Journal of Network and Computer Applications 171 (2020) 102779

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Security in product lifecycle of IoT devices: A survey

Narges Yousefnezhad [a,*], Avleen Malhi [a], Kary Främling [b]

[a] Department of Computer Science, Aalto University, Espoo, Finland
[b] Department of Computing Science, Umeå University, Umeå, Sweden

ARTICLE INFO

Index Terms:
Internet of things
Product lifecycle
Lifecycle phases
Security solutions
Product lifecycle security
Device security

ABSTRACT

The Internet of Things (IoT) paradigm is considerably impacted by security challenges, which has lately demanded substantial consideration. Accordingly, certain reviews and surveys have been presented, focusing on disparate IoT-related domains, including IoT security, intrusion detection systems, and emerging technologies. However, in this article, we solely target IoT security with respect to product lifecycle stages. In that regard, we provide a comprehensive comparison of state-of-the-art surveys in an initial phase which concentrate on distinct parameters required for IoT security. Further, we present prominent solutions for addressing product lifecycle security in IoT. In this context, the contributions of this article are: (a) IoT product lifecycle security, (b) security taxonomy in IoT product lifecycle, (c) security solutions for each lifecycle phase in product lifecycle stages, and (d) open issues in these lifecycle stages that pose new research challenges. Consequently, the advancing research related to IoT security, especially with respect to product lifecycle, is explored through state-of-the-art developments in the domain of product lifecycle security.

1. Introduction

Internet of Things (IoT) is a future Internet's vision consisting of heterogeneous objects such as transportation systems, home appliances, factory machines, smart personal devices, or any intelligent products employed in our day-to-day life on various applications and divergent situations. Recently, researchers realized that to design an ideal IoT, all devices should be inter-connected and in the same vein, sensed data collected into vertical silos should be replaced with communication among vertically-oriented closed systems (Kubler et al., 2015a). Similarly, to make an IoT system ideally secure, vendor-specific security methods (blue arrows in Fig. 1) should be replaced with globally regulated security models used in all platforms (black arrows). For instance, it is more efficient to have a concrete identification system over all the silos rather than having a vendor-specific (e.g., Apple-specific) identification method.

With the development of IoT and the market pressure pushing device manufacturers to launch increasingly smart devices, we see intensify connectivity amongst smart devices. 125 billion devices are forecasted to be connected by 2030 (Howell, 2030). However, many of these devices are deployed without considering the security (Ye et al., 2017); hence, such connectivity causes an entirely new range of security risks. As recently experienced, security and vulnerability of

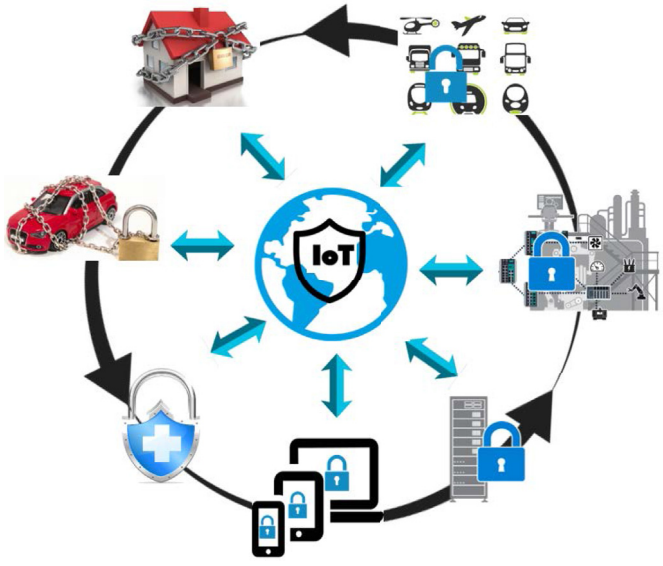

Fig. 1. Ideal IoT security.

* Corresponding author.
E-mail addresses: Narges.Yousefnezhad@aalto.fi (N. Yousefnezhad), Avleen.Malhi@aalto.fi (A. Malhi), kary.framling@umu.se (K. Främling).

https://doi.org/10.1016/j.jnca.2020.102779
Received 25 January 2020; Received in revised form 25 June 2020; Accepted 17 July 2020
Available online 22 August 2020

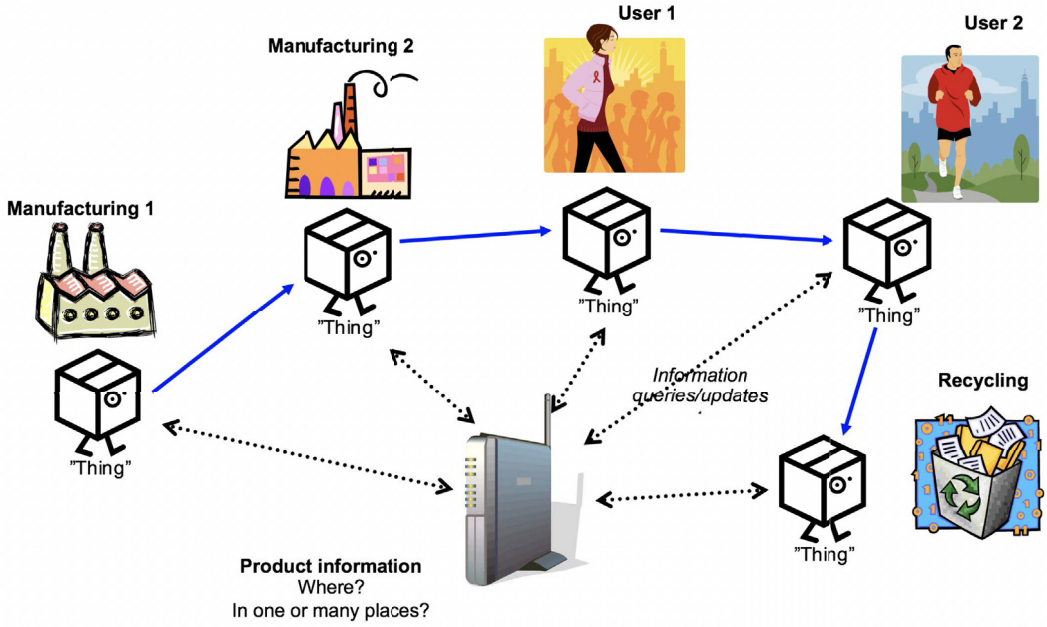

Fig. 2. The product lifecycle seen from an Internet of Things point of view. Information about the "thing" is used and produced during all phases of its lifecycle (Främling and Holmström, 2006).

IoT devices, represent major challenges. Threatpost (O'Donnell, 1441) estimated that over 2 million smart devices are open to hijack without any security solution. Many cyberattacks, like the Mirai Malware and the ransomware, infect a network of smart devices such as home appliances, security cameras, baby monitors, air conditioning/heating controls, and televisions. The subject related to security in IoT has thus far been overlooked by both industry and academia, to be dealt with the later stages of implementation and deployment.

In many projects, security tends to be the systematic consideration that is managed last. The reason for this could be that implementing security mechanisms even with standard technologies requires e.g. certificates, keys, access rights, and firewalls, which may demand much manual work and the involvement of diverse human operators. Many organizations lack any personnel who would know how to e.g. set up secure servers or, manage certificates. In order to also allow such organizations to provide and use lifecycle-related services, it is important to adjust the level of security according to the requirements of the service, rather than always imposing the highest possible level of security. Furthermore, the need to query and update product information during its lifetime as illustrated in Fig. 2 is not limited to organizations only. At least when the users are individuals, extensive security requirements could discourage the use of multiple services. At the same time, privacy issues become even more relevant.

In addition, IoT faces various passive and active malicious attacks compromising the security and privacy of IoT devices that may easily hinder their functionality in any lifecycle phases and nullify the benefits provided by their services. Several recent works have been accomplished to counteract attacks and security issues in order to secure the IoT devices and to find an improved approach to eliminate the risks, or minimize their influence on the security and privacy of user requirements (Yang et al., 2017). Despite a vast number of studies of such security challenges in IoT, there is scant systematic literature of the IoT security challenges, covering security solutions on the entire lifecycle. A secure lifecycle ensures that acceptable levels of security are in place from the device manufacturing phase all the way to the disposal of the device. On the other hand, Product Lifecycle (PLC) is so frequently applied in various areas and diverse industrial products so that all product features should be monitored in full over the lifecycle. IoT devices are one of significant upcoming industrial products which contains confidential data from people all over the world. Besides, the most important feature which should be monitored constantly on IoT systems is the security. Security concerns feature in all the phases of IoT devices from manufacturing to decommissioning. Thus, it is essential to investigate security challenges of IoT devices in all stages and phases of the lifecycle.

1.1. Contributions

- Initially, a comprehensive comparison has been performed to investigate discrete IoT security surveys in literature to establish the importance of the topic of lifecycle.
- The state-of-the-art security solutions are categorized based on the product lifecycle stages of Begining of Life (BoL), Middle of Life (MoL), and End of Life (EoL).
- A comparative study is conducted for the existing security solutions based upon their distinctive properties.
- Some open issues encountered while reinforcing security in each of the lifecycle stages are discussed.

The current article aims to bridge the gap in earlier study by performing a comprehensive analysis of IoT security issues and their solutions in the entire life of a device.

1.2. Article roadmap

This survey article comprehensively discusses the different security solutions available currently from th IoT product lifecycle perspective. The existing security solutions are classified according to security issues in each of the lifecycle phases in lifecycle stages of BoL, MoL, and EoL. The state-of-the-art security solutions are compared based on various security parameters and finally the article discusses the open issues related to disparate security challenges. Fig. 3 shows the article roadmap.

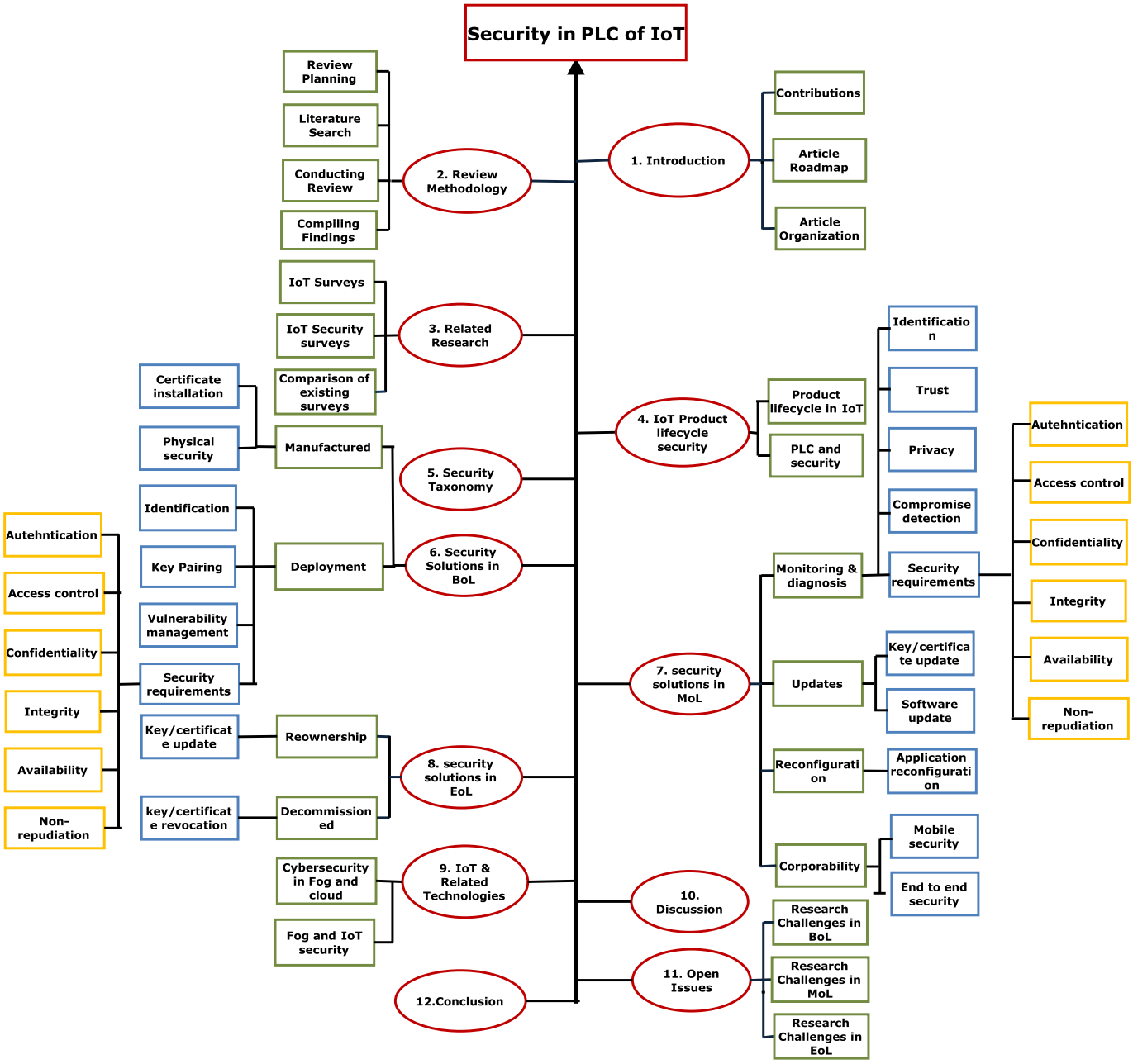

Fig. 3. The roadmap for an article.

1.3. Article organization

The complete paper is organized as follows. First, the methodology adopted for conducting this survey is reviewed in Section 2. Section 3 presents a detailed study of existing literature over the present security surveys. Then, product lifecycle and its relationship with IoT, specifically the security of IoT is discussed in Section 4. Against such a relationship, a taxonomy of security issues and requirements are demonstrated which are categorized based on device lifecycle in Section 5. According to the lifecycle stages BoL, MoL, and EoL in the proposed taxonomy, security solutions are discussed in Sections 6, 7, and 8, respectively. Section 9 discusses the relation between IoT and other technologies by discussing the cybersecurity solutions as well. Finally, after comparing all the solutions in Section 10 and addressing the open issues with the sketch of future work in Section 11, we conclude with our key findings in Section 12.

2. Review methodology

Review methodology was adopted to substantiate the research gap and to highlight the motivational factor for conducting the survey. Accordingly, the systematic process of the current article is shown in Fig. 4. The review process is divided into four steps including Review Planning, Literature Search, Conducting Review, and Compiling Findings, which are explained below.

2.1. Review Planning

2.1.1. Research objective

The purpose of this article is to comprehensively review literature related to security solutions for IoT devices based on their lifecycle phases. Based on this objective, several key scenarios have been identified which require holistic consideration of IoT security.

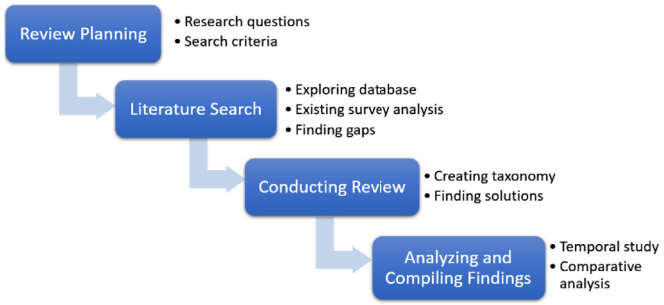

Fig. 4. Review methodology.

2.1.2. Research questions

To achieve our research objective, a set of research questions were formulated:

RQ1 What are the *existing* state-of-the-art surveys and how are they *different* from the current survey? Based on what *security parameters* can they be compared? - *This research question is answered in Section 3.*

RQ2 What is the role of *product lifecycle* in *IoT environment* and how does it impact the *security* of IoT devices? - *This research question is answered in Section 4.*

RQ3 What is the *security taxonomy* which can be proposed for IoT device lifecycle based on different *lifecycle phases* in *lifecycle stages*? - *This research question is answered in Section 5.*

RQ4 What are the distinct *security solutions* that exist in literature for each of the *security challenges* discussed in two of the major lifecycle stages of *BoL and MoL*? Are there any security solutions which can cover both stages? If not, which solution exist for each of the *phase of these lifecycles*? - *This research question is answered in Sections 6, 7.*

RQ5 What are the distinct *security solutions* with respect to *End of Life* for a device which is a major *research challenge*?- *This research question is answered in Section 8.*

RQ6 How can the existing *security solutions* be *compared* based on *lifecycle perspective*? - *This research question is answered in Section 10.*

RQ7 What are the *open issues* identified by the current work and how do they evolve? - *This research question is answered in Section 11.*

These questions will be investigated using literature as a basis. A thorough literature review of the security of IoT device over lifecycle reveals no study describing security challenges in the IoT environment from the lifecycle point of view. In order to fill this gap, this paper presents a literature review of security challenges and solution particularly, and in comparison with the previous security surveys, of IoT in general.

2.1.3. Search criteria

The keywords *IoT* and *security* are present in each research paper's abstract, although the keywords have been selected based on the related sections including literature review, background, and taxonomy.

The present study conducted contains the literature review of the qualitative and quantitative research articles during the last 10 years, from 2009 to 2019 in English language. In this article, we have included research papers from peer reviewed journals, symposiums, conferences, technical reports, lecture notes, workshops and white papers from industry.

2.2. Literature Search

2.2.1. Exploring database

The review methodology selected for this article involves searching appropriate research articles from a collection of databases such as Google Scholar, Springer, ScienceDirect, IEEE eXplore, and ACM Digital Library.

2.2.2. Analyzing existing surveys

Security and privacy have constituted major concerns in IoT networks, therefore extensive research has been conducted in various security and privacy domains of IoT such as key management, authentication and access control, and compromise detection. IoT is a novel topic and to clearly understand the security challenges in such an area, we examine how other surveys review the security aspects of IoT devices. Given this concern, the search started from "IoT survey" and ended in "security survey in IoT".

2.2.3. Finding gaps

Analysis of prior works helped us establish the research gap. None of the previous surveys consider the security of IoT devices based on their lifecycle, and they ignore the importance of security over the entire lifecycle. To fill this gap, we set out to analyze earlier solutions to build a new taxonomy of IoT security.

2.3. Conducting Review

2.3.1. Creating taxonomy

Before creating the taxonomy, it is of utmost importance to meticulously examine the appropriate phases over each lifecycle stage. On the other hand, all security challenges related to IoT devices should be identified. Once the security challenges are recognized, they can be grouped based on the device lifecycle. Such categorization leads to a proper taxonomy.

2.3.2. Finding solutions

Based on the defined taxonomy, the existing security solutions for each security challenge are extracted from the database.

2.4. Compiling Findings

2.4.1. Temporal study of the references in the article

A temporal study of the referenced articles has been performed in this section. It is crucial to evaluate the sequence of events associated with the advancement of IoT security in product lifecycle stages and the related concerns in attaining higher levels of security. Fig. 5 elaborates the publishing trend of the references investigated in the area of IoT security over the past decade from 2009 to 2019. The publishing trend indicates that the research on IoT security has been advancing rapidly over the last few years. Fig. 6 illustrates the related papers' count, demonstrating the solutions proposed in the literature for the corresponding security phase in each lifecycle stage. The evolution of the security problems in the past decade is being depicted in Fig. 7. It demonstrates which security challenges have been more prominently

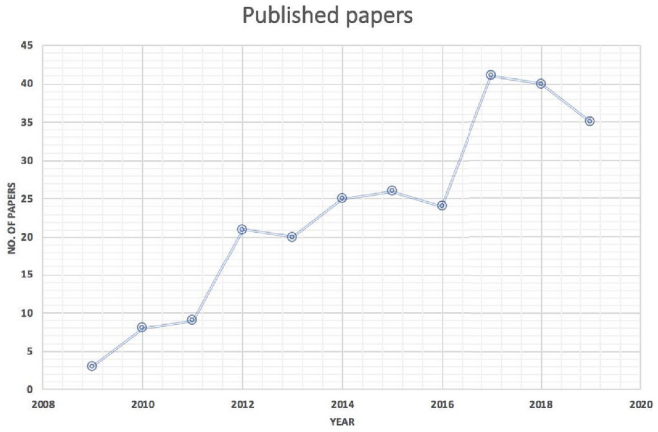

Fig. 5. Publishing trend in the domain of IoT security.

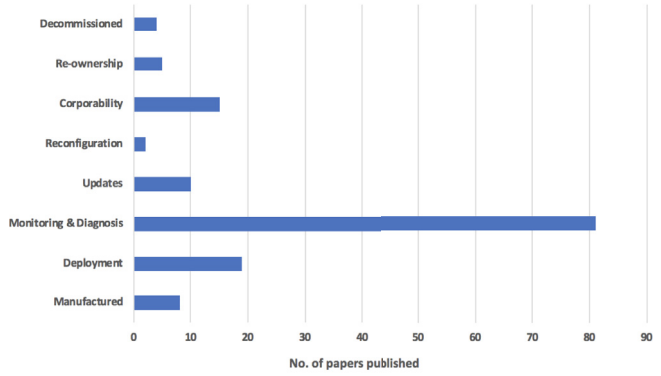

Fig. 6. Papers published in each lifecycle security phase.

targeted by researchers each year, portraying the evolution of the security challenges in the product lifecycle stages in a chronological order.

2.4.2. Comparative analysis

A comparative analysis is described in Section 10 to characterize security challenges and their solutions based on lifecycle of IoT devices.

3. Related research

When reviewing the literature, IoT-related security survey articles can be categorized into two groups: IoT general purpose surveys and IoT security surveys. They are described in detail below.

3.1. IoT surveys

There are several surveys in the area of IoT representing IoT vision (Gubbi et al., 2013; Miorandi et al., 2012; Atzori et al., 2010), architecture (Al-Fuqaha et al., 2015), elements (Gubbi et al., 2013; Al-Fuqaha et al., 2015), applications (Miorandi et al., 2012; Atzori et al., 2010), common standards (Al-Fuqaha et al., 2015), and challenges faced particularly in industry (Xu et al., 2014a). Some of them analyze all of these features for one kind of objects, such as Internet of underwater things (Domingo, 2012). Other surveys focus on protocols belonging to a specific architectural layer, e.g., application layer (Karagiannis et al., 2015). Most of the IoT generic surveys state security issues as a key set of research channel since they play a fundamental role as enablers of IoT applications (Miorandi et al., 2012). IoT surveys which specifically review security aspects in the IoT environment will be demonstrated in the following section.

3.2. IoT security surveys

To gain a comprehensive picture of what currently considered an IoT security survey, we conducted a comprehensive search through the ACM and IEEE literature databases for a security concept in the realm of IoT and collected all existing survey papers about the security in IoT and checked whether such taxonomy (device or product lifecycle) has already been proposed or not. According to our research, none of the previous surveys use lifecycle as taxonomy while most of them adopt IoT architecture layers for categorizing the existing security solutions. In addition, by means of these surveys, we can review the vision of IoT security (or security aspects in IoT) including security attacks, security architecture, security requirements, security issues or challenges, security technologies, and security solutions.

Based on the current literature, *security aspects* in IoT can be classified as security architecture, security model of a node, security bootstrapping, network security, and application security (Heer et al., 2011). If security and privacy were regarded as two separate aspects, security concerns can be classified to three categories including back-end of systems, network, and front-end equipment, whereas privacy concerns should be considered in the device, during communication, in storage, and at the processing stage (Kumar and Patel, 2014). In addition, security concerns can be listed according to security architecture, for example, lightweight encryption and key agreement in the perceptual layer, identification and encryption in the network layer, secure cloud computing and anti-virus in the support layer, authentication and privacy in the application layer are security requirements in each layer (Suo et al., 2012).

Security challenges or issues in IoT can be divided into Identity and Authentication, Access Control, Protocol and Network security, Privacy, Trust, and Fault tolerance (Roman et al., 2013). Other security challenges can be Enforcement, Secure Middleware, Mobile Security (Sicari et al., 2015), Key Management, Security law and Regulations, and Security Requirements (Suo et al., 2012). Some researchers shorten the list and consider only user Privacy, Authentication, Authorization, and Trust Management as possible security challenges in IoT (Abomhara and Køien, 2014). Moreover, such challenges can be analyzed in each

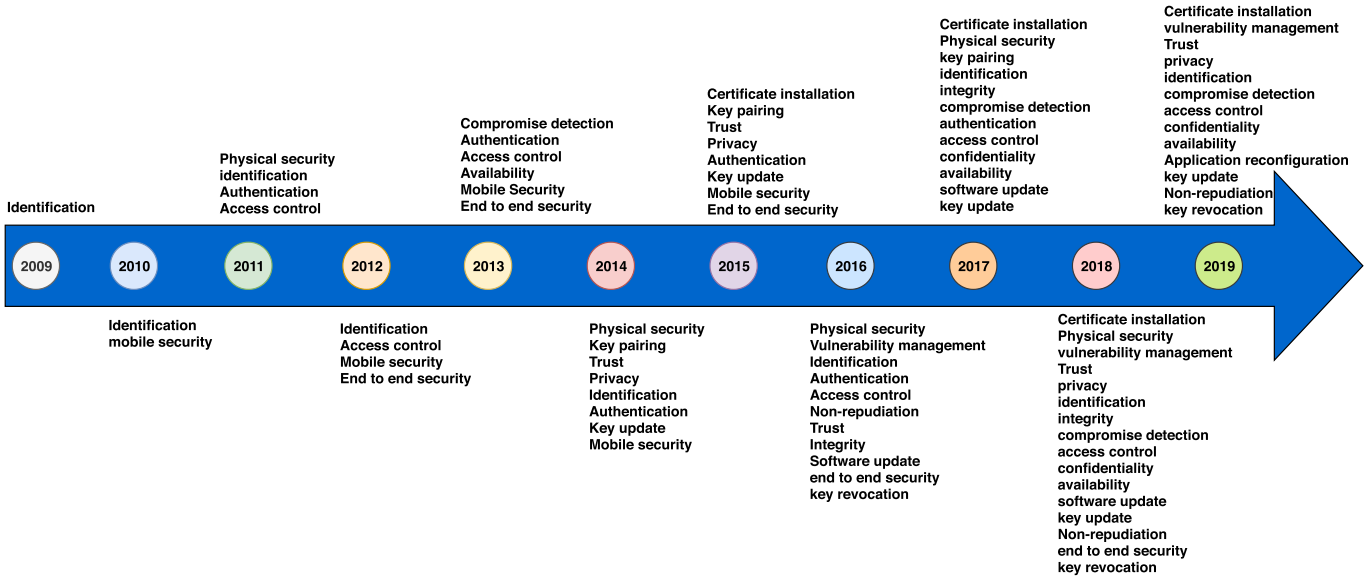

Fig. 7. Evolution of security challenges in product lifecycle: chronological order.

architectural layer of IoT systems including Perception, Network, and Application (Yang et al., 2017; Gou et al., 2013). *Security requirements* as important security challenges are listed as Availability (avoiding DoS), Failure Prevention (preserving integrity), and Confidentiality over code, data, and System Configuration (Sadeghi et al., 2015) along with other requirements such as Authentication, Confidentiality, and Access Control (Sicari et al., 2015). On the other hand, Babar et al. (2010) consider security requirements as Resilience to attacks, Data Authentication, Access Control, Privacy, and so on. Weber (2010) also represents security and privacy requirements in IoT based on security legislation in IoT.

Once we know the requirements and challenges toward IoT security, the next step is to find the *security solutions*. The security solutions can be divided into IP-based security solutions and Wireless Sensor Network (WSN) security (Heer et al., 2011) or they can be presented on each layer of the IoT architecture whether through a 4-layer architecture including Perception (or physical), Network, Middleware, Application layers (Farooq et al., 2015; Granjal et al., 2015) or through 3-layer architecture including Perception, Network, and Application layer (Zhao and Ge, 2013). Generally, most of the existing security technologies such as encryption, communication security, protecting sensor data, and cryptography algorithm can be employed in IoT environments (Suo et al., 2012).

Apart from common security taxonomies, some surveys analyze the security of existing IoT-specific frameworks and middleware. For instance, Ammar et al. (2018) compare the security of the eight main IoT frameworks (set of guiding rules, protocols, and standards) including AWS IoT, ARM mbed IoT, Azure IoT Suite, Brillo/Weave, Calvin, HomeKit, Kura, and SmartThings. Their comparison shows that these frameworks use the same standards for securing communications while different methodologies for other security properties (e.g., authentication and authorization). Additionally, Fremantle and Scott (2017) provide a literature review based on a matrix of security and privacy threats for IoT and review the available middleware such as FIWARE, Device Cloud, DREMS, and OpenIoT and how security is handled in these middleware approaches utilizing various security requirements.

3.3. Comparison of existing security surveys

The comparison of the current security surveys is demonstrated in Table 1. Approximately 40 conference papers and journal articles examine the security problems and solutions for the IoT environment; however we explore only 27 of them which were published in journals. Amongst the security challenges which were raised in the previous subsection, the most common and important challenges are stated in the table, along with the methodology which the authors adopted to categorize such challenges and their solutions. According to the Methodology column, the current literature explores security challenges and countermeasures from the layer-level perspective or other context so that first, the survey paper introduces an architecture or a baseline, then analyzes the security issues such as attacks/threats and/or requirements/measures based on the architecture layers (Alaba et al., 2017). However, we introduce new categories based on lifecycle which includes all possible security issues in all phases and stages of an IoT device.

Moreover, as seen in the table, none of the survey articles could cover all the security challenges, neither the security issue nor the solution. Further, such articles only define the security requirements as mentioned in the table and rarely present solutions for such requirements. In contrast, in the current review, we contribute to all of the essential security requirements by considering the solutions on the beginning and middle of life. As the last comparison criterion, we investigate whether any article applies PLC in their taxonomy or not. There are only two papers on this domain. Nguyen et al. (Nguyen et al., 2015) observe one specific security issue (key bootstrapping) in the bootstrapping phase of lifecycle. Heer et al. (Heer et al., 2011) also list a number of security requirements during the bootstrapping and operational phases. As a comprehensive analysis, we introduce a new taxonomy where security challenges and their solutions are described throughout the entire lifecycle of devices, consisting of the beginning, middle, and end of life.

4. IoT product lifecycle security

Based on the definition presented by (Rink and Swan, 1979), Product LifeCycle (PLC) represents the product's unit sales curve, extending from its first placement in the market to its removal. In other words, PLC is a sequence of stages for a new product, progressing from introduction to growth, maturity, and decline (The product life cycle. Q). *Introduction* is the gradual sales hike which accompanies a new product introduction in the market; *growth* is considered the accelerated sales hike which leads to product acceptance in the market; *maturity* is the crest of sales growth with the product acceptance by potential buyers; and *decline* is expected as the sales decline resulting in product replacement or discontinuation (Jeong, 2010). Depending on the use case, these stages might have less or more importance. For example, in the lifecycle of wind turbines, among these stages, the introduction (or production) and decline (or disposal) are the most important phases (Weinzettel et al., 2009). Additionally, lifecycle processes contradict the targeted products, hence they can be categorized into three stages as *Beginning of Life* (BoL), *Middle of Life* (MoL), and *End of Life* (EoL) (Lehmhus et al., 2015) (Fig. 8). BoL is where everything related to product development is concentrated, including design, testing, and production. Once the device is produced, a longer stage, MoL, materializes to encompass the majority of marketing and sales endeavors, usage, and services. When the product is discontinued, the last stage will be commenced. Depending on the type of product and its possible problems, EOL might be scheduled to recycle, refurbish, or dispose of the product.

Lifecycle-based approaches are necessary to use for evaluation of several industrial systems (e.g., renewable energy systems (Weinzettel et al., 2009)). For instance, in order to evaluate the environmental impact related to a product from material extraction and manufacturing to the disposal, LifeCycle Assessment (LCA) was developed (Weinzettel et al., 2009). LCA identifies the most adequate strategies to improve and avert shifting of burden among various environmental impacts which occur throughout the complete value chain (Hellweg and. i Canals, 2014). Tao et al. (2014a) design one kind of an LCA system based on IoT technologies.

4.1. Product lifecycle in IoT (lifecycle and IoT)

Identically with industrial systems, IoT systems also require analysis through their lifecycles. There are different categories for device lifecycle in IoT. Heer et al. (2011) divide the lifecycle of an IoT device into three stages: Bootstrapping, Operational, and Maintenance and Rebootstrapping. As seen in Fig. 9, the last two stages will be repeated as time passes by. Cai et al. (2014) propose a framework for Product Lifecycle Management (PLM) which covers all requirements given from IoT object identification, abstracting, disposing, and invoking purposes. This framework consists of three dimensions: lifecycle (design, produce, assemble, utility, maintain, and recycle), product structure (product, components, and parts), and information dimension (real objects and data sources). Furthermore, Tao et al. (2016) define PLC as three steps: design, production (comprising manufacturing and assemble), and service (comprising utility, maintenance, and recycling). IoT services which contain service producer and consumer transaction can also be classified based on their lifecycle as deployable, deployed, and operational (Thoma et al., 2012). IoT technology has sparked a multitude of applications in many domains, including manufacturing industry, healthcare, medical, communication, automotive, and aerospace (Tao et al., 2014b). In manufacturing industry, during the PLC, sev-

Table 1
Previous surveys on security aspects of IoT.

Research paper	Physical security	Key management	Security requirements	Compromise detection	Trust	Privacy	Software update	Mobile security	Methodology	Open issues	PLC
Atzori et al. (2010)			authentication, integrity	✓		✓				✓	
Weber (2010)			authentication, access control, resilience to attack			✓			based on legislation		
Heer et al. (2011)		✓				✓		✓	IP-based security for bootsrapping and operational phase		✓
Miorandi et al. (2012)			confidentiality		✓	✓				✓	
Roman et al. (2013)	✓		identity and authentication, access control	✓	✓	✓				✓	
Riahi et al. (2013), Riahi et al. (2014)			identification, authentication		✓	✓			based on systemic approach	✓	
Yan et al. (2014)					✓		✓		trust managements based on 8 taxonomies	✓	
Sadeghi et al. (2015)		✓	availability, integrity, confidentiality	✓							
Granjal et al. (2015)	✓	✓	confidentiality, integrity, authentication, nonrepudiation	✓					based on communication protocols in 3 layers	✓	
Farooq et al. (2015)			Confidentiality, Integrity, Availability (CIA triad), authentication	✓		✓			based on 4 architectural layers		
Sicari et al. (2015)			authentication, AC, confidentiality		✓	✓		✓		✓	
Nguyen et al. (2015)		✓	confidentiality, integrity, authentication, authorization, freshness			✓			security on bootstrapping phase of lifecycle		✓
Alaba et al. (2017)			authentication, authorization, exhaustion of resources	✓	✓	✓			based on application, architecture, communication, data		
Yang et al. (2017)	✓	✓	authentication, access control	✓		✓			based on 4 architectural layer		
Fremantle and Scott (2017)	✓		confidentiality, integrity, availability, authentication, access control, non-reputation	✓	✓	✓			based on 3 aspects (Hardware/Device, Network, Cloud/Server)	✓	
Mosenia and Jha (2017)				✓		✓	✓		vulnerability at (edge nodes, communication, and edge computing	✓	
Lin et al. (2017)				✓	✓	✓			based on 3 layers		
Mendez et al. (2017)			confidentiality, integrity, availability, authentication, access control	✓	✓	✓			based on 3 layers		
Zarpelão et al. (2017)				✓					intrusion detection taxonomies based on 4 features	✓	
Ferrag et al. (2017)			authentication	✓	✓	✓			Authentication in 4 environment (M2M, IoV, IoE, IoS)	✓	
Ammar et al. (2018)			authentication, access control, secure communication						for each IoT frameworks		
Kouicem et al. (2018)			confidentiality, integrity, authentication, non-reputation, availability		✓	✓		✓	based on each application	✓	
Sfar et al. (2018)			identification, access control		✓	✓				✓	
Hassija et al. (2019)				✓		✓			security using (blockchain, fog, ML, edge)	✓	
Farris et al. (2019)			authentication, authorization	✓		✓			security using (SDN/NFV)	✓	
Din et al. (2019)				✓	✓	✓			comprehensive analysis of trust management		

Fig. 8. The phases of product lifecycle (Lehmhus et al., 2015).

eral applications were presented for IoT. For instance, Yan and Huang (2008) employ an integration of IoT and RFID for the monitoring of anti-counterfeiting for supply chain products.

From 2003, IoT was applied as a fundamental information system which can be used to access product information on Internet (Kärkkäinen et al., 2003). This IoT property can have applications for the entire PLC from BoL including the design phase, production phase, and supply chain tracing and tracking, through MoL, which includes operation and maintenance, all the way to EoL which includes how to recycle and dispose the product (Kiritsis et al., 2003). For this purpose, IoT architectures should be adequately adjustable to be employed in any stage or application of PLC. Therefore, an IoT messaging standard, called the O-MI (Open Messaging Interface) messaging standard, previously known as PLM and QLM (Quantum Lifecycle Management) was presented to fulfill the requirements needed to be satisfied by IoT in any closed-loop PLM (Främling and Maharjan, 2013; Främling et al., 2014). Sodhro et al. (2018) review recent works on combining PLM and IoT. They also propose an integration of IoT and PLM to solve the problems with information sharing and collaboration between several communicating parties.

4.2. PLC and security

Although most IoT solutions concentrate on real-time information, *product lifecycle information* requires more attention to keep track of the product during its entire lifecycle (from designing, manufacturing, distributing, operating, maintaining, and recycling) (Kubler et al., 2015a). From the IoT perspective, the device (or product) and its personal data all along the device lifecycle should be secured with upmost attention while coping with the device constraints. Through IoT, attacks can mostly be instigated from smart devices rather than computers and common sources (Yang et al., 2017). Hence, these devices are available everywhere, including all essential information stemming from various resources to perform the attacks. It means enough resources for performing DDoS attacks. These devices also collect personal information (e.g., user names, addresses, and their activities), which introduces privacy concerns for consumers. All in all, in IoT environments attacks or security challenges can derive from any unpredictable resources and all the devices are assumed as potential security risks, requiring security measures.

For investigating the possible attacks in manufacturing systems, Chhetri et al. (2018) analyze various security challenges and propose solutions associated with stages of PLC, considering three security fundamentals including confidentiality, integrity, and availability. However, by turning the environment from a manufacturing system into an IoT system, products will face less security support. For instance, IoT-based consumer products lack support in case of security and privacy violations from five different angles: borrow, rent, gift, resale, and retire. Kan et al. (Khan et al., 2018a) explore these consumer acts at different stages of IoT product lifecycle.

5. Security taxonomy in IoT device lifecycle

In Section 4, we observed how IoT is used to manage industrial PLC. IoT devices are considered industrial products which can be deployed for industrial or business purposes. Therefore, as with any industrial product, the lifecycle of IoT devices could also be divided into three general stages: BoL, MoL, and EoL. Each of these stages can be categorized into subcategories. During BoL, the device is manufactured then installed in the smart environment. Next, in MoL, while the device is communicating with other devices, it should be monitored in order to diagnose the possible faults, and according to the monitoring observation to update or reconfigure the device. Finally, in EoL, the device owner will be modified or at the last phase, the device is required to be withdrawn from its service.

IoT may confront more attacks and threats in the near future and right now it is important to know which security challenges we should be concern about in each stage. We can stop the challenges in later stages by designing and developing a secure system at the first stage. For example, in real-life scenarios, *Secure by Design* is a new practice by governments toward a safe and comprehensive IoT ecosystem for consumers. Given this concern, UK government introduces new IoT security laws for manufacturers of connected devices (Plans announced to introd). Furthermore, regular monitoring during the device running as well as device recycling also ensure that the devices still follow their security criteria which were designed. Security issues specified for each of these stages and their subcategories (i.e., phases) are shown in Fig. 10.

First of all, the device is manufactured at the factory where the original manufacturer settings are installed. Security should be conducted from onset in the device itself to present a reliable and attack-resistant infrastructure for a dynamic environment. One of the security challenges that can occur from beginning as manufacturer setting is *certificate installation*, in which the device certificate creates an identity for each device to be applied later during authentication and private communication between devices. Another security challenge in this phase is *Physical security*, also known as hardware security, securing the silicon elements of a device which might be physically accessed. A large number of physical devices are being deployed throughout IoT environments where the security-related information, for instance, removable storage media, accessing software through USBs and easily dissembling devices are believed as vital threats to security (Bertino and Islam, 2017). Once the device is manufactured, it can be deployed in the target environment where device certificates could also be installed, instead of the previous phase. Setting up and configuring the device is considered a primary process to the vendor for evaluating the security flaws, as several insecurities exist during device configuration (Alrawi et al., 2019). IoT device configuration insecurities can be exploited, for example for gaining access to end-user privilege and spying (Barnes).

To securely build an IoT ecosystem, while on-boarding the IoT devices, a strong and unique identity within each device should be established; the process known as *identification*. During the deployment, devices pair the security keys with other previously deployed devices, establishing a trusted channel between users and their devices. Thus, one security challenge is *pairing* or key agreement between devices without any prior security association. Possible object weakness should be exploited, the activity known as *vulnerability assessment*. All necessary mitigation measures should be considered and implemented at the very beginning since any vulnerability compromises the entire system. Furthermore, before allowing the device to operate, strict security policies should be properly formulated and implemented to configure the device (Alrawi et al., 2019) and enforced throughout their lifecycle (Babar et al., 2011). The importance of these policies underline the significance of considering *Security requirements* including authentication, access control, confidentiality, integrity, and availability. Device *authentication* ensures that only authorized devices can connect to a given service and *access control* limits the device access to the resources. Data *confidentiality* protects data from being accessed by unauthorized parties. *Integrity* means that information is not altered, and the source of the information is original. *Availability* ensures that information is accessible by authorized users.

The device is manufactured and deployed in the environment then it is ready to be used. During the operation stage (i.e., MoL), the device

Fig. 9. Lifecycle of a device in IoT (Heer et al., 2011).

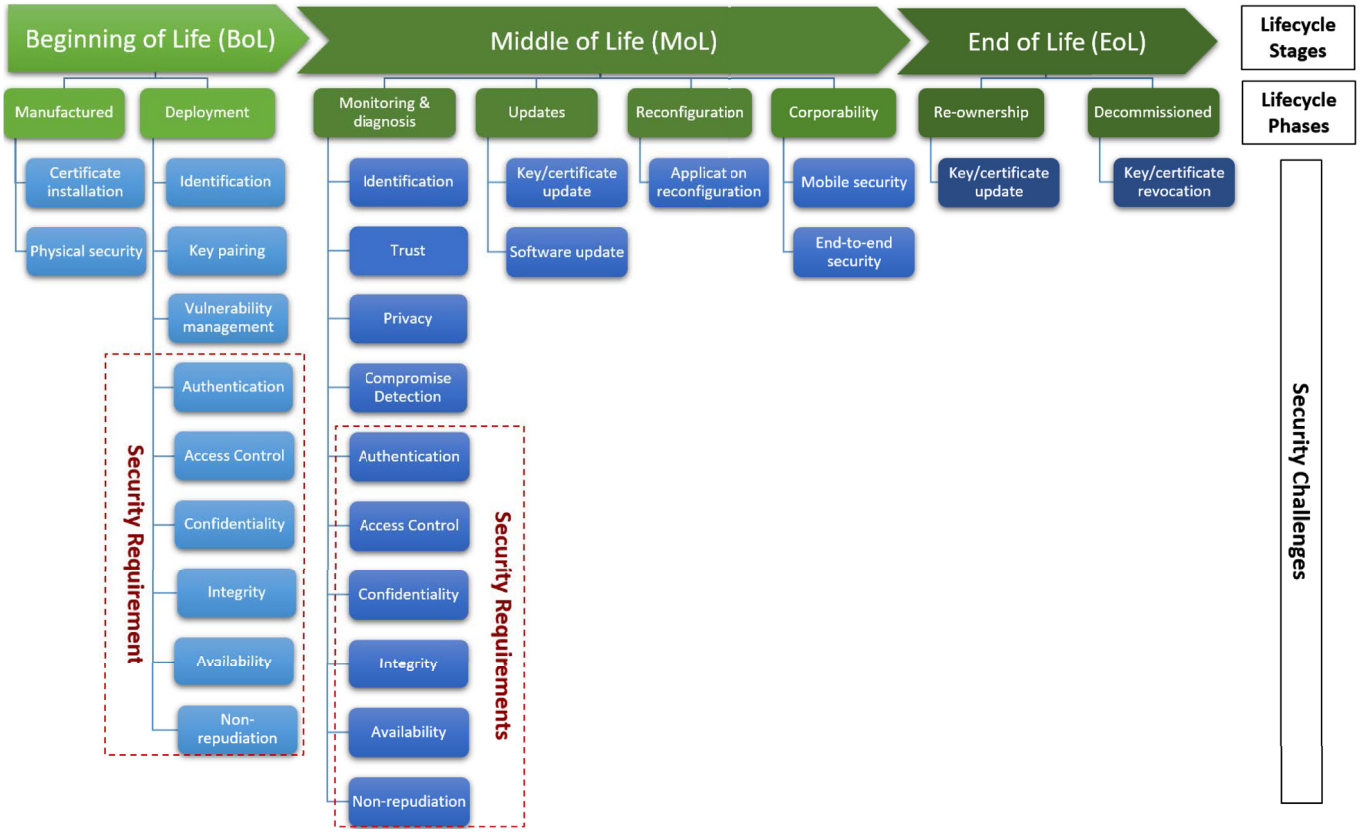

Fig. 10. Security taxonomy in IoT device lifecycle.

has to be monitored continuously so that the possible malicious activity can be diagnosed, patched in subsequent software (or firmware) updates or reconfigured through application. If the device is mobile, the security should also be provided in new clusters. During the phase of *Monitoring & diagnosis*, the main security challenge is in managing the equilibrium between *trust* in the provider of service and privacy of individuals, contemplating automated complex personal information exchange (Daubert et al., 2015). Since the data in IoT are shared between devices and users, the device *privacy* or user's personal information should be preserved. At the same time, to apply the shared data, devices require defined *trust* levels. Prior to managing trust and privacy, the IoT system requires connected devices to have unique identifiers during their operation (*identification*). The next security challenge in this phase is *compromise detection*, where an uncontrollable threat might be found which is often impossible to be identified in advance, in BoL. *Security requirements* are the next problem in the current phase. As mentioned above, they have to be enforced throughout the device lifecycle, particularly when they are running services while communicating with other devices and servers. Such requirements can be defined similarly to those explained in the deployment phase, except they are more significant during their operation in MoL.

Once a threat or malicious activity is diagnosed, managing the software or *firmware updates* for devices in IoT environment is equally fundamental. The session *Key update* also occurs When a device joins or leaves the system for assurance of backward and forward secrecy, specifically in group key agreement. Occasionally, applications should also be reconfigured to improve the flexibility in a dynamic environment; however, it will be challenging since IoT devices have constrained memory and cannot store every possible application. To emphasize device corporability, end devices' security amidst device and service provider, called *end-to-end security*, is one security challenge during the device operation. It assures both devices that communication is confidential and cannot be modified in the transit (Abomhara and Køien, 2014). Additionally, in this step, mobile security is a security issue for consideration since some IoT devices move among the clusters and handling the security aspects of the device in a new cluster is challenging for the device vendor.

Finally, the last stage is EoL (or repurposing), where devices come to the end of their life while being *decommissioned* or facing *re-ownership*. During the re-ownership phase, the device is sold to another person. As a result, all personal or secret information such should be erased or updated from it before handing over the device. One important secret information on all the devices to be updated is key or certificate. Dur-

ing the decommissioned phase, the device is no longer operational and must be disposed of. During removal, it is important to have all secret information such as key and certificates revoked so that no information leaks from the system. EoL including Decommissioned and Reownership is the main contribution of the current paper as none of the surveys in our review examined it. When a device (e.g., smart car) holding private information of the current owner (e.g., location data, Garage door codes, Phone contacts, and address book) is sold to a new owner, it is essential to manage the security aspects.

Five out of eight key challenges in IoT product lifecycle are associated with security issues found in the taxonomy; Network security, Data confidentiality and encryption, Objects safety and security, Information Privacy, and Naming and Identity Management (Khan et al., 2012). Common security solutions are useable in the IoT environment to some extent, although these security solutions require consideration of the specific features of IoT systems. Fig. 11 illustrates the citations of the various security solutions adopted by the earlier researchers in a hierarchical manner to secure various security challenges in various product lifecycle stages. It provides an overview of the general findings of the paper. Table 2 displays the existing studies contributing to each security challenge according to the lifecycle stages of BoL, MoL, and EoL. A detailed description of such security solutions related to each of the categories will be reviewed in the following three sections according to their order at lifecycle.

6. Security solutions in beginning of life (BoL)

This section discusses the proposed security solutions in BoL and categorizes them based on various lifecycle phases of *Manufactured* and *Deployment*.

6.1. Manufactured

This lifecycle phase can involve two security challenges i.e., certificate installation and physical security. The following sections present the proposed solutions for each of these security challenges.

6.1.1. Certificate installation

Deploying certificates in network scenarios has benefits such as no need for extra hardware, no burden on end user, and featuring a simple lifecycle management. Considering these benefits, it can be used for several purposes including mutual authentication, easily deployed with optional automatic installs and renewals, and native compatibility with applications and networks.

The certificate might be installed in beginning of life during the manufactured phase or deployed phase. The IoT device can present manufacturer-installed device certificate as part of the initial authentication process (Pularikkal et al., 2018) or can employ implicit certificates for mutual authentication between end-users and sensors by requesting security-related information and certificates from the trusted authority (Porambage et al., 2014a). However, in the IoT environment, the connection to an online Certificate Authority (CA) is usually unavailable or unstable (Chien, 2018). Therefore, the role of CAs should be assigned to distributed nodes (Won et al., 2018). On the other hand, in the absence of standard protocols for installing and updating the certificates, it is troublesome for the owners of IoT devices to manipulate the certificates for their devices. Thus, device manufacturers often install certificates on the devices on behalf of the device owners. This also increases the leakage risk of privates keys from manufacturers (Won et al., 2018). For this reason, an extra validation center, called certified accreditation center, can verify the validity of the manufacturer and the device (García-Magariño et al., 2019). A summary of solutions for certificate installation in IoT is presented in Table 3.

6.1.2. Physical security

The distributed nature of IoT makes it attractive to a larger attack surface and physical access to the devices. The combination of these two factors makes physical security a viable and potent threat to IoT devices. However, we expect most security attacks to take place at the software level due to its popularity and coverage of a multitude of devices, but most unusual attack happen on physical signals (Xu et al., 2014b). Thus, security should be considered right from the beginning of device design for providing an adjustable base for dynamic detection and prevention, isolation, diagnosis, and remedies counter to strong breaches (Babar et al., 2011).

In general, physical attacks are concentrated on the physical components of the IoT system and the attacker need to be physically close or in the IoT system (Andrea et al., 2015). Some physical attacks pose severe security problems where hardware devices are tampered for example by extracting sensitive information using micro-probing. These attacks can also be triggered by reverse engineering, which has several steps including chip de-packaging, layout reconstruction, and chip modification using particle beam techniques (Babar et al., 2010). On the other hand, physical attacks can occur on the infrastructure of an IoT, e.g., changing the behavior or structure of IoT devices (Nawir et al., 2016). On such a category, an attacker can cause damage to sensor nodes physically or remotely (node tampering), can prevent communication by sending noise signals over the communication channel (RF interference on RFIDs and node jamming in WSN), can control the node or the entire system by means of physically deploying a new malicious node (malicious node injection) or physically injecting codes (malicious code injection), and finally can increase the power consumption by keeping the node awake (sleep deprivation) (Andrea et al., 2015). Fig. 12 shows these two categories and their subcategories for physical attacks.

Physical security is mostly targeted in Perception layers of the IoT architecture in which RFID and WSN are two important components. From the RFID perspective, SCA (Side Channel Attack) can pose a major problem while from the WSN perspective, node and antenna design are considered important (Zhao and Ge, 2013). To address physical security in IoT, Table 4 shows the summary of approaches. For instance, Babar et al. (2011) propose an embedded security framework in which physical security is provided by employing a Trusted Platform module to manage the vulnerabilities of the hardware devices at the physical level. As a hardware-based IoT security approach, Xu et al. (2014b) adopt Computer-aided design (CAD) techniques to address IoT security constraints alongside with energy problems.

In order to discover proper countermeasures to physical attacks, critical physical assets in an environment can be identified assessing the security risks of a smart environment. For instance, Ali and Awad (2018) apply the operationally critical threat, asset, and vulnerability evaluation (OCTAVE) methodology for identification of security risks in smart homes. During the system design and operation phases, a management procedure mixture (e.g. for tracking misplaced devices) and protocols (e.g., internal memory reset, renewal of keys) can be applied as a security framework to configure the devices through a secure channel (Pecorella et al., 2016). Another secure analytical framework for IoT was proposed based on stochastic geometric and queue theory to investigate the delay performance and security performance of IoT networks (Zhang et al., 2017a).

Combining the physical layer security with upper layer security mechanisms could enhance the information security in the multi-access mobile edge computing (MA-MEC) based IoT. Physical layer security approaches involve the secure wiretap coding, resource allocation, signal processing, and multi-node cooperation, along with the physical layer key generation and authentication (Zhang et al., 2017a).

6.2. Deployment

Since not all manufacturers are willing or capable to manage security critical tasks, it is not acceptable to expect manufacturers to provide

Fig. 11. Overview of the literature for security mechanisms in IoT product lifecycle.

Table 2
Security issues in each phase of lifecycle.

Lifecycle stage	Security issue	Citations
BoL	Certificate installation	(Sciancalepore et al., 2015; Hänel et al., 2017; Won et al., 2018; García-Magariño et al., 2019)
	Physical security	(Babar et al., 2011; Xu et al., 2014b; Pecorella et al., 2016; Zhang et al., 2017a; Ali and Awad, 2018)
	Identification	(Attaran and Rashidzadeh, 2016; Miettinen et al., 2017; Berelejis et al., 2017; Corchia et al., 2019)
	Key pairing	(Sciancalepore et al., 2015; Miettinen et al., 2014a; Tsai et al., 2017)
	Vulnerability management	(Alrawi et al., 2019; Samtani et al., 2016; Alghamdi et al., 2018; Wang et al., 2018; Costa et al., 2019)
	Authentication	Neto et al. (2016)
Access control	Neto et al. (2016)	
	Confidentiality	Valea et al. (2019)
	Integrity	(Zhang et al., 2017b; Chamarajnagar and Ashok, 2019)
	Availability	(Wu et al., 2019; Mustafa et al., 2019)
	Non-repudiation	Oriwoh et al. (2016)
MoL	Identification	(Sarma and Girão, 2009; Mahalle et al., 2010; Hu et al., 2011; Horrow and Sardana, 2012; Fremantle et al., 2014; Fremantle and Aziz, 2016; Meidan et al., 2017; Kravitz and Cooper, 2017; Song et al., 2017; Yousefnezhad et al., 2018; Santos et al., 2018, 2019)
	Trust	(García-Magariño et al., 2019; Chen et al., 2014, 2016; Namal et al., 2015; Alexopoulos et al., 2018; Tariq et al., 2019; Alshehri and Hussain, 2019)
	Privacy	(Ukil et al., 2014, 2015; Boussada et al., 2018; Jourdan et al., 2018; Guan et al., 2019)
	Compromise detection	(Raza et al., 2013; Taneja, 2013; Jia et al., 2017; Nguyen et al., 2018; Doshi et al., 2018; Li et al., 2019; Yahyaoui et al., 2019)
	Authentication	(Zhao et al., 2011; Alcaide et al., 2013; Porambage et al., 2014a; Petrov et al., 2014; Mahalle et al., 2014; Shivraj et al., 2015; Crossman and Liu, 2015; Devi et al., 2015; Kalra and Sood, 2015; Fan et al., 2016; Yang et al., 2016; Aman et al., 2017; Li et al., 2017)
	Access control	(Zhang and Gong, 2011; Mahalle et al., 2012a, 2012b, 2013; Anggorojati et al., 2012; Liu et al., 2012; Ramos et al., 2013; Gusmeroli et al., 2013; Moreno-Sanchez et al., 2013; Riad and Zhu, 2017; Huang et al., 2018; Kolluru et al., 2018; Hwang et al., 2018; Bouanani et al., 2019; Pal et al., 2019; Salonikias et al., 2019; Ding et al., 2019)
	Confidentiality	(Purohit et al., 2017; Al-Turjman and Alturjman, 2018; Khalaf and Mohammed, 2018; Eugster et al., 2019; Hurrah et al., 2019)
	Integrity	(Bauer et al., 2016; Bhattacharjee et al., 2017; Aman et al., 2018; Battisti et al., 2018)
	Availability	(Kryvinska and Strauss, 2013; Kolisnyk et al., 2017; Tsai et al., 2018; Qaim and. Özkasap, 2018; Dinh and Kim, 2018; Xiong et al., 2019; Yang and Kim, 2019)
	Non-repudiation	(Abbas et al., 2019; Xu et al., 2019)
	Key/Certificate update	(Mahalle et al., 2014; Abdmeziem et al., 2015; Kung and Hsiao, 2018; Chien, 2018; Arif et al., 2019)
	Software update	(Huth et al., 2016; Weißbach etal., 2016; Boudguiga et al., 2017; Kim et al., 2018; Kolomvatsos, 2018)
	Application reconfiguration	(Zhang et al., 2005; Samir et al., 2019)
	Mobile security	(Yan and Wen, 2010; Miao and Wang, 2012; Zhu et al., 2012; Jara et al., 2013; Gonçalves et al., 2013; Kai et al., 2013; Jeong et al., 2014; Niu et al., 2014; Kubler et al., 2015b)
	End-to-end security	(Brachmann et al., 2012a; Hummen et al., 2013a; Sahraoui and Bilami, 2015; Moosavi et al., 2016; Hossain et al., 2016; Banerjee et al., 2018)
EoL	Key/Certificate update	(Leng et al., 2014; Ghuli et al., 2017; Mamun et al., 2018; Khan et al., 2018b; Aghili et al., 2019)
	Key/Certificate revocation	(Raza et al., 2016; Duan et al., 2018; Bock et al., 2019; Cebe and Akkaya, 2019)

Table 3
Certificate installation solutions in IoT.

Scheme	Method	Remarks
Won et al. (2018)	IoT-PKI, a distributed and secure PKI	assigning the role of CAs to distributed blockchain nodes
Hänel et al. (2017)	ASREID, an adjustable security system for RFID-equipped sensors	reducing the overhead of device pre-equipping of security information by providing various selection for pre-installed certificates
Sciancalepore et al. (2015)	preloading certificates in each device by the network administrator before the deployment of the network	generating ultra-lightweight "implicit" certificates exploiting the Elliptic Curve Qu-Vanstone (ECQV) technique
García-Magariño et al. (2019)	digital certificate for authenticating vehicles	requesting a digital certificate from certifier, checking the vehicle by certified accreditation center, and incorporating private key to the vehicle

security critical services (Sethi and Aura). Thus, security should be considered during other phases such as device deployment and operation. Security issues targeting the deployment phase are discussed below.

6.2.1. Identification

The multitude of physical devices and users rely on trusted services to authenticate with each other, so it is crucial for IoT to have identity authentication (Abomhara and Køien, 2014). The analysis of the five applicable Service Oriented Architecture (SOA)-based identity management, i.e., Higgins, Shibboleth, Card-Space, Liberty Alliance and OpenId demonstrates that IoT requirements are fulfilled by any of them, hence requiring advanced IDM systems (Mahalle et al., 2010). Currently, identities are used as an entity for every end-user device, allowing them to identify themselves using their own identity (Roman et al., 2011a).

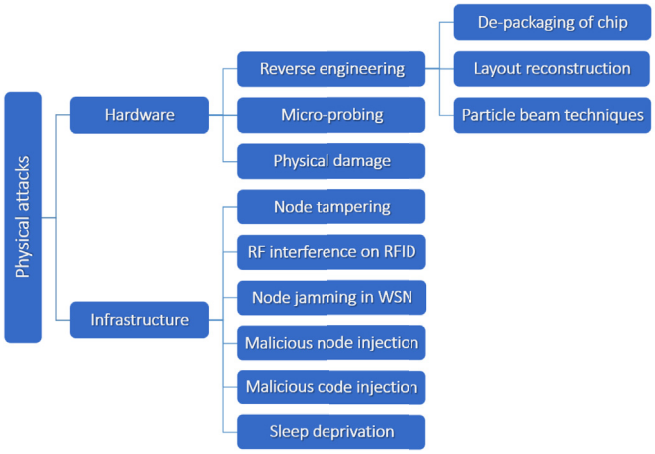

Fig. 12. Physical attacks.

To apply identification in the deployment stage of IoT devices, one possible solution is to improve the installed RFID tags. For this reason, chipless RFID tags were implemented, which can be programmed to a unique code by end-users (Attaran and Rashidzadeh, 2016). Chipless tags are resistant to a harsh environment and thus they can be employed in wearable electronics. To solve the problem of data encoding in tags with no IC, two encoding strategies, resonance-based coding and frequency-shift encoding, were presented by Corchia et al. (2019). In addition, Miettinen et al. (2017) propose an identification method for new devices joining the network (e.g., home network). In the home gateway, it checks the packets coming from the new device, creates a matrix for this device based on its behaviors (column = a packet, row = feature), and uses Random Forest to classify the device either as trusted or non-trusted. If it is untrusted, it can send the packet to internet but not to other trusted nodes inside the network. Device identification can also be verified by an IoT device image which is captured and received from a user device, showing some portion of the environment around the IoT device (Berelejis et al., 2017). A summary of the identification methods in the early stage is presented in Table 5.

6.2.2. Key pairing (key agreement)

Key pairing as initiation step of key management, establishes keys for other security solutions, such as secure communication, authentication, and access control (Miettinen et al., 2018). For this purpose, Roman et al. (2011b) analyze the role of current key management systems in IoT and conclude that they could be employed in Internet-enabled sensor (IoT) networks. For this purpose, first they find security issues of a globally connected WSN including secure channels and key management. Then, they analyze the suitability of public key cryptography (PKC) and the protocols for pre-sharing keys for negotiation of session keys amidst the sensor device and other entities externally in the internet. Finally, they analyze other KMPs for WSN (e.g., mathematical-based KMS) for checking the usage of KMS protocols in negotiation of session keys among the remote entities.

As part of key management, key pairing is a central agreement between personal devices without any prior security association. Table 6 summarizes the current approaches for key pairing. For example, Sciancalepore et al. (2015) adduced a protocol based on key management for IoT systems using Elliptic Curve Cryptography (ECC) providing security benefits such as protection against replay attacks, fast re-keying, lightweight node authentication and robust key negotiation. During pairing, the user is typically involved in verifying the key negotiation for example by comparing the authentication string. However, it is cumbersome and error-prone to involve the user. Thus, Miettinen et al. (2014a) present a secure zero-interaction pairing well suited for wearable and other IoT devices. In this scheme, the correct devices are identified based on sustained co-presence over time by computing a fingerprint of the ambient context.

6.2.3. Vulnerability management

A vulnerability refers to a known weakness in a device where an attacker circumvents the security controls by manipulating any physical device. A considerable number of IoT devices available publicly with consumers are at risk of vulnerability (Williams et al., 2017). Therefore, to ensure the continued security of systems, testing for vulnerabilities is critical for a quick response. Further, vulnerability management is employed by IoT device vendors to identify vulnerabilities within their system and mitigate them prior to exploitation (Samtani et al., 2016). Vulnerability management in IoT firmware is classified into four types: static analysis, symbolic execution, fuzzing on emulators and comprehensive testing (Xie et al., 2017).

Vulnerabilities might be different, depending on the target environment. For instance, in smart homes, exploited vulnerabilities are more likely to stem from lacking security updates, insecure web application and services authentication, insecure services exposed to the internet, and insecure network communications (Costa et al., 2019). Once vulnerabilities and attack techniques are identified by some tools such as IoTVerif (Alghamdi et al., 2018), some mitigation should be proposed. Alrawi et al. (2019) present some mitigation to address vulnerabilities during device deployment in smart homes, relying on analysis of components such as mobile application, service communication channels and end-points. A summary of vulnerability identification and assessment techniques is displayed in Table 7.

6.2.4. Security requirements

Security requirements are measures that are employed to protect the device and device communications. The primary security goals including integrity, availability and confidentiality, are used to derive these security requirements as listed in the following sections.

Authentication: A key contributor to several documented attacks can be weak or IoT services may lack authentication (Alrawi et al., 2019). In order for the attackers to prevent insertion of a malicious activity to

Table 4
Physical security in IoT.

Scheme	Method	Remarks
Babar et al. (2011)	embedded security framework (in-built security in the device)	providing a dynamic prevention, detection, diagnosis, isolation, and countermeasures against breaches
Ali and Awad (2018)	risk assessment approach	identifying security threats and the potential risks emanating from inside and outside smart homes
Xu et al. (2014b)	Computer-aided design (CAD)	using hardware-based security approaches to be more resilient against side-channel and physical attacks
Pecorella et al. (2016)	a security framework for the device initialization	providing a secure and error proof configuration for cryptographic keys of devices
Zhang et al. (2017a)	physical layer security for securing IoT	appropriate for the secure application scenarios with low-cost and energy-limited devices

Table 5
Identification during BoL in IoT.

Scheme	Method	Remarks
Miettinen et al. (2017)	IOT SENTINEL, an automated device-type identification	identifying the types of devices introduced to a network and employing mitigation measures for device-types with potential security vulnerabilities
Attaran and Rashidzadeh (2016)	chipless RFID tags	using micro-electromechanical systems (MEMS) technology
Corchia et al. (2019)	robust chipless identification tags	using two strategies for encoding information in chipless tags
Berelejis et al. (2017)	device identification with an image of the IoT device	capturing the image by user device and transmitting the image from the user device to the IoT device

Table 6
Key pairing in IoT.

Scheme	Method	Remarks
Miettinen et al. (2014a)	zero-interaction pairing	identifying the correct device based on sustained co-presence over time by computing a fingerprint of the ambient context
Sciancalepore et al. (2015)	robust key negotiation, as part of key management protocol	using ECDH algorithm to ensure secrecy
Tsai et al. (2017)	key establishment scheme by Kronecker product	computing the pairwise key with no communication while decreasing the storage cost and computation cost

Table 7
Vulnerability management in IoT.

Scheme	Method	Remarks
Costa et al. (2019)	a method to identify high-risk vulnerabilities in smart home	verifying if a device is vulnerable to the most common vulnerabilities
Alghamdi et al. (2018)	IoTVerif, an automated tool learning and identifying the secure vulnerabilities	verifying SSl/TLS certificate validation of IoT messaging protocols
Samtani et al. (2016)	active and passive vulnerability assessment	Identifying a multitude of vulnerabilities on Supervisory Control and Data Acquisition (SCADA) systems
Wang et al. (2018)	a vulnerability assessment method	Based on attack graph and maximum loss stream; using Common Vulnerability Scoring System (CVSS) to quantify and calculate the potential risk of attack path
Alrawi et al. (2019)	a modeling methodology on home-based IoT devices	understanding attack techniques, proposed mitigation, and stakeholder responsibilities according to component analysis

the network, there is need for device identity authentication. Further, the service provider must be convinced by the devices for the storage of their information (Horrow and Sardana, 2012). Current authentication mechanisms are accessible to malicious attacks and can distort the advancement due to heterogeneity in IoT devices, topology, and protocols (Shivraj et al., 2015). Such mechanisms are usually designed for special use cases and are difficult to apply on all IoT devices in general. Moreover, most of them facilitate authentication during one stage of IoT device lifecycle, or do not consider all stages at once. For this purpose, an authentication method is designed and developed in (Neto et al., 2016) to provide authentication to all stages in a device's lifecycle (See Table 8).

Access Control (AC): While IoT sensing devices, such as RFID devices perceive corresponding information in the IoT environment, security challenges such as unauthorized access of users, or stealing and modification of information by attackers through a counterfeit of legitimate reader, could be met (Li et al., 2011). Therefore, access of users and devices should be partially covered during the IoT device deployment, through access control mechanism. Access control technologies are well-known in preventing legitimate users to access unauthorized resources and in allowing legitimate users to access only authorized resources (Liu et al., 2012). Access control can also be employed to define a security model during design and implementation, similarly to the access control mechanism proposed in (Yousefnezhad et al., 2017) which is able to regulate the access rights for two IoT-specific messaging standards (i.e., O-MI and O-DF).

According to the most recent surveys on access control approaches in IoT, access control models can be categorized into three architectures: Centralized models eg. RBAC and OrBAC; Distributed models eg. O2O, ABAC, multi-OrBAC, PolyOrBAC, UCON and CAPBAC; Hybrid models eg. Smart-OrBAC (Bouanani et al., 2019). Among these models, RBAC and ABAC cannot be directly used in IoT due to their limitations (Hasiba et al., 2018). To adopt ABAC in IoT systems, Neto et al. (2016) combine ABAC with ABC so that the later cryptographically enforces the former (see Table 9). CAPBAC also has some limitation for IoT since it does not consider the access control decision-making process (Bouanani et al., 2019). A survey on various access control protocols and architectures (i.e., AllJoyn, LMW2M, UMA, ACE, OAuth 2.0, SAML, and XACML) and their applicability in IoT is presented in (Bertin et al., 2019).

Confidentiality: The most fundamental data issue in IoT security is data confidentiality. Data confidentiality ensures that the data should be accessed by authorized entities and prevented from being invaded by unauthorized entities (Lu and Xu, 2019). Confidentiality during deployment can be threatened by many attacks such as malicious data attacks, node capture attacks, timing attacks, and replay attacks similarly to the confidentiality of the perception layer (Lu and Xu, 2019). To ensure confidentiality, cybersecurity mechanisms such as access control, authentication, and data hidden techniques can be employed (See Table 10).

Integrity: Compromises might not be attained from the malicious devices themselves but from their malicious input, e.g., data. Data might be tampered or altered during transmission and during storing on device, by human or by mis-configuration in a computing system. Thus, it is vital to guarantee that data are accurate, consistent and reliable over its lifecycle. This process defines the data integrity. The integrity generated by device, the software running on a device, and data stored in cloud all require to be verified by integrity identification

Table 8
Authentication during BoL in IoT.

Scheme	Method	Remarks
Neto et al. (2016)	Authentication of Things (AoT), authentication during deployment of device	relying on identity-based cryptography to distribute keys and authenticate devices

Table 9
Access control during BoL in IoT.

Scheme	Method	Remarks
Neto et al. (2016)	Authentication of Things (AoT), access control during deployment of device	relying on attribute-based cryptography to cryptographically enforce Attribute-Based Access Control (ABAC)
Yousefnezhad et al. (2017)	authentication and access control	defining design and implementation principles for access control and integrating with O-MI reference implementation

Table 10
Confidentiality during BoL in IoT.

Scheme	Method	Remarks
Valea et al. (2019)	secure context saving unit, a hardware module easily implementable inside a System on Chip (SoC)	providing confidentiality by stream cipher based encryption and integrity by Message Authentication Code (MAC) derived from the saved context

Table 11
Integrity during BoL in IoT.

Scheme	Method	Remarks
Chamarajnagar and Ashok (2019)	integrity threat identification framework	detecting from physical attacks on sensor nodes using outlier detection
Zhang et al. (2017b)	random digital watermarking algorithm as data integrity protection scheme	based on fragile watermark to prevent variety of attacks on perception layer

(Chamarajnagar and Ashok, 2019) and protected by the integrity protection framework (Zhang et al., 2017b). Table 11 shows more details about such frameworks.

Availability: Security of connected systems in IoT is challenging not only because it requires protection against a large attack surface but only because it requires system availability and real time response to the presence of threats. One important aspect of availability is node availability, which is considered an essential index for measuring the node performance in wireless networks. The availability of nodes is defined as the probability that the node can work normally in the network or the probability of the available state when the network reaches a steady state. Such a node state analysis method attacked by malicious programs is analyzed in (Wu et al., 2019), as well as the effects of the degree of node on its availability based on the node heterogeneity. Another approach to measure the availability in industrial IoT systems is to apply inputs of end-to-end QoS analysis, as proposed in (Mustafa et al., 2019). According to the analysis, a remote IoT device inside a busy cloud region generates less availability as compared to an IoT device connected to a less busy cloud region. Table 12 represents a summary of these methods.

Non-repudiation: Non-repudiation relates to data ownership by ensuring that no-one can deny their authenticity. In other words, it is impossible for the sender to deny its sent data and for the receiver to deny its received data (Abbas et al., 2019). Hence, non-repudiation is an important security requirement which provides available evidence through TTP to prevent an entity from denying its action taken place via message exchange (Samaila et al., 2017). Lack of effective non-repudiation triggers lack of guarantee for each parties and it also triggers some attacks such as Repudiation Attack, Masquerading.

Non-repudiation of IoT devices, similarity to other security requirements, should be established from the beginning. Oriwoh et al. (2016) believe that these requirements should be realized at the design phase since any IoT device which can enable communication is also able to include embedded security at the manufacturing. Accordingly, as seen in Table 13, they propose a resource-constrained authentication protocol, where non-repudiation is supported using PKC in a connectionless environment. In addition, a physical-layer authentication and non-repudiation system can be used that authenticates the receiver by employing signal processing and checking if the expected transmitter at the expected location is used for transmission. This method has no energy overhead due to allowing reuse of radio signals on physical layer (Trappe et al., 2015).

Table 12
Availability during BoL in IoT.

Scheme	Method	Remarks
Wu et al. (2019)	node availability analysis in Narrowband IoT (NB-IoT)	by presenting a node heterogeneity model based on node distribution and vulnerability differences then using epidemic theory and Markov chain to establish node state transition mode
Mustafa et al. (2019)	an approach to find end-to-end QoS and availability of service-oriented cloud	running experiments on Device-to-cloud, cloud-to-cloud and inside-cloud

Table 13
Non-repudiation during BoL in IoT.

Scheme	Method	Remarks
Oriwoh et al. (2016)	ReCAP, a resource-constrained authentication protocol	demonstrating the feasibility of achieving non-repudiation

7. Security solutions in middle of life (MoL)

In MoL, while the device is communicating with other devices, it should be monitored in order to diagnose the possible faults, and according to the monitoring observation to update or reconfigure the device. During the operation phase, the device needs to be monitored continuously to detect any malicious activity.

7.1. Monitoring and diagnosis

During the phase of Monitoring and diagnosis, the main security challenge is to manage the trust level between the service provider and the individual's privacy need, considering the automatic exchange of manifold personal information. For each of the security problems in this lifecycle phase, various solutions have been adduced in the literature.

7.1.1. Identification

Sarma and Girao (Sarma and Girão, 2009) introduce device identification for handling data privacy in 2009. They propose the use of identities as representations of all entities including persons, devices, and software as the communication endpoints (Identinet). They also suggest that digital shadows be employed that portray entities projections in a communication use or in sessions. Later in 2012, Horrow and Sardana (2012) presented an identity management framework designed for cloud-based IoT. This framework has several basic functions for devices including relocation, addition and deletion of devices, authentication of sender and receiver devices, hosted services identification and registration of sensors and receiver device to the cloud.

To federate the identity of users and devices in IoT, Fremantle and Benjamin (Fremantle and Aziz, 2016) propose a security model which provides secure, random, and anonymised identities that are not shared with third-parties. In their model, all accesses to device data and commands are based on explicit consent from users. In this model, each user's data are handled by a personal cloud instance providing improved security and isolation. To make federated identities alongside with user-directed access control decisions, Fremantle et al. (2014) show that using OAuth2 as part of the MQTT protocol flow and within an MQTT broker, a technology extracting from Web is more effective. Furthermore, for a cellular IoT environment, identity can be federated by reusing the SIM authentication running over the network layer (Santos et al., 2018, 2019).

Additionally, as a device identification operating for the entire lifecycle of devices, Yousefnezhad et al. (2018) propose a framework based on Measurement-based Device Identification (MeDI), which analyzes the traffic and exploits payload data as well as statistical information to identify the IoT devices.

To manage and secure access to the resources and information and also protecting devices' profiles, an association of technologies and processes, called Identity Management (IdM) is relied on (Mahalle et al., 2010). Mahalle et al. (2010) propose an IdM framework to deliver services of devices, while also providing a device management which conceals the complexity of security management from users. Furthermore, several versions of IdM such as a distributed IdM (Kravitz and Cooper, 2017), improved IdM protocol (Song et al., 2017), and IdM specific to emergency situations (Hu et al., 2011) were proposed as described in Table 14.

7.1.2. Trust

An important problem in the IoT environment is the lack of trust on IoT devices. Trust establishment in remote IoT devices can be achieved with the help of a security service called remote attestation, which helps verify the remote computing devices' state (Abera et al., 2016). To allow trust management, in which devices develop trust instantly with a reasonable degree of accuracy, an indispensable part of the correct operation of most IT systems, is needed (Chen et al., 2014). Due to the distributed nature of IoT, a distributed trust management system which can scale to global dimensions is designed by Alexopoulo et al. (Alexopoulos et al., 2018) using distributed ledgers.

Disparate techniques have been proposed in literature for addressing trust management in diverse IoT systems (Table 15). To support SOA-based IoT systems, an adaptive and scalable trust management protocol is proposed by Chen et al., 2014, 2016. In sensor node-powered IoT applications, Tariq et al. (2019) present a Mobile Code-drive trust mechanism to define a confidence level for sensor nodes. Additionally, the trust levels of IoT devices in the network can be employed to explore the attacks. For detection of malicious nodes and on-off attacks involved in bad service provisioning, a fuzzy logic-based approach is proposed (Alshehri and Hussain, 2019) for restriction of their untrusted functionality where it gives false recommendations about other nodes. Trust and reputation policies can be adopted for detecting hijacked vehicles (García-Magariño et al., 2019).

7.1.3. Privacy

As IoT develops, privacy becomes a major implication, which means more than anonymity in IoT. Profiling and data mining services which involve automatic processes including data collection, their storage, sharing, and analysis process, can form a potential harm to individuals (Elkhodr et al., 2012) IoT network traffic can also be analyzed to infer sensitive details about users and their interactions even when the traffic is encrypted. Apthorpe et al. (2017) examine four IoT smart home devices to prove it. According to their results, a technological solution is needed to protect IoT device owner privacy.

Given this concern, privacy-preserving methods are applied in various IoT environments and applications (see Table 16). For instance, an efficient privacy-preserving method is proposed in (Boussada et al., 2018) for E-health systems which relies on a novel identity-based cryptography scheme, called PKE-IBE. To recognize activity and restrict user re-identification at the same time, a privacy-preserving framework is presented by Jourdan et al. (2018). Furthermore, since privacy of sensitive data is a major concern for data aggregation applications in the fog-enhanced IoT environment, Guan et al. (2019) design a device-oriented anonymous scheme to preserve the privacy.

For privacy management in IoT applications, specifically, smart energy management systems, Ukil et al. (2015) propose an involuntary approach (without human-in-loop). To accomplish such an approach, this paper identifies the sensitive content in sensor data and level of privacy control required for such content. In this approach, data privacy will be preserved before the data are shared to third parties and the user will be alerted in case of privacy breach in shareable data. The same authors in (Ukil et al., 2014) had also proposed a simpler version of this privacy management schema in which the data owner can assess the privacy risk of sharing his private data.

Table 14
Identification during MoL in IoT.

Scheme	Method	Remarks
Sarma and Girão (2009)	identification by Identinet and digital shadows	using virtual identities as representations of entities while communicating in SWIFT architecture
Horrow and Sardana (2012)	identity management framework for Cloud based IoT	a Publisher -Subscriber approach for proper functioning
Fremantle and Aziz (2016)	OAuthing, a federated security model	not sharing data and identity without user consent and sharing data anonymously
Fremantle et al. (2014)	FIAM, a federated identity and access management approach	building a prototype using OAuth 2.0 to enable access control to information distributed via MQTT
(Santos et al., 2018, 2019)	identity federation for cellular IoT	reusing the SIM authentication enabling single-sign-on
Meidan et al. (2017)	ProfilIoT, a device identification based on network traffic analysis	using machine learning algorithms to identify IoT device type, based on characteristics of the network traffic it generates
Yousefnezhad et al. (2018)	MeDI, a measurement-based device identification framework	monitoring the data packets coming from smart devices to protect the server from receiving and spreading false data
Mahalle et al. (2010)	identity management framework	managing a device's security credentials and identity, and interacting with service providers on its behalf
Kravitz and Cooper (2017)	distributed identity management	using blockchain for resilient user and device identity and attribute management
Song et al. (2017)	Improved Identity Management (IIDM) Protocol	improving both security and performance by maximizing load balancing to service provider
Hu et al. (2011)	identity-based system for personal location in emergency situations	confirming the identity of the user through the user authentication subsystem and the level of the emergency through the policy subsystem

Table 15
Trust in IoT.

Scheme	Method	Remarks
Namal et al. (2015)	autonomic trust management framework	based on evaluating trust level in cloud based on monitoring, analysing, planning, executing, and presenting knowledge (MAPE-K) feedback loop
Chen et al. (2014)	adaptive trust management protocol	trust evaluation based on past user satisfaction experiences and trust feedbacks from other users with similar social interests
Chen et al. (2016)	adaptive and scalable trust management	trust evaluation based on feedback employing similarity level of friendship, social relationship, and community of interest relationships for filter
Tariq et al. (2019)	MCTM, a mobile code-driven trust mechanism	detecting isolating malicious internal sensor nodes based on their forwarding behaviors
Alshehri and Hussain (2019)	a fuzzy security protocol for trust management	applying a new security protocol to create a secure communication and message exchange between devices
García-Magariño et al. (2019)	trust management on vehicles	by analyzing whether vehicles' messages have any misinformation and using reputation of the vehicle
Alexopoulos et al. (2018)	distributed trust management system	utilizing distributed ledger to maintain all access delegations, and reputation scores of participants in 3 layers: global, group and local layer

Table 16
Privacy in IoT.

Scheme	Method	Remarks
Boussada et al. (2018)	privacy-preserving E-health system	based on Identity-Based Cryptography (IBC) tackling the key escrow issue and ensuring blind partial private key generation
Jourdan et al. (2018)	privacy-preserving framework for activity recognition	limiting the risk of user re-identification by extracting multiple features from raw signal and analyzing their impact on both the activity recognition and the user re-identification
Guan et al. (2019)	APPA, a device-oriented Anonymous Privacy-Preserving scheme	using Authentication for data aggregation applications in fog-enhanced IoT system
Ukil et al. (2015)	privacy management for smart energy management systems	addressing the problem of involuntary privacy breaching risk minimization by minimizing the capability of privacy intruders
Ukil et al. (2014)	privacy management scheme for smart meter devices	enabling the user to assess the risk of sharing his private data

7.1.4. Compromise detection

Compromise is a circumstance where a threat such as malware, intrusion, attack or a newly discovered incident occurs which might harm the overall system. It is impossible or difficult to identify these threats in advance. Thus, they should be analyzed during their use. Since currently most IoT vendors provide no mechanism to automatically update the devices, compromises will grow in the IoT environment. As a countermeasure for this problem, ISP networks require feasible techniques to detect IoT malicious activity (Van der Elzen and van Heugten, 2017). Compromises might have three steps (Pa et al., 2016): intrusion, in which attackers exploit the weaknesses to login to devices; infection, in which after a successful intrusion, attackers upload and execute malicious codes to the device; monetization, in which malicious codes are controlled by attackers to spread the malware to other vulnerable devices.

Due to growing popularity of IoT and weak security IoT devices have, new categories of malware have emerged such as Hajime decentralized Internet warm (Edwards and Profetis, 2016), Persirai botnet (Yeh et al., 2017), BrickerBot (Radware. Brickerbot resul), Mirai (Antonakakis et al., 2017; Kolias et al., 2017), and other botnets which explicitly target IoT devices. Since these malware affect the behaviour of IoT devices and reveal an unknown traffic pattern, one solution for

Table 17
Compromise detection in IoT.

Scheme	Method	Remarks
Nguyen et al. (2018)	DÏoT, self-learning distributed compromise detection of devices	using federated learning for device-type specific anomaly detection
Raza et al. (2013)	SVELTE: Real-time intrusion detection	safeguarding network from known attacks and adapting existing IDS to IoT-specific protocols, e.g., 6LoWPAN
Doshi et al. (2018)	signature-based approach for distributed DoS (DDoS) detection	employing variety of machine learning algorithms to performs data collection, feature extraction, and binary classification
Jia et al. (2017)	ContexIoT, a context-based permission system	detection of malicious app by discovering sensitive actions
Li et al. (2019)	CBSigIDS, collaborative blockchained signature-based intrusion detection	no need for trusted intermediary
Yahyaoui et al. (2019)	anomaly based intrusion detection	SVM for WSN intrusion detection, and deep learning technique for gateway intrusion detection
Taneja (2013)	An Analytic framework	detecting compromised IoT devices using mobility behavior

defeating them is to check whether the traffic pattern matches the normal pattern or not. To do so, Nguyen et al. (2018) presented a self-learning distributed system for detecting compromised IoT devices effectively. In this system, devices are classified and profiled based on their device type and their normal communication behavior which is used for anomaly detection.

Since IoT devices are controlled by smartphone applications and smartphones are involved with invasion of privacy and information leakage, it is necessary to detect abnormal behaviors occurring on mobile devices to achieve reliable IoT services. For this purpose, several mobile malware detection techniques exist which are summarized as follows. 1. Signature-based detection which employs either static or dynamic methods to define the signature; 2. Behavior-based detection analyzes predetermined attack patterns and process behaviors by monitoring information inside a device (host-based) or gathering information via network (network-based); 3. Dynamic analysis-based detection (taint analysis) marks specific data and monitors their process to track the data flow. Tabassum et al. (2019) also present another category for intrusion detection techniques which is divided into four groups: signature-based, anomaly-based, specification-based and hybrid.

The static *signature-based* solution is a traditional method which is unsuited for dynamic environments and the dynamic signature-based one requires large amount of storage for finding certain patterns. Taint analysis is also highly dependent on the underlying system while an analysis system in diversified environments must be flexible enough to adopt different systems (Zhang et al., 2014). Signature-based with some extensions can be suitable for IoT environments. For instance, Sun et al. (2017) provide a technique for cloud-based malware detection presenting a reliable data privacy protection for IoT resource-constrained devices. To detect the malware, this technique proposes a signature-based mechanism for the cloud server and a lightweight content scanning agent for the client. *Behavior-based* detection techniques which have recently received most attention, exploit machine learning methods to enable automated malware classification. For example, Ham et al. (2014) apply a linear support vector machine for exploring malware on Android phones. Vasseur and Seewald (2016) also proposed a dynamic anomaly detection method based on machine learning algorithms to make the network learn from its mistakes and eliminate the false positive alarms.

Malware detection tools: IoTSeeker (Qian) is an example of available tools for malware detection and/or prevention. This tool scans an IoT network to detect if they are using the default credentials or not and helps to find Mirai-based malware. After capturing malware samples, in order to analyze and examine the attacks in depth, a malware analysis environment, called IoTPOT (Pa et al., 2016), was proposed. In addition, one common solution for understanding the dynamic threat landscape without exposing critical assets is honeypot. For this purpose, an automatic and intelligent honeypot called IoTCandyJar (Luo et al., 2017) was proposed to check behaviors of different types of IoT devices by gathering responses to the honeypot's requests, specifically ones expected from attackers, leveraging machine learning techniques (See Table 17).

7.1.5. Security requirements

This section presents the proposed solutions for the security requirements required in operation stage (MoL).

Authentication: The authentication mechanisms for IoT are classified as: two-factor authentication, two-phase authentication, mutual authentication, group authentication, and anonymous authentication. Examples for each class are presented in Table 18. Most of these schemes are vulnerable to key theft since they employ local key management and need infrastructure support for key storage (Shivraj et al., 2015). They have no fine grained control, either, and are impractical in real-world usecases.

More authentication methods along with detailed comparison considering their weakness and strength are available in previous surveys conducted for Authentication in IoT (Ferrag et al., 2017; Saadeh et al., 2016; El-hajj et al., 2017; Atwady and Hammoudeh, 2017). For instance, Ferrag et al. (2017) categorize the authentication protocols for IoT systems based on the target environment including M2M communications, IoV, IoE, and IoS and represent performance and limitation of protocols based on such a category.

Access Control (AC): For providing end-to-end data protection, both in storage and in transit, a cryptographic access control based approach is proposed by Wrona (2015) which is also based upon Object Level Protection standard. An integrated approach is proposed by Mahalle et al. (2013) for authentication and control of IoT devices access known as Identity Authentication and Capability based Access Control (IACAC) model. The same authors in (Mahalle et al., 2012a) already proposed a capability based approach called IECAC leveraging ECC. More Access control approaches from the perspective of IoT are displayed in Table 19.

Confidentiality: Although confidentiality is important during deployment, it is also considered the main security issue during IoT device communication. Security solutions provided to address confidentiality during the phase of MoL are described in Table 20.

Integrity: An IoT device produces a large amount of sensitive data which are susceptible to cyber attacks including integrity attacks. Integrity attacks known as tampering attacks are extremely dangerous since they might go unnoticed till the unavailability of the physical system (Battisti et al., 2018). Data tampering attacks can be divided into two types: data modification and data injection. Among these attacks,

Table 18
Authentication during MoL in IoT.

Scheme	Type	Method	Remarks
Shivraj et al. (2015)	Two-factor authentication	an One-Time Password (OTP) scheme using lightweight identity-based Elliptic curve method and Lamport's OTP algorithm	1. Scalable, lightweight, and robust scheme 2. Requiring less resources and smaller key size
Crossman and Liu (2015)	Two-factor authentication	a smart two-factor authentication utilizing the existing protocols, hash functions, and encryption algorithms with a modification of workflow only	1. Less sensitive to user behavior 2. Putting user in full control
Porambage et al. (2014a)	Two-phase Authentication	a certificate-based authentication approach including Registration and Authentication phase for WSNs in distributed environment	1. Supporting resource restriction of sensors 2. Supporting heterogeneity of entities, due to implicit certificates
Porambage et al. (2014b)	Two-phase Authentication	a pervasive lightweight authentication and keying (PAuthKey) technique for WSNs in distributed environment	1. Supporting distributed IoT applications because of lightweight certificate 2. Safeguarded against certain kinds of attacks
Aman et al. (2017)	Mutual Authentication	a light-weight challenge-response mechanism based on physical unclonable functions (PUFs) which not save any secret in the IoT devices and requires low storage on the server	1. Robust against different types of attacks 2. Having very low energy, memory, and communication overhead
Li et al. (2017)	Mutual Authentication	a lightweight authentication protocol based on novel public key encryption scheme for resource-constrained devices	1. Better than existing RSA and ECC based protocols 2. Less times to run, shorter bits and no TTP during device setup
Zhao et al. (2011)	Mutual Authentication	an asymmetric authentication method utilizing feature extraction, secure hash algorithm (SHA), and ECC	1. Light computation and communication cost 2. Secure and feasible for applications in IoT
Devi et al. (2015)	Mutual Authentication	a new authentication scheme using two approaches including login with hashing password or with the help of MAC password	1. Less time to authentication for first approach and better results for second one 2. Highly resistance against node compromise, robust to packet loss, immediate authentication, and message entropy
Kalra and Sood (2015)	Mutual Authentication	a secure ECC-based authentication protocol applying g Hyper Text Transfer Protocol (HTTP) cookies	1. Robust against multiple security attacks 2. Having low computation cost
Fan et al. (2016)	Mutual Authentication	a lightweight RFID-based authentication protocol having cache on the reader and storing recent visited tags	1. Less computational and transmission cost, higher efficiency and stronger security 2. A little larger storage space in the reader
Petrov et al. (2014)	Group Authentication	a novel many-to-many authentication technique, according to passive NFC tags instead of battery-powered devices using data encryption scheme	1. Cost-efficient, scalable, and secure 2. Enabling user to modify passphrases for any IS in an uncontrolled manner
Mahalle et al. (2014)	Group Authentication	a Threshold Cryptography-based Group Authentication (TCGA) scheme verifying authenticity of all the participants (devices) in the group communication using probabilistic asymmetric public key encryption system	1. Lightweight, scalable, and reducing the consequence of battery exhaustion attack 2. Avoiding replay and MIMA attack
Alcaide et al. (2013)	Anonymous Authentication	a fully decentralized authentication protocol implemented within privacy-preserving self-adaptive model	1. Not rely on any central organization 2. Data collected in anonymous manner
Yang et al. (2016)	Anonymous Authentication	a lightweight entity authentication scheme outsourcing the task of witness update and using dynamic accumulator for credential revocation	1. Solving the main bottleneck of anonymous credentials 2. Efficient for resource-constrained IoT devices

data modification attacks (main type of data tampering attack), which disrupt the state of the applications, cause widespread damage. To detect these attacks, Aman et al. (2018) propose a detection mechanism using a random time hopping sequence and random permutations to hide validation information.

Another type of attacks targeting data integrity is data injection (or deception attack) where the tampered data is injected in the communication channel. To identify such an attack, Battisti et al. (2018) design a secure mechanism based on coding the output of the system using permutation matrices created by flipping. Further approaches to integrity protection are demonstrated in Table 21. Apart from the attack type, the level of data integrity can be scored based on the manipulation level of adversary (Bhattacharjee et al., 2017) or the data can be signed by elliptic curve based algorithms to provide end-to-end integrity protection (Bauer et al., 2016).

Availability: The availability of IoT systems can be threatened by cyber attacks such as impersonations or DoS. Thus, it is essential to investigate the effect of successful attacks on the availability factor of the IoT system. Given this concern, Kolisnyk et al. (2017) analyze the possible types of attacks and mathematically assess the availability factors on smart business. Once the availability level has been measured, the availability of smart devices should be enhanced to improve their performance along with their security. Table 22 demonstrates several approaches to improve (Xiong et al., 2019), optimize (Yang and Kim, 2019), and ensure (Qaim and. Özkasap, 2018) data availability on IoT infrastructure.

Non-repudiation: In industrial IoT with a service-provisioning scheme, malicious services might be provided by untrusted service providers. Similarly, acquirement of correct services might be repudiated by dishonest service users for their own advantages or disruption purposes. To avoid these problems, non-repudiation mechanisms whether with or without TTP should be presented. However, both of these two approaches are insufficient for IoT systems due to being decentralized and having recourse-constrained devices. Given this concern, a non-repudiation model is proposed by (Xu et al., 2019) for service-provisioning scenarios using blockchain technology. The non-repudiation issue can also be addressed along with other security requirements such as authentication and confidentiality to provide a security service. FSS (Abbas et al., 2019) is an example for these kind of services given in Table 23.

Table 19
Access control during MoL in IoT.

Scheme	Method	Remarks
Mahalle et al. (2013)	Capability-based approach	compatible with underline access technologies like Bluetooth, 4G, WiMax and Wi-Fi
Mahalle et al. (2012a)	Capability-based approach	using Elliptic Curve Diffie-Hellman (ECDH) to establish shared secret keys between two devices (not providing details on the communication technologies employed, based on central entity)
Ramos et al. (2013)	Distributed Capability-based	cryptographic solution
Zhang and Gong (2011)	Usage Control (UCON) model	based on fuzzy theory and some central entities which manage usage control decisions and trust values of devices and services
Gusmeroli et al. (2013)	Capability-based	based on a central Policy Decision Point (PDP) which handles authorization decisions
Mahalle et al. (2012b)	Capability-based	exchanging capabilities in conjunction with a SHA-1 message digest, which is used to check the tampering and forgery of the capabilities (not providing details on the communication technologies employed)
Anggorojati et al. (2012)	capability-based and context-aware access control (CCAAC)	authorizing a delegation request from a delegator (central entity)
Liu et al. (2012)	Role-Based Access Control (RBAC-based) approach	using the thing's particular role(s) and application(s)
Bouanani et al. (2019)	pervasive-based access control method (PerBAC)	presenting a multi-layer and proactive method based on ABAC with additional features from OrBAC
Riad and Zhu (2017)	Trust-Based Access Control (TB-AC)	using user trust level to modify his assigned permissions, based on 3 factors (multi-factor); not IoT oriented
Hasiba et al. (2018)	Hybrid model, combining RBAC with ABAC	solving the problem of context-awareness while avoiding explosion in the number of roles or rules in the security policy
Huang et al. (2018)	delegation mechanism based on hierarchical attribute-based encryption (HABE)	outsourcing several effortful operations to cloud server and gateway
Kolluru et al. (2018)	Next Generation Access Control (NGAC-based) solution, one kind of ABAC	achieving fine-grain service level access control between IoT devices
Hwang et al. (2018)	block-chain (dynamic) based access control	increasing scalability and usability by generating policies on access permissions even after requesting data
Moreno-Sanchez et al. (2013)	network access control implementation	carrying authentication for network access based on PANA protocol
Pal et al. (2019)	Policy-based approach	using attributes, roles, and capabilities to provide a hybrid approach
Salonikias et al. (2019)	an access control architecture for IIoT	based on virtualization technologies
Ding et al. (2019)	ABAC-based	using blockchain to record the distribution of attributes in order to avoid single point failure and data tampering

Table 20
Confidentiality during MoL in IoT.

Scheme	Method	Remarks
Purohit et al. (2017)	confidentiality and authentication	securing the IoT communication
Al-Turjman and Alturjman (2018)	agile confidential framework	using ECC for collecting the sensed data to enable confidentiality and integrity
Khalaf and Mohammed (2018)	Confidentiality and Integrity	by encrypting all data that sensors send to IoT server
Eugster et al. (2019)	STYX architecture, providing confidentiality against an adversary having full access to servers	no burden for the programmer using Partially Homomorphic Encryption (PHE) to perform computations over encrypted data
Hurrah et al. (2019)	RCSMMA, a robust data hiding framework providing data confidentiality during transmission for multimedia analytic	using random block and coefficient selection approach to improve robustness of embedded data

Table 21
Integrity during MoL in IoT.

Scheme	Method	Remarks
Aman et al. (2018)	data tampering detection	by reducing the computational complexity as well reducing the transmission energy
Battisti et al. (2018)	a secure control system to identify deception attack	encoding the system output based on a secret pattern created by Fibonacci p-sequences
Bauer et al. (2016)	end-to-end integrity protection	using elliptic curve based signatures
Bhattacharjee et al. (2017)	Bayesian inference framework for data integrity scoring	under opportunistic data manipulation by an adversary

7.2. Updates

Under some circumstances, IoT devices and their secret belongings (i.e., secret keys and certificates) are required to be updated.

7.2.1. Key/Certificate update

All keys associated with a specified user or device should be updated to guarantee forward and backward secrecy, when devices or users join and leave the system. To efficiently handle key updates (or re-keying) during membership change inside user or device groups, a Group Key Management (GKM) scheme was proposed in (Kung and Hsiao, 2018)

Table 22
Availability during MoL in IoT.

Scheme	Method	Remarks
Kolisnyk et al. (2017)	a mathematical model to assess availability	by considering the influence of different kinds of DDoS attacks on availability factor
Tsai et al. (2018)	a middleware layer framework	to enhance availability by filtering and integrating the vast amounts of information
Xiong et al. (2019)	PADC, a privacy and availability data clustering scheme	based on k-means algorithm and differential privacy, improving the selection of the initial center points and the distance calculation method from other points to center point
Yang and Kim (2019)	high availability architecture	dynamically optimizing the availability according to various features of service
Qaim and. Özkasap (2018)	DRAW, a fully distributed hop-by-hop data replication technique	ensuring maximum data availability under high node failures to preserve data
Kryvinska and Strauss (2013)	performance analysis of services availability and interoperability	providing an effective service delivery to attach IoT-enabled enterprise's customers more tightly
Dinh and Kim (2018)	a cost-efficient availability preserving scheme over cloud	augmenting the availability of service function chaining (SFC) by evaluating the improvement potential of VNFs for VNF redundancy allocation

Table 23
Non-repudiation during MoL in IoT.

Scheme	Method	Remarks
Xu et al. (2019)	blockchain-based non-repudiation service provisioning scheme	using tamper-resistant blockchain as service publisher and an evidence recorder
Abbas et al. (2019)	FSS, a novel fog security service	addressing the authentication, confidentiality, and non-repudiation for IoT devices via Private Key Generator (PKG) at fog layer

which combines two existing GKMs, one used within user and device groups and another for communicating with multiple user groups. Additionally, a group authentication scheme is proposed by Mahalle et al. (2014) for an IoT system for verifying the authenticity of all the devices which take part in the group communication. This scheme has five modules including a key update which generates a public/private key pair for Group Authority (GA) and changes the private keys of other members of the group. On the other hand, certificates which specify the public key to owners also require periodic renewal, e.g., by a dynamic public key certificate (Chien, 2018). More re-keying approaches, as part of key management (Abdmeziem et al., 2015) or as a separate solution (Arif et al., 2019) are demonstrated in Table 24.

7.2.2. Software update

The IoT environment consists of various hardware modules including their own firmware in each module which should be up-to-date during the IoT device lifecycle (Sulkamo, 2018) since IoT devices are not secured by design (Boudguiga et al., 2017). On the other hand, vendors do not deliver software updates before attackers exploit a vulnerability found by a good node. This is the main reason for device failures in the network, as Beresford (2016) reports. Therefore, it is essential to keep track of disclosed vulnerabilities and patch them in subsequent software or firmware updates so that hackers will be unable to enroll them into botnets.

Many IoT devices like modern vehicles require firmware updates due to their vulnerabilities and outdated configuration settings. Providing such an update may highlight new issues for constrained devices (IAB). The update can occur during or after the end-of-life of a device. It can also occur on the device or on the cloud but both solutions are challenging. IoT resource-constrained devices cannot rely only on their limited resources. Obtaining updates from the cloud also makes these devices perform heavy operations (Chiang and Zhang, 2016). As a consequence, a new solution is needed to distribute the update responsibility among the IoT devices. As an example (Boudguiga et al., 2017), proposes a peer-to-peer mechanism for spreading updates between IoT devices. They apply blockchain infrastructure to improve the security of updates with the focus on availability. More approaches are described in Table 25.

7.3. Reconfiguration

The security solutions for the various problems in the Reconfiguration phase are discussed in this section.

7.3.1. Application reconfiguration

Similarly to sensor networks, flexibility is a key issue of application in IoT systems. Application reconfiguration is the main approach for improving the flexibility of the system. Such an approach presents

Table 24
Key/Certificate update during MoL in IoT.

Scheme	Method	Remarks
Kung and Hsiao (2018)	GroupIT, a two-tier GKM	grouping similar devices and managing keys between groups through upper tiers (users) and inside group through lower tiers
Mahalle et al. (2014)	key update as part of threshold cryptography-based group authentication	generating key pairs for GA and updating private keys of others
Chien (2018)	DPKC, a dynamic public key certificate	updating public/private key pair without connecting to CA for a new certificate, verifier can use the original CA-issued certificate to verify the claimed public keys
Abdmeziem et al. (2015)	re-keying as part of decentralized and batch-based group key management protocol	reducing re-keying overhead triggered by membership changes and providing forward and backward secrecy for multicast communications
Arif et al. (2019)	re-keying by LT-SMM, a logical tree-based secure mobility management scheme	providing secure group communication employing group deployment, mobile node joining and mobile node migration protocols

Table 25
Software update in IoT.

Scheme	Method	Remarks
Boudguiga et al. (2017)	peer-to-peer update mechanism	using blockchain to ensure updates availability
Huth et al. (2016)	a security protocol for a secure software update on malicious devices integrating different trust establishing techniques	integrating physically unclonable functions, software-based attestation, and proof of secure erasure
Kim et al. (2018)	remote software update	using low-power wide area network (LPWAN) as a long-range IoT networking technology and a mobile edge cloud to improve computing efficiency
Kolomvatsos (2018)	distributed updates management scheme enhancing the autonomous nature of nodes	nodes autonomously deciding the time for the update process activation
Weißbach etal., 2016	dynamic software update	coordinating the update of multiple distributed nodes involved in a running service

Table 26
Application reconfiguration in IoT.

Scheme	Method	Remarks
Zhang et al. (2005)	EAAR, an environment adaptive application reconfiguration in WSN	utilizing rule-based knowledge to analyze the change of environment to efficiently perform self-adaptive application reconfiguration
Samir et al. (2019)	Dynamic Partial Reconfiguration (DPR)-enabled system	configuring the hardware security module based on the available power budget

a powerful mechanism to adapt component-based distributed applications in the dynamic environment. However, implementing application reconfiguration in IoT is challenging since identically with sensor nodes, memory-constrained devices in IoT are unable to store all possible applications in their local memories. An example of executing application reconfiguration in sensor networks is proposed by Zhang et al. (2005) (see Table 26). This approach is unapplicable in IoT systems since it does not support the dynamic addition of new knowledge.

Recently, IoT hardware reconfiguration has also become a popular since IoT applications are often constrained by the dual requirements of high performance and resource limitation (Johnson et al., 2017). For instance, energy-limited IoT applications confront the challenge of trade-off between security strength and power budget. To resolve the power constraint issue in low-power IoT applications, Samir et al. (2019) propose Dynamic Partial Reconfiguration (DPR) technology, where multiple encryption modes can be implemented with various security levels. Adversary can exploit remote DPR capability of the devices to launch hardware-related attacks on commonly used security applications. Johnson et al. (2017) demonstrate four examples of remotely-launched attacks on remote DPR, where a bitstream is transferred remotely over the network to reconfigure one or more applications embedded on the reconfigurable device.

7.4. Corporability

7.4.1. Mobile security

IoT will potentially connect billions of devices from multiple organizations and in some environment, e.g., smart cities, these devices move from one cluster to another. When the device moves, organizations will face many concerns regarding security requirements for the network and the device itself. The IoT network requires identity checks for the mobile device when it enters the network. The IoT mobile device, on the other hand, requires a transparent identification so that it can comfortably interact with other mobile nodes, while enjoying the secure service. For instance, when a car arrives in Helsinki, the security concerns are associated with e.g. its access to city information, the access rights of other devices in Helsinki to the information related to the new car, and the trust level of new car.

For providing privacy protection and rapid identification authentication for a mobile node joining the new cluster, Miao and Wang (2012) present a cryptography-based protocol from the class of single-step protocol. The protocol rapidly implements authentication using a valid request message and an answer authentication message.

Since device mobility is increasing in IoT applications making it difficult to communicate with them directly using their IP address (e.g., due to access restrictions or the presence of NAT), the messaging standards are designed for providing standardized and generic application-level interfaces to achieve two-way communication among other things (Kubler et al., 2015b).

The mobile solution was attracted by several IoT services such as secure healthcare service. For these mobile platforms, deploying a security architecture is necessary. For this purpose, Goncalves et al. (Gonçalves et al., 2013) define a basic security architecture to support secured and authenticated interactions, enabling an easy deployment of m-health applications. Adopting mobile solutions in the same IoT environment, a novel security and privacy mechanism was proposed in (Kai et al., 2013) for protecting the patients' security and privacy in a healthcare context including trustworthiness, authentication, and cryptography credentials.

Mobile devices force the environments to integrate with the wireless network, where wireless access to networks represents security threats. Thus, an efficient and secure mobile-IPS (*m*-IPS) is presented in (Jeong et al., 2014) for business activities for human-centric computing which utilize mobile devices in mobile environments.

Mobility of low-level technologies such as mobile radio frequency identification (RFID) technology, used in electronic product code (EPC) information service, also causes security and privacy concerns for tags and readers. To protect the mobile RFID (or mobile reader) systems, security and privacy protection schemes were presented in (Zhu et al., 2012), (Yan and Wen, 2010), and (Niu et al., 2014) (see Table 27).

7.4.2. End-to-end security

To enable safe end-to-end corporability, an end-to-end security solution is required relying on protection measures implemented on the terminal hosts (Sahraoui and Bilami, 2015). As a solution for end-to-end security, establishing interoperable network security between end peers, various conventional end-to-end security protocols have been recently proposed (Moosavi et al., 2016). An end-to-end security protocol safeguards the message payload from the data source until reaching the target. This type of protocol is usually implemented in the network or application layer with different levels of protection compared to the link layer, since end-to-end security is not provided by lower layer security protocols (Kothmayr et al., 2012).

Table 27
Mobile security in IoT.

Scheme	Method	Remarks
Miao and Wang (2012)	a rapid identification authentication protocol for mobile nodes joining a new cluster	resisting replay attack, eavesdropping attack, and tracking or location privacy attack.
Jara et al. (2013)	a secure and scalable mobility management scheme	supporting scalable inter-domain authentication and secure location update and binding transfer for the mobility process
Gonçalves et al. (2013)	security architecture for mobile platforms	establishing and managing a medication prescription service in mobility context using electronic Personal Health Records
Kubler et al. (2015b)	Quantum Lifecycle Management (QLM) messaging standard	enabling real-time communications and two-way communications with nodes located behind firewall/NAT systems
Kai et al. (2013)	Health-IoT, a secure healthcare service	establishing a trust IoT application market (IAM) by exchanging the feature of application in marketplace and behavior of applications on end-devices
Jeong et al. (2014)	*m*-IPS, a mobile intrusion prevention system	Providing precise access control by checking users' temporal spatial information, profiles, and role information
Zhu et al. (2012)	SPMMRFID-IOT, a security and privacy model for mobile RFID systems	supporting the privacy of tags and readers, tag corruption, reader corruption, multiple readers, and mutual authenticated key exchange (AKE) protocols
Yan and Wen (2010)	mobile RFID network architecture	embedding the reader into mobile phone, no need for proxy
Niu et al. (2014)	a novel ultra-lightweight and privacy-preserving authentication protocol for mobile RFID	using only bitwise XOR and several special constructed pseudo-random number generators, providing privacy properties (e.g., tag anonymity, tag location privacy, reader privacy, mutual authentication) and resisting attacks (e.g., replay attacks, de-synchronization attacks)

Table 28
End-to-end security in IoT.

Scheme	Method	Remarks
Banerjee et al. (2018)	protocol extension for DTLS	through the design of reconfigurable energy efficient cryptographic accelerators and a dedicated protocol controller
Brachmann et al. (2012a)	end-to-end transport security	by proposing a mapping between TLS and DTLS in homogeneous networks
Hummen et al. (2013a)	lightweight protocol extensions for HIP DEX during handshake	proposing a comprehensive session resumption mechanism to reduce handshake costs, a collaborative puzzle-based DoS protection mechanism for network heterogeneity, and a refined retransmission mechanism for processing time
Sahraoui and Bilami (2015)	CD-HIP, Compressed and Distributed HIP for lightweight end-to-end security	combination of an efficient distribution scheme for key exchange and an optimal 6LoWPAN model for protocol header
Moosavi et al. (2016)	end-to-end security scheme for mobility enabled healthcare	providing a secure and efficient end-user authentication and authorization, secure end-to-end communication, and robust mobility
Hossain et al. (2016)	biometrics-based secure communication	using biometrics and pairing-based cryptography for end-to-end security between different layers

Several studies have been conducted of IoT end-to-end security protocols. Among them, some research presented a lightweight IP security protocol for end-to-end security in IoT such as minimal IKEv2 (IPsec) (Kivinen, 2012), HIP HIP Diet Exchange (DEX) (Moskowitz and Hummen, 2012) and Datagram TLS (DTLS) (Rescorla and Modadugu, 2012). To improve the applicability of these protocols, recent research shifted its focus to proposing a new end-to-end protocol by adding an extension to previous protocols. For instance, due to computational costs of DTLS, Banerjee et al. (2018) and Brachmann et al. (2012a) contribute to DTLS and make it a practical solution for implementing end-to-end security on resource-constrained IoT devices. For boosting HIP-based protocols in IoT, some lightweight protocol extensions were proposed by (Hummen et al., 2013a) and (Sahraoui and Bilami, 2015). Table 28 discusses these security protocols in more detail, similarly to other end-to-end security solutions, in particular platforms such as mobility enabled healthcare (Moosavi et al., 2016) and biometrics-based communication (Hossain et al., 2016).

8. Security solutions in end of life (EoL)

A device reaches the end of its life due to obsolescence or when transferring to a new owner.

8.1. Re-ownership

One of the fundamental problems in IoT is Ownership management. This problem triggers several security concerns, including access control of smart devices after ownership transfer, privacy preservation, and secret update. Devices in the context of IoT require an ownership which can be obtained, verified and transferred through a vast communications network in a fast and secure way (Leng et al., 2014). When a new owner purchases the device, the ownership should be transferred from the current owner, a process known as ownership transfer or re-ownership. Both parties involved in device re-ownership must be protected as they are both potential adversaries (Khan et al., 2018b). Once the ownership is transferred, all the rights available to the previous owner should be assigned to a new owner who should be unable to trace back previous owner's communication with others. Meanwhile, when the ownership of the old owner is revoked, the old owner should be unable to track any current communication of the new user (Aghili et al., 2019).

8.1.1. Key/Certificate update

If the device is transferred, a new set of initial secret keys will be needed by the new owner to access its device servers in BoL. Privacy

Table 29
Key/Certificate update during EoL in IoT.

Scheme	Method	Remarks
Leng et al. (2014)	an outline of an ownership management system	handling ownership transfer through TTP checking the ownership proof and validity of ownership transfer
Mamun et al. (2018)	OTP-IoT, a secure RFID ownership transfer protocol	preventing MITM attack and supporting mutual authentication while enabling owners to transfer the ownership of multiple tags simultaneously
Ghuli et al. (2017)	decentralized re-ownership scheme	using blockchain transactions to reduce the dependency on a central cloud
Aghili et al. (2019)	LACO, a lightweight authentication and ownership transfer protocol	preserving the user privacy by considering ownership transfer of users
Khan et al. (2018b)	chownIoT, automated re-ownership of devices	combining authentication, profile management, data protection, and ownership change

Table 30
Key/Certificate revocation in IoT.

Scheme	Method	Remarks
Raza et al. (2016)	key revocation as part of key management architecture	marking the key as used in the sliding window to induce it unusable
Bock et al. (2019)	key revocation and re-keying for Adaptive Key Establishment Scheme (AKES)	not routing messages via evicted nodes in Node Revocation List (NRL)
Cebe and Akkaya (2019)	a distributed CRL management scheme by utilizing distributed hash trees	providing less overhead with reasonable access time regardless of network size
Duan et al. (2018)	two novel lightweight CRL protocols	based on generalized Merkle hash tree and Bloom filter

leakage of the device (e.g., secret keys) is the main privacy issue in an ownership transfer protocol during the ownership transfer process from the current owner to a new owner. Re-ownership can be managed by a trusted party to simplify the operations or without trusted party when complex architectures are unfeasible.

One example of ownership management based on a Trusted Third Party (TTP) structure is proposed by Leng et al. (2014), in which TTP handles both ownership establishment and ownership transfer steps (see Table 29). Although relying on TTP can guarantee the owner's privacy, it excessively burdens the trusted server. To solve the problem, a number of intermediate servers called semi-trusted parties (STP) is proposed to securely transfer the ownership of RFID tag (Mamun et al., 2018). By employing STP, during re-ownership process, tag owners only require communication to a nearest STP instead of interacting with the main server. This re-ownership method supports forward privacy secrecy because of updating the session key after each transaction, thus the new reader is unable to interpret the tag's previous transactions and the current reader is also unable to trace the tag. One approach to removing involvement of the third party in device re-ownership is to exploit blockchain technology so that the transfer of one user to another user is managed like a normal blockchain transaction, where the owner controls the ownership of the device, and can independently transfer it to any other user (Ghuli et al., 2017). Another solution is to automatically secure ownership changes. Khan et al. (2018b) adopt this type of solution to address privacy issues related to ownership of smart home devices in a system called chownIoT. This system automatically detects the ownership change using the context of IoT devices, manages the profile for authenticating owners, and encrypts the data and isolates the profile for owner privacy.

Furthermore, in order to transfer the ownership of information in e-health systems, a situation where accessibility to patient information can be revoked from one doctor and transferred to another, an ownership transfer phase is proposed in the LACO scheme (Aghili et al., 2019). In the ownership transfer phase, the server uses the identity and password of the new owner to update the HACO string (i.e., owner identity, some dynamic and static attributes about owner's situation and owner password) and encrypts it with the new owner key and sends it to the new owner, thus the old owner cannot decrypt the string.

8.2. Decommissioned

As more devices are being added to our life, the issue of devices that stop functioning and are decommissioned is growing. Decommissioning occurs at the end of one of two cycles: duty cycle or usefulness cycle (Grebler, 2017). The first one might terminate before ending the usefulness of the device. However, the latter, also known as death by old age, terminates when its service stops being useful or becomes boring for the owner/user after which devices stop being used and become unplugged. When the device is removed from the domain (decommissioning), some security services/functionalities should be managed by the server. Such services consist of deleting device-sensitive user data and state, including crypto-keying material, and passwords to resources. At the same time, the server should remove its own copies of all passwords related to the device, keying material, and user-related sensitive data (Miettinen et al., 2018).

8.2.1. Key/Certificate revocation

Keys must be revoked if a client is compromised or a service agreement between the client and server is canceled. This can occur by means of a key revocation message, which the trust anchor sends to the server, as part of the key management scheme (Raza et al., 2016) or as a complement to the existing key management (Bock et al., 2019). Similarly, for certificates a long validity period is an immense threat if the IoT device be compromised. Thus, Kim et al. (2016) define a validity period for certificates based on risk factors (e.g., public devices have the lowest period) and after expiration of validity, the certificate will be revoked or updated. When a certificate is revoked, its serial number and revocation date can be stored in Certificate Revocation List (CRL), which is a common method for managing certificate revocation. During communication, one can determine the validity or status of the certificate by verifying whether it is or in CRL or not. Table 30 demonstrates some models for managing the CRL.

9. IoT and related technologies

Data processing on IoT device can be considered same as edge computing where the data is processed on the device itself with no data

transferring to other sources. Cloud and fog are other technologies related to IoT with outsourced data processing. Cloud computing is considered a trusted platform to deliver IoT services (Zarpelão et al., 2017). However, due to several challenges in cloud computing, such as the fast increment in a large number of IoT devices, the novel concept of fog computing has been proposed. Fog computing is a platform to decentralize the cloud and bring the services closer to the end system (Dizdarevic et al., 2019).

9.1. Cybersecurity in fog and cloud

Fog and cloud have their exclusive security solutions. For instance, to detect DDos attacks in cloud systems, Wahab et al. (2020) propose an optimal load distribution solution. Another cloud-based detection and defense strategy against multiple types of attacks is presented in (Wahab et al., 2019). More security mechanisms in various paradigms, such as fog computing, mobile edge computing, and mobile cloud computing are analyzed by Roman et al. (2018). Such security countermeasures seem to be applicable in the IoT platform but it is impossible to apply them directly, due to IoT features consisting of the constraint computing power of IoT devices, a large number of connected devices, and data sharing among users and devices (Zarpelão et al., 2017).

9.2. Fog and IoT security

Fog relation with IoT security is two-fold. On one hand, fog can trigger new security challenges, dissimilar to cloud where cloud infrastructures are already protected by cloud operators from various attacks. Distributed inherent feature of fog induces it more vulnerable to attacks. Some fog systems are so small that they might not be resourceful the same as cloud to implement a proper protection mechanism or intelligence for detecting threats (Chiang and Zhang, 2016). Since fog was originally introduced to present new applications and services to the IoT environment, several security problems in this area have been solved already. Diro et al. (2017) employ a cryptography method, ECC, to present a secure fog-based publish-subscribe lightweight protocol for IoT. A cybersecurity framework in fog and cloud environment is presented in (Sohal et al., 2018) to identify malicious edge (or IoT) devices. For this purpose, they apply a combination of three common technologies consisting of Markov model, Intrusion Detection System (IDS), and Virtual Honeypot Device (VHD).

On the other hand, fog can address security challenges, due to its locality on the edge and proximity to the end system. For example, fog as a security layer between IoT device and cloud overcomes man-in-the-middle attack (MIMA) since abnormal activities can be identified and reduced through this layer before reaching the system (Hassija et al., 2019). Security features over fog, in general, can have higher impact on IoT networks rather than cloud. Possible impact of various security considerations such as access control, authentication, and CIA when fog computing is compromised is analyzed in (Butun et al., 2019). For instance, although fog computing acts as a gateway between IoT devices and cloud, it is impossible to access the databases of cloud from fog gateway, however, fog gateway is able to conquer the IoT devices. Thus, a compromised fog gateway trigger higher level of risk on IoT network compared to cloud.

10. Discussion

Overall, as a comparison of all the security techniques introduced in previous sections, Table 31 presents the security solutions according to the stage and phase of lifecycle where the related issues are resolved. The pseudonym for each security solution or the generally known name for the solution, if there is no pseudonym is mentioned as *Method* in the table. The relevant domains, including the smart environment, application, and sensor type, which are targeted by such security solution, are discussed in the table as *Domain*. Among the extracted domain, smart home and WSN attracted more attention for security analysis and implementation.

The study demonstrates that amongst security issues, security requirements in the deployment phase of BoL and application reconfiguration during the operation phase are in lower priority to be analyzed and tackled. Moreover, non-repudiation as an important security requirement, whether in BoL or MoL, offers insufficient contribution. Further, key pairing as part of key management has recently been regarded as less attractive by the researchers, still requiring more investigation. As an advantage of such a study, a solution is available for all the security problems in various network layers (i.e., physical layer, link layer, and so on) but with the exception of one paper, none of them follow the device lifecycle in their method definition and implementation. However, a security solution is efficient for IoT systems only if it can be technically secure throughout the entire device lifecycle not only during installation or operation.

The following abbreviations have been introduced here from the *"Solution"* column of discussion table if they are not the method name. These are being abbreviated in the discussion table to increase its readability and give more clarity to the compared approaches. KMP: Key Management Protocol; PRW: Position Random Watermark; CB: Context-based; MEMS: Microelectromechanical Systems; LoF: Local Outlier Factor; TM: Trust Management; PP: Privacy Preserving; PPDM: Privacy Preserving Data Mining; CoT: cloud of Things; PUFs: Physically Unclonable Functions; AWMA: Asymmetric Weighted Moving Average; VNF: virtual Network Functions; ANN: Artificial Neural Network; AAL: Ambient Assisted Living; HIP: Host Identity Protocol; DTLS: Datagram Transport Layer Security; ML: machine learning;

11. Open issues

The previously analyzed security aspects in IoT with respect to product lifecycle, raise challenges and opportunities for further research. This section discusses the major research directions required for addressing the unique IoT challenges (Bertin et al., 2019).

1. **Resolving identities of IoT devices:** The attribute based access control concerns with the device identity issues. Hence, the attribute combination for assertion of requester authenticity, i.e., manufacturer, owner or current location can be used. Nevertheless, user identification for the device is still questionable.
2. **Dynamic AC policies:** A privacy policy must specify who interacts with what data, where, how, and when. Easy-to-understand policies need to be built that are dynamic according to the IoT context with increased data flow combinations in IoT applications.
3. **Openness:** The basic IoT requirement is that the solutions provided by the third parties and various industry partners should be integral. Such openness can be provided by the use of open standards, which can be used for all IoT devices. Industry partners should be able to integrate such open standards for their devices to enable cross platform integration of applications.
4. **Heterogeneity:** New objects are deployed which need backward compatibility to integrate with the already deployed old objects. Hence, new AC protocols will be required to ensure this.
5. **Personal data:** Extensive personal data are generated by IoT systems, with end users taking charge of them. The conflicting interests of users need to be managed by IoT systems.
6. **Scalability:** As IoT systems escalate, they should be able to handle large user groups, applications, decision points and policy enforcement.

Table 31
Classification of security issues of IoT devices based on their lifecycle.

Lifecycle stage	Lifecycle phase	Citation & year	Security issue	Solution	Method	Domain	Description
BoL	Manufactured	Sciancalepore et al. (2015)	Certificate installation	preloading certificates in each device by the network administrator before the deployment of the network	KMP	IIoT	generating ultra-lightweight "implicit" certificates exploiting the Elliptic Curve Qu-Vanstone (ECQV) technique
BoL	Manufactured	Hänel et al. (2017)	Certificate installation	adjustable security system	ASREID	RFID-equipped sensor	reducing the overhead of device pre-equipping of security information by providing various selection for pre-installed certificates
BoL	Manufactured	Won et al. (2018)	Certificate installation	distributed and secure PKI	IoT-PKI	–	assigning the role of CAs to distributed blockchain nodes
BoL	Manufactured	García-Magariño et al. (2019)	Certificate installation	digital certificate for authentication	–	smart vehicle	requesting a digital certificate from certifier, checking the vehicle by certified accreditation center, and incorporating private key to the vehicle
BoL	Manufactured	Babar et al. (2011)	Physical security	embedded security framework	–	in-built security	providing a dynamic prevention, detection, diagnosis, isolation, and countermeasures against breaches
BoL	Manufactured	Xu et al. (2014) (Xu et al., 2014b)	Physical security	Computer-aided design	CAD	hardware-based security	using hardware-based security approaches to be more resilient against side-channel and physical attacks
BoL	Manufactured	Pecorella et al. (2016)	Physical security	security framework for the device initialization	–	e-health	providing a secure and error proof configuration for cryptographic keys of devices
BoL	Manufactured	Ali and Awad (2018)	Physical security	risk assessment approach	OCTAVE Allegro	smart home	identifying security threats and the potential risks emanating from inside and outside of environment
BoL	Deployment	Miettinen et al. (2014) (Miettinen et al., 2014a)	Key pairing	zero-interaction pairing	CB	wearable devices	identifying the correct device based on sustained co-presence over time by computing a fingerprint of the ambient context
BoL	Deployment	Sciancalepore et al. (2015)	Key pairing	robust key negotiation	KMP	IIoT	using ECDH algorithm to ensure secrecy
BoL	Deployment	Tsai et al. (2017)	Key pairing	key establishment scheme by Kronecker	KMP	WSN	computing the pairwise key with no communication while decreasing the storage cost and computation cost
BoL	Deployment	Samtani et al. (2016)	Vulnerability management	active and passive vulnerability assessment	–	critical infrastructure	Identifying a multitude of vulnerabilities on Supervisory Control and Data Acquisition (SCADA) systems
BoL	Deployment	Alghamdi et al. (2018)	Vulnerability management	automated tool for vulnerability assessment	IoTVerif	client applications	verifying SSl/TLS certificate validation of IoT messaging protocols
BoL	Deployment	Wang et al. (2018)	Vulnerability management	vulnerability assessment and quantification method	–	IIoT	Based on attack graph and maximum loss stream; CVSS scale to quantify and calculate the potential risk of attack path
BoL	Deployment	Costa et al. (2019)	Vulnerability management	identification of high-risk vulnerabilities	–	smart home	verifying if a device is vulnerable to the most common vulnerabilities
BoL	Deployment	Alrawi et al. (2019)	Vulnerability management	a modeling methodology	SoK	smart home	understanding attack techniques, proposed mitigation, and stakeholder responsibilities according to component analysis

(*continued on next page*)

Table 31 *(continued)*

Lifecycle stage	Lifecycle phase	Citation & year	Security issue	Solution	Method	Domain	Description
BoL	Deployment	Attaran and Rashidzadeh (2016)	Identification	chipless RFID tags	MEMS	RFID sensors	using micro-electromechanical systems technology
BoL	Deployment	Miettinen et al. (2017)	Identification	automated device-Type identification	IOT SENTINEL	smart home	identifying the types of devices introduced to a network and employing mitigation measures for device-types with potential security vulnerabilities
BoL	Deployment	Berelejis et al. (2017)	Identification	device identification with an image of the device	–	smart home	apturing the image by user device and transmitting the image from the user device to the IoT device
BoL	Deployment	Corchia et al. (2019)	Identification	robust chipless identification tags	encoding	wearable electronics	using two strategies for encoding information in chipless tags
BoL	Deployment	Neto et al. (2016)	Authentication & Access control	Authentication of Things	AoT	entire lifecycle	relying on identity-based and attribute-based cryptography to distribute keys, authenticate devices, and cryptographically enforce ABAC
BoL	Deployment	Yousefnezhad et al. (2017)	Authentication & Access control	security model	O-MI	smart home	defining design and implementation principles for access control and integrating with O-MI reference implementation
BoL	Deployment	Valea et al. (2019)	Confidentiality	secure context saving unit, a hardware module easily implementable inside a SoC	SCSU	processor-based devices	providing confidentiality by stream cipher based encryption and integrity by MAC derived from the saved context
BoL	Deployment	Zhang et al. (2017) (Zhang et al., 2017b)	Integrity	random digital watermarking algorithm as data integrity protection scheme	PRW	WSN	based on fragile watermark to prevent variety of attacks on perception layer
BoL	Deployment	Chamarajnagar and Ashok (2019)	Integrity	integrity threat identification framework	LOF	precision agriculture	detecting from physical attacks on sensor nodes using outlier detection
BoL	Deployment	Wu et al. (2019)	Availability	node availability analysis	NBIOT-HWSN	NB-IoT	by presenting a node heterogeneity model based on node distribution and vulnerability differences then using epidemic theory and Markov chain to establish node state transition mode
BoL	Deployment	Mustafa et al. (2019)	Availability	availability analysis of service-oriented cloud	QoS	IIoT	running experiments on Device-to-cloud, cloud-to-cloud and inside-cloud
BoL	Deployment	Oriwoh et al. (2016)	Non-repudiation	resource-constrained authentication protocol	ReCAP	CPS	demonstrating the feasibility of achieving non-repudiation
BoL	Deployment	(Fremantle et al., 2014)	Identification	federated identity and access management approach	FIAM	Iot protocols	building a prototype using OAuth 2.0 to enable access control to information distributed via MQTT
BoL	Deployment	Meidan et al. (2017)	Identification	device identification based on network traffic analysis	ProfilIoT	ML-based	using machine learning algorithms to identify IoT device type, based on characteristics of the network traffic it generates
BoL	Deployment	Song et al. (2017)	Identification	improved identity management	IIDM	5G	improving both security and performance by maximizing load balancing to service provider
BoL	Deployment	Yousefnezhad et al. (2018)	Identification	measurement-based device identification framework	MeDI	smart campus	monitoring the data packets coming from smart devices to protect the server from receiving and spreading false data
MoL	Monitoring & diagnosis	Namal et al. (2015)	Trust	autonomic trust management framework	MAPE-K	cloud-based	evaluating trust level by monitoring, analysing, planning, executing, and presenting knowledge feedback loop
MoL	Monitoring & diagnosis	Chen et al. (2016)	Trust	adaptive and scalable trust management	TM	SOA-based	trust evaluation based on feedback employing similarity level of friendship, social relationship, and community of interest relationships for filter
MoL	Monitoring & diagnosis	Alexopoulos et al. (2018)	Trust	distributed trust management system	DL-TM	smart contract	utilizing distributed ledger to maintain all access delegations, and reputation scores of participants in 3 layers: global, group and local layer

(*continued on next page*)

Table 31 *(continued)*

Lifecycle stage	Lifecycle phase	Citation & year	Security issue	Solution	Method	Domain	Description
MoL	Monitoring & diagnosis	Tariq et al. (2019)	Trust	mobile code-driven trust mechanism	MCTM	SN-powered	detecting isolating malicious internal sensor nodes based on their forwarding behaviors
MoL	Monitoring & diagnosis	Alshehri and Hussain (2019)	Trust	fuzzy security protocol for managing trust	Fuzzy-IoT	cluster-based	applying a new security protocol to create a secure communication and message exchange between devices
MoL	Monitoring & diagnosis	Ukil et al. (2014)	Privacy	privacy measurement and quantification	PPDM	smart meter	enabling the user to assess the risk of sharing his private data
MoL	Monitoring & diagnosis	Ukil et al. (2015)	Privacy	dynamic privacy analyzer	DPA	smart energy	addressing the problem of involuntary privacy breaching risk minimization by minimizing the capability of privacy intruders
MoL	Monitoring & diagnosis	Boussada et al. (2018)	Privacy	privacy-preserving system	PKE-IBE	smart e-health	based on Identity-Based Cryptography tackling the key escrow issue and ensuring blind partial private key generation
MoL	Monitoring & diagnosis	Jourdan et al. (2018)	Privacy	privacy-preserving activity recognition framework	PP	personal health-care/wearable device	limiting the risk of user re-identification by extracting multiple features from raw signal and analyzing their impact on both the activity recognition and the user re-identification
MoL	Monitoring & diagnosis	Guan et al. (2019)	Privacy	device-oriented Anonymous Privacy-Preserving scheme	APPA	fog-enhanced	using Authentication for data aggregation applications in fog-enhanced IoT system
MoL	Monitoring & diagnosis	Raza et al., 2013)	Compromise detection	real-time intrusion detection	SVELTE	routing	safeguarding network from known attacks and adapting existing IDS to IoT-specific protocols, e.g., 6LoWPAN
MoL	Monitoring & diagnosis	Taneja (2013)	Compromise detection	compromise analysis framework	analytical	M2M devices	detecting compromised IoT devices using mobility behavior
MoL	Monitoring & diagnosis	Jia et al. (2017)	Compromise detection	context-based permission system	ContexIoT	smartphone	detection of malicious app by discovering sensitive actions
MoL	Monitoring & diagnosis	Nguyen et al. (2018)	Compromise detection	self-learning distributed compromise detection	DÏoT	smart home	using federated learning for device-type specific anomaly detection
MoL	Monitoring & diagnosis	Mahalle et al. (2014)	Authentication	threshold cryptography-based group authentication	TCGA	WiFi devices	verifying authenticity of all devices in the group communication using probabilistic asymmetric public key encryption system
MoL	Monitoring & diagnosis	Porambage et al. (2014) (Porambage et al., 2014b)	Authentication	pervasive lightweight authentication	PAuthKey	WSN	establishing secure link between sensors in two phases
MoL	Monitoring & diagnosis	Fan et al. (2016)	Authentication	lightweight RFID-based mutual authentication	LRMAPC	5G	using cache on the reader and storing recent visited tags
MoL	Monitoring & diagnosis	Yang et al. (2016)	Authentication	lightweight anonymous authentication scheme	self-blinding	anonymity-based	outsourcing the task of witness update and using dynamic accumulator for credential revocation
MoL	Monitoring & diagnosis	Anggorojati et al. (2012)	Access control	capability-based and context-aware access control scheme	CCAAC	Federated IoT	authorizing a delegation request from a delegator (central entity)
MoL	Monitoring & diagnosis	Riad et al. (2017) (Riad and Zhu, 2017)	Access control	trust-based access control model	TB-AC	cloud-based	using user trust level to modify his assigned permissions, based on multiple factors
MoL	Monitoring & diagnosis	Hasiba et al. (2018)	Access control	combination of RBAC with ABAC models	hybrid	multimodal applications	solving the problem of context-awareness while avoiding explosion in the number of roles or rules in the security policy
MoL	Monitoring & diagnosis	Bouanani et al. (2019)	Access control	pervasive-based access control model	PerBAC	smart parking	presenting a multi-layer and proactive method based on ABAC with additional features from OrBAC

(*continued on next page*)

Table 31 *(continued)*

Lifecycle stage	Lifecycle phase	Citation & year	Security issue	Solution	Method	Domain	Description
MoL	Monitoring & diagnosis	Al-Turjman and Alturjman (2018)	Confidentiality	agile confidential framework	ECC	WSN	using ECC for collecting the sensed data to enable confidentiality and integrity
MoL	Monitoring & diagnosis	Khalaf and Mohammed (2018)	Confidentiality	confidentiality and Integrity services	AES, RSA	smart home	encrypting all data that sensors send to server
MoL	Monitoring & diagnosis	Eugster et al. (2019)	Confidentiality	confidentiality-preserving system	STYX	CoT	providing confidentiality against an adversary having full access to servers
MoL	Monitoring & diagnosis	Hurrah et al. (2019)	Confidentiality	robust data hiding framework	RCSMMA	multimedia	providing data confidentiality during transmission for analytic
MoL	Monitoring & diagnosis	Bauer et al. (2016)	Integrity	end-to-end integrity protection	ECDSA	RERUM project	using elliptic curve based signatures
MoL	Monitoring & diagnosis	Bhattacharjee et al. (2017)	Integrity	Bayesian inference framework	AWMA	On-Off attack	data integrity scoring under opportunistic data manipulation by an adversary
MoL	Monitoring & diagnosis	Aman et al. (2018)	Integrity	data tampering detection	PUF	cyber attacks	by reducing the computational complexity as well reducing the transmission energy
MoL	Monitoring & diagnosis	Battisti et al. (2018)	Integrity	secure control system	permutation matrix	IoT-based CPS	encoding the system output based on a secret pattern created by Fibonacci p-sequences to identify deception attack
MoL	Monitoring & diagnosis	Dinh and Kim (2018)	Availability	cost-efficient availability scheme	VNF	fog-core cloud	augmenting the availability of service function chaining by evaluating the improvement potential of VNFs for VNF redundancy allocation
MoL	Monitoring & diagnosis	Qaim and Özkasap (2018) (Qaim and. Özkasap, 2018)	Availability	fully distributed hop-by-hop data replication technique	DRAW	WSN	ensuring maximum data availability under high node failures to preserve data
MoL	Monitoring & diagnosis	Xiong et al. (2019)	Availability	privacy and availability data clustering scheme	PADC	electricity services	improving the selection of the initial center points and the distance calculation method from other points to center point
MoL	Monitoring & diagnosis	Yang and Kim (2019)	Availability	high availability architecture	VNF	IoT-Cloud	dynamically optimizing the availability according to various features of service
MoL	Monitoring & diagnosis	Abbas et al. (2018) (Abbas et al., 2019)	Non-repudiation	fog security service	FSS	fog computing	addressing the authentication, confidentiality, and non-repudiation for IoT devices via Private Key Generator
MoL	Monitoring & diagnosis	(Xu et al., 2019)	Non-repudiation	non-repudiation service provisioning scheme	blockchain-based	IIoT	using tamper-resistant blockchain as service publisher and an evidence recorder
MoL	Updates	Mahalle et al. (2014)	Key/Certificate update	key update in group authentication	TCGA	WiFi device	generating key pairs for group authentication and updating private keys of others
MoL	Updates	Abdmeziem et al. (2015)	Key/Certificate update	decentralized and batch-based group key management protocol	DBGK	mobile objects	reducing re-keying overhead triggered by membership changes and providing forward and backward secrecy for multicast communications

(*continued on next page*)

Table 31 *(continued)*

Lifecycle stage	Lifecycle phase	Citation & year	Security issue	Solution	Method	Domain	Description
MoL	Updates	Kung et al. (2018) (Kung and Hsiao, 2018)	Key/Certificate update	lightweight group key management	GroupIT	dynamic IoT	grouping similar devices and managing keys between groups through upper tiers (users) and inside group through lower tiers
MoL	Updates	Chien (2018)	Key/Certificate update	dynamic public key certificate	DPKC	WSN	updating public/private key pair without connecting to CA for a new certificate
MoL	Updates	Huth et al. (2016)	Software update	security protocol for a secure software update	–	smart home	integrating physically unclonable functions, software-based attestation, and proof of secure erasure
MoL	Updates	Weißbach etal., 2016	Software update	dynamic software update	decentralized	smart grid	coordinating the update of multiple distributed nodes involved in a running service
MoL	Updates	Kim et al. (2018)	Software update	remote software update	LPWAN	mobile edge computing	using low-power wide area network as a long-range networking technology
MoL	Updates	Kolomvatsos (2018)	Software update	distributed updates management scheme	ANN	pervasive computing	enhancing the autonomous nature of nodes by allowing them to decide about the update time
MoL	Re-configuration	Zhang et al. (2015) (Zhang et al., 2005)	Application reconfiguration	environment adaptive application reconfiguration	EAAR	WSN	utilizing rule-based knowledge to analyze the change of environment to efficiently perform self-adaptive application reconfiguration
MoL	Re-configuration	Samir et al. (2019)	Application reconfiguration	dynamic partial reconfiguration	AEAD	hardware-based	configuring the hardware security module based on the available power budget
MoL	Corporability	Zhu et al. (2012)	Mobile security	security and privacy model for mobile RFID systems	SPMMRFID-IOT	RFID devices	supporting the privacy of tags and readers, tag corruption, reader corruption, multiple readers, and mutual authenticated key exchange protocols
MoL	Corporability	Jara et al. (2013)	Mobile security	secure and scalable mobility management scheme	HIMALIS	inter-domain	supporting scalable inter-domain authentication and secure location update and binding transfer for the mobility process
MoL	Corporability	Gonçalves et al. (2013)	Mobile security	security architecture for mobile platforms	AAL	m-health	establishing and managing a medication prescription service in mobility context using electronic Personal Health Records
MoL	Corporability	(Kai et al., 2013)	Mobile security	secure healthcare service	Health-IoT	smart e-health	establishing a trust IoT application market (IAM) by exchanging the feature of application in marketplace and behavior of applications on end-devices
MoL	Corporability	Hummen et al. (2013) (Hummen et al., 2013a)	End-to-end security	lightweight protocol extensions for HIP DEX during handshake	–	–	reducing handshake cost by session resumption, handling network heterogeneity by puzzle-based DoS protection, and reducing processing time by refined retransmission
MoL	Corporability	Sahraoui and Bilami (2015)	End-to-end security	compressed and distributed HIP for lightweight end-to-end security	CD-HIP	WSN	combination of an efficient distribution scheme for key exchange and an optimal 6LoWPAN model for protocol header
MoL	Corporability	Moosavi et al. (2016)	End-to-end security	end-to-end security scheme for mobility enabled healthcare	SEA	smart e-health	providing a secure and efficient end-user authentication and authorization, secure end-to-end communication, and robust mobility
MoL	Corporability	Banerjee et al. (2018)	End-to-end security	protocol extension for DTLS	DTLS	hardware-based	designing of reconfigurable energy efficient cryptographic accelerators and a dedicated protocol controller

(*continued on next page*)

Table 31 *(continued)*

Lifecycle stage	Lifecycle phase	Citation & year	Security issue	Solution	Method	Domain	Description
EoL	Re-ownership	Leng et al. (2014)	Key/Certificate update	ownership management system	–	–	handling ownership transfer through TTP checking the ownership proof and validity of ownership transfer
EoL	Re-ownership	Ghuli et al. (2017)	Key/Certificate update	decentralized re-ownership scheme	–	cloud-based	using blockchain transactions to reduce the dependency on a central cloud
EoL	Re-ownership	Mamun et al. (2018)	Key/Certificate update	secure RFID ownership transfer protocol	OTP-IoT	RFID tags	preventing MITM attack and supporting mutual authentication while enabling owners to transfer the ownership of multiple tags simultaneously
EoL	Re-ownership	Khan et al. (2018) (Khan et al., 2018b)	Key/Certificate update	automated re-ownership of devices	chownIoT	smart home	combining authentication, profile management, data protection, and ownership change
EoL	Re-ownership	Aghili et al. (2019)	Key/Certificate update	lightweight authentication and ownership transfer protocol	LACO	E-health	preserving the user privacy by considering ownership transfer of users
EoL	De-commissioned	Raza et al. (2016)	key/certificate revocation	key revocation as part of key management architecture	S3K	secure DTLS	marking the key as used in the sliding window to induce it unusable
EoL	De-commissioned	Duan et al. (2018)	key/certificate revocation	two novel lightweight CRL protocols	HCRL, BfCRL	PKI-based	based on generalized Merkle hash tree and Bloom filter
EoL	De-commissioned	Bock et al. (2019)	key/certificate revocation	key revocation and re-keying for adaptive key establishment scheme	AKES	link layer security	not routing messages via evicted nodes in Node Revocation List
EoL	De-commissioned	Cebe and Akkaya (2019)	key/certificate revocation	distributed CRL management scheme	DHT-based CRL	smart city	utilizing distributed hash trees to provide less overhead with reasonable access time regardless of network size

Trust Management (TM) is an important consideration enhancing security in IoT devices, although posing certain challenges in its implementation at a broader level. The following objectives are rarely considered in the literature: (Yan et al., 2014):

- Trust Relationship and Decision (TRD): TM should measure the trust relationships of entities in all layers (physical, network and application layer) and help them to make a wise decision for their communication.
- Data Fusion and Mining Trust (DFMT): TM should process and analyze data in a trustworthy way (considering reliability, holographic data process, privacy preserving, and accuracy) in the network layer. It should also mine user demands based on their social behaviors.
- System Security and Robustness (SSR): TM should counter attacks in all system layers to apply security and dependability (reliability and availability)
- Generality (G): TM should be generic for wide use.
- Human-Computer Trust Interaction (HCTI): TM should be easily acceptable to users in the application layer.

There is no comprehensive TM approach which considers all objectives of trust. Previous TM approaches (which are not Machine learning(ML)-based) estimated the trustworthiness of a trustee by its previous behaviors while this knowledge (e.g., a trust path between trustor and trustee) may not be available locally to the trustor. So what should we do if there is no knowledge about past behavior? ML algorithms can be applied to more efficiently estimate agent trustworthiness. MetaTrust (Xin et al., 2011) is an ML framework for identifying trust relying on discriminant analysis (DA), and it controls meta information using the trustor's local knowledge. Lopez et al. (López and Maag, 2015) also apply a supervised ML technique, Support Vector Machine (SVM) for TM. Tinghuai et al. (Ma et al., 2005) exploit another ML method, Case-Based Reasoning (CBR) to achieve a context-aware technique for smart homes. Miettinen et al. (2014b) use classification for a context-aware technique for access control. Motti et al. (2012) motivate the use of ML approaches for context-aware adaptation and Wang and Ahmad (Wang Ahmadet al, 2010) propose a context-aware ML framework for Android platform. However, we cannot use these solutions in the IoT context because of IoT constraints such as existence of limited power devices and heterogeneous technologies. To address these challenges, we should use lightweight methods to make these ML solutions implementable in IoT context. For instance, Che et al. (2015) propose ML algorithms for producing a lightweight TM. Perhaps, we could apply this algorithm in IoT for the same purpose. The other open issues concerning trust management are as follows:

1. Current TM solutions for data perception trust (reliable data sensing and collection) are too heavy and complicated for wireless sensor nodes. We therefore need lightweight trust mechanisms suitable for small entities (Yan et al., 2014).
2. A trust management survey (Yan et al., 2014) defines five crucial TM objectives for a trustworthy IoT: Trust Relationship and Decision (TRD), Privacy Protection (PP), System security and robustness (SSR), Generality (G), Identity Trust (IT). There are few works on PP. To obtain a TM with vertical objectives, we need to integrate PP with other TM mechanisms. The PP approach should be applied in all layers and for resource-restricted devices.
3. Many previous analysis of Secure Multi-Party Computation (SMC) address the problem of secure computation among untrusted participants. Unfortunately, most of them are impractical for IoT due to computation complexity, communication costs, and flexibility. We need a new SMC method that supports the vertical TM objectives (Yan et al., 2014).
4. Transmitting and computing trust between different networks is difficult (Yan et al., 2014).
5. TM should work fast and consume less energy. Previous research neglected power efficiency of TM methods in IoT (Yan et al., 2014).
6. There is no previous work in realizing an automatic TM (Yan et al., 2014).
7. Since there is a huge amount of raw data created by things in IoT, it is important to achieve trustworthy data fusion to reduce the cost (Yan et al., 2014).
8. One important factor influencing trust is context, which includes purpose of trust, environment of trust, and risk of trust. The current TM approaches do not focus on context awareness, so the trust results are impersonalized. They cannot provide intelligent services (context-aware services) in the application layer (Yan et al., 2014). Some examples of context-aware services include a real-time traffic update or even a live video feed of a planned route for a motor vehicle user (Wikipedia. Context aware). This service is also known as "Only here, only now and only me".
9. It is necessary to determine a well-defined and commonly-accepted trust negotiation language for semantic interoperability of the IoT context (Sicari et al., 2015).

These can be categorized based on product lifecycle and various research challenges can be listed. These can be an important consideration for an industry to address while designing and manufacturing their products. The open issues can be presented in general as shown in Table 32.

11.1. Research challenges in BoL

1. **Vulnerability in resource-constrained devices:** The IoT devices with constrained resources (like edge devices) are particularly susceptible to attacks. It has been shown by penetration studies that even though it takes less power to implement of better practice security for edge nodes, their accessibility to harmful threats still remains immense.
2. **Inter-fog sharing of resources**: It is one such domain requiring further research since when the requests are not processed in the fog layer because of heavy load, they are forwarded to cloud. The neighboring fog layers can do resource sharing, thus preventing the transfer of unwanted requests to cloud.
3. **Near real-time data analysis**: The near real-time data analysis in the IoT device proximity is imperative for the successful implementation of IoT applications. Different machine learning-based approaches could be designed to analyze the data within the node and to prevent the transit of data, thus enhancing the application security.
4. **Security at gateway level:** The security layer at the gateways is required between different layers in IoT as they grant an easy access point to intruders in system. A promising solution is to provide end-to-end encryption, which will be a big challenge for securing data through gateways. The decryption of the data should only take place at the destinations and not at the gateways in the middle of protocol translation. This further requires unified standards for data transmission rather than different protocols which may require translations at the gateways leading to attack vulnerability.
5. **Interoperability between protocols:** The challenges related to the development of appropriate security models with context to heterogeneity of IoT systems, is an important security consideration. Indeed, the core design and development principle in IoT relies on interoperability and its benefits should be remarkable in the security domain. In this context, the recent efforts to orchestrate security approaches for Network function virtualization (NFV) and Software-defined networking (SDN) environments merit research to form a basis for enhanced future IoT environments.
6. **X.509 certificates validity:** Future IoT applications may require approaches which support online verification of X.509 certificates

Table 32
The open issues overview and description.

Open Issue	Brief description of the cause
Standards	There are several standardization effortss across multiple domains
Mobility support	There are not enough reliable proposals for addressing mobility support in IoT
Transport protocol	The connection setup and congestion control mechanisms of existing transport protocols fail in IoT scenarios as they require high buffering in connected objects.
Traffic characterisation	The data traffic generated by IoT is significantly different from those observed in the internet.
Quality of Service (QoS) support	It will be mandatory to define new QoS requirements for IoT
Authentication	Authentication in IoT requires appropriate authentication infrastructures as things have scarcity of resources compared to present computing devices. Another problem is man-in-middle attack.
Data Integrity	The password lengths supported by IoT devices may be too short to support strong protection level.
Privacy	The connected devices can collect more private information from a person without its awareness. Control on such information is hard with current technologies.
Digital Forgetting	The person's collected information can be retained for several years which can be used to retrieve any information with data mining techniques.

particularly for the Constrained Application Protocol (CoAP) certificates security mode. Further research is required on adopting these kind of mechanisms.

7. **Trade-off between security and energy consumption:** The proposed asymmetric cryptographic solutions in IoT are flexible, making them efficient with complexity and scalability issues but they are not energy efficient. These classic asymmetric approaches (RSA, NTRU, and ECC) are subsequently investigated in several studies. The major challenge lies in establishing trade-off between security and energy consumption to achieve a desirable security level. The solutions should reduce the energy consumption in resource-constrained devices, while ensuring an acceptable security level.
8. **Support of public- keys and digital certificates:** The current computing platforms of the sensing platforms pose a constraint on certificate processing. The certificate overhead problem in constrained sensing platforms has been addressed in (Hummen et al., 2013b) by discussing the various design approaches. The certificate pre-validation and session resumption are the proposed approaches where certificate pre-validation involves a security gateway to support certificate validation before handshake message forwarding to the destination and session resumption. It helps in maintaining minimal session state after session breakdown.
9. **Exponential increase in the number of weak links:** As most IoT devices have limited computation and storage resources, and considering cost factors, the available devices in market do not support highly secure cryptography. Hence, it has led to emergence of many weak links in the network which can easily be compromised by any attacker to target the entities in the network which are presumed to be secure. Many studies (Use Smart Doorbell to Ha, 2016) (Hacking into Internet Co, 2016) demonstrate how edge nodes can be targeted for extraction of the home user's WiFi password where one attack (Use Smart Doorbell to Ha, 2016) uses light bulbs and other (Hacking into Internet Co, 2016) uses user's smart lock. The diverse nature of IoT devices and applications amplifies the impact.

11.2. Research challenges in MoL

1. **Unsecure update process for a medical device:** The dosage limit on medication to be given to the patient was raised by a hacker using a Hospira drug infusion pump (Scully) in 2015. The main concern emerged from an insecure library update process and communication modules for the pumps. The question arises if the updates in the software or firmware are digitally signed or authenticated.
2. **Efficient and reliable consensus mechanisms:** The current consensus algorithms are less efficient as they are highly resource hungry. Hence there is need to design consensus among the nodes to prevent rampant consumption of computation power.
3. **Limitations of blockchain architecture:** This architecture is limited in the number of permissioned network nodes and in permissionless network throughput. To support high throughput with an increase in users or nodes, various consensus algorithms need to be designed.
4. **DTLS limitations:** Datagram Transport Layer Security (DTLS) is considered a supporting protocol in the application layer using CoAP. DTLS has some limitations which allow the other approaches to be used for providing security in the application layer. The work has already been going on in the CORE working group to propose and evaluate new security approaches. DTLS limitations motivate research on alternative proposals for securing IoT communications at the application level using CoAP.
5. **Adoption of ECC:** Evaluation of the impact of DTLS on sensing platforms with distinct characteristics is important because if there is efficient availability of Advanced Encryption Standard (AES) in hardware in IEEE 802.15.4 sensing platforms. A significant impact can be imposed by the DTLS handshake (for authentication and key agreement) on the devices with constrained resources, in particular while consideration of ECC public-key cryptography for supporting authentication and key agreement. The support of ECC for 6LoWPAN environments requires more research since ECC is currently incompletely viable for resource-constrained sensing devices.
6. **Multicast communications:** Another important aspect of consideration is the inadequacy of suitable key management methods for supporting CoAP multicast communications which are secure. Multicast communications are not supported by DTLS (Garcia-Morchon et al., 2013), (Brachmann et al., 2012b), which is an essential requirement in most IoT applications. Again, more applicable group key mechanisms are required to support session key establishments among the various participating devices in secure CoAP multicast communications.
7. **Object security in CoAP:** The employment of object security approaches compared to transport layer security is considered for securing COAP communications. The usage of new CoAP options (Granjal et al., 2013) was considered (i) to enable the identification of application of security to given CoAP message a responsible entity, (ii) to enable data transportation for authenticating and authorizing a CoAP client, and (iii) to enable security data transportation of security-related data.
8. **Unexpected uses of data:** With the widespread use of IoT applications, an adverse effect on the private information of citizens can be inferred from presumed non-critical data which is not well known or understood. McKenna et al. (2012) provided the residents with private information such as the count of residents, daily routines, and personal habits which are inferred from electricity load data of smart meters in smart homes. These research attempts exploit unexpected use of data associated with connected sensors for smart city environments.

11.3. Research challenges in EoL

1. **The tamper-proof feature of blockchain:** There is a body of tamper-proof blockchain data which is never deleted leading to an accumulation of a large amount of garbage addresses and data. Hence the performance of the application becomes affected and there is a need for better ways for efficiently handling the garbage data in a blockchain.

12. Conclusion

There are ample research efforts for IoT security, but they are scattered. A systematic schema is required to identify the security gaps and address the security issues. The current paper has presented a detailed study of product lifecycle from the IoT perspective of security by providing the necessary background required for IoT and product lifecycle. Further, an in-depth security analysis of product lifecycle is conducted out by listing the state-of-the-art security solutions over the last decade by categorizing them based on lifecycle stages. The survey addresses and compares a broad range of techniques, methods, models, functionalities, systems, applications, and middleware solutions related to IoT, IoT security, and device lifecycle. The comparison and assessment of the available security mechanisms in product lifecycle can aid in selecting the appropriate secure techniques. Thus, the review is useful for implementing security in dynamic applications as per user requirements.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The research leading to this publication is supported by the European Union's Horizon 2020 research and innovation program (bIoTope; grant 688203 and FINEST TWINS; grant 856602) and Academy of Finland (Open Messaging Interface; grant 296096).

References

Abbas, N., Asim, M., Tariq, N., Baker, T., Abbas, S., 2019. A mechanism for securing iot-enabled applications at the fog layer. J. Sens. Actuator Netw. 8 (1), 16, https://doi.org/10.3390/jsan8010016 [Online]. Available.

Abdmeziem, M.R., Tandjaoui, D., Romdhani, I., 2015. A decentralized batch-based group key management protocol for mobile internet of things (DBGK). In: 15th IEEE International Conference on Computer and Information Technology, CIT 2015; 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015; 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015; 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, Liverpool, United Kingdom, October 26-28, 2015, pp. 1109–1117, https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.166 [Online]. Available.

Abera, T., Asokan, N., Davi, L., Koushanfar, F., Paverd, A., Sadeghi, A., Tsudik, G., 2016. Invited - things, trouble, trust: on building trust in iot systems. pp. 121:1121:6. In: Proceedings of the 53rd Annual Design Automation Conference, DAC 2016, Austin, TX, USA, June 5-9, 2016, https://doi.org/10.1145/2897937.2905020 [Online]. Available.

Abomhara, M., Kien, G.M., 2014. Security and privacy in the internet of things: current status and open issues. In: 2014 International Conference on Privacy and Security in Mobile Systems, PRISMS 2014, Aalborg, Denmark, May 11-14, 2014, pp. 1–8, https://doi.org/10.1109/PRISMS.2014.6970594 [Online]. Available.

Aghili, S.F., Mala, H., Shojafar, M., Peris-Lopez, P., 2019. LACO: lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in iot. Future Generat. Comput. Syst. 96, 410–424, https://doi.org/10.1016/j.future.2019.02.020 [Online]. Available.

Al-Fuqaha, A.I., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M., 2015. Internet of things: a survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials 17 (4), 2347–2376, https://doi.org/10.1109/COMST.2015.2444095 [Online]. Available.

Al-Turjman, F., Alturjman, S., 2018. Confidential smart-sensing framework in the iot era. J. Supercomput. 74 (10), 5187–5198, https://doi.org/10.1007/s11227-018-2524-1 [Online]. Available.

Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F., 2017. Internet of things security: a survey. J. Netw. Comput. Appl. 88, 10–28, https://doi.org/10.1016/j.jnca.2017.04.002 [Online]. Available.

Alcaide, A., Palomar, E., Montero-Castillo, J., Ribagorda, A., 2013. Anonymous authentication for privacy-preserving iot target-driven applications. Comput. Secur. 37, 111–123, https://doi.org/10.1016/j.cose.2013.05.007 [Online]. Available.

Alexopoulos, N., Habib, S.M., Mhlhuser, M., 2018. Towards secure distributed trust management on a global scale: an analytical approach for applying distributed ledgers for authorization in the iot. In: Proceedings of the 2018 Workshop on IoT Security and Privacy, IoT S&P@SIGCOMM 2018, Budapest, Hungary, August 20, 2018, pp. 49–54, https://doi.org/10.1145/3229565.3229569 [Online]. Available.

Alghamdi, K., Alqazzaz, A., Liu, A., Ming, H., 2018. Iotverif: an automated tool to verify SSL/TLS certificate validation in android MQTT client applications. In: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, CODASPY 2018, Tempe, AZ, USA, March 19-21, 2018, pp. 95–102, https://doi.org/10.1145/3176258.3176334 [Online]. Available.

Ali, B., Awad, A.I., 2018. Cyber and physical security vulnerability assessment for iot-based smart homes. Sensors 18 (3), 817, https://doi.org/10.3390/s18030817 [Online]. Available.

Alrawi, O., Lever, C., Antonakakis, M., Monrose, F., 2019. Sok: security evaluation of home-based iot deployments. In: 2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019, pp. 1362–1380, https://doi.org/10.1109/SP.2019.00013 [Online]. Available.

Alshehri, M.D., Hussain, F.K., 2019. A fuzzy security protocol for trust management in the internet of things (fuzzy-iot). Computing 101 (7), 791–818, https://doi.org/10.1007/s00607-018-0685-7 [Online]. Available.

Aman, M.N., Chua, K.C., Sikdar, B., 2017. Mutual authentication in iot systems using physical unclonable functions. IEEE Internet of Things J. 4 (5), 1327–1340, https://doi.org/10.1109/JIOT.2017.2703088 [Online]. Available.

Aman, M.N., Sikdar, B., Chua, K.C., Ali, A., 2018. Low power data integrity in iot systems. IEEE Internet of Things J. 5 (4), 3102–3113, https://doi.org/10.1109/JIOT.2018.2833206 [Online]. Available.

Ammar, M., Russello, G., Crispo, B., 2018. Internet of things: a survey on the security of iot frameworks. J. Inf. Sec. Appl. 38, 8–27, https://doi.org/10.1016/j.jisa.2017.11.002 [Online]. Available.

Andrea, I., Chrysostomou, C., Hadjichristofi, G.C., 2015. Internet of things: security vulnerabilities and challenges. In: 2015 IEEE Symposium on Computers and Communication, ISCC 2015, Larnaca, Cyprus, July 6-9, 2015, pp. 180–187, https://doi.org/10.1109/ISCC.2015.7405513 [Online]. Available.

Anggorojati, B., Mahalle, P.N., Prasad, N.R., Prasad, R., 2012. Capability-based access control delegation model on the federated iot network. In: The 15th International Symposium on Wireless Personal Multimedia Communications, WPMC 2012, Taipei, Taiwan, September 24-27, 2012, pp. 604–608 [Online]. Available http://ieeexplore.ieee.org/document/6398784/.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., Zhou, Y., 2017. Understanding the mirai botnet. In: 26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017, pp. 1093–1110 [Online]. Available https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis.

Apthorpe, N., Reisman, D., Feamster, N., 2017. A smart home is no castle: privacy vulnerabilities of encrypted iot traffic. vol. abs/1705.06805 CoRR. [Online]. Available http://arxiv.org/abs/1705.06805.

Arif, M., Shi, P., Ullah, A., Mahmood, K., Abid, M., Luo, X., 2019. Logical tree based secure rekeying management for smart devices groups in iot enabled WSN. IEEE Access 7, 76699–76711, https://doi.org/10.1109/ACCESS.2019.2921999 [Online]. Available.

Attaran, A., Rashidzadeh, R., 2016. Chipless radio frequency identification tag for iot applications. IEEE Internet of Things J. 3 (6), 1310–1318, https://doi.org/10.1109/JIOT.2016.2589928 [Online]. Available.

Atwady, Y., Hammoudeh, M., 2017. A survey on authentication techniques for the internet of things. In: Proceedings of the International Conference on Future Networks and Distributed Systems, ICFNDS 2017, Cambridge, United Kingdom, July 19-20, 2017, p. 8, https://doi.org/10.1145/3102304.3102312 [Online]. Available.

Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: a survey. Comput. Network. 54 (15), 2787–2805, https://doi.org/10.1016/j.comnet.2010.05.010 [Online]. Available.

Babar, S., Mahalle, P., Stango, A., Prasad, N.R., Prasad, R., 2010. Proposed security model and threat taxonomy for the internet of things (iot). In: Recent Trends in Network Security and Applications - Third International Conference, CNSA 2010, Chennai, India, July 23-25, 2010. Proceedings, pp. 420–429, https://doi.org/10.1007/978-3-642-14478-3_42 [Online]. Available.

Babar, S., Stango, A., Prasad, N., Sen, J., Prasad, R., 2011. Proposed embedded security framework for internet of things (iot). In: Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on. IEEE, pp. 1–5.

Banerjee, U., Juvekar, C., Wright, Arvind, A., Chandrakasan, A.P., 2018. An energy-efficient reconfigurable DTLS cryptographic engine for end-to-end security in iot applications. In: 2018 IEEE International Solid-State Circuits Conference, ISSCC 2018, San Francisco, CA, USA, February 11-15, 2018, pp. 42–44, https://doi.org/10.1109/ISSCC.2018.8310174 [Online]. Available.

Barnes, M., Alexa, are you listening? F-secure. [Online]. Available https://labs.f-secure.com/archive/alexa-are-you-listening/.

Battisti, F., Bernieri, G., Carli, M., Lopardo, M., Pascucci, F., 2018. Detecting integrity attacks in iot-based cyber physical systems: a case study on hydra testbed. In: 2018 Global Internet of Things Summit, GIoTS 2018, Bilbao, Spain, June 4-7, 2018, pp. 1–6, https://doi.org/10.1109/GIOTS.2018.8534437 [Online]. Available.

Bauer, J., Staudemeyer, R.C., Phls, H.C., Fragkiadakis, A.G., 2016. ECDSA on things: iot integrity protection in practise. In: Information and Communications Security - 18th International Conference, ICICS 2016, Singapore, November 29-December 2, 2016, Proceedings, pp. 3–17, https://doi.org/10.1007/978-3-319-50011-9_1 [Online]. Available.

G. Berelejis, D. Zehavi, and E. D. Ilsar, Method and apparatus for identifying a physical iot device, Apr. 18 2017, uS Patent 9,628,691.

Beresford, A.R., 2016. Whack-a-mole security: incentivising the production, delivery and installation of security updates (invited paper). In: Proceedings of the 1st International Workshop on Innovations in Mobile Privacy and Security, IMPS 2016, Co-located with the International Symposium on Engineering Secure Software and Systems (ESSoS 2016), London, UK, April 6, 2016, pp. 9–10 [Online]. Available http://ceur-ws.org/Vol-1575/invited_paper_1.pdf.

Bertin, E., Hussein, D., Sengul, C., Frey, V., 2019. Access control in the internet of things: a survey of existing approaches and open research questions. Ann. Telecommun. 74 (78), 375–388, https://doi.org/10.1007/s12243-019-00709-7 [Online]. Available.

Bertino, E., Islam, N., 2017. Botnets and internet of things security. IEEE Comput. 50 (2), 76–79, https://doi.org/10.1109/MC.2017.62 [Online]. Available.

Bhattacharjee, S., Salimitari, M., Chatterjee, M., Kwiat, K.A., Kamhoua, C.A., 2017. Preserving data integrity in iot networks under opportunistic data manipulation. In: 15th IEEE Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, DASC/PiCom/DataCom/CyberSciTech 2017, Orlando, FL, USA, November 6-10, 2017, pp. 446–453, https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.87 [Online]. Available.

Bock, B., Matysik, J., Krentz, K., Meinel, C., 2019. Link layer key revocation and rekeying for the adaptive key establishment scheme. In: 5th IEEE World Forum on Internet of Things, WF-IoT 2019, Limerick, Ireland, April 15-18, 2019, pp. 374–379, https://doi.org/10.1109/WF-IoT.2019.8767211 [Online]. Available.

Bouanani, S.E., Kiram, M.A.E., Achbarou, O., Outchakoucht, A., 2019. Pervasive-based access control model for iot environments. IEEE Access 7, 54575–54585, https://doi.org/10.1109/ACCESS.2019.2912975 [Online]. Available.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., Sirdey, R., 2017. Towards better availability and accountability for iot updates by means of a blockchain. In: 2017 IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2017, Paris, France, April 26-28, 2017, pp. 50–58, https://doi.org/10.1109/EuroSPW.2017.50 [Online]. Available.

Boussada, R., Elhdhili, M.E., Sadane, L.A., 2018. A lightweight privacy-preserving solution for iot: the case of e-health. In: 20th IEEE International Conference on High Performance Computing and Communications; 16th IEEE International Conference on Smart City; 4th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018, Exeter, United Kingdom, June 28-30, 2018, pp. 555–562, https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00104 [Online]. Available.

Brachmann, M., Keoh, S.L., Morchon, O.G., Kumar, S.S., 2012. End-to-end transport security in the ip-based internet of things. In: 21st International Conference on Computer Communications and Networks, ICCCN 2012, Munich, Germany, July 30-August 2, 2012, pp. 1–5, https://doi.org/10.1109/ICCCN.2012.6289292 [Online]. Available.

Brachmann, M., Garcia-Mochon, O., Keoh, S.-L., Kumar, S.S., 2012. Security considerations around end-to-end security in the ip-based internet of things. In: Workshop on Smart Object Security, in Conjunction with IETF83, Paris, France, March 23, 2012.

Butun, I., Sari, A., sterberg, P., 2019. Security implications of fog computing on the internet of things. In: IEEE International Conference on Consumer Electronics, ICCE 2019, Las Vegas, NV, USA, January 11-13, 2019. IEEE, pp. 1–6, https://doi.org/10.1109/ICCE.2019.8661909. [Online]. Available.

Cai, H., Xu, L.D., Xu, B., Xie, C., Qin, S., Jiang, L., 2014. Iot-based configurable information service platform for product lifecycle management. IEEE Trans. Indust. Inform. 10 (2), 1558–1567, https://doi.org/10.1109/TII.2014.2306391 [Online]. Available.

Cebe, M., Akkaya, K., 2019. Efficient certificate revocation management schemes for iot-based advanced metering infrastructures in smart cities. Ad Hoc Netw. 92, https://doi.org/10.1016/j.adhoc.2018.10.027 [Online]. Available.

Chamarajnagar, R., Ashok, A., 2019. Integrity threat identification for distributed iot in precision agriculture. In: 16th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2019, Boston, MA, USA, June 10-13, 2019, pp. 1–9, https://doi.org/10.1109/SAHCN.2019.8824841 [Online]. Available.

Che, S., Feng, R., Liang, X., Wang, X., 2015. A lightweight trust management based on bayesian and entropy for wireless sensor networks. Secur. Commun. Network. 8 (2), 168–175, https://doi.org/10.1002/sec.969 [Online]. Available.

Chen, I., Guo, J., Bao, F., 2014. Trust management for service composition in soa-based iot systems. In: IEEE Wireless Communications and Networking Conference, WCNC 2014, Istanbul, Turkey, April 6-9, 2014, pp. 3444–3449, https://doi.org/10.1109/WCNC.2014.6953138 [Online]. Available.

Chen, I., Guo, J., Bao, F., 2016. Trust management for soa-based iot and its application to service composition. IEEE Trans. Serv. Comput. 9 (3), 482–495, https://doi.org/10.1109/TSC.2014.2365797 [Online]. Available.

Chhetri, S.R., Faezi, S., Rashid, N., Faruque, M.A.A., 2018. Manufacturing supply chain and product lifecycle security in the era of industry 4.0. J. Hardware Syst. Secur. 2 (1), 51–68, https://doi.org/10.1007/s41635-017-0031-0 [Online]. Available.

Chiang, M., Zhang, T., 2016. Fog and iot: an overview of research opportunities. IEEE Internet of Things J. 3 (6), 854–864, https://doi.org/10.1109/JIOT.2016.2584538 [Online]. Available.

Chien, H., 2018. Dynamic public key certificates for iot and WSN scenarios. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference, COMPSAC 2018, Tokyo, Japan, 23-27 July 2018, vol. 2, pp. 646–651, https://doi.org/10.1109/COMPSAC.2018.10311 [Online]. Available.

Corchia, L., Benedetto, E.D., Monti, G., Cataldo, A., Angrisani, L., Arpaia, P., Tarricone, L., 2019. Radio-frequency identification based on textile, wearable, chipless tags for iot applications. In: 2nd Workshop on Metrology for Industry 4.0 and IoT MetroInd4.0&IoT 2019, Naples, Italy, June 4-6, 2019, pp. 1–5, https://doi.org/10.1109/METROI4.2019.8792919 [Online]. Available.

Costa, L., Barros, J.P., Tavares, M., 2019. Vulnerabilities in iot devices for smart home environment. In: Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, Prague, Czech Republic, February 23-25, 2019, pp. 615–622, https://doi.org/10.5220/0007583306150622 [Online]. Available.

Crossman, M.A., Liu, H., 2015. Study of authentication with iot testbed. In: Technologies for Homeland Security (HST), 2015 IEEE International Symposium on. IEEE, pp. 1–7.

Daubert, J., Wiesmaier, A., Kikiras, P., 2015. A view on privacy & trust in iot,. In: IEEE International Conference on Communication, ICC 2015, London, United Kingdom, June 8-12, 2015, Workshop Proceedings, pp. 2665–2670, https://doi.org/10.1109/ICCW.2015.7247581 [Online]. Available.

Devi, G.U., Balan, E.V., Priyan, M., Gokulnath, C., 2015. Mutual authentication scheme for iot application. Indian J. Sci. Technol. 8 (26).

Din, I.U., Guizani, M., Kim, B., Hassan, S., Khan, M.K., 2019. Trust management techniques for the internet of things: a survey. IEEE Access 7, 29763–29787, https://doi.org/10.1109/ACCESS.2018.2880838 [Online]. Available.

Ding, S., Cao, J., Li, C., Fan, K., Li, H., 2019. A novel attribute-based access control scheme using blockchain for iot. IEEE Access 7, 38431–38441, https://doi.org/10.1109/ACCESS.2019.2905846 [Online]. Available.

Dinh, N., Kim, Y., 2018. An efficient availability guaranteed deployment scheme for iot service chains over fog-core cloud networks. Sensors 18 (11), 3970, https://doi.org/10.3390/s18113970 [Online]. Available.

Diro, A.A., Chilamkurti, N., Kumar, N., 2017. Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing. MONET 22 (5), 848–858, https://doi.org/10.1007/s11036-017-0851-8 [Online]. Available.

Dizdarevic, J., Carpio, F., Jukan, A., Masip-Bruin, X., 2019. A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. pp. 116:1116:29 ACM Comput. Surv. 51 (6), https://doi.org/10.1145/3292674 [Online]. Available.

Domingo, M.C., 2012. An overview of the internet of underwater things. J. Netw. Comput. Appl. 35 (6), 1879–1890, https://doi.org/10.1016/j.jnca.2012.07.012 [Online]. Available.

Doshi, R., Apthorpe, N., Feamster, N., 2018. Machine learning ddos detection for consumer internet of things devices. In: 2018 IEEE Security and Privacy Workshops, SP Workshops 2018, San Francisco, CA, USA, May 24, 2018, pp. 29–35, https://doi.org/10.1109/SPW.2018.00013 [Online]. Available.

Duan, L., Li, Y., Liao, L., 2018. Flexible certificate revocation list for efficient authentication in iot. pp. 7:17:8. In: Proceedings of the 8th International Conference on the Internet of Things, IOT 2018, Santa Barbara, CA, USA, October 15-18, 2018, https://doi.org/10.1145/3277593.3277595 [Online]. Available.

Edwards, S., Profetis, I., 2016. Hajime: analysis of a decentralized internet worm for iot devices. Rapid. Netw. 16.

El-hajj, M., Chamoun, M., Fadlallah, A., Serhrouchni, A., 2017. Taxonomy of authentication techniques in internet of things (iot). In: Research and Development (SCOReD), 2017 IEEE 15th Student Conference on. IEEE, pp. 67–71.

Elkhodr, M., Shahrestani, S., Cheung, H., 2012. A review of mobile location privacy in the internet of things,. In: 2012 Tenth International Conference on ICT and Knowledge Engineering. IEEE, pp. 266–272.

Eugster, P., Kumar, S., Savvides, S., Stephen, J.J., 2019. Ensuring confidentiality in the cloud of things. IEEE Perv. Comput. 18 (1), 10–18, https://doi.org/10.1109/MPRV.2018.2877286 [Online]. Available.

Fan, K., Gong, Y., Liang, C., Li, H., Yang, Y., 2016. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for iot in 5g. Secur. Commun. Network. 9 (16), 3095–3104, https://doi.org/10.1002/sec.1314 [Online]. Available.

Farooq, M.U., Waseem, M., Khairi, A., Mazhar, S., 2015. A critical analysis on the security concerns of internet of things (iot). In: International Journal of Computer Applications, vol. 111, no. 7.

Farris, I., Taleb, T., Khettab, Y., Song, J., 2019. A survey on emerging SDN and NFV security mechanisms for iot systems. IEEE Communications Surveys and Tutorials 21 (1), 812–837, https://doi.org/10.1109/COMST.2018.2862350 [Online]. Available.

Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L., 2017. Authentication protocols for internet of things: a comprehensive survey. pp. 6562953:16562953 Secur. Commun. Network. 2017 (41), https://doi.org/10.1155/2017/6562953 [Online]. Available.

Frmling, K., Holmstrm, J., 2006. How to create evolving information models by a layered information architecture. In: Proceedings of the Modern Information Technology in the Innovation Processes of the Industrial Enterprises (MITIP2006), pp. 173–178.

Frmling, K., Maharjan, M., 2013. Standardized communication between intelligent products for the iot. IFAC Proceed. Vol. 46 (7), 157–162.
Frmling, K., Kubler, S., Buda, A., 2014. Universal messaging standards for the iot from a lifecycle management perspective. IEEE Internet of Things J. 1 (4), 319–327, https://doi.org/10.1109/JIOT.2014.2332005 [Online]. Available.
Fremantle, P., Aziz, B., 2016. Oauthing: privacy-enhancing federation for the internet of things. In: 2016 Cloudification of the Internet of Things, CIoT 2016, Paris, France, November 23-25, 2016, pp. 1–6, https://doi.org/10.1109/CIOT.2016.7872911 [Online]. Available.
Fremantle, P., Scott, P., 2017. A survey of secure middleware for the internet of things. PeerJ Comp. Sci. 3, e114, https://doi.org/10.7717/peerj-cs.114 [Online]. Available.
Fremantle, P., Aziz, B., Kopeck, J., Scott, P., 2014. Federated identity and access management for the internet of things. In: 2014 International Workshop on Secure Internet of Things, SIoT 2014, Wroclaw, Poland, September 10, 2014, pp. 10–17, https://doi.org/10.1109/SIoT.2014.8 [Online]. Available.
Garca-Magario, I., Sendra, S., Lacuesta, R., Lloret, J., 2019. Security in vehicles with iot by prioritization rules, vehicle certificates, and trust management. IEEE Internet of Things J. 6 (4), 5927–5934, https://doi.org/10.1109/JIOT.2018.2871255 [Online]. Available.
Garcia-Morchon, O., Kumar, S., Struik, R., Keoh, S., Hummen, R., 2013. Security Considerations in the Ip-Based Internet of Things.
Ghuli, P., Kumar, U.P., Shettar, R., 2017. A review on blockchain application for decentralized decision of ownership of iot devices. Adv. Comput. Sci. Technol. 10 (8), 2449–2456.
Gonalves, F., Macedo, J., Nicolau, M.J., Santos, A., 2013. Security architecture for mobile e-health applications in medication control. In: 21st International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2013, Split-Primosten, Croatia, September 18-20, 2013, pp. 1–8, https://doi.org/10.1109/SoftCOM.2013.6671901 [Online]. Available.
Gou, Q., Yan, L., Liu, Y., Li, Y., 2013. Construction and strategies in iot security system. In: 2013 IEEE International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things (iThings) and IEEE Cyber, Physical and Social Computing (CPSCom), Beijing, China, August 20-23, 2013, pp. 1129–1132, https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.195 [Online]. Available.
Granjal, J., Monteiro, E., Silva, J.S., 2013. Application-layer security for the wot: extending coap to support end-to-end message security for internet-integrated sensing applications. In: International Conference on Wired/Wireless Internet Communication. Springer, pp. 140–153.
Granjal, J., Monteiro, E., Silva, J.S., 2015. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys and Tutorials 17 (3), 1294–1312, https://doi.org/10.1109/COMST.2015.2388550 [Online]. Available.
Grebler, L., 2017. Why do iot devices die? . [Online]. Available https://medium.com/iotforall/why-do-iot-devices-die-e4df0c7a075d.
Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., Hu, J., 2019. APPA: an anonymous and privacy preserving data aggregation scheme for fog-enhanced iot. J. Netw. Comput. Appl. 125, 82–92, https://doi.org/10.1016/j.jnca.2018.09.019 [Online]. Available.
Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of things (iot): a vision, architectural elements, and future directions. Future Generat. Comput. Syst. 29 (7), 1645–1660, https://doi.org/10.1016/j.future.2013.01.010 [Online]. Available.
Gusmeroli, S., Piccione, S., Rotondi, D., 2013. A capability-based security approach to manage access control in the internet of things. Math. Comput. Model. 58 (56), 1189–1205, https://doi.org/10.1016/j.mcm.2013.02.006 [Online]. Available.
Ham, H., Kim, H., Kim, M., Choi, M., 2014. Linear svm-based android malware detection for reliable iot services. pp. 594501:1594501 J. Appl. Math. 2014 (10), https://doi.org/10.1155/2014/594501 [Online]. Available.
Hnel, T., Bothe, A., Helmke, R., Gericke, C., Aschenbruck, N., 2017. Adjustable security for rfid-equipped iot devices. In: 2017 IEEE International Conference on RFID Technology & Application (RFID-TA). IEEE, pp. 208–213.
Hasiba, B.A., Kahloul, L., Benharzallah, S., 2018. A new hybrid access control model for security policies in multimodal applications environments. J. UCS 24 (4), 392–416 [Online]. Available, http://www.jucs.org/jucs_24_4/a_new_hybrid_access.
Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B., 2019. A survey on iot security: application areas, security threats, and solution architectures. IEEE Access 7, 82721–82743, https://doi.org/10.1109/ACCESS.2019.2924045 [Online]. Available.
Heer, T., Morchon, O.G., Hummen, R., Keoh, S.L., Kumar, S.S., Wehrle, K., 2011. Security challenges in the ip-based internet of things. Wireless Pers. Commun. 61 (3), 527–542, https://doi.org/10.1007/s11277-011-0385-5 [Online]. Available.
Hellweg, S., i Canals, L.M., 2014. Emerging approaches, challenges and opportunities in life cycle assessment. Science 344 (6188), 1109–1113.
Horrow, S., Sardana, A., 2012. Identity management framework for cloud based internet of things. In: First International Conference on Security of Internet of Things, SECURIT 12, Kollam, India - August 17-19, 2012, pp. 200–203, https://doi.org/10.1145/2490428.2490456 [Online]. Available.
Hossain, M.S., Muhammad, G., Rahman, S.M.M., Abdul, W., Alelaiwi, A., Alamri, A., 2016. Toward end-to-end biomet rics-based security for iot infrastructure. IEEE Wireless Commun. 23 (5), 44–51.
Howell, J., Number of connected iot devices will surge to 125 billion by 2030, ihs markit says. IHS Markit. [Online]. Available https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030- ihs-markit-says.
Hu, C., Zhang, J., Wen, Q., 2011. An identity-based personal location system with protected privacy in iot. In: 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology. IEEE, pp. 192–195.
Huang, Q., Wang, L., Yang, Y., 2018. DECENT: secure and fine-grained data access control with policy updating for constrained iot devices. World Wide Web 21 (1), 151–167, https://doi.org/10.1007/s11280-017-0462-0 [Online]. Available.
Hummen, R., Wirtz, H., Ziegeldorf, J.H., Hiller, J., Wehrle, K., 2013. Tailoring end-to-end IP security protocols to the internet of things. In: 2013 21st IEEE International Conference on Network Protocols, ICNP 2013, Gttingen, Germany, October 7-10, 2013, pp. 1–10, https://doi.org/10.1109/ICNP.2013.6733571 [Online]. Available.
Hummen, R., Ziegeldorf, J.H., Shafagh, H., Raza, S., Wehrle, K., 2013. Towards viable certificate-based authentication for the internet of things. In: Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy. ACM, pp. 37–42.
Hurrah, N.N., Parah, S.A., Sheikh, J.A., Al-Turjman, F., Muhammad, K., 2019. Secure data transmission framework for confidentiality in iots. Ad Hoc Netw. 95, https://doi.org/10.1016/j.adhoc.2019.101989 [Online]. Available.
Huth, C., Duplys, P., Gneysu, T., 2016. Secure software update and IP protection for untrusted devices in the internet of things via physically unclonable functions,. In: 2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2016, Sydney, Australia, March 14-18, 2016, pp. 1–6, https://doi.org/10.1109/PERCOMW.2016.7457156 [Online]. Available.
Hwang, D., Choi, J., Kim, K., 2018. Dynamic access control scheme for iot devices using blockchain. In: International Conference on Information and Communication Technology Convergence, ICTC 2018, Jeju Island, Korea (South), October 17-19, 2018, pp. 713–715, https://doi.org/10.1109/ICTC.2018.8539659 [Online]. Available.
IAB, Internet of things software update workshop (iotsu). [Online]. Available https://www.iab.org/activities/workshops/iotsu/.
Jara, A.J., Kafle, V.P., Gmez-Skarmeta, A.F., 2013. Secure and scalable mobility management scheme for the internet of things integration in the future internet architecture. IJAHUC 13 (3/4), 228–242, https://doi.org/10.1504/IJAHUC.2013.055468 [Online]. Available.
Jeong, J., 2010. Stages of the product life cycle, Wiley International Encyclopedia of Marketing.
Jeong, Y., Lee, J.D., Lee, J., Jung, J., Park, J.H., 2014. An efficient and secure *m*-ips scheme of mobile devices for human-centric computing. pp. 198580:1198580 J. Appl. Math. 2014 (8), https://doi.org/10.1155/2014/198580 [Online]. Available.
Jia, Y.J., Chen, Q.A., Wang, S., Rahmati, A., Fernandes, E., Mao, Z.M., Prakash, A., 2017. Contexlot: towards providing contextual integrity to appified iot platforms. In: 24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26-March 1, 2017 [Online]. Available https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/contexlot-towards-providing-contextual-integrity-appified-iot-platforms/.
Johnson, A.P., Patranabis, S., Chakraborty, R.S., Mukhopadhyay, D., 2017. Remote dynamic partial reconfiguration: a threat to internet-of-things and embedded security applications, Microprocessors and Microsystems - Embedded Hardware Design, vol. 52, pp. 131–144, https://doi.org/10.1016/j.micpro.2017.06.005 [Online]. Available.
Jourdan, T., Boutet, A., Frindel, C., 2018. Toward privacy in iot mobile devices for activity recognition. In: Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, MobiQuitous 2018, 5-7 November 2018, New York City, NY, USA, pp. 155–165, https://doi.org/10.1145/3286978.3287009 [Online]. Available.
Kai, K., pang, Z.-b., Cong, W., 2013. Security and privacy mechanism for health internet of things. J. China Univ. Posts Telecommun. 20, 64–68.
Kalra, S., Sood, S.K., 2015. Secure authentication scheme for iot and cloud servers. Pervasive Mob. Comput. 24, 210–223, https://doi.org/10.1016/j.pmcj.2015.08.001 [Online]. Available.
Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., Alonso-Zarate, J., 2015. A survey on application layer protocols for the internet of things. Trans. IoT Cloud Comput. 3 (1), 11–17.
Krkkinen, M., Holmstrm, J., Frmling, K., Artto, K., 2003. Intelligent products - a step towards a more effective project delivery chain. Comput. Ind. 50 (2), 141–151, https://doi.org/10.1016/S0166-3615(02)00116-1 [Online]. Available.
Khalaf, R.H., Mohammed, A.H., 2018. Confidentiality and integrity of sensing data transmission in iot application. Int. J. Eng. Technol. 7 (4.25), 240–245.
Khan, R., Khan, S.U., Zaheer, R., Khan, S., 2012. Future internet: the internet of things architecture, possible applications and key challenges. In: 10th International Conference on Frontiers of Information Technology, FIT 2012, Islamabad, Pakistan, December 17-19, 2012, pp. 257–260, https://doi.org/10.1109/FIT.2012.53 [Online]. Available.
Khan, W.Z., Aalsalem, M.Y., Khan, M.K., 2018. Five acts of consumer behavior: a potential security and privacy threat to internet of things. In: IEEE International Conference on Consumer Electronics, ICCE 2018, Las Vegas, NV, USA, January 12-14, 2018, pp. 1–3, https://doi.org/10.1109/ICCE.2018.8326124 [Online]. Available.
Khan, M.S.N., Marchal, S., Buchegger, S., Asokan, N., 2018. chowniot: enhancing iot privacy by automated handling of ownership change. In: Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data - 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers, pp. 205–221, https://doi.org/10.1007/978-3-030-16744-8_14 [Online]. Available.
Kim, H., Wasicek, A., Mehne, B., Lee, E.A., 2016. A secure network architecture for the internet of things based on local authorization entities. In: 4th IEEE International Conference on Future Internet of Things and Cloud, FiCloud 2016, Vienna, Austria, August 22-24, 2016, pp. 114–122, https://doi.org/10.1109/FiCloud.2016.24 [Online]. Available.

Kim, D., Kim, S., Park, J.H., 2018. Remote software update in trusted connection of long range iot networking integrated with mobile edge cloud. IEEE Access 6, 66831–66840, https://doi.org/10.1109/ACCESS.2017.2774239 [Online]. Available.
Kiritsis, D., Bufardi, A., Xirouchakis, P., 2003. Research issues on product lifecycle management and information tracking using smart embedded systems. Adv. Eng. Inf. 17 (34), 189–202.
Kivinen, T., 2012. Minimal Ikev2.
Kolias, C., Kambourakis, G., Stavrou, A., Voas, J.M., 2017. Ddos in the iot: mirai and other botnets. IEEE Comput. 50 (7), 80–84, https://doi.org/10.1109/MC.2017.201 [Online]. Available.
Kolisnyk, M., Kharchenko, V.S., Piskachova, I., Bardis, N.G., 2017. A markov model of iot system availability considering ddos attacks and energy modes of server and router. In: Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI 2017, Kyiv, Ukraine, May 15-18, 2017, pp. 699–712 [Online]. Available http://ceur-ws.org/Vol-1844/10000699.pdf.
Kolluru, K.K., Paniagua, C., van Deventer, J., Eliasson, J., Delsing, J., DeLong, R.J., 2018. An AAA solution for securing industrial iot devices using next generation access control. In: IEEE Industrial Cyber-Physical Systems, ICPS 2018, Saint Petersburg, Russia, May 15-18, 2018, pp. 737–742, https://doi.org/10.1109/ICPHYS.2018.8390799 [Online]. Available.
Kolomvatsos, K., 2018. An intelligent, uncertainty driven management scheme for software updates in pervasive iot applications. Future Generat. Comput. Syst. 83, 116–131, https://doi.org/10.1016/j.future.2018.01.036 [Online]. Available.
Kothmayr, T., Schmitt, C., Hu, W., Brnig, M., Carle, G., 2012. A DTLS based end-to-end security architecture for the internet of things with two-way authentication. In: 37th Annual IEEE Conference on Local Computer Networks, Workshop Proceedings, Clearwater Beach, FL, USA, October 22-25, 2012, pp. 956–963, https://doi.org/10.1109/LCNW.2012.6424088 [Online]. Available.
Kouicem, D.E., Bouabdallah, A., Lakhlef, H., 2018. Internet of things security: a top-down survey. Comput. Network. 141, 199–221, https://doi.org/10.1016/j.comnet.2018.03.012 [Online]. Available.
Kravitz, D.W., Cooper, J., 2017. Securing user identity and transactions symbiotically: iot meets blockchain. In: Global Internet of Things Summit, GIoTS 2017, Geneva, Switzerland, June 6-9, 2017, pp. 1–6, https://doi.org/10.1109/GIOTS.2017.8016280 [Online]. Available.
Kryvinska, N., Strauss, C., 2013. Conceptual model of business services availability vs. interoperability on collaborative iot-enabled ebusiness platforms. In: Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence, pp. 167–187, https://doi.org/10.1007/978-3-642-34952-2_7 [Online]. Available.
Kubler, S., Yoo, M., Cassagnes, C., Frmling, K., Kiritsis, D., Skilton, M., 2015. Opportunity to leverage information-as-an-asset in the iot - the road ahead. In: 3rd International Conference on Future Internet of Things and Cloud, FiCloud 2015, Rome, Italy, August 24-26, 2015, pp. 64–71, https://doi.org/10.1109/FiCloud.2015.63 [Online]. Available.
Kubler, S., Frmling, K., Buda, A., 2015. A standardized approach to deal with firewall and mobility policies in the iot. Pervasive Mob. Comput. 20, 100–114, https://doi.org/10.1016/j.pmcj.2014.09.005 [Online]. Available.
Kumar, J.S., Patel, D.R., 2014. A survey on internet of things: security and privacy issues. Int. J. Comput. Appl. 90 (11).
Kung, Y., Hsiao, H., 2018. Groupit: lightweight group key management for dynamic iot environments. IEEE Internet of Things J. 5 (6), 5155–5165, https://doi.org/10.1109/JIOT.2018.2840321 [Online]. Available.
Lehmhus, D., Wuest, T., Wellsandt, S., Bosse, S., Kaihara, T., Thoben, K., Busse, M., 2015. Cloud-based automated design and additive manufacturing: a usage data-enabled paradigm shift. Sensors 15 (12), 32079–32122, https://doi.org/10.3390/s151229905 [Online]. Available.
Leng, X., Mayes, K., Lien, Y., 2014. Ownership management in the context of the internet of things. In: 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2014, Shanghai, China, October 13-15, 2014, pp. 150–153, https://doi.org/10.1109/CyberC.2014.34 [Online]. Available.
Li, X., Xuan, Z., Wen, L., 2011. Research on the architecture of trusted security system based on the internet of things. In: 2011 Fourth International Conference on Intelligent Computation Technology and Automation, vol. 2. IEEE, pp. 1172–1175.
Li, N., Liu, D., Nepal, S., 2017. Lightweight mutual authentication for iot and its applications. T-SUSC 2 (4), 359–370, https://doi.org/10.1109/TSUSC.2017.2716953 [Online]. Available.
Li, W., Tug, S., Meng, W., Wang, Y., 2019. Designing collaborative blockchained signature-based intrusion detection in iot environments. Future Generat. Comput. Syst. 96, 481–489, https://doi.org/10.1016/j.future.2019.02.064 [Online]. Available.
Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W., 2017. A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things J. 4 (5), 1125–1142, https://doi.org/10.1109/JIOT.2017.2683200 [Online]. Available.
Liu, J., Xiao, Y., Chen, C.L.P., 2012. Authentication and access control in the internet of things. In: 32nd International Conference on Distributed Computing Systems Workshops (ICDCS 2012 Workshops), Macau, China, June 18-21, 2012, pp. 588–592, https://doi.org/10.1109/ICDCSW.2012.23 [Online]. Available.
Lpez, J., Maag, S., 2015. Towards a generic trust management framework using a machine-learning-based trust model. In: 2015 IEEE TrustCom/BigDataSE/ISPA, Helsinki, Finland, August 20-22, 2015, vol. 1, pp. 1343–1348, https://doi.org/10.1109/Trustcom.2015.528 [Online]. Available.
Lu, Y., Xu, L.D., 2019. Internet of things (iot) cybersecurity research: a review of current research topics. IEEE Internet of Things J. 6 (2), 2103–2115, https://doi.org/10.1109/JIOT.2018.2869847 [Online]. Available.
Luo, T., Xu, Z., Jin, X., Jia, Y., Ouyang, X., 2017. Iotcandyjar: towards an intelligent-interaction honeypot for iot devices. Black Hat.
Ma, T., Kim, Y., Ma, Q., Tang, M., Zhou, W., 2005. Context-aware implementation based on CBR for smart home. In: 2005 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2005, Montreal, Canada, August 22-14, 2005, vol. 4, pp. 112–115, https://doi.org/10.1109/WIMOB.2005.1512957 [Online]. Available.
Mahalle, P., Babar, S., Prasad, N.R., Prasad, R., 2010. Identity management framework towards internet of things (iot): roadmap and key challenges. In: Recent Trends in Network Security and Applications - Third International Conference, CNSA 2010, Chennai, India, July 23-25, 2010. Proceedings, pp. 430–439, https://doi.org/10.1007/978-3-642-14478-3_43 [Online]. Available.
Mahalle, P., Anggorojati, B., Prasad, N.R., Prasad, R., 2012. Identity establishment and capability based access control (IECAC) scheme for internet of things. In: The 15th International Symposium on Wireless Personal Multimedia Communications, WPMC 2012, Taipei, Taiwan, September 24-27, 2012, pp. 187–191 [Online]. Available http://ieeexplore.ieee.org/document/6398758/.
Mahalle, P.N., Anggorojati, B., Prasad, N.R., Prasad, R., 2012. Identity driven capability based access control (ICAC) scheme for the internet of things. In: IEEE International Conference on Advanced Networks and Telecommuncations Systems, ANTS 2012, Bangalore, India, 16-19 December, 2012, pp. 49–54, https://doi.org/10.1109/ANTS.2012.6524227 [Online]. Available.
Mahalle, P.N., Anggorojati, B., Prasad, N.R., Prasad, R., et al., 2013. Identity authentication and capability based access control (iacac) for the internet of things. J. Cyber Secur. Mob. 1 (4), 309–348.
Mahalle, P.N., Prasad, N.R., Prasad, R., 2014. Threshold cryptography-based group authentication (TCGA) scheme for the internet of things (iot). In: 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems, VITAE 2014, Aalborg, Denmark, May 11-14, 2014, pp. 1–5, https://doi.org/10.1109/VITAE.2014.6934425 [Online]. Available.
Mamun, M.S.I., Su, C., Yang, A., Miyaji, A., Ghorbani, A., 2018. Otp-iot: an ownership transfer protocol for the internet of things. J. Inf. Sec. Appl. 43, 73–82, https://doi.org/10.1016/j.jisa.2018.10.009 [Online]. Available.
McKenna, E., Richardson, I., Thomson, M., 2012. Smart meter data: balancing consumer privacy concerns with legitimate applications. Energy Pol. 41, 807–814.
Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J.D., Ochoa, M., Tippenhauer, N.O., Elovici, Y., 2017. Profiliot: a machine learning approach for iot device identification based on network traffic analysis. In: Proceedings of the Symposium on Applied Computing, SAC 2017, Marrakech, Morocco, April 3-7, 2017, pp. 506–509, https://doi.org/10.1145/3019612.3019878 [Online]. Available.
Mendez, D.M., Papapanagiotou, I., Yang, B., 2017. Internet of things: survey on security and privacy. vol. abs/1707.01879 CoRR. [Online]. Available http://arxiv.org/abs/1707.01879.
Miao, J., Wang, L., 2012. Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection. JNW 7 (7), 1099–1105, https://doi.org/10.4304/jnw.7.7.1099-1105 [Online]. Available.
Miettinen, M., Asokan, N., Nguyen, T.D., Sadeghi, A., Sobhani, M., 2014. Context-based zero-interaction pairing and key evolution for advanced personal devices. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014, pp. 880–891, https://doi.org/10.1145/2660267.2660334 [Online]. Available.
Miettinen, M., Heuser, S., Kronz, W., Sadeghi, A.-R., Asokan, N., 2014. Conxsense: automated context classification for context-aware access control. In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security. ACM, pp. 293–304.
Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A., Tarkoma, S., 2017. Iot SENTINEL: automated device-type identification for security enforcement in iot. In: 37th IEEE International Conference on Distributed Computing Systems, ICDCS 2017, Atlanta, GA, USA, June 5-8, 2017, pp. 2177–2184, https://doi.org/10.1109/ICDCS.2017.283 [Online]. Available.
Miettinen, M., van Oorschot, P.C., Sadeghi, A., 2018. Baseline functionality for security and control of commodity iot devices and domain-controlled device lifecycle management. vol. abs/1808.03071 CoRR. [Online]. Available http://arxiv.org/abs/1808.03071.
Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I., 2012. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 10 (7), 1497–1516, https://doi.org/10.1016/j.adhoc.2012.02.016 [Online]. Available.
Moosavi, S.R., Gia, T.N., Nigussie, E., Rahmani, A., Virtanen, S., Tenhunen, H., Isoaho, J., 2016. End-to-end security scheme for mobility enabled healthcare internet of things. Future Generat. Comput. Syst. 64, 108–124, https://doi.org/10.1016/j.future.2016.02.020 [Online]. Available.
Moreno-Sanchez, P., Lpez, R.M., Gmez-Skarmeta, A.F., 2013. PANATIKI: a network access control implementation based on PANA for iot devices. Sensors 13 (11), 14888–14917, https://doi.org/10.3390/s131114888 [Online]. Available.
Mosenia, A., Jha, N.K., 2017. A comprehensive study of security of internet-of-things. IEEE Trans. Emerg. Top. Comput. 5 (4), 586–602, https://doi.org/10.1109/TETC.2016.2606384 [Online]. Available.
Moskowitz, R., Hummen, R., 2012. Hip diet exchange (dex), draft-moskowitz-hip-dex-00 (WiP), IETF.
Motti, V.G., Mezhoudi, N., Vanderdonckt, J., 2012. Machine learning in the support of context-aware adaptation. In: Proceedings of the Workshop on Context-Aware Adaptation of Service Front-Ends, Pisa, Italy, November 13, 2012, [Online]. Available http://ceur-ws.org/Vol-970/paper9.pdf.

Mustafa, J., Sandstrm, K., Ericsson, N., Rizvanovic, L., 2019. Analyzing availability and qos of service-oriented cloud for industrial iot applications. In: 24th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2019, Zaragoza, Spain, September 10-13, 2019, pp. 1403–1406, https://doi.org/10.1109/ETFA.2019.8869274 [Online]. Available.

Namal, S., Gamaarachchi, H., Lee, G.M., Um, T., 2015. Autonomic trust management in cloud-based and highly dynamic iot applications. In: 2015 ITU Kaleidoscope: Trust in the Information Society, Barcelona, Spain, December 9-11, 2015, pp. 1–8, https://doi.org/10.1109/Kaleidoscope.2015.7383635 [Online]. Available.

Nawir, M., Amir, A., Yaakob, N., Lynn, O.B., 2016. Internet of things (iot): taxonomy of security attacks. In: Electronic Design (ICED), 2016 3rd International Conference on. IEEE, pp. 321–326.

Neto, A.L.M., Souza, A.L.F., Cunha, .S., Nogueira, M., Nunes, I.O., Cotta, L., Gentille, N., Loureiro, A.A.F., Aranha, D.F., Patil, H.K., Oliveira, L.B., 2016. Aot: authentication and access control for the entire iot device life-cycle. In: Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems, SenSys 2016, Stanford, CA, USA, November 14-16, 2016, pp. 1–15, https://doi.org/10.1145/2994551.2994555 [Online]. Available.

Nguyen, K.T., Laurent, M., Oualha, N., 2015. Survey on secure communication protocols for the internet of things. Ad Hoc Netw. 32, 17–31, https://doi.org/10.1016/j.adhoc.2015.01.006 [Online]. Available.

Nguyen, T.D., Marchal, S., Miettinen, M., Dang, M.H., Asokan, N., Sadeghi, A., 2018. Diot: a crowdsourced self-learning approach for detecting compromised iot devices. vol. abs/1804.07474 CoRR. [Online]. Available http://arxiv.org/abs/1804.07474.

Niu, B., Zhu, X., Chi, H., Li, H., 2014. Privacy and authentication protocol for mobile RFID systems. Wireless Pers. Commun. 77 (3), 1713–1731, https://doi.org/10.1007/s11277-014-1605-6 [Online]. Available.

Oriwoh, E., al Khateeb, H., Conrad, M., 2016. Responsibility and non-repudiation in resource-constrained internet of things scenarios. In: International Conference on Computing and Technology Innovation (CTI 2015).

O'Donnell, L., 2 million iot devices vulnerable to complete takeover. threatpost. [Online]. Available https://threatpost.com/iot-devices-vulnerable-takeover/144167/.

Pa, Y.M.P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., Rossow, C., 2016. Iotpot: a novel honeypot for revealing current iot threats. JIP 24 (3), 522–533, https://doi.org/10.2197/ipsjjip.24.522 [Online]. Available.

Pal, S., Hitchens, M., Varadharajan, V., Rabehaja, T.M., 2019. Policy-based access control for constrained healthcare resources in the context of the internet of things. J. Netw. Comput. Appl. 139, 57–74, https://doi.org/10.1016/j.jnca.2019.04.013 [Online]. Available.

Pecorella, T., Brilli, L., Mucchi, L., 2016. The role of physical layer security in iot: a novel perspective. Information 7 (3), 49, https://doi.org/10.3390/info7030049 [Online]. Available.

Petrov, V., Edelev, S., Komar, M., Koucheryavy, Y., 2014. Towards the era of wireless keys: how the iot can change authentication paradigm. In: IEEE World Forum on Internet of Things, WF-IoT 2014, Seoul, South Korea, March 6-8, 2014, pp. 51–56, https://doi.org/10.1109/WF-IoT.2014.6803116 [Online]. Available.

Plans announced to introduce new laws for internet connected devices. UK government [Online]. Available. https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A.V., Ylianttila, M., 2014. Two-phase authentication protocol for wireless sensor networks in distributed iot applications. In: IEEE Wireless Communications and Networking Conference, WCNC 2014, Istanbul, Turkey, April 6-9, 2014, pp. 2728–2733, https://doi.org/10.1109/WCNC.2014.6952860 [Online]. Available.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A.V., Ylianttila, M., 2014. Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications. IJDSN 10, https://doi.org/10.1155/2014/357430 [Online]. Available.

Pularikkal, B., Patil, S., Anantha, S., Chakraborty, S., 2018. Blockchain Based Wi-Fi Onboarding Simplification, Identity Management and Device Profiling for Iot Devices in Enterprise Networks.

Purohit, K.C., Bisht, S., Joshi, A., Bhatt, J., 2017. Hybrid approach for securing iot communication using authentication and data confidentiality. In: 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall). IEEE, pp. 1–6.

Qaim, W.B., zkasap, ., 2018. DRAW: data replication for enhanced data availability in iot-based sensor systems. In: 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, DASC/PiCom/DataCom/CyberSciTech 2018, Athens, Greece, August 12-15, 2018, pp. 770–775, https://doi.org/10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00133 [Online]. Available.

Qian, J., Iotseeker. [Online]. Available https://github.com/rapid7/IoTSeeker.

Radware. Brickerbot results in pdos attack. [Online]. Available. https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/.

Ramos, J.L.H., Jara, A.J., Marn, L., Skarmeta, A.F., 2013. Distributed capability-based access control for the internet of things. J. Internet Serv. Inf. Secur. 3 (3/4), 1–16, https://doi.org/10.22667/JISIS.2013.11.31.001 [Online]. Available.

Raza, S., Wallgren, L., Voigt, T., 2013. SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw. 11 (8), 2661–2674, https://doi.org/10.1016/j.adhoc.2013.04.014 [Online]. Available.

Raza, S., Seitz, L., Sitenkov, D., Selander, G., 2016. S3K: scalable security with symmetric keys - DTLS key establishment for the internet of things. IEEE Trans. Autom. Sci. Eng. 13 (3), 1270–1280, https://doi.org/10.1109/TASE.2015.2511301 [Online]. Available.

Rescorla, E., Modadugu, N., 2012. Datagram transport layer security version 1.2. RFC 6347, 1–32, https://doi.org/10.17487/RFC6347 [Online]. Available.

Riad, K., Zhu, Y., 2017. Multi-factor synthesis decision-making for trust-based access control on cloud. Int. J. Cooper. Inf. Syst. 26 (4), 1–33, https://doi.org/10.1142/S0218843017500034 [Online]. Available.

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., Bouabdallah, A., 2013. A systemic approach for iot security. In: IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS 2013, Cambridge, MA, USA, May 20-23, 2013, pp. 351–355, https://doi.org/10.1109/DCOSS.2013.78 [Online]. Available.

Riahi, A., Natalizio, E., Challal, Y., Mitton, N., Iera, A., 2014. A systemic and cognitive approach for iot security. In: International Conference on Computing, Networking and Communications, ICNC 2014, Honolulu, HI, USA, February 3-6, 2014, pp. 183–188, https://doi.org/10.1109/ICCNC.2014.6785328 [Online]. Available.

Rink, D.R., Swan, J.E., 1979. Product life cycle research: a literature review. J. Bus. Res. 7 (3), 219–242.

Roman, R., Najera, P., Lpez, J., 2011. Securing the internet of things. IEEE Comput. 44 (9), 51–58, https://doi.org/10.1109/MC.2011.291 [Online]. Available.

Roman, R., Alcaraz, C., Lpez, J., Sklavos, N., 2011. Key management systems for sensor networks in the context of the internet of things. Comput. Electr. Eng. 37 (2), 147–159, https://doi.org/10.1016/j.compeleceng.2011.01.009 [Online]. Available.

Roman, R., Zhou, J., Lpez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Comput. Network. 57 (10), 2266–2279, https://doi.org/10.1016/j.comnet.2012.12.018 [Online]. Available.

Roman, R., Lpez, J., Mambo, M., 2018. Mobile edge computing, fog etal.: a survey and analysis of security threats and challenges. Future Generat. Comput. Syst. 78, 680–698, https://doi.org/10.1016/j.future.2016.11.009 [Online]. Available.

Saadeh, M., Sleit, A., Qatawneh, M., Almobaideen, W., 2016. Authentication techniques for the internet of things: a survey. In: Cybersecurity and Cyberforensics Conference (CCC), 2016. IEEE, pp. 28–34.

Sadeghi, A., Wachsmann, C., Waidner, M., 2015. Security and privacy challenges in industrial internet of things. pp. 54:154:6. In: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015, https://doi.org/10.1145/2744769.2747942 [Online]. Available.

Sahraoui, S., Bilami, A., 2015. Efficient hip-based approach to ensure lightweight end-to-end security in the internet of things. Comput. Network. 91, 26–45, https://doi.org/10.1016/j.comnet.2015.08.002 [Online]. Available.

Salonikias, S., Gouglidis, A., Mavridis, I., Gritzalis, D., 2019. Access control in the industrial internet of things. In: Security and Privacy Trends in the Industrial Internet of Things, pp. 95–114, https://doi.org/10.1007/978-3-030-12330-7_5 [Online]. Available.

Samaila, M.G., Neto, M., Fernandes, D.A., Freire, M.M., Incio, P.R., 2017. Security challenges of the internet of things. In: Beyond the Internet of Things. Springer, pp. 53–82.

Samir, N., Gamal, Y., El-Zeiny, A.N., Mahmoud, O., Shawky, A., Saeed, A., Mostafa, H., 2019. Energy-adaptive lightweight hardware security module using partial dynamic reconfiguration for energy limited internet of things applications. In: IEEE International Symposium on Circuits and Systems, ISCAS 2019, Sapporo, Japan, May 26-29, 2019, pp. 1–4, https://doi.org/10.1109/ISCAS.2019.8702315 [Online]. Available.

Samtani, S., Yu, S., Zhu, H., Patton, M.W., Chen, H., 2016. Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. In: IEEE Conference on Intelligence and Security Informatics, ISI 2016, Tucson, AZ, USA, September 28-30, 2016, pp. 25–30, https://doi.org/10.1109/ISI.2016.7745438 [Online]. Available.

Santos, B., van Thuan, D., Feng, B., Do, T.V., 2018. Identity federation for cellular internet of things. In: Proceedings of the 7th International Conference on Software and Computer Applications, ICSCA 2018, Kuantan, Malaysia, February 08-10, 2018, pp. 223–228, https://doi.org/10.1145/3185089.3185132 [Online]. Available.

Santos, B., Dzogovic, B., Feng, B., Do, V.T., Jacot, N., Do, T.V., 2019. Enhancing security of cellular iot with identity federation. In: Advances in Intelligent Networking and Collaborative Systems - the 11th International Conference on Intelligent Networking and Collaborative Systems, INCoS 2019, Oita, Japan, September 5-7, 2019, pp. 257–268, https://doi.org/10.1007/978-3-030-29035-1_25 [Online]. Available.

Sarma, A., Giro, J., 2009. Identities in the future internet of things. Wireless Pers. Commun. 49 (3), 353–363, https://doi.org/10.1007/s11277-009-9697-0 [Online]. Available.

Sciancalepore, S., Capossele, A., Piro, G., Boggia, G., Bianchi, G., 2015. Key management protocol with implicit certificates for iot systems. In: Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Industrial Systems, IoT-Sys@MobiSys 2015, Florence, Italy, May 18, 2015, pp. 37–42, https://doi.org/10.1145/2753476.2753477 [Online]. Available.

Scully, P., Understanding iot security (part 2 of 3): iot cyber security for cloud and lifecycle management. [Online]. Available https://dzone.com/articles/understanding-iot-security-part-2-of-3-iot-cyber-security.

M. Sethi and T. Aura, Iot security and the role of manufacturers: a story of unrealistic design expectations.

Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z., 2018. A roadmap for security challenges in the internet of things. Digit. Commun. Netw. 4 (2), 118–137.

Shivraj, V., Rajan, M., Singh, M., Balamuralidhar, P., 2015. One time password authentication scheme based on elliptic curves for internet of things (iot). In: Information Technology: towards New Smart World (NSITNSW), 2015 5th National Symposium on. IEEE, pp. 1–6.
Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., 2015. Security, privacy and trust in internet of things: the road ahead. Comput. Network. 76, 146–164, https://doi.org/10.1016/j.comnet.2014.11.008 [Online]. Available.
Sodhro, A.H., Pirbhulal, S., Sangaiah, A.K., 2018. Convergence of iot and product lifecycle management in medical health care. Future Generat. Comput. Syst. 86, 380–391, https://doi.org/10.1016/j.future.2018.03.052 [Online]. Available.
Sohal, A.S., Sandhu, R., Sood, S.K., Chang, V., 2018. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. 74, 340–354, https://doi.org/10.1016/j.cose.2017.08.016 [Online]. Available.
Song, B., Cheong, Y., Lee, T., Jeong, J., 2017. Design and security analysis of improved identity management protocol for 5g/iot networks. In: Recent Advances in Information Systems and Technologies - Volume 2 [WorldCIST17, Porto Santo Island, Madeira, Portugal, April 11-13, 2017], pp. 311–320, https://doi.org/10.1007/978-3-319-56538-5_32 [Online]. Available.
Sulkamo, V., 2018. Iot from Cyber Security Perspective.
Sun, H., Wang, X., Buyya, R., Su, J., 2017. Cloudeyes: cloud-based malware detection with reversible sketch for resource-constrained internet of things (iot) devices. Software Pract. Ex. 47 (3), 421–441, https://doi.org/10.1002/spe.2420 [Online]. Available.
Suo, H., Wan, J., Zou, C., Liu, J., 2012. Security in the internet of things: a review. IEEE. In: Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, pp. 648–651.
Tabassum, A., Erbad, A., Guizani, M., 2019. A survey on recent approaches in intrusion detection system in iots. In: 15th International Wireless Communications & Mobile Computing Conference, IWCMC 2019, Tangier, Morocco, June 24-28, 2019, pp. 1190–1197, https://doi.org/10.1109/IWCMC.2019.8766455 [Online]. Available.
Taneja, M., 2013. An analytics framework to detect compromised iot devices using mobility behavior. In: International Conference on Information and Communication Technology Convergence, ICTC 2013, Jeju Island, South Korea, 4-16 October 2013, pp. 38–43, https://doi.org/10.1109/ICTC.2013.6675302 [Online]. Available.
Tao, F., Zuo, Y., Da Xu, L., Lv, L., Zhang, L., 2014. Internet of things and bom-based life cycle assessment of energy-saving and emission-reduction of products. IEEE Trans. Indust. Inform. 10 (2), 1252–1261.
Tao, F., Zuo, Y., Xu, L.D., Zhang, L., 2014. Iot-based intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE Trans. Indust. Inform. 10 (2), 1547–1557, https://doi.org/10.1109/TII.2014.2306397 [Online]. Available.
Tao, F., Wang, Y., Zuo, Y., Yang, H., Zhang, M., 2016. Internet of things in product life-cycle energy management. J. Indust. Inform. Integr. 1, 26–39.
Tariq, N., Asim, M., Maamar, Z., Farooqi, M.Z., Faci, N., Baker, T., 2019. A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot. J. Parallel Distr. Comput. 134, 198–206, https://doi.org/10.1016/j.jpdc.2019.08.013 [Online]. Available.
The product life cycle. Quick MBA, internal center for management and business administrative inc. [Online]. Available. http://www.quickmba.com/marketing/product/lifecycle.
Thoma, M., Meyer, S., Sperner, K., Meissner, S., Braun, T., 2012. On iot-services: survey, classification and enterprise integration. In: 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, GreenCom/iThings/CPSCom 2012, Besancon, France, November 20-23, 2012, pp. 257–260, https://doi.org/10.1109/GreenCom.2012.47 [Online]. Available.
Trappe, W., Howard, R.E., Moore, R.S., 2015. Low-energy security: limits and opportunities in the internet of things. IEEE Secur. Priv. 13 (1), 14–21, https://doi.org/10.1109/MSP.2015.7 [Online]. Available.
Tsai, I., Yu, C., Yokota, H., Kuo, S., 2017. Key management in internet of things via kronecker product. In: 22nd IEEE Pacific Rim International Symposium on Dependable Computing, PRDC 2017, Christchurch, New Zealand, January 22-25, 2017, pp. 118–124, https://doi.org/10.1109/PRDC.2017.25 [Online]. Available.
Tsai, Y., Wang, S., Yan, K., Chen, C., 2018. Availability enhancement in a four-layer based iot use three-phase scheduling. J. Ambient Intell. Human. Comput. 9 (4), 1275–1291, https://doi.org/10.1007/s12652-017-0605-2 [Online]. Available.
Ukil, A., Bandyopadhyay, S., Pal, A., 2014. Iot-privacy: to be private or not to be private. In: 2014 Proceedings IEEE INFOCOM Workshops, Toronto, ON, Canada, April 27-May 2, 2014, pp. 123–124, https://doi.org/10.1109/INFCOMW.2014.6849186 [Online]. Available.
Ukil, A., Bandyopadhyay, S., Pal, A., 2015. Privacy for iot: involuntary privacy enablement for smart energy systems. In: 2015 IEEE International Conference on Communications, ICC 2015, London, United Kingdom, June 8-12, 2015, pp. 536–541, https://doi.org/10.1109/ICC.2015.7248377 [Online]. Available.
Valea, E., Silva, M.D., Flottes, M., Natale, G.D., Dupuis, S., Rouzeyre, B., 2019. Providing confidentiality and integrity in ultra low power iot devices. In: 14th International Conference on Design & Technology of Integrated Systems in Nanoscale Era, DTIS 2019, Mykonos, Greece, April 16-18, 2019, pp. 1–6, https://doi.org/10.1109/DTIS.2019.8735090 [Online]. Available.
Van der Elzen, I., van Heugten, J., 2017. Techniques for detecting compromised iot devices. University of Amsterdam.
Vasseur, J., Seewald, M.G., Threat detection and mitigation for iot systems using self learning networks (sln). presentation. Cisco. [Online]. Available https://docbox.etsi.org/Workshop/2016/201606_SECURITYWS/S05_MITIGATINGMECHANISMS/CISCO_SEEWALD.pdf.
Wahab, O.A., Bentahar, J., Otrok, H., Mourad, A., 2019. Resource-aware detection and defense system against multi-type attacks in the cloud: repeated bayesian stackelberg game. IEEE Trans. Dependable Secure Comput.
Wahab, O.A., Bentahar, J., Otrok, H., Mourad, A., 2020. Optimal load distribution for the detection of vm-based ddos attacks in the cloud. IEEE Trans. Serv. Comput. 13 (1), 114–129, https://doi.org/10.1109/TSC.2017.2694426 [Online]. Available.
Wang, A.I., Ahmad, Q.K., et al., 2010. Camf-context-aware machine learning framework for android. In: Proceedings of the International Conference on Software Engineering and Applications (SEA 2010), CA, USA.
Wang, H., Chen, Z., Zhao, J., Di, X., Liu, D., 2018. A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow. IEEE Access 6, 8599–8609, https://doi.org/10.1109/ACCESS.2018.2805690 [Online]. Available.
Weber, R.H., 2010. Internet of thingsnew security and privacy challenges. Comput. Law Secur. Rep. 26 (1), 23–30.
Weißbach, M., Taing, N., Wutzler, M., Springer, T., Schill, A., Clarke, S., 2016. Decentralized coordination of dynamic software updates in the internet of things. In: 3rd IEEE World Forum on Internet of Things, WF-IoT 2016, Reston, VA, USA, December 12-14, 2016, pp. 171–176, https://doi.org/10.1109/WF-IoT.2016.7845450 [Online]. Available.
Weinzettel, J., Reenaas, M., Solli, C., Hertwich, E.G., 2009. Life cycle assessment of a floating offshore wind turbine. Renew. Energy 34 (3), 742–747.
Wikipedia. Context aware services. [Online]. Available. https://en.wikipedia.org/wiki/Context-aware_services.
Williams, R., McMahon, E., Samtani, S., Patton, M.W., Chen, H., 2017. Identifying vulnerabilities of consumer internet of things (iot) devices: a scalable approach. In: 2017 IEEE International Conference on Intelligence and Security Informatics, ISI 2017, Beijing, China, July 22-24, 2017, pp. 179–181, https://doi.org/10.1109/ISI.2017.8004904 [Online]. Available.
Won, J., Singla, A., Bertino, E., Bollella, G., 2018. Decentralized public key infrastructure for internet-of-things. In: 2018 IEEE Military Communications Conference, MILCOM 2018, Los Angeles, CA, USA, October 29-31, 2018, pp. 907–913, https://doi.org/10.1109/MILCOM.2018.8599710 [Online]. Available.
Wrona, K.S., 2015. Securing the internet of things a military perspective. In: 2nd IEEE World Forum on Internet of Things, WF-IoT 2015, Milan, Italy, December 14-16, 2015, pp. 502–507, https://doi.org/10.1109/WF-IoT.2015.7389105 [Online]. Available.
Wu, X., Cao, Q., Jin, J., Li, Y., Zhang, H., 2019. Nodes availability analysis of nb-iot based heterogeneous wireless sensor networks under malware infection. pp. 4392839:14392839 Wireless Commun. Mobile Comput. 2019 (9), https://doi.org/10.1155/2019/4392839 [Online]. Available.
Xie, W., Jiang, Y., Tang, Y., Ding, N., Gao, Y., 2017. Vulnerability detection in iot firmware: a survey. In: 23rd IEEE International Conference on Parallel and Distributed Systems, ICPADS 2017, Shenzhen, China, December 15-17, 2017, pp. 769–772, https://doi.org/10.1109/ICPADS.2017.00104 [Online]. Available.
Xin, L., Trdan, G., Datta, A., 2011. Metatrust: discriminant analysis of local information for global trust assessment. In: 10th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2011), Taipei, Taiwan, May 2-6, 2011, vols. 13, pp. 1071–1072 [Online]. Available http://portal.acm.org/citation.cfm?id2034423&CFID69154334&CFTOKEN&45298625.
Xiong, J., Ren, J., Chen, L., Yao, Z., Lin, M., Wu, D., Niu, B., 2019. Enhancing privacy and availability for data clustering in intelligent electrical service of iot. IEEE Internet of Things J. 6 (2), 1530–1540, https://doi.org/10.1109/JIOT.2018.2842773 [Online]. Available.
Xu, L.D., He, W., Li, S., 2014. Internet of things in industries: a survey. IEEE Trans. Indust. Inform. 10 (4), 2233–2243, https://doi.org/10.1109/TII.2014.2300753 [Online]. Available.
Xu, T., Wendt, J.B., Potkonjak, M., 2014. Security of iot systems: design challenges and opportunities. In: The IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2014, San Jose, CA, USA, November 3-6, 2014, pp. 417–423, https://doi.org/10.1109/ICCAD.2014.7001385 [Online]. Available.
Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., Zhang, Y., 2019. A blockchain-based nonrepudiation network computing service scheme for industrial iot. IEEE Trans. Indust. Inform. 15 (6), 3632–3641, https://doi.org/10.1109/TII.2019.2897133 [Online]. Available.
Yahyaoui, A., Abdellatif, T., Attia, R., 2019. Hierarchical anomaly based intrusion detection and localization in iot. In: 15th International Wireless Communications & Mobile Computing Conference, IWCMC 2019, Tangier, Morocco, June 24-28, 2019, pp. 108–113, https://doi.org/10.1109/IWCMC.2019.8766574 [Online]. Available.
Yan, B., Huang, G., 2008. Application of rfid and internet of things in monitoring and anti-counterfeiting for products. In: Business and Information Management, 2008. ISBIM08. International Seminar on, vol. 1, pp. 392–395 IEEE.
Yan, T., Wen, Q., 2010. A secure mobile rfid architecture for the internet of things. In: 2010 IEEE International Conference on Information Theory and Information Security. IEEE, pp. 616–619.
Yan, Z., Zhang, P., Vasilakos, A.V., 2014. A survey on trust management for internet of things. J. Netw. Comput. Appl. 42, 120–134, https://doi.org/10.1016/j.jnca.2014.01.014 [Online]. Available.
Yang, H., Kim, Y., 2019. Design and implementation of high-availability architecture for iot-cloud services. Sensors 19 (15), 3276, https://doi.org/10.3390/s19153276 [Online]. Available.
Yang, Y., Cai, H., Wei, Z., Lu, H., Choo, K.R., 2016. Towards lightweight anonymous entity authentication for iot applications. In: Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I, pp. 265–280, https://doi.org/10.1007/978-3-319-40253-6_16 [Online]. Available.

Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H., 2017. A survey on security and privacy issues in internet-of-things. IEEE Internet of Things J. 4 (5), 1250–1258, https://doi.org/10.1109/JIOT.2017.2694844 [Online]. Available.
Ye, Y., Li, T., Adjeroh, D.A., Iyengar, S.S., 2017. A survey on malware detection using data mining techniques. pp. 41:141:40 ACM Comput. Surv. 50 (3) [Online]. Available: http://doi.acm.org/10.1145/3073559.
Yeh, T., Chiu, D., Lu, K., May 2017. Persirai: new internet of things (iot) botnet targets ip cameras. TrendLabs Secur. Intell. Blog. [Online]. Available https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/.
Yousefnezhad, N., Filippov, R., Javed, A., Buda, A., Madhikermi, M., Frmling, K., 2017. Authentication and access control for open messaging interface standard. In: Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Melbourne, Australia, November 7-10, 2017, pp. 20–27, https://doi.org/10.1145/3144457.3144461 [Online]. Available.
Yousefnezhad, N., Madhikermi, M., Frmling, K., 2018. Medi: Measurement-based device identification framework for internet of things. In: 16th IEEE International Conference on Industrial Informatics, INDIN 2018, Porto, Portugal, July 18-20, 2018, pp. 95–100, https://doi.org/10.1109/INDIN.2018.8472080 [Online]. Available.
Zarpelo, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C., 2017. A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. 84, 25–37, https://doi.org/10.1016/j.jnca.2017.02.009 [Online]. Available.
Zhang, G., Gong, W., 2011. The research of access control based on UCON in the internet of things. J. SW 6 (4), 724–731, https://doi.org/10.4304/jsw.6.4.724-731 [Online]. Available.
Zhang, D., Ma, H., Liu, L., Tao, D., 2005. EAAR: an approach to environment adaptive application reconfiguration in sensor network. In: Mobile Ad-Hoc and Sensor Networks, First International Conference, MSN 2005, Wuhan, China, December 13-15, 2005, Proceedings, pp. 259–268, https://doi.org/10.1007/11599463_26 [Online]. Available.
Zhang, Z., Cho, M.C.Y., Wang, C., Hsu, C., Chen, C.K., Shieh, S., 2014. Iot security: ongoing challenges and research opportunities. In: 7th IEEE International Conference on Service-Oriented Computing and Applications, SOCA 2014, Matsue, Japan, November 17-19, 2014, pp. 230–234, https://doi.org/10.1109/SOCA.2014.58 [Online]. Available.
Zhang, S., Peng, J., Huang, K., Xu, X., Zhong, Z., 2017. Physical layer security in iot: a spatial-temporal perspective. In: 9th International Conference on Wireless Communications and Signal Processing, WCSP 2017, Nanjing, China, October 11-13, 2017, pp. 1–6, https://doi.org/10.1109/WCSP.2017.8171138 [Online]. Available.
Zhang, G., Kou, L., Zhang, L., Liu, C., Da, Q., Sun, J., 2017. A new digital watermarking method for data integrity protection in the perception layer of iot. pp. 3126010:13126010 Secur. Commun. Network. 2017 (12), https://doi.org/10.1155/2017/3126010 [Online]. Available.
Zhao, K., Ge, L., 2013. A survey on the internet of things security. In: Ninth International Conference on Computational Intelligence and Security, CIS 2013, Emei Mountain, Sichan Province, China, December 14-15, 2013, pp. 663–667, https://doi.org/10.1109/CIS.2013.145 [Online]. Available.
Zhao, G., Si, X., Wang, J., Long, X., Hu, T., 2011. A novel mutual authentication scheme for internet of things. In: Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on. IEEE, pp. 563–566.
Zhu, W., Yu, J., Wang, T., 2012. A security and privacy model for mobile rfid systems in the internet of things. In: 2012 IEEE 14th International Conference on Communication Technology. IEEE, pp. 726–732.
Hacking into internet connected light bulbs. http://www.contextis.com/resources/blog/hacking-internet-connected-light-bulbs/, (Accessed 26 October 2019).
Use smart Doorbell to hack WiFi password. http://thehackernews.com/2016/01/doorbell-hacking-wifi-pasword.html/, (Accessed 26 October 2019).

Narges Yousefnezhad is a PhD candidate at Aalto University with particular interest in Internet of Things, Network Security, and Machine Learning. Currently she works on context awareness of sensor data in IoT platform focused on identification, authorization, and access control problems. Prior to enrolling for doctoral study, she worked for one year as research assistant at Aalto to the Secure Systems group headed by Prof. N. Asokan. During this period, she worked on access control in various networks including mobile communication and physical interaction. She holds a master's degree in Information Technology (IT) Engineering, a branch of Computer Science focuses on computer networks and security, from Sharif University of Technology, Iran.

Avleen Malhi is a postdoc researcher in the department of Computer Science at Aalto University since 2019. She has also been working as Assistant Professor at Thapar University India since 2016. She has completed her PhD in the area of information security and her research interests include security, IoT and machine learning. She has 16 SCIE journal publications and 20 International conferences mainly in the area of Machine Learning, IoT and Security.

Prof. Kary Främling is working as full Professor at Umeå University Sweden and Adjunt Professor at Aalto University Finland. He is one of the first movers in the space of IoT and have worked with many industrial partners such as BMW, Nokia etc. He is founder of a successful startup, ControlThings. Prof. Kary Främling is the Chairman of the IoT Work Group of The Open Group, which published the first IoT standards that address all IoT-connected systems on October 16th, 2014: the Open Messaging Interface (O-MI) and Open Data Format (O-DF). Prof. Kary Främling is, indeed, the main architect and author of those standards, whose potential impact for the IoT is similar to the impact of HTTP and HTML for the World Wide Web when they were published. The project will immensely benefit from the insights and the network that Prof. Kary Främling will provide and he is committed to this project beyond research and through to commercialization.