**Range (x)**
Low	$0\% \leq x \leq 1.0\%$
Medium	$1.0\% < x \leq 2.5\%$
High	$2.5\% < x \leq 4.0\%$
Very High	$4.0\% < x \leq 100\%$

A. Spread of Publications Throughout the Years (RQ2)

Figure 4 shows the number of publications between 2011 and 2019. Security research for the IIoT starts first appearing around 2011, being initially dormant but slowly growing from 2013 onward. In 2017, a drastic increase in activity can be seen. While it is tempting to attribute this growth to the fact that 2016 saw several serious IoT and

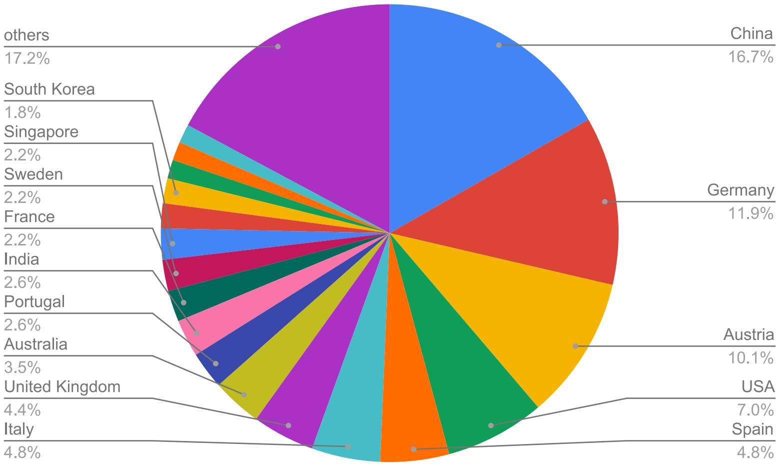

Fig. 5. Demographic: geographical distribution of research activity based on first author's country of affiliation.

industry related security incidents (such as Mirai [4] and Crashoverride/Industroyer [6]), which served to illustrate the importance of security on these devices, it should be noted that this is in line with the overall growth of IoT as a research area. In 2018 and 2019, the growth in activity continued, showing that the research community deems IIoT security to be of high importance.

B. Geographical Distribution of IIoT Security Research (RQ3)

The geographical distribution of research activity is shown in Figure 5. The data for this was obtained by extracting the country of affiliation of the first author of the considered studies.

German-speaking countries are strongly represented, making for a total of 22% of contributions. One possible explanation is that one of our search terms, *Industry 4.0*, was originally coined by the German government [253], thus, it might have seen higher adoption in German-speaking countries. This raises the question of whether our search terms were successful in providing a good global sample of studies in this field. We believe they were, since the field we are considering is very narrow; we specifically searched for *Industrial* challenges in order to be able to extract security requirements unique to this field. Furthermore, we have conducted reverse snowball sampling to ensure a fair research scope.

China and the United States of America are the two other major contributors. This can be attributed to the size of their industries and thus the relevance of research in this area. However, interestingly, 54% of the studies originate from Europe, showing that this topic is also regarded as highly relevant in countries with smaller industries.

The 'others' group consists of the 23 countries that have 3 or fewer publications in this field: Algeria, Belgium, Brazil, Czech Republic, Finland, Greece, Hungary, Iran, Ireland, Japan, Malaysia, Morocco, New Zealand, Norway, Pakistan, Qatar, Romania, Russia, Saudi Arabia, Serbia, Taiwan, Turkey, Ukraine.

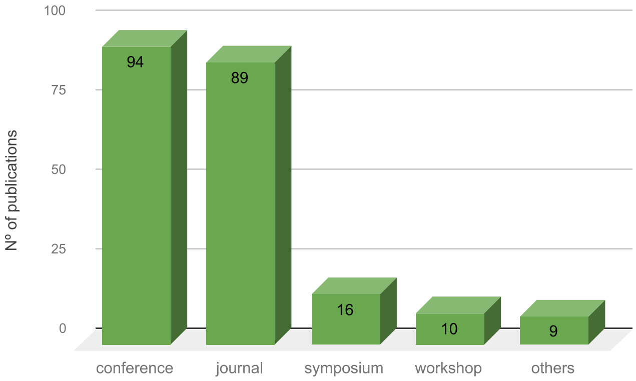

Fig. 6. Popularity of different venue types.

C. Venue Types for Publication (RQ4)

We have grouped the studies based on the venue type of their publication, which is shown in Figure 6. As can be seen, conference proceedings are the most popular dissemination method, followed by journals. The 'others' category consists of venue types in which 4 or fewer publications were published: congresses, summits, and forums.

Looking at the specific venues of publication (Figure 7), it can be seen that the IEEE Transactions on Industrial Informatics journal is by far the most popular venue, with 25 publications. One noteworthy observation here is that, out of all considered studies, only 16 were published in venues focused on security. The vast majority of IIoT security-related works appears to be published in venues targeting industrial systems or IoT instead.

VII. Opportunities Enabled by Fog Computing

In Section V, we have extracted security requirements for the IIoT from the investigated literature and discussed a number of challenges that stand in the way of the adoption of conventional solutions to address these requirements. In this section, we reflect on the challenges and discuss how Fog computing shows promise as a remedy to a number of those.

It is important to note that Fog computing is a relatively new paradigm the exact definition of which is still being debated

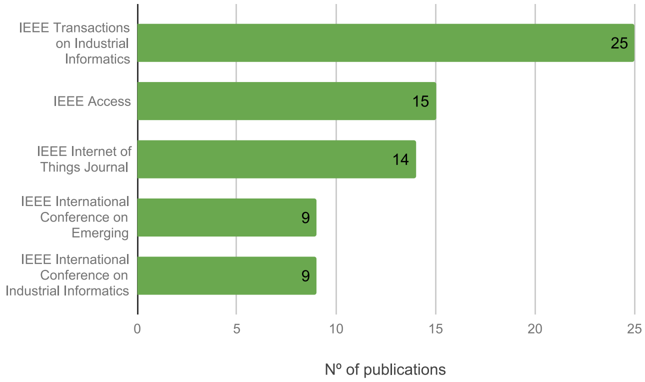

Fig. 7. Popularity of specific venues for publications.

in the scientific community and often intersects with similar paradigms, such as Edge computing, Mobile Edge computing, and Mobile Cloud computing. To maintain consistency with earlier work, we use the definition of Fog computing as used in [254]; a paradigm that extends the Cloud and integrates Edge and IoT, while providing a new, horizontally scalable highly virtualized layer that distributes computing, storage, control, and networking capabilities across the Cloud-To-Things spectrum [8]. For a more detailed treatise on the differences between Fog, Edge, and other paradigms we refer the interested reader to [254].

Also, we are aware that a comprehensive and thorough discussion on how Fog computing could tackle the IIoT security requirements would require a dedicated treatment that would result in an entire paper itself, which is out of the scope of this work (for instance, in [255] we focus on how Cloud requirements can impact IoT). Thus, the aim of this section is to provide food for thought on the topic and a source of inspiration for future research, rather than an exhaustive analysis.

In detail, we first give the definition of Fog computing assumed in this work. Then, we revisit the majority of topics covered in Section V and depicted in Figure 8: authentication, access control, maintainability, resilience, data security and data sharing, security monitoring, and network security. For each of these, we discuss how we envision what Fog-enabled solutions might look like and suggest potential research opportunities, but we leave confirmation of the validity of these ideas as a topic for further research. We close the section with a discussion on limitations and open challenges for Fog computing.

A. Fog Computing

Fog computing is a relatively recent computing paradigm born from the necessity to provide the missing link in the Cloud-to-Thing continuum [8].

According to the IEEE standard 1934-2018 [256], Fog computing is "a horizontal, system-level architecture that distributes computing, storage, control, and networking functions closer to the users along a cloud-to-thing continuum". Thus, Fog computing can be considered as an extension of Cloud computing that distributes the benefits of the Cloud closer to the IIoT and across multiple layers of the network topology.

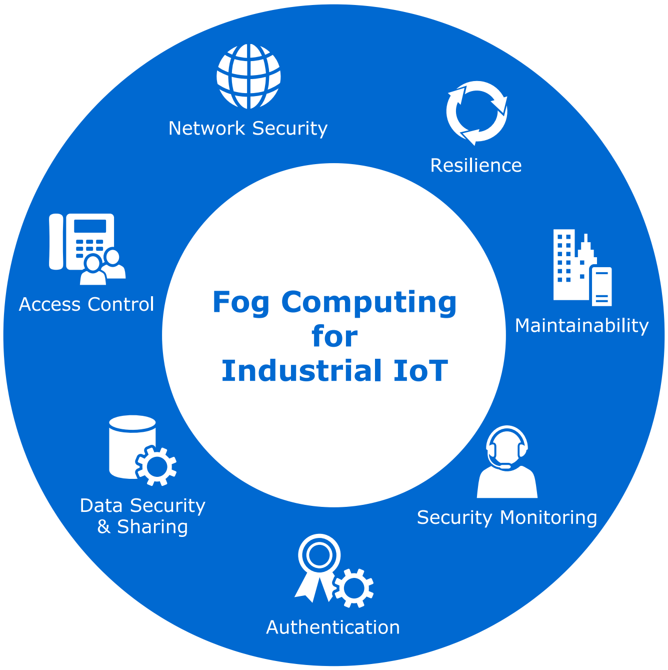

Fig. 8. Fog computing opportunities for IIoT security.

Any system that wants to be compliant with the aforementioned definition of Fog computing needs to present the following attributes, also referred to as pillars: security, scalability, openness, autonomy, reliability, availability, serviceability, agility, hierarchy, and programmability. A thorough discussion of these pillars can be found in [8], [256].

In this setting, the fog node is "the physical and logical network element that implements fog computing services" [8]. Since Fog nodes can be placed on-premises, they can be accessed by devices even when the connection to the outside world is failing. This helps us in identifying research opportunities for issues arising from intermittent connectivity. Note that this can be generalized: if there is a connection failure anywhere on the route from the (local) Fog node to the (remote) Cloud, then all Fog nodes that are positioned *before* the unreachable hop are still reachable and thus able to provide the local system with their services.

B. Fog-Enabled Authentication

When looking at the authentication challenges discussed in Section V-B, it can be observed that there are a number of points where a Fog node can be helpful in addressing them.

A first intuitive way of applying Fog computing to these challenges can be found by considering existing authentication solutions that require third-party servers in their setup or execution, such as [63], [86], [93]. A Fog node fits the requirements for these servers perfectly, as it is not severely restrained by computational or energy resources, is on-premises, and has very low response times. If Fog computing nodes are considered as part of the infrastructure, many of the issues with relying on a third-party server are thus addressed "for free".

Secondly, Fog nodes can serve to enhance traditional PKI infrastructures, where Fog nodes can act as "certificate authorities" for local devices or help establish a federated and robust key infrastructure through, e.g., peer-to-peer networking capabilities with other Fog nodes. To our knowledge, no work investigating this currently exists.

In dynamic environments, Fog nodes can potentially help alleviate issues relating to node addition, removal, and rekeying as well. For example, it could serve as a trusted "gateway" to which Edge devices are paired, preventing them from communicating directly with any other system. This is not unlike how Bluetooth devices can be paired with smartphones and other devices. Node addition, removal, and rekeying can then be handled from the Fog node.

As we have seen in Section V-B2, some proposed solutions require biometric features ([72], [77]), smart cards ([72]) or NFC tags ([36], [37], [67], [225]), in the authentication process. Also here there is potential for Fog nodes: not every lightweight system might be equipped with the necessary sensors for this. However, it might be possible to equip Fog nodes with sensors and use them as proxies for sensor readings. This would increase scalability, as a Fog node can be positioned so that it is more easily accessible than the Edge devices connected to it. Thus, if maintenance engineers would want to, e.g., authenticate updates for the devices by using NFC keys or biometrics, they will only need to seek out the Fog node and present the relevant keys to it, as opposed to seeking out every relevant device separately.

Fog nodes might also enable the possibility of bringing TPM and/or TEE capabilities to Edge devices that do not contain these modules themselves. For that to be possible, the Edge devices need to set up a trusted channel between the Fog node's TPM/TEE module, which could be possible through some form of a key setup protocol that involves a one-time pairing step. Fog nodes could be equipped with multiple TPM or TEE modules to serve more than one Edge device (or itself) at the same time, such as the recently introduced Intel SGX cards [257]. Trusted hardware capabilities in Fog nodes can also be used for attestation purposes in various settings (against remote Fog nodes, against Edge devices, and so on). We expect that there are a lot of fruitful research directions for the combination of Fog nodes and trusted hardware.

C. Fog-Enabled Access Control

As with authentication, Fog nodes have the potential for enhancing AC challenges in industrial scenarios.

Firstly, some AC policies could be outsourced from extremely resource-constrained devices to a Fog node (e.g., accessing sensitive files from a central repository), or if the scenario is suited for it, AC can be managed completely by a Fog node. Another identified challenge for AC frameworks is that while managing policies centrally gives more flexibility, it introduces new risks due to the central server now being a single point of failure. Fog nodes could provide a "hybrid" middle ground where AC is federated between various Fog nodes on-premises, and that Edge devices can then query these Fog nodes, thus increasing the overall reliability and scalability. To the best of our knowledge, this is still an open research area.

As mentioned in Section V-C, compatibility with legacy devices is another issue in the IIoT. Fog nodes could act as a bridge between newer devices and legacy devices with poor security, keeping them sufficiently isolated from the wider network and providing security measures where necessary in exposed interfaces, possibly through a ZTN approach.

D. Fog-Enabled Maintainability

Fog computing can bring large benefits to the maintainability of industrial systems.

By their very nature, industrial systems are connected to the Internet, and thus enable the possibility of managing software and configuration updates for attached Edge devices. Fog nodes are perfectly situated to verify the validity of such updates and perform in-depth tests such as performing the updates in a sandboxed environment and then observing for anomalies before deploying them on real devices, while at the same time allowing for the application of updates with minimal disturbance to the services themselves. In practice, this would turn the solution proposed by [111] into a Fog application.

Fog nodes also provide an ideal target platform for an "industrial app marketplace" such as proposed in [113]. It is not difficult to envision a system where a Fog node would allow users to view software packages together with their version number and update information for all connected devices, in an ordered and user-friendly way. Moreover, Fog nodes could go further and allow for management of configuration files for connected Edge devices as well. For example, one could think of an application where configuration files are retrieved from a Cloud service, verified by the Fog node and subsequently delivered to specified Edge devices, filling in sensitive information fields as necessary so as to prevent the Cloud from requiring access to this information.

As Fog nodes could provide an easily accessible location for the reading of NFC tags or other hardware authentication modules, one could easily extend maintenance processes with those extra authentication factors without requiring engineers to physically attend to each affected device individually.

The ideas described here are merely speculative, and there is plenty of room for research in any of these areas. We expect a variety of maintainability-enhancing applications of Fog computing will be identified and researched in the future.

E. Fog-Enabled Resilience

Fog nodes could act as reactive security agents, isolating or disabling connected devices when they appear compromised. This allows security personnel to then further investigate the issue, while the system itself can continue operations. This is also discussed in [258], where a number of Fog use-cases and research challenges are listed. The authors state that automatic fault detection and reconfiguration is essential, and identify the potential for Fog nodes to do this autonomously, but state that this is a challenging topic that requires addressing. However, a solution to this challenge would enable resiliency as it is defined by the ICS.

A second challenge that can be overcome through Fog computing, is maintaining normal operation through intermittent Internet connectivity. To an extent, a Fog node can take over processes normally executed in the Cloud. Thus, when the connection to the Cloud fails, the operational capability of Edge devices is not affected. Related to this, some devices continuously or periodically need to transmit data to the cloud, where it can then be processed. If this were done directly, data loss is a risk in case of intermittent connectivity. As an alternative to introducing some data storage capabilities on the Edge devices themselves, a Fog node could collect data from the devices, and forward it to the Cloud. Then, when there is no connection to the Internet, the Fog node can act as a buffer and send the buffered information upwards to the Cloud once the connection is restored. This way, Edge devices do not need to worry about failing Internet connectivity at all.

Finally, Fog nodes and their application-independent software can be developed to satisfy resiliency-related indicator points, which in turn can aid in providing contractual service guarantees as is currently often seen in Cloud service agreements.

F. Fog-Enabled Data Security and Data Sharing

Whenever it is necessary for a device to access sensitive data that should be stored securely, this requires the device to firstly have the storage capacity, and secondly the means to secure this data at rest. For lightweight systems that do not have the capacity to store and secure data securely, Fog nodes can provide a solution; they are not tied to severe resource constraints and can be equipped with ample storage and computational capacity for common encryption methods. Additionally, Fog nodes can be deployed on the local network, meaning data will never have to leave the premises. Even for extremely large amounts of data, Fog nodes could act as middleware between external Cloud storage, and encrypt/decrypt data stored in the Cloud transparently, e.g., using the techniques described in [149], [159]. To the Edge devices, it can be presented as originating from the Fog node, and they do not need to be aware of the underlying storage and security mechanisms.

As Fog nodes can be positioned between Edge devices and external parties as gateways, this also unlocks the opportunity to secure and control data flow to these external parties. A Fog node can set up and maintain highly secure, authenticated channels with remote parties, potentially alleviating some of the challenges involved in designing lightweight Edge devices that need to interact with these parties, as they only need to concern themselves with secure communication with the Fog node. If the Fog node additionally has the ability to access the message content of traffic passing through it, it can enforce data flow policies, e.g., as described in [164], allowing fine-grained data security mechanisms on top of encryption techniques.

In Section V-F4 we stated that the protection of sensitive data is in many cases now a legal requirement in the European Union. Fog nodes present a very natural way of meeting these requirements, as they can store data locally, while at the same time allowing for fine-grained data sharing with third parties, should a user allow this. Moreover, it can become easier to manage user rights such as the right to be forgotten.

G. Fog-Enabled Security Monitoring

Because Fog nodes can take on central positions in Industrial networks, they provide a great platform for security monitoring solutions.

For example, a Fog node could run IDS software to detect anomalies or attack signatures. This also provides an opportunity for the Fog and Cloud to augment each other. Intrusion detection models could be trained in a Cloud environment, while executed on a Fog node, thereby addressing the latency issues normally apparent in Cloud solutions. Examples of this can be found in [115], [193]. Because Fog nodes stand in direct connection to sensor devices, they can also perform simple anomaly detection techniques such as ensuring that sensor values are within a certain value range, without adding overhead to the sensors themselves.

Another use of Fog nodes as a security monitoring tool could be the deployment of an anti-malware for IoT devices that is supported by the Fog infrastructure [259]. Indeed, De Donno *et al.* [260], [261] propose an anti-malware software for IoT and they discuss how the use of Fog computing helps to solve some of the challenges intrinsic in the deployment.

Fog nodes can also potentially take action based on incoming traffic patterns, enabling the mitigation of DoS attacks aimed at very specific devices, even when those devices are not able to protect themselves against those attacks. This also presents the opportunity for dynamic traffic shaping, and other techniques that might help reduce battery consumption on lightweight IoT devices connected to the Fog node.

H. Fog-Enabled Network Security

Also in network infrastructure, Fog computing can potentially help in overcoming current challenges.

With the rise of SDN and NFV technologies, Fog nodes can possibly play a role as a platform for some of these. For example, they can create isolated network environments between themselves and each connected device.

Fog nodes could also be equipped to handle TSN standards when there is a need for deterministic and timely delivery of network traffic between two connected devices. By moving the management of these interfaces to a Fog node, opportunities are created for easier (remote) management and reconfiguration of time-critical systems, even going so far as to move entire control applications to Fog nodes. As an extreme manifestation of this vision, one could imagine “plug-and-play” industrial hardware that can be connected to a Fog node which will then autonomously configure and use it.

We also see opportunities for Fog nodes to improve the availability of critical services, in two ways. Firstly, Fog nodes could run critical applications in a federated fashion, allowing migration or load balancing of tasks between them. This way, the application only becomes unavailable when all participating Fog nodes fail. Secondly, a Fog node can act as a middleware for a critical service running in the Cloud. By deploying this service on multiple Cloud providers, Edge applications relying on it will not be affected by the outage of any one cloud provider; the Fog node can automatically route requests to the remaining available providers.

Finally, Fog nodes could potentially aid in securing wireless infrastructure, by incorporating wireless technologies in security monitoring solutions. This way, jamming attacks or other anomalies in the wireless spectrum can be detected.

I. Challenges and Limitations

Fog computing is not a panacea capable of filling any Cloud-IIoT gap without much issue. The paradigm is very much in its early stages, and deployment so far has been extremely limited. Open challenges include practical federation frameworks, resource offloading, and resilience [262]. While we believe that solutions to these challenges are capable of satisfying the security requirements collected in this work, we acknowledge that every solution comes with its own tradeoffs, and a thorough analysis of the benefits and drawbacks of Fog computing can only be done once enough Fog-based systems exist to investigate. Nevertheless, one can attempt to make an analysis based on the current state-of-the-art. Thus, in this section, we briefly discuss what we consider some of the biggest potential drawbacks.

Firstly, Fog systems add extra workload to maintenance personnel, and will likely require special training, making it more costly than the Cloud. Whereas Cloud infrastructure is maintained by a specialized team on the Cloud service provider's end, the Fog paradigm shifts this responsibility to users of the system. The spread of functionality across the Cloud-to-Things continuum potentially complicates this even more. If a security issue is found in a well-known piece of Fog infrastructural software, it is the responsibility of maintainers *at every point in the continuum* to update their software, as opposed to having to update just the Cloud infrastructure, which is managed by one entity. If one maintainer of a Fog node fails to do this within an appropriate time-window, this can put all entities making use of that node at risk.

Secondly, incident response might be hampered by the distributed nature of Fog systems. We believe this might manifest itself in multiple ways: necessary security expertise might not be available on-site, and specialized incident response teams will have to be called in from external parties. Further, complex incidents might require cooperation between multiple entities along the continuum for forensic analysis, which might not always be possible or add a lot of overhead.

Finally, compatibility between Fog nodes can potentially be a huge issue. If standards are not well-defined or not followed rigorously, it will be very hard to meet the harsh requirements set by industrial environments with nodes from different providers that cannot interoperate efficiently and accurately. This, in turn, can negatively impact the ability to federate and offload tasks to other nodes in the local network, as well as potentially violate security policies if some nodes in the system are unable to uphold the necessary requirements.

VIII. Conclusion

In this work, we have performed a systematic literature review about security for the IIoT.

As in any mapping study, it is challenging to take all studies of the field into account, but it is more important to have a good representation of studies rather than a high number of studies [20]. To achieve a good representation, we have methodologically constructed the search queries and queried multiple literature repositories. After that, we utilized reverse snowball sampling to further increase the quality, and to mitigate any possible selection bias. Our initial search queries resulted in 356 possibly relevant papers, which we brought down to a selection of 218 papers through the use of a systematic approach comprised of several phases. These papers were fully read and analyzed for the purposes of this study.

At glance, the work has elaborated around four main research questions: (RQ1) what security requirements exist for the IIoT, (RQ2) how scientific publications about IIoT security are spread during the years, (RQ3) how IIoT security research activity is geographically distributed, and (RQ4) what publication venues are the most popular for IIoT security.

First, we have answered question RQ1 by extracting security requirements for the IIoT from the investigated works and exploring them, along with the related challenges that make these requirements hard to meet with existing solutions and a measure of their interest in the research community. Then, we have addressed questions (RQ2)-(RQ4) by providing a quantitative analysis of the investigated IIoT security research. Finally, we provided a discussion on how Fog computing can play a role in meeting the requirements posed by industrial environments, by taking a Fog computing perspective and revisiting the requirements that were extracted during our investigation, as well as pointing out what limitation and challenges still need to be faced to achieve massive Fog computing deployment.

This work identifies an abundance of research opportunities in the IIoT security area and shows that Fog computing, as a rising computing paradigm, can become a powerful tool in securing a variety of connected industrial environments, once its limitations and challenges are overcome.

References

[1] P. Daugherty and B. Berthon, “Winning with the industrial Internet of Things: How to accelerate the journey to productivity and growth,” Accenture, Dublín, Ireland, Rep., 2015.

[2] N. Dragoni, A. Giaretta, and M. Mazzara, “The Internet of hackable things,” in *Proc. 5th Int. Conf. Softw. Eng. Defence Appl.*, 2017, pp. 129–140.

[3] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, “Analysis of DDoS-sapable IoT malwares,” in *Proc. IEEE Feder. Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, 2017, pp. 807–816.

[4] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, “DDoS-capable IoT malwares: Comparative analysis and Mirai investigation,” *Security Commun. Netw.*, vol. 2018, Feb. 2018, Art. no. 7178164.

[5] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May/Jun. 2011.

[6] R. Lee, “CRASHOVERRIDE: Analysis of the threat to electric grid operations,” Dragos Inc., Hanover, MD, USA, Rep. TR-2018-19, 2017.

[7] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the Internet of Things,” in *Proc. ACM 1st Ed. MCC Workshop Mobile Cloud Comput. (MCC)*, 2012, pp. 13–16.

[8] “OpenFog reference architecture for fog computing,” OpenFog Consortium, Fremont, CA, USA, Rep. OPFRA001.020817, Feb. 2017. [Online]. Available: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf

[9] “Good practices for security of Internet of Things in the context of smart manufacturing,” ENISA, Heraklion, Greece, Rep. TP-04-18-940-EN-N, 2018.

[10] X. Yu and H. Guo, "A survey on IIoT security," in *Proc. IEEE VTS Asia–Pac. Wireless Commun. Symp. (APWCS)*, 2019, pp. 1–5.

[11] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019.

[12] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.

[13] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.

[14] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for industry 4.0 in the current literature: A reference framework," *Comput. Ind.*, vol. 103, pp. 97–110, Dec. 2018.

[15] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[16] F. Hofer, "Architecture, technologies and challenges for cyber-physical systems in industry 4.0: A systematic mapping study," in *Proc. 12th ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas. (ESEM)*, 2018, pp. 1–10.

[17] A. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd Annu. Design Autom. Conf. (DAC)*, 2015, pp. 1–6.

[18] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[19] G. Hansch, P. Schneider, K. Fischer, and K. Böttinger, "A unified architecture for industrial IoT security requirements in open platform communications," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2019, pp. 325–332.

[20] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[21] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," EBSE, Goyang, South Korea, Rep. EBSE-2007-01, 2007.

[22] J. Beel and B. Gipp, "Google scholar's ranking algorithm: An introductory overview," in *Proc. 12th Int. Conf. Scientometrics Informetrics (ISSI)*, 2009, pp. 439–446.

[23] A. Bécue *et al.*, "Cyberfactory#1—Securing the industry 4.0 with cyber-ranges and digital twins," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, 2018, pp. 1–4.

[24] M. Beltrán, M. Calvo, and S. González, "Federated system-to-service authentication and authorization combining PUFs and tokens," in *Proc. 12th Int. Symp. Reconfig. Commun. Centric Syst. Chip (ReCoSoC)*, 2017, pp. 1–8.

[25] A. Bicaku *et al.*, "Towards trustworthy end-to-end communication in industry 4.0," in *Proc. IEEE 15th Int. Conf. Ind. Informat. (INDIN)*, 2017, pp. 889–896.

[26] M. W. Condry and C. B. Nelson, "Using smart edge IoT devices for safer, rapid response with industry IoT control operations," *Proc. IEEE*, vol. 104, no. 5, pp. 938–946, 2016.

[27] J. Delsing, "Local cloud Internet of Things automation: Technology and business model features of distributed Internet of Things automation solutions," *IEEE Ind. Electron. Mag.*, vol. 11, no. 4, pp. 8–21, Dec. 2017.

[28] A. Esfahani *et al.*, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.

[29] C. Esposito, A. Castiglione, B. Martini, and K. R. Choo, "Cloud manufacturing: Security, privacy, and forensic concerns," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 16–22, Jul./Aug. 2016.

[30] C. Esposito, A. Castiglione, F. Palmieri, and A. D. Santis, "Integrity for an event notification within the industrial Internet of Things by using group signatures," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3669–3678, Aug. 2018.

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

[32] X. Jiang, Z. Pang, M. Luvisotto, F. Pan, R. Candell, and C. Fischione, "Using a large data set to improve industrial wireless communications: Latency, reliability, and security," *IEEE Ind. Electron. Mag.*, vol. 13, no. 1, pp. 6–12, Mar. 2019.

[33] E. Kail, A. Banati, E. Lászlo, and M. Kozlovszky, "Security survey of dedicated IoT networks in the unlicensed ISM bands," in *Proc. IEEE 12th Int. Symp. Appl. Comput. Intell. Informat. (SACI)*, 2018, pp. 449–454.

[34] S. Katsikeas *et al.*, "Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2017, pp. 1193–1200.

[35] T. Kumar, A. Braeken, V. Ramani, I. Ahmad, E. Harjula, and M. Ylianttila, "SEC-blockEdge: Security threats in blockchain-edge based industrial IoT networks," in *Proc. 11th Int. Workshop Resilient Netw. Design Model. (RNDM)*, 2019, pp. 1–7.

[36] C. Lesjak, T. Ruprechter, H. Bock, J. Haid, and E. Brenner, "ESTADO—Enabling smart services for industrial equipment through a secured, transparent and ad-hoc data transmission online," in *Proc. IEEE 9th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, 2014, pp. 171–177.

[37] C. Lesjak, T. Ruprechter, J. Haid, H. Bock, and E. Brenner, "A secure hardware module and system concept for local and remote industrial embedded system identification," in *Proc. IEEE Emerg. Technol. Factory Autom. (ETFA)*, 2014, pp. 1–7.

[38] C. Lesjak *et al.*, "Securing smart maintenance services: Hardware-security and TLS for MQTT," in *Proc. IEEE 13th Int. Conf. Ind. Informat. (INDIN)*, 2015, pp. 1243–1250.

[39] C. Lesjak, D. Hein, and J. Winter, "Hardware-security technologies for industrial IoT: Trustzone and security controller," in *Proc. 41st Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, 2015, pp. 2589–2595.

[40] C. Lesjak, H. Bock, D. Hein, and M. Maritsch, "Hardware-secured and transparent multi-stakeholder data exchange for industrial IoT," in *Proc. IEEE 14th Int. Conf. Ind. Informat. (INDIN)*, 2016, pp. 706–713.

[41] Z. Ma, A. Hudic, A. Shaaban, and S. Plosz, "Security viewpoint in a reference architecture model for cyber-physical production systems," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS PW)*, 2017, pp. 153–159.

[42] S. Maksuti, A. Bicaku, M. Tauber, S. Palkovits-Rauter, S. Haas, and J. Delsing, "Towards flexible and secure end-to-end communication in industry 4.0," in *Proc. IEEE 15th Int. Conf. Ind. Informat. (INDIN)*, 2017, pp. 883–888.

[43] H. Mouratidis and V. Diamantopoulou, "A security analysis method for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4093–4100, Sep. 2018.

[44] E. T. Nakamura and S. L. Ribeiro, "A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems," in *Proc. IEEE Global Internet Things Summit (GIoTS)*, 2018, pp. 1–6.

[45] M. Niedermaier, F. Fischer, and A. von Bodisco, "PropFuzz—An it-security fuzzing framework for proprietary ICs protocols," in *Proc. IEEE Int. Conf. Appl. Electron. (AE)*, 2017, pp. 1–4.

[46] Y. Nozaki and M. Yoshikawa, "Countermeasure of lightweight physical unclonable function against side-channel attack," in *Proc. Cybersecurity Cyberforensics Conf. (CCC)*, 2019, pp. 30–34.

[47] "2018 OWASP IoT top 10," OWASP, Rockville, MD, USA, Rep., Dec. 2018. [Online]. Available: https://www.accenture.com/t00010101T000000Z__w__/it-it/_acnmedia/PDF-5/Accenture-Industrial-Internet-of-Things-Positioning-Paper-Report-2015.pdf

[48] M. S. Pardeshi and S. Yuan, "SMAP fog/edge: A secure mutual authentication protocol for fog/edge," *IEEE Access*, vol. 7, pp. 101327–101335, 2019.

[49] T. Pereira, L. Barreto, and A. Amaral, "Network and information security challenges within industry 4.0 paradigm," *Procedia Manuf.*, vol. 13, pp. 1253–1260, Jun. 2017.

[50] D. Preuveneers, W. Joosen, and E. Ilie-Zudor, "Data protection compliance regulations and implications for smart factories of the future," in *Proc. IEEE 12th Int. Conf. Intell. Environ. (IE)*, 2016, pp. 40–47.

[51] G. Shaabany and R. Anderl, "Security by design as an approach to design a secure industry 4.0-capable machine enabling online-trading of technology data," in *Proc. IEEE Int. Conf. Syst. Sci. Eng. (ICSSE)*, 2018, pp. 1–5.

[52] T. Ulz, T. Pieber, C. Steger, S. Haas, and R. Matischek, "Secured remote configuration approach for industrial cyber-physical systems," in *Proc. IEEE Ind. Cyber Phys. Syst. (ICPS)*, 2018, pp. 812–817.

[53] K. Wallis, F. Kemmer, E. Jastremskoj, and C. Reich, "Adaption of a privilege management infrastructure (PMI) approach to industry 4.0," in *Proc. 5th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, 2017, pp. 101–107.

[54] Z. Yang, J. He, Y. Tian, and J. Zhou, "Faster authenticated key agreement with perfect forward secrecy for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6584–6596, Oct. 2020.

[55] L. Zhou, K.-H. Yeh, G. Hancke, Z. Liu, and C. Su, "Security and privacy for the industrial Internet of Things: An overview of approaches to safeguarding endpoints," *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 76–87, Sep. 2018.

[56] O. Bergmann, S. Gerdes, and C. Bormann, "Simple keys for simple smart objects," in *Proc. Workshop Smart Object Security*, 2012, pp. 172–182.

[57] U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for wireless sensor networks," in *Proc. 3rd Int. Conf. Commun. Syst. Softw. Middleware Workshops (COMSWARE)*, 2008, pp. 791–798.

[58] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN compressed DTLS for CoAP," in *Proc. IEEE 8th Int. Conf. Distrib. Comput. Sensor Syst.*, 2012, pp. 287–289.

[59] D. Airehrour, J. Gutierrez, and S. K. Ray, "Securing RPL routing protocol from blackhole attacks using a trust-based mechanism," in *Proc. IEEE 26th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, 2016, pp. 115–120.

[60] A. AlAbdullatif, K. AlAjaji, N. S. Al-Serhani, R. Zagrouba, and M. AlDossary, "Improving an identity authentication management protocol in IIoT," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Security (ICCAIS)*, 2019, pp. 1–6.

[61] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial IoT," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2019, pp. 1173–1180.

[62] S. Blanch-Torné, F. Cores, and R. M. Chiral, "Agent-based PKI for distributed control system," in *Proc. IEEE World Congr. Ind. Control Syst. Security (WCICSS)*, 2015, pp. 28–35.

[63] M. H. Eldefrawy, N. Pereira, and M. Gidlund, "Key distribution protocol for industrial Internet of Things without implicit certificates," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 906–917, Feb. 2019.

[64] K. Huang *et al.*, "Building redactable consortium blockchain for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3670–3679, Jun. 2019.

[65] D. W. McKee, S. J. Clement, J. Almutairi, and J. Xu, "Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems," *CAAI Trans. Intell. Technol.*, vol. 3, no. 2, pp. 75–82, 2018.

[66] D. W. McKee, S. J. Clement, J. Almutairi, and J. Xu, "Massive-scale automation in cyber-physical systems: Vision & challenges," in *Proc. IEEE 13th Int. Symp. Auton. Decentralized Syst. (ISADS)*, 2017, pp. 5–11.

[67] T. Ulz, T. Pieber, C. Steger, S. Haas, H. Bock, and R. Matischek, "Bring your own key for the industrial Internet of Things," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, 2017, pp. 1430–1435.

[68] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," *Inf. Syst. Front.*, vol. 17, no. 2, pp. 261–274, 2015.

[69] L. Marchegiani and I. Posner, "Long-term driving behaviour modelling for driver identification," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, 2018, pp. 913–919.

[70] F. Al-Turjman and S. Alturjman, "Context-sensitive access in industrial Internet of Things (IIoT) healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2736–2744, Jun. 2018.

[71] P. Autenrieth, C. Lörcher, C. Pfeiffer, T. Winkens, and L. Martin, "Current significance of it-infrastructure enabling industry 4.0 in large companies," in *Proc. IEEE Int. Conf. Eng. Technol. Innov. (ICE/ITMC)*, 2018, pp. 1–8.

[72] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[73] B. D. Deebak, F. Al-Turjman, M. Aloqaily, and O. Alfandi, "An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT," *IEEE Access*, vol. 7, pp. 135632–135649, 2019.

[74] S. Garg, K. Kaur, G. Kaddoum, and K. R. Choo, "Towards secure and provable authentication for Internet of Things: Realizing industry 4.0," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4598–4606, May 2020.

[75] S. Hussain and S. A. Chaudhry, "Comments on 'biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment'," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10936–10940, Dec. 2019.

[76] K. K. Kolluru, C. Paniagua, J. van Deventer, J. Eliasson, J. Delsing, and R. J. DeLong, "An AAA solution for securing industrial IoT devices using next generation access control," in *Proc. IEEE Ind. Cyber Phys. Syst. (ICPS)*, 2018, pp. 737–742.

[77] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018.

[78] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, "A robust and energy efficient authentication protocol for industrial Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018.

[79] M. Loske, L. Rothe, and D. G. Gertler, "Context-aware authentication: State-of-the-art evaluation and adaption to the IIoT," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, 2019, pp. 64–69.

[80] Z. Ma *et al.*, "EmIr-Auth: Eye-movement and Iris based portable remote authentication for smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6597–6606, Oct. 2020.

[81] Q. Tian *et al.*, "New security mechanisms of high-reliability IoT communication based on radio frequency fingerprint," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7980–7987, Oct. 2019.

[82] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Netw.*, vol. 20, pp. 1–15, Sep. 2014.

[83] R. Ankele, S. Marksteiner, K. Nahrgang, and H. Vallant, "Requirements and recommendations for IoT/IIoT models to automate security assurance through threat modelling, security analysis and penetration testing," in *Proc. 14th Int. Conf. Availability Rel. Security (ARES)*, 2019, pp. 1–8.

[84] F. Fraile, T. Tagawa, R. Poler, and A. Ortiz, "Trustworthy industrial IoT gateways for interoperability platforms and ecosystems," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4506–4514, Dec. 2018.

[85] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3701–3711, Aug. 2018.

[86] F. Li, J. Hong, and A. A. Omala, "Efficient certificateless access control for industrial Internet of Things," *Future Gener. Comput. Syst.*, vol. 76, pp. 285–292, Nov. 2017.

[87] C. Lin, D. He, X. Huang, K. R. Choo, and A. V. Vasilakos, "BSein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018.

[88] F. Rezaeibagha, Y. Mu, X. Huang, W. Yang, and K. Huang, "Fully secure lightweight certificateless signature scheme for IIoT," *IEEE Access*, vol. 7, pp. 144433–144443, 2019.

[89] V. Sklyar and V. Kharchenko, "Challenges in assurance case application for industrial IoT," in *Proc. 9th IEEE Int. Conf. Intell. Data Acq. Adv. Comput. Syst. Technol. Appl. (IDAACS)*, vol. 2, 2017, pp. 736–739.

[90] T. Wu, C. Chen, K. Wang, and J. M. Wu, "Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 49232–49239, 2019.

[91] W. Yang, S. Wang, X. Huang, and Y. Mu, "On the security of an efficient and robust certificateless signature scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 91074–91079, 2019.

[92] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5099–5108, Sep. 2019.

[93] H. Cui, R. H. Deng, J. K. Liu, X. Yi, and Y. Li, "Server-aided attribute-based signature with revocation for resource-constrained industrial-Internet-of-Things devices," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3724–3732, Aug. 2018.

[94] S. Paliwal, "Hash-based conditional privacy preserving authentication and key exchange protocol suitable for industrial Internet of Things," *IEEE Access*, vol. 7, pp. 136073–136093, 2019.

[95] A. Hoeller and R. Toegl, "Trusted platform modules in cyber-physical systems: On the interference between security and dependability," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS PW)*, 2018, pp. 136–144.

[96] H. Laaki, Y. Miche, and K. Tammi, "Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery," *IEEE Access*, vol. 7, pp. 20325–20336, 2019.

[97] E. Weippl and P. Kieseberg, "Security in cyber-physical production systems: A roadmap to improving it-security in the production system lifecycle," in *Proc. AEIT Int. Annu. Conf.*, 2017, pp. 1–6.

[98] Z. Bakhshi, A. Balador, and J. Mustafa, "Industrial IoT security threats and concerns by considering CISCO and Microsoft IoT reference models," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, 2018, pp. 173–178.

[99] G. Chen and W. S. Ng, "An efficient authorization framework for securing industrial Internet of Things," in *Proc. IEEE Region 10 Conf. (TENCON)*, 2017, pp. 1219–1224.

[100] G. Falco, C. Caldera, and H. Shrobe, "IIoT cybersecurity risk modeling for SCADA systems," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4486–4495, Dec. 2018.

[101] X. Feng, J. Wu, J. Li, and S. Wang, "Efficient secure access to IEEE 21451 based wireless IIoT using optimized teds and MIB," in *Proc. IEEE 44th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, 2018, pp. 5221–5227.

[102] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3472–3481, Oct. 2011.

[103] Y. Kim, Y. Lee, and J. Kim, "RIPPLE: Adaptive fine-grained access control in multi-hop LLNs," in *Proc. IEEE Int. Conf. Inf. Netw. (ICOIN)*, 2018, pp. 863–868.

[104] A. Lahbib, K. Toumi, A. Laouiti, and S. Martin, "DRMF: A distributed resource management framework for industry 4.0 environments," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, 2019, pp. 1–9.

[105] M. Langfinger, M. Schneider, D. Stricker, and H. D. Schotten, "Addressing security challenges in industrial augmented reality systems," in *Proc. IEEE 15th Int. Conf. Ind. Informat. (INDIN)*, 2017, pp. 299–304.

[106] F. Martinelli, P. Mori, A. Saracino, and F. Di Cerbo, "Obligation management in usage control systems," in *Proc. 27th Euromicro Int. Conf. Parallel Distrib. Netw. Based Process. (PDP)*, 2019, pp. 356–364.

[107] D. Preuveneers, W. Joosen, and E. Ilie-Zudor, "Identity management for cyber-physical production workflows and individualized manufacturing in industry 4.0," in *Proc. ACM Symp. Appl. Comput. (SAC)*, 2017, pp. 1452–1455.

[108] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access control policy enforcement for zero-trust-networking," in *Proc. IEEE 29th Irish Signals Syst. Conf. (ISSC)*, 2018, pp. 1–6.

[109] X. Yao, H. Kong, H. Liu, T. Qiu, and H. Ning, "An attribute credential based public key scheme for fog computing in digital manufacturing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2297–2307, Apr. 2019.

[110] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, 2018.

[111] I. Mugarza, J. Parra, and E. Jacob, "Cetratus: Towards a live patching supported runtime for mixed-criticality safe and secure systems," in *Proc. IEEE 13th Int. Symp. Ind. Embedded Syst. (SIES)*, 2018, pp. 1–8.

[112] I. Mugarza, A. Amurrio, E. Azketa, and E. Jacob, "Dynamic software updates to enhance security and privacy in high availability energy management applications in smart cities," *IEEE Access*, vol. 7, pp. 42269–42279, 2019.

[113] A. Seitz, D. Henze, D. Miehle, B. Bruegge, J. Nickles, and M. Sauer, "Fog computing as enabler for blockchain-based IIoT app marketplaces—A case study," in *Proc. IEEE 5th Int. Conf. Internet Things Syst. Manag. Security*, 2018, pp. 182–188.

[114] G. Yadav and K. Paul, "PatchRank: Ordering updates for SCADA systems," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2019, pp. 110–117.

[115] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, Feb. 2018.

[116] L. Zhou and H. Guo, "Anomaly detection methods for IIoT networks," in *Proc. IEEE Int. Conf. Service Oper. Logist. Informat. (SOLI)*, 2018, pp. 214–219.

[117] P. Priller, A. Aldrian, and T. Ebner, "Case study: From legacy to connectivity migrating industrial devices into the world of smart services," in *Proc. IEEE Emerg. Technol. Factory Autom. (ETFA)*, 2014, pp. 1–8.

[118] A. W. Atamli and A. Martin, "Threat-based security analysis for the Internet of Things," in *Proc. Int. Workshop Secure Internet Things*, 2014, pp. 35–43.

[119] E. Bauer *et al.*, "Towards a security baseline for IaaS-cloud back-ends in industry 4.0," in *Proc. IEEE 12th Int. Conf. Internet Technol. Secured Trans. (ICITST)* 2017, pp. 427–432.

[120] A. Bicaku, C. Schmittner, M. Tauber, and J. Delsing, "Monitoring industry 4.0 applications for security and safety standard compliance," in *Proc. IEEE Ind. Cyber Phys. Syst. (ICPS)*, 2018, pp. 749–754.

[121] B. Dieber and B. Breiling, "Security considerations in modular mobile manipulation," in *Proc. 3rd IEEE Int. Conf. Robot. Comput. (IRC)*, 2019, pp. 70–77.

[122] M. Ehrlich, H. Trsek, L. Wisniewski, and J. Jasperneite, "Survey of security standards for an automated industrie 4.0 compatible manufacturing," in *Proc. 45th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, vol. 1, 2019, pp. 2849–2854.

[123] "Industrial Internet of Things volume G4: Security framework," Ind. Internet Consortium, Needham, MA, USA, Rep. IIC:PUB:g4:V1.0:PB:20160926, Sep. 2016. [Online]. Available: https://www.iiconsortium.org/IISF.htm

[124] *Security for Industrial Automation and Control Systems*, IEC Standard 62443, 2018.

[125] F. Januário, C. Carvalho, A. Cardoso, and P. Gil, "Security challenges in SCADA systems over wireless sensor and actuator networks," in *Proc. 8th Int. Congr. Ultra Mod. Telecommun. Control Syst. Workshops (ICUMT)*, 2016, pp. 363–368.

[126] A. Laszka, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Synergistic security for the industrial Internet of Things: Integrating redundancy, diversity, and hardening," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, 2018, pp. 153–158.

[127] B. Leander, A. Čaušević, and H. Hansson, "Applicability of the IEC 62443 standard in industry 4.0/IIoT," in *Proc. 14th Int. Conf. Availability Rel. Security (ARES)*, 2019, pp. 1–8.

[128] V. Sklyar and V. Kharchenko, "ENISA documents in cybersecurity assurance for industry 4.0: IIoT threats and attacks scenarios," in *Proc. 10th IEEE Int. Conf. Intell. Data Acq. Adv. Comput. Syst. Technol. Appl. (IDAACS)*, vol. 2, 2019, pp. 1046–1049.

[129] N. Benias and A. P. Markopoulos, "A review on the readiness level and cyber-security challenges in industry 4.0," in *Proc. IEEE South Eastern Eur. Design Autom. Comput. Eng. Comput. Netw. Soc. Media Conf. (SEEDA-CECNSM)*, 2017, pp. 1–5.

[130] S. R. Chhetri, N. Rashid, S. Faezi, and M. A. A. Faruque, "Security trends and advances in manufacturing systems in the era of industry 4.0," in *Proc. 36th Int. Conf. Comput.-Aided Design (ICCAD)*, 2017, pp. 1039–1046.

[131] R. Chong and W. Lee, "Accelerating elGamal partial homomorphic encryption with GPU platform for industrial Internet of Things," in *Proc. Int. Conf. Green Human Inf. Technol. (ICGHIT)*, 2019, pp. 108–112.

[132] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial Internet of Things," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, 2015, pp. 795–800.

[133] N. Jazdi, "Cyber physical systems in the context of industry 4.0," in *Proc. IEEE Int. Conf. Autom. Qual. Test. Robot.*, 2014, pp. 1–4.

[134] M. Kiss, G. Breda, and L. Muha, "Information security aspects of industry 4.0," *Procedia Manuf.*, vol. 32, pp. 848–855, Apr. 2019.

[135] M. Ma, D. He, N. Kumar, K.-K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 759–767, Feb. 2018.

[136] J. Moyne, S. Mashiro, and D. Gross, "Determining a security roadmap for the microelectronics industry," in *Proc. IEEE 29th Annu. SEMI Adv. Semicond. Manuf. Conf. (ASMC)*, 2018, pp. 291–294.

[137] K.-H. Niemann, "IT security extensions for PROFINET," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, vol. 1, 2019, pp. 407–412.

[138] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2018.

[139] M. Zhang, B. Peng, and Y. Chen, "An efficient image encryption scheme for industrial Internet-of-Things devices," in *Proc. 2nd Int. ACM Workshop Security Privacy Internet Things (IoT S&P)*, 2019, pp. 38–43.

[140] Y. Zhang, H. Huang, L.-X. Yang, Y. Xiang, and M. Li, "Serious challenges and potential solutions for the industrial Internet of Things with edge intelligence," *IEEE Netw.*, vol. 33, no. 5, pp. 41–45, Sep./Oct. 2019.

[141] Y. Zhao, L. T. Yang, and J. Sun, "Privacy-preserving tensor-based multiple clusterings on cloud for industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2372–2381, Apr. 2019.

[142] H. Klaus, F. Hetzelt, P. Hofmann, A. Blecker, and D. Schwaiger, "Challenges and solutions for industry-grade secure connectivity," in *Proc. Int. Conf. Netw. Syst. (NetSys)*, 2019, pp. 1–5.

[143] S. Marksteiner, "Reasoning on adopting OPC UA for an IoT-enhanced smart energy system from a security perspective," in *Proc. IEEE 20th Conf. Bus. Informat. (CBI)*, vol. 2, 2018, pp. 140–143.

[144] V. Nigam and C. Talcott, "Formal security verification of industry 4.0 applications," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2019, pp. 1043–1050.

[145] W. Mahnke, S.-H. Leitner, and M. Damm, *OPC Unified Architecture*. Berlin, Germany: Springer-Verlag, 2009, doi: 10.1007/978-3-540-68899-0.

[146] B. Chen, L. Wu, N. Kumar, K. R. Choo, and D. He, "Lightweight searchable public-key encryption with forward privacy over IIoT outsourced data," *IEEE Trans. Emerg. Topics Comput.*, early access, Jun. 5, 2019, doi: 10.1109/TETC.2019.2921113.

[147] L. Deng, "Anonymous aggregate encryption scheme for industrial Internet of Things," *IEEE Syst. J.*, vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[148] T. M. Fernandez-Carames and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019.

[149] J. Fu, Y. Liu, H. Chao, B. K. Bhargava, and Z. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[150] Z. Guan, X. Lu, N. Wang, J. Wu, X. Du, and M. Guizani, "Towards secure and efficient energy trading in IIoT-enabled energy Internet: A blockchain approach," *Future Gener. Comput. Syst.*, to be published.

[151] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[152] Y. Jiang, Y. Zhong, and X. Ge, "Smart contract-based data commodity transactions for industrial Internet of Things," *IEEE Access*, vol. 7, pp. 180856–180866, 2019.

[153] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K. Li, "A secure FaBric blockchain-based data transmission technique for industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3582–3592, Jun. 2019.

[154] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, Jun. 2019.

[155] Y. Miao, Q. Tong, K. R. Choo, X. Liu, R. H. Deng, and H. Li, "Secure online/offline data sharing framework for cloud-assisted industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8681–8691, Oct. 2019.

[156] P. Nikander, J. Autiosalo, and S. Paavolainen, "Interledger for the industrial Internet of Things," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, vol. 1, 2019, pp. 908–915.

[157] A. S. Sani *et al.*, "Xyreum: A high-performance and scalable blockchain for IIoT security and privacy," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2019, pp. 1920–1930.

[158] N. Stifter, M. Eckhart, B. Brenner, and E. Weippl, "Avoiding risky designs when using blockchain technologies in cyber-physical systems," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2019, pp. 1623–1626.

[159] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3712–3723, Aug. 2018.

[160] Y. Yu, R. Chen, H. Li, Y. Li, and A. Tian, "Toward data security in edge intelligent IIoT," *IEEE Netw.*, vol. 33, no. 5, pp. 20–26, Sep./Oct. 2019.

[161] X. Zhang, C. Xu, H. Wang, Y. Zhang, and S. Wang, "FS-PEKS: Lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial Internet of Things," *IEEE Trans. Depend. Secure Comput.*, early access, Apr. 30, 2019, doi: 10.1109/TDSC.2019.2914117.

[162] R. Al-Ali, R. Heinrich, P. Hnetynka, A. Juan-Verdejo, S. Seifermann, and M. Walter, "Modeling of dynamic trust contracts for industry 4.0 systems," in *Proc. 12th Eur. Conf. Softw. Archit. (ECSA)*, 2018, pp. 1–4.

[163] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti, "Design patterns for the industrial Internet of Things," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, 2018, pp. 1–10.

[164] J. Schütte and G. S. Brost, "LUCON: Data flow control for message-based IoT systems," in *Proc. 17th IEEE Int. Conf. Trust Security Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, 2018, pp. 289–299.

[165] D. Conzon, M. R. A. Rashid, X. Tao, A. Soriano, R. Nicholson, and E. Ferrera, "BRAIN-IoT: Model-based framework for dependable sensing and actuation in intelligent decentralized IoT Systems," in *Proc. 4th Int. Conf. Comput. Commun. Security (ICCCS)*, 2019, pp. 1–8.

[166] *Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR)*, document 32016R0679, Eur. Parliament Council Eur. Union, Brussels, Belgium, Apr. 2016. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj

[167] G. Han, X. Miao, H. Wang, L. Liu, J. Jiang, and Y. Peng, "A dynamic multipath scheme for protecting source-location privacy using multiple sinks in WSNs intended for IIoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5527–5538, Aug. 2020.

[168] Z. A. Solangi *et al.*, "The future of data privacy and security concerns in Internet of Things," in *Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD)*, 2018, pp. 1–4.

[169] M. Usman, M. A. Jan, A. Jolfaei, M. Xu, X. He, and J. Chen, "DaaC: A distributed and anonymous data collection framework based on multilevel edge computing architecture," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6114–6123, Sep. 2020.

[170] M. Al-Hawawreh and E. Sitnikova, "Industrial Internet of Things based ransomware detection using stacked variational neural network," in *Proc. 3rd Int. Conf. Big Data Internet Things (BDIOT)*, 2019, pp. 126–130.

[171] M. Al-Hawawreh, E. Sitnikova, and F. den Hartog, "An efficient intrusion detection model for edge system in brownfield industrial Internet of Things," in *Proc. 3rd Int. Conf. Big Data Internet Things (BDIOT)*, 2019, pp. 83–87.

[172] C. Alcaraz, G. Bernieri, F. Pascucci, J. Lopez, and R. Setola, "Covert channels-based stealth attacks in industry 4.0," *IEEE Syst. J.*, vol. 13, no. 4, pp. 3980–3988, Dec. 2019.

[173] S. Alem, D. Espes, E. Martin, L. Nana, and F. De Lamotte, "A hybrid intrusion detection system in industry 4.0 based on ISA95 standard," in *Proc. IEEE/ACS 16th Int. Conf. Comput. Syst. Appl. (AICCSA)*, 2019, pp. 1–8.

[174] R. Antrobus, B. Green, S. Frey, and A. Rashid, "The forgotten I in IIoT: A vulnerability scanner for industrial Internet of Things," in *Proc. Living Internet Things (IoT)*, 2019, pp. 1–8.

[175] R. F. Babiceanu and R. Seker, "Cyber resilience protection for industrial Internet of Things: A software-defined networking approach," *Comput. Ind.*, vol. 104, pp. 47–58, Jan. 2019.

[176] G. Bernieri, M. Conti, and F. Pascucci, "MimePot: A model-based honeypot for industrial control networks," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, 2019, pp. 433–438.

[177] Z. Birnbaum, A. Dolgikh, V. Skormin, E. O'Brien, and D. Muller, "Unmanned aerial vehicle security using recursive parameter estimation," in *Proc. Int. Conf. Unmanned Aircraft Syst. (ICUAS)*, 2014, pp. 692–702.

[178] R. Colelli, S. Panzieri, and F. Pascucci, "Securing connection between IT and OT: The fog intrusion detection system prospective," in *Proc. II Workshop Metrol. Ind. 4.0 IoT (MetroInd4.0 IoT)*, 2019, pp. 444–448.

[179] V. Deshpande, L. George, and H. Badis, "PulSec: Secure element based framework for sensors anomaly detection in industry 4.0," *IFAC PapersOnLine*, vol. 52, no. 13, pp. 1204–1209, 2019.

[180] S. D. D. Anton, M. Strufe, and H. D. Schotten, "Modern problems require modern solutions: Hybrid concepts for industrial intrusion detection," in *Proc. 24th ITG Symp. Mobile Commun. Technol. Appl.*, 2019, pp. 1–5.

[181] C. Enăchescu, H. Sándor, and B. Genge, "A multi-model-based approach to detect cyber stealth attacks in industrial Internet of Things," in *Proc. Int. Conf. Softw. Telecommun. Comput. Netw. (SoftCOM)*, 2019, pp. 1–6.

[182] J. L. Flores and I. Mugarza, "Runtime vulnerability discovery as a service on industrial Internet of Things (IIoT) systems," in *Proc. IEEE 23rd Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 1, 2018, pp. 948–955.

[183] B. Genge, P. Haller, and C. Enachescu, "Anomaly detection in aging industrial Internet of Things," *IEEE Access*, vol. 7, pp. 74217–74230, 2019.

[184] M. M. Hasan and H. T. Mouftah, "Cloud-centric collaborative security service placement for advanced metering infrastructures," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1339–1348, Mar. 2019.

[185] Y. Hu, D. Zhang, G. Cao, and Q. Pan, "Network data analysis and anomaly detection using CNN technique for industrial control systems security," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, 2019, pp. 593–597.

[186] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.

[187] P. Kadera and P. Novák, "Performance modeling extension of directory facilitator for enhancing communication in FIPA-compliant multiagent systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 688–695, Apr. 2017.

[188] M. E. Khoda, T. Imam, J. Kamruzzaman, I. Gondal, and A. Rahman, "Robust malware defense in industrial IoT applications using machine learning with selective adversarial samples," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4415–4424, Jul./Aug. 2020.

[189] B. Kim and Y. Kang, "Abnormal traffic detection mechanism for protecting IIoT environments," in *Proc. IEEE Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, 2018, pp. 943–945.

[190] V. Krundyshev and M. Kalinin, "Prevention of false data injections in smart infrastructures," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, 2019, pp. 1–5.

[191] A. Melis, D. Berardi, C. Contoli, F. Callegati, F. Esposito, and M. Prandini, "A policy checker approach for secure industrial SDN," in *Proc. IEEE 2nd Cyber Security Netw. Conf. (CSNet)*, 2018, pp. 1–7.

[192] R. Mitchell and I. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 5, pp. 593–604, May 2014.

[193] N. Moustafa, E. Adi, B. Turnbull, and J. Hu, "A new threat intelligence scheme for safeguarding industry 4.0 systems," *IEEE Access*, vol. 6, pp. 32910–32924, 2018.

[194] D. M. Nedeljkovic, Z. B. Jakovljevic, Z. D. Miljkovic, and M. Pajic, "Detection of cyber-attacks in electro-pneumatic positioning system with distributed control," in *Proc. 27th Telecommun. Forum (TELFOR)*, 2019, pp. 1–4.

[195] M. Niedermaier, F. Fischer, D. Merli, and G. Sigl, "Network scanning and mapping for IIoT edge node device security," in *Proc. Int. Conf. Appl. Electron. (AE)*, 2019, pp. 1–6.

[196] S. Potluri, C. Diedrich, S. R. R. Nanduru, and K. Vasamshetty, "Development of injection attacks toolbox in MATLAB/Simulink for attacks simulation in industrial control system applications," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, vol. 1, 2019, pp. 1192–1198.

[197] M. Smache, A. Olivereau, T. Franco-Rondisson, and A. Tria, "Autonomous detection of synchronization attacks in the industrial Internet of Things," in *Proc. IEEE 38th Int. Perform. Comput. Commun. Conf. (IPCCC)*, 2019, pp. 1–9.

[198] G. Settanni, F. Skopik, A. Karaj, M. Wurzenberger, and R. Fiedler, "Protecting cyber physical production systems using anomaly detection to enable self-adaptation," in *Proc. IEEE Ind. Cyber Phys. Syst. (ICPS)*, 2018, pp. 173–180.

[199] V. Sharma, G. Choudhary, Y. Ko, and I. You, "Behavior and vulnerability assessment of drones-enabled industrial Internet of Things (IIoT)," *IEEE Access*, vol. 6, pp. 43368–43383, 2018.

[200] S. Tamy, H. Belhadaoui, M. A. Rabbah, N. Rabbah, and M. Rifi, "An evaluation of machine learning algorithms to detect attacks in SCADA network," in *Proc. 7th Mediterr. Congr. Telecommun. (CMT)*, 2019, pp. 1–5.

[201] A. Wadsworth, M. I. Thanoon, C. McCurry, and S. Z. Sabatto, "Development of IIoT monitoring and control security scheme for cyber physical systems," in *Proc. SoutheastCon*, 2019, pp. 1–5.

[202] T. Wang, P. Wang, S. Cai, Y. Ma, A. Liu, and M. Xie, "A unified trustworthy environment establishment based on edge computing in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6083–6091, Sep. 2020.

[203] H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, and L. Lu, "Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection," *IEEE Netw.*, vol. 33, no. 5, pp. 75–81, Sep./Oct. 2019.

[204] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proc. HotNets*, Philadelphia, PA, USA, 2015, pp. 1–7.

[205] L. Zhou, H. Guo, and G. Deng, "A fog computing based approach to DDoS mitigation in IIoT systems," *Comput. Security*, vol. 85, pp. 51–62, May 2020.

[206] M. Zolanvari, M. A. Teixeira, and R. Jain, "Effect of imbalanced datasets on security of industrial IoT using machine learning," in *Proc. IEEE Int. Conf. Intell. Security Informat. (ISI)*, 2018, pp. 112–117.

[207] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019.

[208] E. Zugasti, M. Iturbe, I. Garitano, and U. Zurutuza, "Null is not always empty: Monitoring the null space for field-level anomaly detection in industrial IoT environments," in *Proc. IEEE Global Internet Things Summit (GIoTS)*, 2018, pp. 1–6.

[209] Y. Ai, M. Cheffena, T. Ohtsuki, and H. Zhuang, "Secrecy performance analysis of wireless sensor networks," *IEEE Sensors Lett.*, vol. 3, no. 5, pp. 1–4, May 2019.

[210] C. Alcaraz, R. Roman, P. Najera, and J. Lopez, "Security of industrial sensor network-based remote substations in the context of the Internet of Things," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 1091–1104, 2013.

[211] A. Bluschke *et al.*, "FastVPN—Secure and flexible networking for industry 4.0," in *Proc. 12th ITG Symp. Broadband Coverage Germany*, 2018, pp. 1–8. [Online]. Available: https://imld.de/en/research/research-projects/fastvpn/

[212] M. Cheminod, L. Durante, L. Seno, F. Valenza, A. Valenzano, and C. Zunino, "Leveraging SDN to improve security in industrial networks," in *Proc. IEEE 13th Int. Workshop Factory Commun. Syst. (WFCS)*, 2017, pp. 1–7.

[213] B. Czybik, S. Hausmann, S. Heiss, and J. Jasperneite, "Performance evaluation of MAC algorithms for real-time Ethernet communication systems," in *Proc. 11th IEEE Int. Conf. Ind. Informat. (INDIN)*, 2013, pp. 676–681.

[214] S. Jeong, W. Na, J. Kim, and S. Cho, "Internet of Things for smart manufacturing system: Trust issues in resource allocation," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4418–4427, Dec. 2018.

[215] C. Lipps, M. Strufe, S. B. Mallikarjun, and H. D. Schotten, "Physical layer security for IIoT and CPPS: A cellular-network security approach," in *Proc. 24th ITG Symp. Mobile Commun. Technol. Appl.*, 2019, pp. 1–5.

[216] C. Lipps, D. Krummacker, and H. D. Schotten, "Securing industrial wireless networks: Enhancing SDN with PhySec," in *Proc. Conf. Next Gener. Comput. Appl. (NextComp)*, 2019, pp. 1–7.

[217] J. O'Raw, D. Laverty, and D. J. Morrow, "Securing the industrial Internet of Things for critical infrastructure (IIoT-CI)," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, 2019, pp. 70–75.

[218] P. Hu, "A system architecture for software-defined industrial Internet of Things," in *Proc. IEEE Int. Conf. Ubiquitous Wireless Broadband (ICUWB)*, 2015, pp. 1–5.

[219] T. Kobzan, S. Schriegel, S. Althoff, A. Boschmann, J. Otto, and J. Jasperneite, "Secure and time-sensitive communication for remote process control and monitoring," in *Proc. IEEE 23rd Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 1, 2018, pp. 1105–1108.

[220] T. Lackorzynski, S. Köpsell, and T. Strufe, "A comparative study on virtual private networks for future industrial communication systems," in *Proc. 15th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, 2019, pp. 1–8.

[221] G. Marchetto, R. Sisto, J. Yusupov, and A. Ksentinit, "Formally verified latency-aware VNF placement in industrial Internet of Things," in *Proc. IEEE 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, 2018, pp. 1–9.

[222] M. Alaluna, L. Ferrolho, J. R. Figueira, N. Neves, and F. M. V. Ramos, "Secure multi-cloud virtual network embedding," 2017. [Online]. Available: arXiv:1703.01313.

[223] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577, 2017.

[224] F. Kurtz, C. Bektas, N. Dorsch, and C. Wietfeld, "Network slicing for critical communications in shared 5G infrastructures—An empirical evaluation," in *Proc. IEEE 4th IEEE Conf. Netw. Softw. Workshops (NetSoft)*, 2018, pp. 393–399.

[225] T. Ulz, T. Pieber, C. Steger, S. Haas, and R. Matischek, "Sneakernet on wheels: Trustworthy NFC-based robot to machine communication," in *Proc. IEEE Int. Conf. RFID Technol. Appl. (RFID-TA)*, 2017, pp. 260–265.

[226] Q. Wang, H. Dai, H. Wang, G. Xu, and A. K. Sangaiah, "UAV-enabled friendly jamming scheme to secure industrial Internet of Things," *J. Commun. Netw.*, vol. 21, no. 5, pp. 481–490, 2019.

[227] N. Accettura and G. Piro, "Optimal and secure protocols in the IETF 6TISCH communication stack," in *Proc. IEEE 23rd Int. Symp. Ind. Electron. (ISIE)*, 2014, pp. 1469–1474.

[228] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: Deterministic IP-enabled industrial Internet (of Things)," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 36–41, Dec. 2014.

[229] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on LPWA technology: LoRa and NB-IoT," *ICT Exp.*, vol. 3, no. 1, pp. 14–21, 2017.

[230] H. C. Pöhls *et al.*, "RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, 2014, pp. 122–127.

[231] H. Aranha, M. Masi, T. Pavleska, and G. P. Sellitto, "Securing mobile e-health environments by design: A holistic architectural approach," in *Proc. Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, 2019, pp. 1–6.

[232] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018.

[233] B. Craggs, A. Rashid, C. Hankin, R. Antrobus, O. Serban, and N. Thapen, "A reference architecture for IIoT and industrial control systems testbeds," in *Proc. Living Internet Things (IoT)*, 2019, pp. 1–8.

[234] M. Eckhart, A. Ekelhart, A. Lüder, S. Biffl, and E. Weippl, "Security development lifecycle for cyber-physical production systems," in *Proc. 45th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, vol. 1, 2019, pp. 3004–3011.

[235] H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek, and H. Adamczyk, "Analysis of the cyber-security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2016, pp. 1–4.

[236] Y. Huang, W. Sun, and Y. Tang, "3aRAM: A 3-layer AHP-based risk assessment model and its implementation for an industrial IoT cloud," in *Proc. IEEE 19th Int. Conf. Softw. Qual. Rel. Security Companion (QRS-C)*, 2019, pp. 450–457.

[237] R. A. Isbell, C. Maple, B. Hallaq, and H. Boyes, "Development of a capability maturity model for cyber security in IIoT enabled supply chains," in *Proc. Living Internet Things (IoT)*, 2019, pp. 1–8.

[238] I. Ivkic, A. Mauthe, and M. Tauber, "Towards a security cost model for cyber-physical systems," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2019, pp. 1–7.

[239] V. Kharchenko, S. Dotsenko, O. Illiashenko, and S. Kamenskyi, "Integrated cyber safety security management system: Industry 4.0 issue," in *Proc. 10th Int. Conf. Depend. Syst. Services Technol. (DESSERT)*, 2019, pp. 197–201.

[240] A. Kondeva, V. Nigam, H. Ruess, and C. Carlan, "On computer-aided techniques for supporting safety and security co-engineering," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops (ISSREW)*, 2019, pp. 346–353.

[241] L. Liang, Y. Liu, Y. Yao, T. Yang, Y. Hu, and C. Ling, "Security challenges and risk evaluation framework for industrial wireless sensor networks," in *Proc. IEEE 4th Int. Conf. Control Decis. Inf. Technol. (CoDIT)*, 2017, pp. 0904–0907.

[242] J. M. Mcginthy and A. J. Michaels, "Secure industrial Internet of Things critical infrastructure node design," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8021–8037, Oct. 2019.

[243] N. Mohamed and J. Al-Jaroodi, "Applying blockchain in industry 4.0 applications," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, 2019, pp. 0852–0858.

[244] S. Pasandideh, L. Gomes, and P. Maló, "Improving attack trees analysis using Petri net modeling of cyber-attacks," in *Proc. IEEE 28th Int. Symp. Ind. Electron. (ISIE)*, 2019, pp. 1644–1649.

[245] R. Sharpe, K. van Lopik, A. Neal, P. Goodall, P. P. Conway, and A. A. West, "An industrial evaluation of an industry 4.0 reference architecture demonstrating the need for the inclusion of security and human components," *Comput. Ind.*, vol. 108, pp. 37–44, Jun. 2019.

[246] L. Shu, M. Mukherjee, M. Pecht, N. Crespi, and S. N. Han, "Challenges and research issues of data management in IoT for large-scale petrochemical plants," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2509–2523, Sep. 2018.

[247] *TrustZone*. Accessed: Jul. 2, 2019. [Online]. Available: https://developer.arm.com/ip-products/security-ip/trustzone

[248] *Intel—Software Guard Extensions*. Accessed: Jul. 2, 2019. [Online]. Available: https://software.intel.com/en-us/sgx

[249] I. O. Standardization/International Electrotechnical Commission, *Information Technology-Trusted Platform Module—Part 1: Overview*, ISO/IEC 11889-1, 2015.

[250] *Axiomtek's Fanless Embedded System With TPM 1.2 and Flexible Expansions*. Accessed: Jul. 2, 2019. [Online]. Available: https://www.axiomtek.com/Default.aspx?MenuId=News&FunctionId=NewsView&ItemId=12845

[251] (2019). *CC2652R SimpleLink Multiprotocol 2.4-GHz Wireless MCU*. [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2652r.pdf

[252] "The 3rd generation partnership project website," 3GPP, Sophia Antipolis, France Rep., 2020. [Online]. Available: https://www.3gpp.org

[253] H. Kagermann, W. Wahlster, and J. Helbig, *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0—Securing the Future of German Manufacturing Industry*, Nat. Acad. Sci. Eng., Washington, DC, USA, Apr. 2013. [Online]. Available: http://forschungsunion.de/pdf/industrie_4_0_final_report.pdf

[254] M. De Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: Cloud, IoT, edge, and fog," *IEEE Access*, vol. 7, pp. 150936–150948, 2019.

[255] M. De Donno, A. Giaretta, N. Dragoni, A. Bucchiarone, and M. Mazzara, "Cyber-storms come from clouds: Security of cloud computing in the IoT era," *Future Internet*, vol. 11, no. 6, p. 127, 2019.

[256] *IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing*, IEEE Standard 1934-2018, 2018.

[257] R. Skillern, "Intel—SGX data protections now available for mainstream cloud platforms," Intel, San Jose, CA, USA, Rep., 2019. Accessed: Feb. 27, 2019. [Online]. Available: https://itpeernetwork.intel.com/sgx-data-protection-cloud-platforms/#gs.c31lxv

[258] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying fog computing in industrial Internet of Things and industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4674–4682, Oct. 2018.

[259] M. De Donno, J. M. D. Felipe, and N. Dragoni, "ANTIBIoTIC 2.0: A fog-based anti-malware for Internet of Things," in *Proc. Eur. Workshop Security Privacy Edge Comput. (EuroSPEC)*, 2019, pp. 11–20.

[260] M. De Donno and N. Dragoni, "Combining AntibIoTic with fog computing: AntibIoTic 2.0," in *Proc. IEEE 3rd Int. Conf. Fog Edge Comput. (ICFEC)*, 2019, pp. 1–6.

[261] M. De Donno, N. Dragoni, A. Giaretta, and M. Mazzara, "AntibIoTic: Protecting IoT devices against DDoS attacks," in *Proc. Int. Conf. Softw. Eng. Defence Appl.*, 2016, pp. 59–72.

[262] A. Yousefpour *et al.*, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *J. Syst. Archit.*, vol. 98, pp. 289–330, Sep. 2019.

Koen Tange (Graduate Student Member, IEEE) received the B.Sc. degree in software science from the Eindhoven University of Technology, Eindhoven, The Netherlands, in 2016, and the joint M.Sc. degree in engineering, security, and mobile computing from the Technical University of Denmark, Lyngby, Denmark, and Aalto University, Espoo, Finland, in 2018, as part of the Nordic Masters Programme in Security and Mobile Computing. He is currently pursuing the Ph.D. degree with the DTU Compute, Technical University of Denmark, under the supervision of Prof. N. Dragoni. His research interests include information security, fog computing, trusted hardware, and distributed systems.

Michele De Donno (Student Member, IEEE) received the M.Sc. degree in computer engineering from Politecnico di Torino, Turin, Italy, in 2017. He is currently pursuing the Ph.D. degree with the DTU Compute, Technical University of Denmark, Denmark, under the supervision of Prof. N. Dragoni. His main research interests include cyber-security, networking, distributed systems, Internet-of-Things, and fog computing.

Xenofon Fafoutis (Senior Member, IEEE) received the B.Sc. degree in informatics and telecommunications from the University of Athens, Greece, in 2007, the M.Sc. degree in computer science from the University of Crete, Greece, in 2010, and the Ph.D. degree in embedded systems engineering from the Technical University of Denmark in 2014. From 2014 to 2018, he held various researcher positions with the University of Bristol, U.K., and he was a core member of SPHERE: U.K.'s flagship Interdisciplinary Research Collaboration on Healthcare Technology. He is currently an Associate Professor with the Embedded Systems Engineering Section, Department of Applied Mathematics and Computer Science, Technical University of Denmark. His research interests primarily lie in wireless embedded systems as an enabling technology for digital health, smart cities, and the (Industrial) Internet of Things.

Nicola Dragoni received the M.Sc. (*cum laude*) and Ph.D. degrees in computer science from the University of Bologna, Italy. He is a Professor in secure pervasive computing with DTU Compute, Technical University of Denmark, where he also serves as the Deputy Head of the Ph.D. School. He is also part-time Professor in computer engineering with the Centre for Applied Autonomous Sensor Systems, Örebro University, Sweden, and he is affiliated with the Copenhagen Center for Health Technology (CACHET) and the Nordic IoT Hub. He has coauthored over 110 peer-reviewed articles and he has edited three journal special issues and one book. He is active in a number of national and international projects. His main research interests include pervasive computing and cybersecurity, with current focus on Internet-of-Things, fog computing, and mobile systems.