


REVIEW

Open Access



A decade of research on patterns and architectures for IoT security

Tanusan Rajmohan¹, Phu H. Nguyen^{2*}  and Nicolas Ferry³

Abstract

Security of the Internet of Things (IoT)-based Smart Systems involving sensors, actuators and distributed control loop is of paramount importance but very difficult to address. Security patterns consist of domain-independent time-proven security knowledge and expertise. How are they useful for developing secure IoT-based smart systems? Are there architectures that support IoT security? We aim to systematically review the research work published on patterns and architectures for IoT security (and privacy). Then, we want to provide an analysis on that research landscape to answer our research questions. We follow the well-known guidelines for conducting systematic literature reviews. From thousands of candidate papers initially found in our search process, we have systematically distinguished and analyzed *thirty-six* (36) papers that have been peer-reviewed and published around patterns and architectures for IoT security and privacy in the last decade (January 2010–December 2020). Our analysis shows that there is a rise in the number of publications tending to patterns and architectures for IoT security in the last three years. We have not seen any approach of applying systematically architectures and patterns together that can address security (and privacy) concerns not only at the architectural level, but also at the network or IoT devices level. We also explored how the research contributions in the primary studies handle the different issues from the OWASP Internet of Things (IoT) top ten vulnerabilities list. Finally, we discuss the current gaps in this research area and how to fill in the gaps for promoting the utilization of patterns for IoT security and privacy by design.

Keywords: Internet of Things, IoT, Security, Privacy, Architecture, Pattern, Review, SLR

Introduction

The Internet of Things (IoT) is becoming more popular as many “things” are getting more intelligent and connected, e.g., smartphones, smart cars, smart energy grids, smart cities. The IEEE Standards Association defines an IoT system as “a system of entities (including cyber-physical devices, information resources, and people) that exchange information and interact with the physical world by sensing, processing information, and actuating” (IEEE SA 2018). In 2019, the International Data Corporation (IDC) made a forecast that there will be 41.6 billion IoT devices in the field by 2025.¹ Most of the critical infrastructures pointed in the EU’s Directive

on security of network and information systems² such as for energy, water, transport, and healthcare are or will be IoT-based. For instance, smart cities are integrating IoT sensors with analytic to streamline spending, improve infrastructural efficiency.³ Internet-connected pacemakers have been implanted for millions to help control their abnormal heart rhythms. The IoT will thus play a key role in the digitalization of the society and IoT security issues will “affect not only bits and bytes”, but also “flesh and blood” (Schneier 2017). Without solid security in place, attacks and malfunctions in IoT-based

¹ <https://www.idc.com/>.

² NIS Directive, <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.

³ A. Dasgupta, The Continuum: Big Data, Cloud & Internet of Things, IBM Internet of Things blog, 2017.

*Correspondence: phu.nguyen@sintef.no

² SINTEF, Oslo, Norway

Full list of author information is available at the end of the article

critical infrastructures may outweigh any of its benefits (Roman et al. 2011). On the other hand, privacy is also very important in the IoT. Many “things” that people use in daily activities at work and at home are now connected to the Internet. This means that sensitive private data can be exposed via the Internet. Privacy challenges are just as important to tackle in comparison to security challenges in the IoT. The heterogeneous networking technologies and resource-constrained devices of the IoT that can only afford lightweight security and privacy solutions are proven to be weak links for IoT systems (Porambage et al. 2016). It is also possible that security and privacy are often overlooked by IoT solutions providers (Richa 2021), e.g., because of complexity, time-to-market pressure, or due to a lack of knowledge. A way to address this issue could be based on security patterns, which have proven to be very valuable for practitioners, especially non-security experts (Schumacher et al. 2013; Fernandez-Buglioni 2013).

In the software engineering discipline, patterns document well-known solutions that contain domain-independent knowledge and expertise in a reusable way. The solutions documented by patterns are known to be sound because they are tested over time (Schmidt and Buschmann 2003). Moreover, the pros and cons of a pattern are often explicitly documented. Therefore, sketching a solution based on a pattern can provide a good baseline for building the system. Using patterns and architecture alone is not enough but can provide an important support in the development methods for secure systems such as the ones surveyed in Nguyen et al. (2015). Security patterns consist of domain-independent, time-proven security knowledge, and expertise. Security patterns can contribute to the security and privacy of systems because they offer invaluable help in applying solid design solutions that, for example, secure the user authentication, information processing and storing, secure communication with other devices and with the server. Books and catalogs of security patterns, such as Schumacher et al. (2013), Fernandez-Buglioni (2013), Nguyen et al. (2015) and Steel and Nagappan (2006) should be useful for users to unravel security challenges by utilizing time-proven security knowledge and expertise.

However, the IoT era introduces new security challenges that existing approaches and methods cannot address.⁴ For example, the cross-domain cyber-to-physical (C2P) attack is the least understood one comparing to P2C, C2C, or P2P attack categories (Yampolskiy et al. 2013). IoT systems, especially mission-critical ones,

having intrinsic complexity and heterogeneity, broader attack surfaces, often live under uncertainty, which exacerbates security issues (Ciccozzi et al. 2017). Indeed, nowadays IoT systems often span across the Cloud layer, the Fog/Edge layer, and the IoT field-devices layer consisting of many smart, connected devices. The explosion in connectivity created a larger attack surface area (Covington and Carskadden 2013). Besides, the IoT field-devices often operate under dynamic (physical) execution environments, involving dynamic actuation, but have limited data delivery and storage facilities. In other words, uncertainty is inherent in IoT systems. We are very much interested in examining the landscape of patterns and architectures being applied for the IoT domain, whose security (and privacy) challenges are huge. How have the existing security patterns been applied in tackling IoT security challenges? Are there any new security patterns that have been specifically introduced to address new security challenges in IoT?

To make sense of the research landscape of methodologies around patterns for security and privacy in IoT, we have conducted a systematic literature review (SLR) following the most popular guidelines from Kitchenham et al. (2011), Kitchenham and Charters (2007), Petersen et al. (2015) and Wohlin (2014). Our SLR has three fundamental objectives. First, we need to find out the approaches around patterns and architectures for IoT security and privacy, called the primary studies of our SLR. Second, by analyzing the primary studies, we can perceive gaps in the state-of-the-art of patterns and architectures for IoT security and privacy. We are particularly interested in how advanced patterns and architectures are, and their approaches to address IoT security. Third, based on the results, we identify the gaps to support security and privacy in modern IoT systems and propose further research to fill the gaps. The main contributions of this work are our responses to the accompanying research questions (RQ)s.

- **RQ1** *What are the publication statistics of the research on patterns and architectures for IoT security and privacy?*
- **RQ2** *What are the technical details of these security patterns and architectures for addressing IoT security and privacy?*
- **RQ3** *What are the “gaps” to make security patterns and architectures more applicable for IoT?*

From thousands of candidate papers initially found in our search process, we have systematically distinguished and analyzed 36 papers that have been published around patterns and architectures for IoT security in the last decade. Our analysis results show

⁴ Gartner, The Death of IoT Security as You Know It, Gartner, 2017.

the trend of an increasing number of published papers in this research area in three recent years. We have performed our analysis based on a taxonomy that we built for this research area. Our analysis sheds some light on the state of the art around patterns and architectures for IoT security and the current limitations. Based on our analysis, we provide some suggestions for a way forward of this research topic. Specifically, the contributions in this paper include:

- We have an exhaustive database search process. Moreover, we manually conducted snowballing (backward and forward as suggested in Wohlin 2014). We identified and included six new primary studies from this snowballing process. Therefore, our final set of primary studies reported in this paper is 36 (see “[Our systematic literature review approach](#)” section).
- We have defined a clear taxonomy (see “[Taxonomy of the research area](#)” section) and provided in-depth analyses on the architectures and patterns from the primary studies (see “[Technical aspects of the primary studies \(RQ2\)](#)” section). For example, we summarize all the patterns from the primary studies and also discuss how the architectures from the primary studies cover the seven layers of the IoT World Forum Reference Model of the IoT architecture (Juxtology 2018).
- We have provided discussion on the existing gaps and limitations in “[Gaps and limitations \(RQ3\)](#)” section. For example, we discuss the gaps in the research contributions from the primary studies regarding how they handle the different issues presented by the OWASP IoT top ten vulnerabilities list (OWASP 2018). Last but not least, we explicitly discuss the possible threats to validity of our study in “[Threats to validity](#)” section to give readers more insights in this work.

In the remainder of this paper: “[Background](#)” section gives some background definitions. In “[Our systematic literature review approach](#)” section, we present our SLR approach. To facilitate data extraction and comparison, “[Taxonomy of the research area](#)” section describes our classification schemes for the primary studies. We present the results of our SLR in “[Results](#)” section. Related work is discussed in “[Related work](#)” section. In “[Threats to validity](#)” section, we analyze possible threats to the validity of this work. Finally, we conclude the paper with summarizing the main findings in “[Conclusions](#)” section.

Background

We give the definitions of SLR in the “[Systematic literature review](#)” section, (security) design patterns in the “[Design pattern](#)” section, and security architecture in the “[Security architecture](#)” section that were used to define the scope of this work.

Systematic literature review

A SLR is a study that “reviews all the primary studies relating to a specific research question”, and “uses a well-defined methodology to identify, analyze and interpret all available evidence related to that specific research question in a way that is unbiased and (to a degree) repeatable.” (Kitchenham et al. 2011)

Design pattern

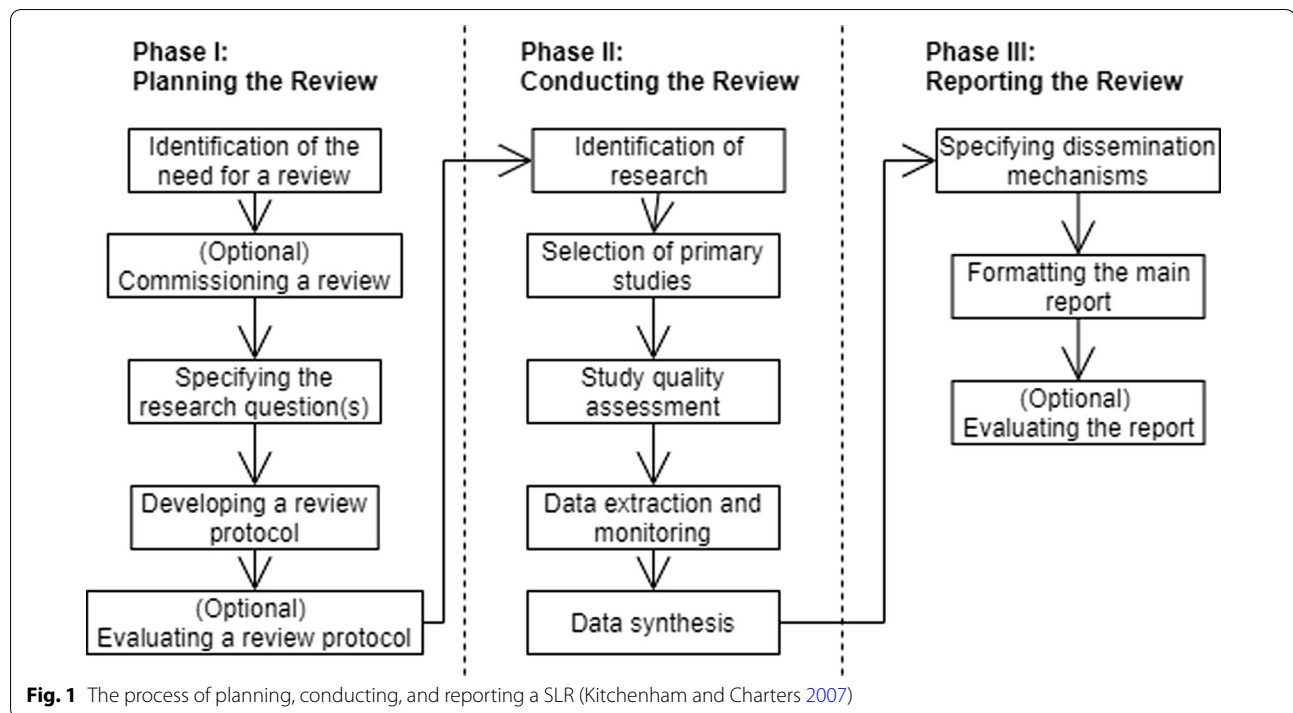
The primary understanding for a design pattern is that it is a reusable solution for a typical occurring issue in software design. A pattern is ordinarily abstract with the goal that it may be reused, and it is a proven solution for solving a software design problem. A design pattern is not a complete implementation that can be executed and utilized, but more a plan or template for how to take care of an issue that can serve in various circumstances/contexts (Gamma et al. 1994; Fernandez-Buglioni 2013).

According to Schumacher et al. (2013), “a security pattern describes a particular recurring security problem that arises in specific contexts, and presents a well-proven generic solution for it. The solution consists of a set of interacting roles that can be arranged into multiple concrete design structures, as well as a process to create one particular such structure.”

Note that there are key security patterns such as from Schumacher et al. (2013), Fernandez-Buglioni (2013) and Steel and Nagappan (2006) that provide guidance at the architecture level. These patterns may also be called security architectures but yet they are design patterns and should be considered as patterns. In other words, we clearly call architectural patterns as patterns, not architectures. This definition means that we only consider an architecture as a pattern if it is explicitly described as a pattern. Any architecture for IoT security that is not a pattern is called “security architecture” in this paper.

Security architecture

The term software architecture typically refers to the structure of a software system, including software elements and the relationships between them. Within our SLR, we want to include architectures for IoT security or architectures that were specifically designed with IoT security concerns in mind. When architectures are not formalized as a pattern, we call them IoT security



architectures, as opposed to architectural patterns. When a security architecture is generic enough to be used in different contexts, it is called an IoT security reference architecture. It is worth discussing the relationship between IoT security reference architectures and IoT security patterns: (1) IoT security patterns can be extracted from an IoT security reference architecture, and (2) an IoT security reference architecture can leverage and be composed of one or several patterns, including IoT security patterns. By analyzing not only security patterns but also security architectures, our study aims to cover security aspects encompassing not only one layer of IoT systems but also multiple layers when architectures are key to address.

Our systematic literature review approach

We conducted our SLR using the most popular guidelines from Kitchenham et al. (2011), Kitchenham and Charters (2007), Petersen et al. (2015) and Wohlin (2014). Three main phases of an SLR are: Planning the Review, Conducting the Review, Reporting the Review (see Fig. 1) (Kitchenham and Charters 2007).

We map the stages associated with planning our SLR with where we present them in this paper:

- *Identification of the need for a review*: In the “Introduction” section, we have presented the motivation of our SLR.

- *Specifying the research question(s)*: the “Research questions” section.
- *Developing a review protocol*: Our review protocol is developed according to the guidelines in Kitchenham and Charters (2007). The main parts of our review protocol are the research questions (“Research questions” section), the inclusion and exclusion criteria (“Inclusion and exclusion criteria” section), the search and selection strategy (“Search and selection strategy” section), and the taxonomy for data extraction and synthesis (“Taxonomy of the research area” section).

The stages associated with conducting our SLR:

- *Identification of research*: Search and selection strategy (“Search and selection strategy” section).
- *Selection of primary studies*: Search and selection strategy (“Search and selection strategy” section).
- *Study quality assessment*: We only selected peer-reviewed papers with enough details as the primary studies of this SLR (“Inclusion and exclusion criteria” section).
- *Data extraction and monitoring*: We extracted data based on the taxonomy defined in “Taxonomy of the research area” section.
- *Data synthesis*: We synthesized the extracted data to answer our research questions in “Results” section.

The stages associated with reporting our SLR:

- *Specifying dissemination mechanisms:* We specified the journal to publish the results of our SLR.
- *Formatting the main report:* This paper.

With the particular context and motivation displayed in “**Introduction**” section, we introduce our RQs for this paper in “**Research questions**” section. In “**Inclusion and exclusion criteria**” section, we explain the criteria for choosing primary studies to explicitly portray the scope of our SLR and diminish possible bias in our selection procedure. “**Search and selection strategy**” section shows our search strategy to locate the primary studies for answering the RQs.

Research questions

This SLR aims to answer the three RQs presented in “**Introduction**” section. Each is extended with sub-questions.

RQ1 includes three sub-RQs. **RQ1.1** *In which year(s) are the primary studies published?* Answering this question allows us to know when this research topic became fascinating as well as how recent the research on this topic is. It could give an indicator of how much attention security patterns and secure architectures for IoT get from the research community. **RQ1.2**—*What are the types (i.e., Journal, Conference, Workshop) and target domains (e.g., IoT, Network, Cloud and Software Engineering (SE)) of the venues where the primary studies were published?* Answering this question allows us to recognize the target domain for each paper. Note that security patterns are presented in publications across a few related research areas, e.g., IoT, Cloud, SE, Network. The type of paper can give a few hints on the maturity of the primary study. Journal papers should report more mature studies than conference papers. **RQ1.3**—*How is the distribution of publications in terms of papers affiliated with industry and the academic?* We classify a paper as *academic* if all the associated authors are with a university or a research institute. Moreover, we group papers as *industrial* if all related authors are with an industrial organization, and characterize the papers as *both* if there is a coordinated effort of both academia and industry. Answering RQ1.3 will display the collaboration effort between industry and scholar communities. It also demonstrates the interest and needs of IoT security patterns in the industry.

RQ2 has three sub-RQs. **RQ2.1**—*What type (e.g., security pattern, architecture) of contribution do the primary studies create or use, and how the distribution is between them?* Answering RQ2.1 shows how the distribution of patterns and architectures are, as well as how the contribution is used or for what purpose. **RQ2.2**—*How well do*

the patterns and architectures cover security and privacy issues? Answering this RQ shows what security patterns and architectures focus on IoT systems’ specific security and privacy concerns. It also shows us what current security and privacy concerns are most covered today. **RQ2.3**—*What application domains have been addressed by the security patterns and architectures?* This RQ can help us to see what application domains have got more attention in the application of security patterns and architectures.

RQ3 also has two sub-RQs. **RQ3.1**—*What are the current limitations of the IoT security patterns and architectures research?* **RQ3.2**—*What research directions could be recommended for tackling the current limitations?* These RQs help to express and suggest the current issues and possible directions for future work.

Inclusion and exclusion criteria

Considering the RQs and the basis of our study introduced in “**Introduction**” section, we predefined the inclusion and exclusion criteria to decrease bias in our methodology of search and selection of primary studies. The primary studies must meet ALL the accompanying inclusion criteria (IC):

- 1 (IC1) Contain patterns or architectures (one or more) in some form relevant for IoT systems.
- 2 (IC2) Be specifically within the area of IoT, either in a generally applicable domain or in a specific application domain of IoT.
- 3 (IC3) Present security (or privacy) concerns explicitly in system design, architecture, or infrastructure.
- 4 (IC4) Have a minimum length of four pages in double-column format or six pages in single-column format.

Moreover, when a single approach is presented in more than one paper describing different parts of the approach (e.g., approach itself, empirical study, evaluation), we include all these papers, but still consider them as a single approach (study). When encountering more than one paper describing the same or similar approaches, which were published in different venues, we only include the most recent one that has the most complete description of the approach.

We excluded papers that are not written in English, non-peer-reviewed papers (e.g., “grey” literature, white papers in industry), and papers that are only accessible as extended abstracts, posters, or presentations (not full version). We also did not include multivocal surveys as primary studies because they are secondary studies. We do discuss the surveys on related topics as related work

in “[Related work](#)” section. We also mainly focused our review for the publications in the duration 2010–2020 (see “[Search and selection strategy](#)” section).

Search and selection strategy

The search strategy utilized is a blend of various kinds, to thoroughly scan for IoT security pattern and architecture papers. The objective is to locate the most relevant papers and, along these lines, discover as many essential IoT security pattern and architecture papers as possible.

Database search

Using online inquiry components of popular publication databases is the most notable approach to scan for essential primary studies when directing supplemental studies (Kitchenham and Charters 2007). We used five of the popular publication databases IEEE Xplore,⁵ ACM Digital Library,⁶ ScienceDirect,⁷ Web of Knowledge (ISI),⁸ and Scopus⁹ to search for potential primary studies. Scopus and ACM DL already index SpringerLink¹⁰ (Tran et al. 2017). The five picked databases contain peer-reviewed articles, which give advanced search capacities. Following the guidelines from Kitchenham and Charters (2007), based on the research questions and keywords utilized in some related articles, we have defined our search keywords. The search query was adopted to fit each of the search engines of the five publication databases. Note that we did not include “misuse pattern” in the search query because misuse patterns (from the point of view of the attacker) are out of scope of this study.

(“Internet of Things” OR “IoT” OR “Cyber Physical Systems” OR “Web of Things”)

AND

(“Security Pattern” OR “Design Pattern” OR “Security Design Pattern” OR “Privacy Pattern” OR “Security Architecture” OR “Secure Architecture”)

During our database search process, we did conduct many rounds of testing the search query on the search engines. On the one hand, this testing process helped us to improve our search query and customize it for better fit the search features. On the other hand, we also saw very few hits returned by the search engines for the

duration 2000–2010. Therefore, we mainly focused our review for the publications in the duration 2010–2020.

For every candidate paper, we originally reviewed the paper’s title and abstract, trailed by skimming through the contents. On the off chance that an applicant paper shows up in more than one database, we show them in the other database results. When merging to the first set of primary studies, we consolidate the outcomes, so we get the right number of papers without copies. It is portrayed step by step in Fig. 2.

Manual search

It is unrealistic to guarantee the database search results can cover all IoT security patterns and architectures in our study. We have, therefore, attempted to supplement the database search by doing a manual search. We started by manually searching through published papers from previous journals and conferences. The conferences and journals we went through to find papers were: The International Conference on the Internet of Things,¹¹ Pattern Languages of Programs (PLoP),¹² EuroPLoP,¹³ IEEE ICIOT,¹⁴ ACM Transactions on Internet of Things (TIOT)¹⁵ and IEEE Internet of Things Journal.¹⁶ We also manually did snowballing (backward and forward) on all the primary studies found as suggested in Wohlin (2014). In the wake of looking through these journals and conferences as well as doing snowballing, we concluded that most of the relevant papers posted or found from our manual search were earlier discovered from the database search, or they did not satisfy our criteria. The papers from the manual search were checked against the automatic results, and vice versa. In the end, we had found six more primary studies from the manual search process.

Note that any candidate paper in doubt was kept for evaluation and cross-checked among the reviewers at each phase of our search and selection process. Our gathering conversations have finally yielded a set of 36 primary studies for data extraction and synthesis to answer the RQs¹⁷.

Taxonomy of the research area

In this section, we define a taxonomy for IoT security patterns and architectures. This taxonomy helps us to extract and synthesize data from the primary studies

⁵ <https://ieeexplore.ieee.org>.

⁶ <https://dlnext.acm.org>.

⁷ <https://sciencedirect.com/>.

⁸ <http://apps.webofknowledge.com>.

⁹ <https://scopus.com>.

¹⁰ <https://www.springer.com>.

¹¹ <https://iot-conference.org/iot2020/>.

¹² <https://hillside.net/conferences>.

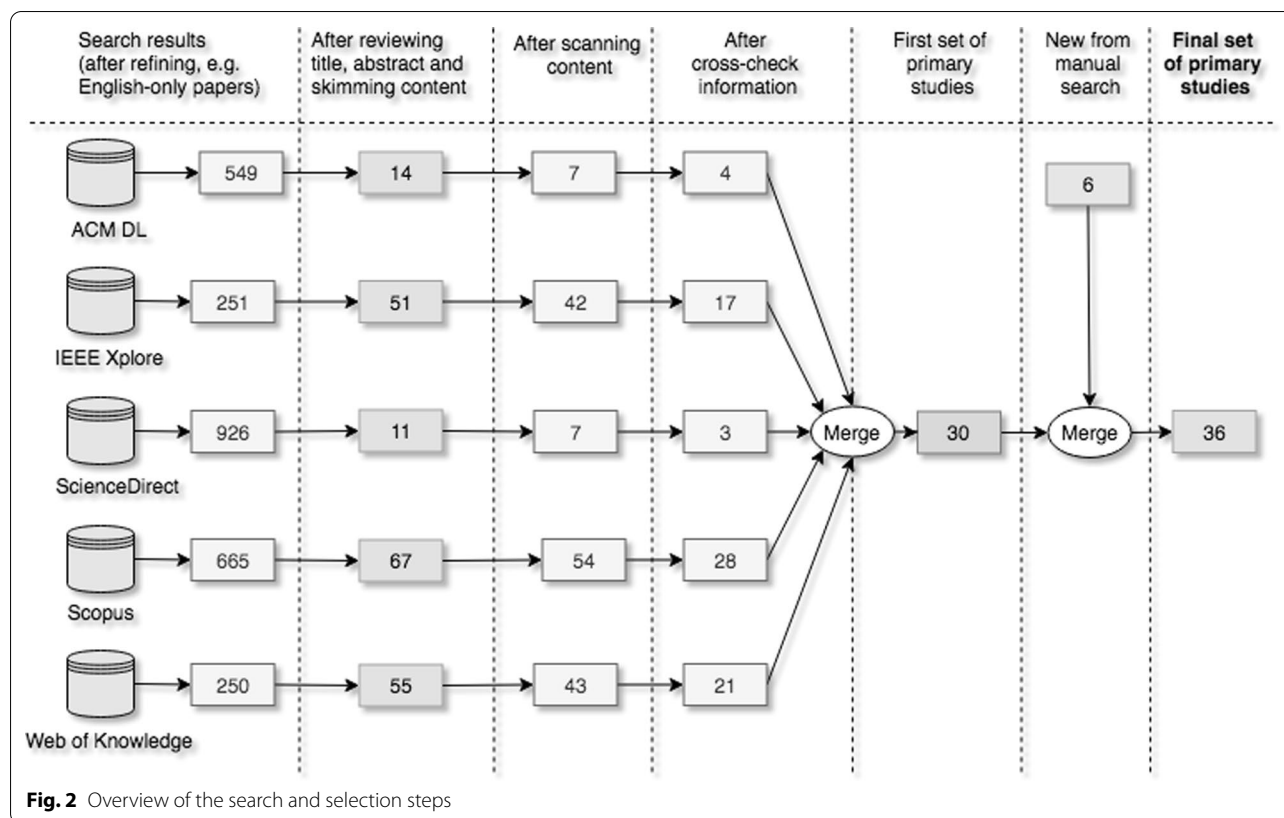
¹³ <https://www.europlop.net/>.

¹⁴ <https://conferences.computer.org/iciot/2019/>.

¹⁵ <https://dl.acm.org/journal/tiot>.

¹⁶ <https://ieee-iotj.org/>.

¹⁷ Our search and selection process for the primary studies concluded in December 2020



for answering the RQs. We applied a *top-down* strategy to process data from the literature around IoT, security patterns, IoT architectures, and design patterns to create a first version of the taxonomy. We also tried to validate and enrich the taxonomy by a *bottom-up* approach. The *bottom-up* approach is for extracting data from a test set of primary studies. This test set consists of the initial ten primary studies chosen. It helped us to characterize and determine the significant methods and terminology utilized in the primary studies.

Domain specificity

We characterize the domain specificity in the same manner as (Washizaki et al. 2020) with minor tweaks. It is essential to examine the applicability and reusability of each IoT security pattern.

- 1 **General** IoT security design patterns, and security architectures, which apply to any IoT system and software.
- 2 **Specific** IoT security design patterns, and security architectures that address specific problem domains (such as healthcare) and technical domains (such as the brain-computer interaction).

Categorization of security pattern research

We classify security patterns according to the main categories presented in Yskout et al. (2006). First, we distinguish security patterns based on how they affect the software application or the environment (e.g., infrastructure, middleware) in which the application will eventually be deployed.

- **Application architecture (AA):** A pattern’s introduction can affect an extensive part of the application, e.g., by introducing new components in the application, or modifying existing components.
- **Application design (AD):** A pattern’s introduction only has local implications. For example, a pattern can introduce some form of encapsulation of security data.
- **System (S)/Execution environment:** A pattern’s introduction only affects the environment in which the application will be deployed.

We classify the (security, privacy) objectives of the patterns as presented below in “[Security and privacy concerns](#)” section. More importantly, we detail the patterns by their main properties from the software design pattern template by the Gang of Four (Gamma et al. 1994):

- **Intent:** What (in what context) is the pattern used for? What is the purpose of the pattern?
- **Problem:** What problem that the pattern can address. This may also include the different forces (and context) that lead to the problem.
- **Solution:** A description of the solution provided by the pattern.

We also characterize patterns by *purpose*, *method*, and *research implementation*, which is similar to how Washizaki et al. (2018) did in their paper.

C1 purpose: This part includes the topics addressed by the research, software life-cycle, and the intended users.

C2 method: This part refers to the methodology and modeling methods to define the pattern's structure and design.

C3 research implementation/validation: This part includes where, how and if the contributions were implemented and tested/validated, and in which context. It also includes analysis of a test case or scenario. Whether the results are automated and encapsulated in a tool, and whether case studies or experiments are conducted to evaluate the results relevant to the original research purpose.

IoT architecture

Many IoT architecture exist in the literature, all decomposed in a different number of layers. In our taxonomy, we leverage the IoT World Forum Reference Model of the IoT architecture (Juxtology 2018). This architecture provides a fine-grained granularity over the different layers that typically compose an IoT system. It has recently been adopted in many large scale IoT systems, for instance, as indicated in Create-IoT (2018), all of the H2020 IoT large scale pilots at the exception of one, have adopted this architecture. It consists of the following seven layers:

L1 physical devices and controllers: Physical layer consisting of devices or “things” of the IoT. The “things”, sensors, and Edge Node devices are classified within this layer.

L2 connectivity: Connectivity spans from the “middle” of an Edge Node device up through transport to the Cloud. This layer maps data from the logical and physical technologies used, the communication between the physical layer and the computing layer, and above.

L3 edge computing: Layer that brings computation and data storage closer to the location it is needed. Protocol conversion, routing to higher-layer soft-

ware functions, and even “fast path” logic for low latency decision making will be implemented at this layer.

L4 data accumulation: Intermediate storage of incoming storage and outgoing traffic queued for delivery to lower layers. Pure SQL is what the layer is implemented with, but it may require more advanced solutions, i.e., Hadoop & Hadoop File System, Mongo, Cassandra, Spark, or other NoSQL solutions.

L5 data abstraction: Data is made clear and understandable, centers around rendering data and its storage in manners that enable developing more straightforward, performance-enhanced applications. This layer speeds up high priority traffic or alarms, and sort incoming data from the data lake into the appropriate schema and streams for upstream processing. Likewise, application information bound for downstream layers is reformatted appropriately for device communication and queued for processing.

L6 application layer: At the application layer, information interpretation of multiple IoT sensors or measurements occur, and logic is executed. Monitoring, process optimization, alarm management, statistical analysis, control logic, logistics, consumer patterns, are just a few examples of IoT applications.

L7 collaboration and processes: Application processing to its users, and data processed at lower layers are integrated with business applications. This layer consists of human interaction with all the layers of the IoT system, and economic value is delivered.

Another simpler IoT architecture largely adopted in the literature consists of three layers: perception (L1), network (grouping L2 and L3), and application (grouping L4, L5, L6, L7, and L8). We map how the contributions of today fit in both the IoT World Forum Reference Model of the IoT architecture and the three-layer IoT architecture.

Security and privacy concerns

We analyze the primary studies according to the following security and privacy concerns: confidentiality, integrity, availability (CIA), accountability, and privacy (Ross et al. 2016; Kuhn et al. 2001; Yskout et al. 2006). These concerns are what we consider essential to IoT systems and devices. We also classify security mechanisms such as authentication and authorization when such information are available in the primary studies. We want to see what patterns and architectures uphold and protect against these security and privacy concerns. Their definitions are as follows.

- **Confidentiality:** Ensures the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** Maintains and ensures the accuracy and completeness of the data during its life-cycle.
- **Availability:** The information/service is available when needed.
- **Authentication:** The system/device can verify a claim of identity.
- **Authorization:** The system can determine what resources the entities that have been identified and authenticated can access and what actions they can perform within/on the system.
- **Accountability:** Enables the tracing of important (or all) actions performed on the system back to a particular user, usually by means of logging.
- **Privacy:** The data collected is legally collected and stored, how data is shared, and follow regulatory restrictions from the GDPR (mostly EU), and HIPAA (Office for Civil Rights 2013), GLBA (Federal Trade Commission 1999) (mostly in the US).

Results

This section presents the main results of our SLR and how our research questions are answered. Table 1 shows an overview of the primary studies that have been found in this review regarding patterns and architectures for IoT security and privacy. Based on the taxonomy in “[Taxonomy of the research area](#)” section, we have extracted and synthesized the primary studies’ data to answer the RQs. “[High-level statistics \(RQ1\)](#)” section shows high-level statistics that help us to answer RQ1. Then, we present low-level details of the primary studies in “[Technical aspects of the primary studies \(RQ2\)](#)” section that help us to answer RQ2. Based on our answers to RQ1 and RQ2, we discuss the gaps and limitations as our answer to RQ3.

High-level statistics (RQ1)

In this section, we provide our answers to the RQ1-*What are the publication statistics of the research on patterns and architectures for IoT security and privacy?*

Answering RQ1.1 *In which year(s) are the primary studies published?* Fig. 3 shows a rise in the number of conference (C) and journal (J) publications related to IoT security patterns and architectures in the recent three years (2018: 7C, 2019: 5C, 4J and 2020¹⁸: 5C, 5J). This spike shows that security patterns and architectures are gaining more focus over the years and that there is

a demand for IoT security pattern and architecture research.

Answering RQ1.2 *What are the types (i.e., Journal, Conference, Workshop) and target domains (e.g., IoT, Network, Cloud and Software Engineering (SE)) of the venues where the primary studies were published?* Research on the IoT, with its heterogeneous nature, traverses through various important research areas, among which we perceived Software Engineering (SE), Cloud, Blockchain, Network, and recently specialized IoT research (Borgia et al. 2016). Figure 4 shows the research focus areas of the publication venues where the primary studies have been published. The main research areas that we found are between IoT: 36, Cloud: 4, Network: 7, Blockchain: 7. Note that publication venues often have several research areas in their calls for papers, e.g., IoT, network. Therefore a portion of the papers could be classified in several research areas at the same time (e.g., IoT, network). These numbers do reflect the different dimensions of IoT research, with IoT research domain getting progressively more visible. In other words, IoT-oriented conferences and journals are becoming more popular and have attracted research contributions on patterns and architectures for IoT security and privacy.

The number of primary studies that are published as conference papers are more than double the number of primary studies published in journals. From the number of publications found, we distinguished the distribution of conference papers (~ 69%) and journal papers (~ 31%). It is reasonable that conference papers tend to be published more often and quickly. But, we also see that the number of journal papers has increased since our last study (Rajmohan et al. 2020). We do, however, believe and encourage a continued increase of journal papers around this topic. Especially seeing that the growth of IoT is increasing rapidly and that journal papers contribute to more detailed and elaborated contributions.

Answering RQ1.3 *How is the distribution of publications in terms of papers affiliated with industry and the academic?* Because IoT systems and devices are broadly utilized and growing in the industry and consumer market, we explored how the affiliations of the authors are dispersed from the primary studies. Would the affiliations of the authors have any implication on the publication of security patterns and architectures for IoT? From our analysis, we see that a significant amount of the authors who have published results on IoT security patterns or architectures are from academia (~ 75%). While there are no contributions exclusively from industry, authors working in industry do publish in joint efforts with co-authors from academia. In this work, we call the papers that have such joint efforts of academia-industry collaboration as “joint papers”. We discovered

¹⁸ Our search and selection process covers the period until December 2020.

Table 1 Overview of the primary IoT security pattern and architecture studies

Paper #	Year	Title (click to open the corresponding publication)	v	f
Vijayakumaran et al. (2020)	2020	A reliable next generation cyber security architecture for industrial internet of things environment (https://www.scopus.com/record/display.uri?eid=2-s2.0-85073370260&origin=resultslist&sort=plf-f&src=s&st1=A+reliable+next+generation+cyber+security+architecture+for+industrial+internet+of+things+environment&st2=&sid=6def2778e8748aeae199dcd24e81ae5&sot=b&sdt=b&sl=115&s=TITLE-ABS-KEY%28A+reliable+next+generation+cyber+security+architecture+for+industrial+internet+of+things+environment%29&relpos=0&citeCnt=2&searchTerm=)	C	A
Vithya Vijayalakshmi and Arockiam (2020)	2020	A secured architecture for IoT healthcare system (https://www.scopus.com/record/display.uri?eid=2-s2.0-85083648091&origin=resultslist&sort=plf-f&src=s&st1=A+Secured+Architecture+for+IoT+Healthcare+System&st2=&sid=6def2778e8748aeae199dcd24e81ae5&sot=b&sdt=b&sl=63&s=TITLE-ABS-KEY%28A+Secured+Architecture+for+IoT+Healthcare+System%29&relpos=0&citeCnt=1&searchTerm=)	C	A
Portal et al. (2020)	2020	An edge decentralized security architecture for industrial IoT applications (https://ieeexplore.ieee.org/document/9221176)	C	A
Karaarslan et al. (2020)	2020	Design and implementation of SDN-based secure architecture for IoT-Lab (https://www.scopus.com/record/display.uri?eid=2-s2.0-85083427175&origin=resultslist&sort=plf-f&src=s&st1=Design+and+Implementation+of+SDN-Based+Secure+Architecture+for+IoT-Lab&st2=&sid=6def2778e8748aeae199dcd24e81ae5&sot=b&sdt=b&sl=85&s=TITLE-ABS-KEY%28Design+and+Implementation+of+SDN-Based+Secure+Architecture+for+IoT-Lab%29&relpos=0&citeCnt=0&searchTerm=)	C	A
Perera et al. (2020)	2020	Designing privacy-aware internet of things applications (https://www.sciencedirect.com/science/article/pii/S0020025519309120)	J	A
Dhieb et al. (2020)	2020	Scalable and secure architecture for distributed IoT systems (https://ieeexplore.ieee.org/document/9140108)	C	A
Koo et al. (2020)	2020	Security architecture for cloud-based command and control system in IoT environment (https://www.scopus.com/record/display.uri?eid=2-s2.0-85081588195&origin=resultslist&sort=plf-f&src=s&st1=Security+Architecture+for+Cloud-Based+Command+and+Control+System+in+IoT+Environment&st2=&sid=8baa12fe1401019180971c95019fe27a&sot=b&sdt=b&sl=98&s=TITLE-ABS-KEY%28Security+Architecture+for+Cloud-Based+Command+and+Control+System+in+IoT+Environment%29&relpos=0&citeCnt=1&searchTerm=)	J	A
Robles Enciso et al. (2020)	2020	Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems (https://www.scopus.com/record/display.uri?eid=2-s2.0-85082792671&origin=resultslist&sort=plf-f&src=s&st1=Security+architecture+for+defining+and+enforcing+security+profiles+in+DLT%2FSDN-based+IoT+systems&st2=&sid=8baa12fe1401019180971c95019fe27a&sot=b&sdt=b&sl=110&s=TITLE-ABS-KEY%28Security+architecture+for+defining+and+enforcing+security+profiles+in+DLT%2FSDN-based+IoT+systems%29&relpos=0&citeCnt=1&searchTerm=)	J	A
Park (2020)	2019	Security architecture for secure multicast CoAP applications (https://ieeexplore.ieee.org/document/8974263)	J	A
Koshy et al. (2020)	2020	Sliding window blockchain architecture for Internet of Things (https://ieeexplore.ieee.org/document/8974263)	J	A
Attia et al. (2019)	2019	An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application (https://ieeexplore.ieee.org/document/8763849)	C	A
Pape and Rannenber (2019)	2019	Applying privacy patterns to the Internet of Things' (IoT) architecture (https://www.scopus.com/record/display.uri?eid=2-s2.0-85054572626&origin=resultslist&sort=plf-f&src=s&st1=Applying+Privacy+Patterns+to+the+Internet+of+Things+Architecture&st2=&sid=94e759f4e7106d7f9b416c4471289e65&sot=b&sdt=b&sl=79&s=TITLE-ABS-KEY%28Applying+Privacy+Patterns+to+the+Internet+of+Things+Architecture%29&relpos=1&citeCnt=0&searchTerm=)	J	P
Fysarakis et al. (2019)	2019	Architectural patterns for secure IoT orchestrations (https://ieeexplore.ieee.org/document/8766425/)	C	P
Tiburski et al. (2019)	2019	Lightweight security architecture based on embedded virtualization and trust mechanisms for IoT edge devices (https://ieeexplore.ieee.org/document/8647115)	J	A
Zhang et al. (2019)	2019	Overview of IoT security architecture (https://ieeexplore.ieee.org/document/8923665/)	C	A
Karmakar et al. (2019)	2019	SDN enabled secure IoT architecture (https://ieeexplore.ieee.org/document/8717819/)	C	A
Durresi et al. (2019)	2019	Secure communication architecture for internet of things using smartphones and multi-access edge computing in environment monitoring (https://link.springer.com/article/10.1007/s12652-018-0759-6)	J	A

Table 1 (continued)

Paper #	Year	Title (click to open the corresponding publication)	v	f
Jerald et al. (2019)	2019	Secured architecture for integrated IoT enabled smart services (https://www.scopus.com/record/display.uri?eid=2-s2.0-85073499499&origin=resultslist&sort=plf-f&src=s&st1=Secured+architecture+for+integrated+IoT+enabled+smart+services&st2=&sid=4c4a3ce90627aab79cc656fe0eed1fc2&sot=b&sdt=b&sl=77&s=TITLE-ABS-KEY%28Secured+architecture+for+integrated+IoT+enabled+smart+services%29&relpos=0&citeCnt=0&searchTerm=)	J	A
Petroulakis et al. (2019)	2019	SEMloTICS architectural framework: end-to-end security, connectivity and interoperability for industrial IoT (https://ieeexplore.ieee.org/document/8766399/)	C	A
Syed et al. (2018)	2018	A misuse pattern for DDoS in the IoT (https://dl.acm.org/doi/abs/10.1145/3282308.3282343)	C	P
Witti and Konstantas (2018)	2018	A secure and privacy-preserving Internet of Things framework for smart city (https://dl.acm.org/doi/abs/10.1145/3301551.3301607)	C	A
Pahl et al. (2018)	2018	An architecture pattern for trusted orchestration in IoT edge clouds (https://ieeexplore.ieee.org/document/8364046)	C	P
Zhu and Badr (2018)	2018	Fog computing security architecture for the Internet of Things using blockchain-based social networks (https://ieeexplore.ieee.org/document/8726571)	C	A
Schuß et al. (2018)	2018	IoT device security the hard(ware) way (https://dl.acm.org/doi/abs/10.1145/3282308.3282329)	C	P
Alphand et al. (2018)	2018	IoTChain: a blockchain security architecture for the Internet of Things (https://ieeexplore.ieee.org/document/8377385)	C	A
Pacheco et al. (2019)	2018	Security framework for IoT cloud services (https://ieeexplore.ieee.org/document/8612808/)	C	A
Lee and Law (2017)	2017	A case study in applying security design patterns for IoT software system (https://ieeexplore.ieee.org/document/7988402/)	C	P
Ye and Qian (2017)	2017	A security architecture for networked Internet of Things devices (https://www.scopus.com/record/display.uri?eid=2-s2.0-85046455493&origin=resultslist&sort=plf-f&src=s&st1=A+Security+Architecture+for+Networked+Internet+of+Things+Devices&st2=&sid=69f79eb51b98090742db2d001e68b1e9&sot=b&sdt=b&sl=79&s=TITLE-ABS-KEY%28A+Security+Architecture+for+Networked+Internet+of+Things+Devices%29&relpos=12&citeCnt=4&searchTerm=)	C	A
Pacheco et al. (2018)	2017	IoT security framework for smart water system (https://ieeexplore.ieee.org/document/8308438/)	C	A
Ntuli and Abu-Mahfouz (2016)	2016	A simple security architecture for smart water management system (https://www.sciencedirect.com/science/article/pii/S1877050916302721)	J	A
Pacheco et al. (2016)	2016	IoT security development framework for building trustworthy smart car services (https://ieeexplore.ieee.org/document/7745481/)	C	A
Lessa dos Santos et al. (2015)	2015	A DTLS-based security architecture for the Internet of Things (https://ieeexplore.ieee.org/document/7405613/)	C	A
Vučinić et al. (2015)	2015	OSCAR: object security architecture for the Internet of Things (https://ieeexplore.ieee.org/document/6918975)	J	A
Ur-Rehman and Zivic (2015)	2015	Secure design patterns for security in smart metering systems (https://ieeexplore.ieee.org/document/7579841/)	C	P
Garcia-Morchon et al. (2013)	2013	Securing the IP-based internet of things with HIP and DTLS (https://dl.acm.org/doi/abs/10.1145/2462096.2462117)	C	A
Goncalves et al. (2013)	2013	Security architecture for mobile E-health applications in medication control (https://ieeexplore.ieee.org/document/6671901/)	C	A

^vVenue type: J = Journal (11), C = Conference (25)

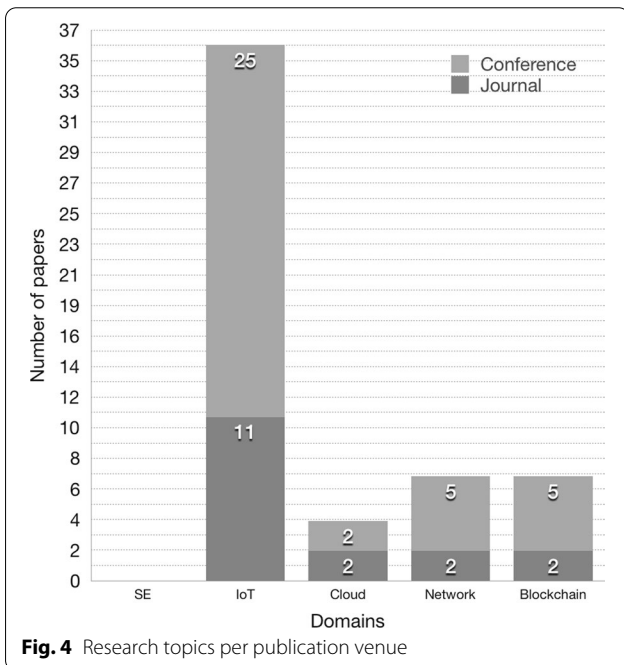
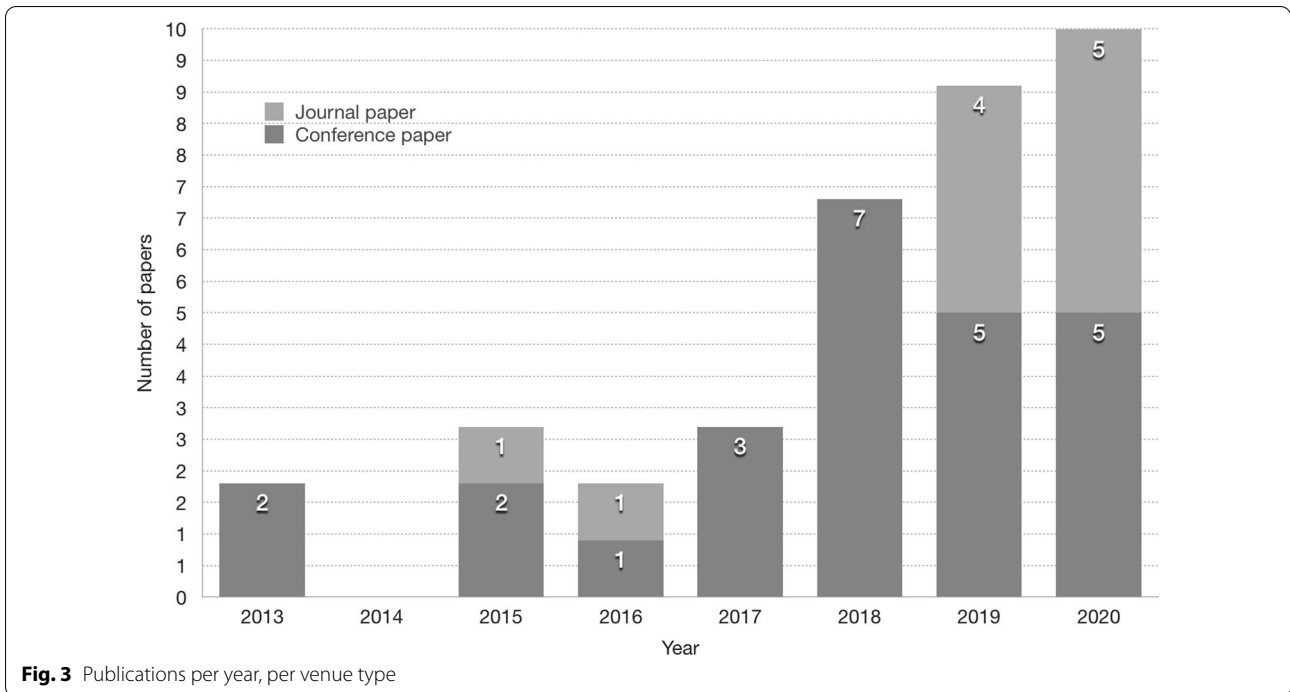
^fFocus: P = pattern (7), A = Architecture (29)

* sorted by year of publication

some papers of this type (~ 25%). The percentage of joint papers here is not high, but still remarkable compared to less than 10% of joint papers as primary studies reported in another review on security for cyber-physical systems (Nguyen et al. 2017).

Joint papers tend to have more usage examples and illustration contrasted with papers purely from academia. We saw in our study that 89% of the joint papers had

graphical illustrations of their contribution in terms of architectural structure or pattern usage areas. The number of joint papers among academia and industry shows a promising collaboration level. We trust that this number continues to grow. The collaboration is win-win for the state of the art and practice, which can lead to the utilization of patterns and architectures proposed to improve products, production process, and internal processes



that use IoT devices or systems further. We would be intrigued to see more implementations or examples of security patterns or architectures used by industry in the future.

Technical aspects of the primary studies (RQ2)

All the patterns and architectures in Table 1 have been examined according to our taxonomy (“Taxonomy of the research area” section), to give us meaningful information as well as pinpoint how the papers are relevant and where they contribute. The taxonomy was used to ensure that the primary studies have information relevant to this study. We can draw out some key examples, such as papers (Vijayakumaran et al. 2020; Vithya Vijayalakshmi and Arockiam 2020; Jerald et al. 2019; Pacheco et al. 2018), which are the ones who cover most security concerns (“Security and privacy concerns” section). We based on the (more fine-grained) data extracted from the primary studies to answer RQ2: *What are the technical details of these security patterns and architectures for addressing IoT security and privacy?*

Answering RQ2.1 *What type (e.g., security pattern, architecture) of contribution do the primary studies create or use, and how the distribution is between them?* After finalizing the primary studies set, we found that the primary studies’ main contributions are either architectures (~ 81%) or patterns (~ 19%). These contributions are mostly solution proposals, where some have proper testing and validation (~ 57%) of their concept. Other papers have use case examples (~ 23%) in some form, and some papers even have implementations of their concept (~ 20%). As we presented in “Security architecture” section, papers describing frameworks are categorized as architectures (not patterns, if patterns are not explicitly

mentioned). Therefore, we see a more significant contribution and more focus on architectures compared to patterns.

Claiming security solely based on a good architecture can be inadequate because it is typically not enough for end-to-end IoT security. We have seen other cases where architectures are not enough to solve the specific issues regarding e.g., user verification on the devices, firmware manipulation, and an attacker disconnects the devices upon will. Such issues are hard to handle only with security architecture solutions. The lack of security patterns is a result of its youth within the domain and security not being the main priority when developing IoT systems. Certain areas of an IoT system may need more attention than others regarding security, and architectures may not solve those issues. From our experience and information gathering, we have seen that the architecture solutions for IoT security have focused a lot on the whole system and all its layers (e.g., Cloud, Edge, IoT devices Juxtology 2018), more general system issues, and can target specific domains, but are very seldom enough to solve a specific problem. The architectures tend to focus on multiple layers (e.g., Cloud, Edge Juxtology 2018) and are harder to address a single layer issue or an issue in a small part of one of the architectural layers, where some specific security patterns may apply well.

As mentioned, a good architecture is only part of the solution and can be inadequate if we encounter specific security issues for a smaller area rather than the whole system, e.g., the breach on a casino's thermostat in a fish tank to access customer data (Williams-Grut 2018). This breach shows the challenge to ensure end-to-end security for IoT systems, especially at their weakest links, e.g., a thermostat. Therefore, it would be exaggerating to tackle security only at the architectural level. A more straightforward solution would have been a security pattern for authentication of users or networks not to allow external communication to pass through IoT devices or verify the device when communication is sent. A more complete solution would be to employ suitable specific security patterns in a well-designed architecture. In other words, a high-level architecture supporting IoT security is only one side of the coin. The other side of the coin is to address specific IoT security challenges at any weak links such as IoT devices where some specific security patterns can help.

Table 2 shows which concerns regarding security and privacy for IoT are addressed by each of the 36 primary studies. When we compare the number of primary studies to the number of candidate papers we first found while doing the automatic search, there is a big difference. This means that security and IoT are popular keywords in many publications but "security patterns" for IoT is not.

However, we still believe 36 is a reasonable amount, yet it ought to be higher with the goal that security patterns become increasingly frequent and accessible for industry and users who want to develop secure IoT systems.

Table 2 also shows us the distribution of the specificity of the various contributions. We see that most contributions fall under the "Generic" regarding application domains ("Domain specificity" section), which means that a substantial number of papers are adaptable for a widespread of IoT systems. These "Generic" solutions cover the core functionalities of an IoT system, which is why we labeled them "Generic" compared to the domain-specific solutions, which work within a specific domain for a specific purpose (e.g., smart cars, smart meters, and healthcare systems). As we can see, most of the contributions cover authentication, which is a crucial aspect of any system. One may link the amount of authentication coverage to the fact that several smart devices have been hacked due to a lack of authentication (Wright 2020). Even though authentication is the most focused concern in the primary studies, more efforts are needed for end-to-end security, including weak links in IoT systems. We would like to see more of such solutions and solutions for IoT pressing problems, e.g., communication, compatibility, integration, and scalability.

Answering RQ2.2 *How well do the patterns and architectures cover security and privacy issues?*

Table 2 shows a more detailed list of the concerns mentioned previously and what type of application domain the contributions have. We marked the concerns with an "x" if the concern was directly mentioned in the paper. The concern regarding privacy was only marked if it was explicitly mentioned, and not if they handle only the security concerns even they can contribute to privacy coverage.

Figure 5 displays the mapping of our security concerns based on the contribution. We weight how much each (security or privacy) concern was addressed in the primary studies compared to each other. We do so by simply calculating the percentage of how many times a concern was addressed compared to the total number of the times that all concerns were addressed. Note that as shown in Table 2, most primary studies address more than one concern. As Fig. 5 shows, there is a widespread of focus between the security concerns (Confidentiality ~ 16%, Integrity ~ 19%, Availability ~ 8%, Authentication ~ 25%, and Authorization ~ 17%). Privacy (~ 15%) is relatively focused comparing to the security issues in terms of coverage within the primary studies. The low coverage for the availability concern could come from a lack of explicit explanation in the primary studies or availability was not considered in their solutions at all. In the first case, this is

Table 2 Application domains and security & privacy concerns from the primary studies

Primary study #*	f	Domain	Security					P
			C	I	Av	AuthN	AuthZ	
Vithya Vijayalakshmi and Arockiam (2020)	A	Healthcare	X	X	X	X	X	X
Portal et al. (2020)	A	Industrial Environments		X	X	X	X	X
Karaarslan et al. (2020)	A	Laboratorium		X		X		X
Koshy et al. (2020)	A	Smart Home		X		X		X
Attia et al. (2019)	A	Healthcare	X		X			X
Pacheco et al. (2019)	A	Cloud Services			X			X
Pacheco et al. (2018)	A	Smart Water System	X	X	X	X	X	
Ntuli and Abu-Mahfouz (2016)	A	Smart Water System		X		X	X	
Pacheco et al. (2016)	A	Smart Car	X	X			X	
Goncalves et al. (2013)	A	Healthcare			X	X	X	
Ur-Rehman and Zivic (2015)	P	Smart Metering	X	X				X
Vijayakumaran et al. (2020)	A	Generic	X	X		X	X	X
Perera et al. (2020)	A	Generic						X
Dhieb et al. (2020)	A	Generic				X	X	X
Koo et al. (2020)	A	Generic	X	X		X	X	
Robles Enciso et al. (2020)	A	Generic	X	X		X	X	X
Park (2020)	A	Generic	X	X		X		
Tiburski et al. (2019)	A	Generic	X	X		X		
Zhang et al. (2019)	A	Generic				X	X	X
Karmakar et al. (2019)	A	Generic				X	X	
Durresi et al. (2019)	A	Generic	X			X		
Jerald et al. (2019)	A	Generic	X	X		X	X	X
Petroulakis et al. (2019)	A	Generic			X	X		
Witti and Konstantas (2018)	A	Generic	X	X		X	X	X
Zhu and Badr (2018)	A	Generic				X	X	
Alphand et al. (2018)	A	Generic		X			X	X
Ye and Qian (2017)	A	Generic	X	X		X		
Lessa dos Santos et al. (2015)	A	Generic				X		
Vučinić et al. (2015)	A	Generic	X	X		X	X	
Garcia-Morchon et al. (2013)	A	Generic	X	X		X	X	
Pape and Rannenberg (2019)	P	Generic				X		X
Fysarakis et al. (2019)	P	Generic	X	X	X			X
Syed et al. (2018)	P	Generic			X	X	X	X
Pahl et al. (2018)	P	Generic	X	X		X		
Schuß et al. (2018)	P	Generic	X	X	X	X		
Lee and Law (2017)	P	Generic				X	X	
Number of patterns and architectures that address the corresponding quality characteristic			19	22	10	29	20	18

* The paper number is referenced from Table 1

f, focus; P, pattern; A, architecture

C, confidentiality; I, integrity; Av, availability; AuthN, authentication; AuthZ, authorization; P, privacy

comprehensible as availability is a concern whose scope is broader than the only security domain. Indeed, preserving the availability of a system is tightly coupled to the ability of scaling it. Load scalability is the ability of a service to sustain variable workload while fulfilling quality of service (QoS) requirements, possibly by consuming

a variable amount of underlying resources (Ferry et al. 2014). It is a core concern when engineering and designing complex system, and, as a result, many design patterns, including architectural patterns, have been defined in the literature from other fields (e.g., Big data, Cloud computing, large-scale systems, middleware).

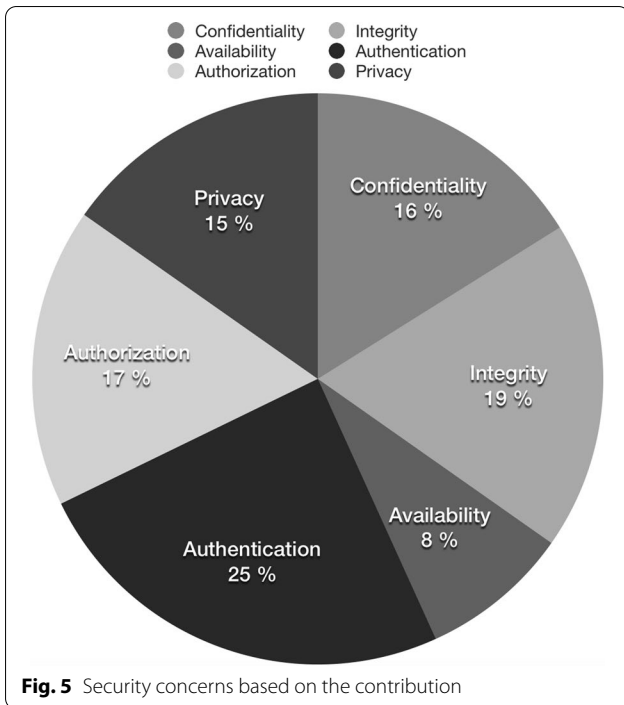


Fig. 5 Security concerns based on the contribution

papers out of seven security pattern papers cover the whole CIA (Confidentiality, Integrity, and Availability) triad, while security architecture papers have two out of 29 papers. Availability is the least covered concern in the primary studies. We are unsure if it is because the contributions focus mostly on authentication, but since many of these systems process or share information, we would argue that the basic CIA triad should be focused. Figure 6 illustrates the different security considerations and privacy, and shows which ones are more focused on in the papers found. Authentication is most focused by the primary studies. This point is understandable because authentication is often the foundation for building other security mechanisms such as for authorization, confidentiality, or privacy. But, the low focus on availability is something that should be drawn attention to because availability is crucial in many IoT systems, especially critical ones.

Another thing to notice is that privacy is considered in 18 out of the 36 papers. This number shows that privacy has gained nearly as much attention as security concerns in the primary studies. As mentioned previously, some papers and concerns may contribute indirectly to privacy, e.g., concerns such as authentication and authorization that verify and provide the correct access to users, which can be one way to preserve users'

Table 2 can give a closer look on how many contributions of patterns and architectures focusing on the various concerns. For patterns, we see that only two

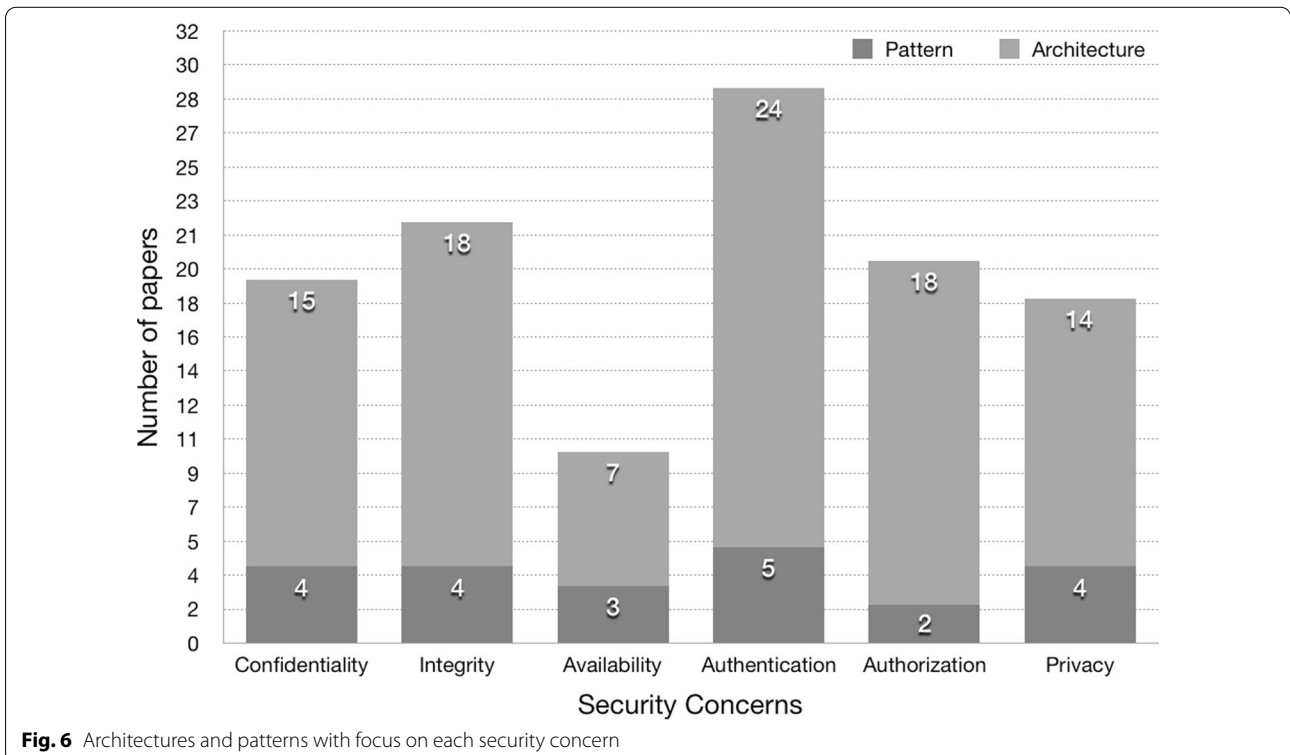


Fig. 6 Architectures and patterns with focus on each security concern

Table 3 IoT security & privacy patterns from the primary studies

Scope affect	Pattern name	Focus	Pattern properties			Paper #
			Intent	Problem	Solution	
AD	Personal data store	P	Users should be able to keep control over their personal data	User may lose control over their data when submitting it to a server	Only store personal data on a personal device	Pape and Ramnberg (2019)
AD	Data isolation at different entities	P	Make it harder to profile users	Data or usage information is stored in one place	Data or usage information are distributed among several entities such that all of the entities can only see a part of the data	Pape and Ramnberg (2019)
AD	Decoupling content and location information visibility	P	Protect the users' locations	Users normally access the services provided by the nearest fog node	Vertically clustering the fog nodes	Pape and Ramnberg (2019)
AD	Added noise measurement obfuscation	P	Avoid revealing personal user information over time such as personal habits	Providers can aggregate usage information to deduce further information about users	Add some noise to the measurements that cancels itself in the long term	Pape and Ramnberg (2019)
AD	Aggregation of data	P	Prevent the leakage of further information because of the aggregation of data	The usage information aggregated over time may reveal further information	Aggregation by a trustworthy provider or by the users themselves, or use a homomorphic encryption (e.g., Paillier 1999)	Pape and Ramnberg (2019)
AD	Aggregation gateway	P	Avoid revealing personal information about the users (e.g., personal habits) over time	When a service provider needs a continuous measurement and adding noise is not acceptable	Use homomorphic encryption (e.g. Paillier 1999) and a trusted third party aggregating the measurements of multiple users	Pape and Ramnberg (2019)
AD	Single point of contact	P	Provide a specialised privacy management	Distributed storage, distributed service providers make it difficult to manage privacy	The cloud computing service can manage and coordinate the storage on different fog nodes by issuing security tokens, authenticate local domain users as an Identity Service Provider, certify attributes as an Attribute Provider, and accept external claims as a Relying Party	Pape and Ramnberg (2019)

Table 3 (continued)

Scope affect	Pattern name	Focus	Pattern properties	Intent	Problem	Solution	Notes	Paper #
AA	The <i>Recipes</i> approach and SPDI patterns	S, P		The generation (and adaptation) of orchestrations in ways that are guaranteed to satisfy required SPDI properties	Adding new devices to an IoT/IoT environment with manually designed composite services is time-consuming and error-prone, but also unfeasible	Different and heterogeneous orchestration models required for IoT and IIoT applications that are guaranteed to satisfy required SPDI properties		Fysarakis et al. (2019)
S	Distributed denial of service in IoT	Av		Misuse Pattern: An attacker intends to make a target unavailable by flooding its resources with a large volume of traffic using IoT devices	How to flood the target with messages from IoT devices to consume all its bandwidth and/or resources making it unavailable for its legitimate users	Use vulnerable IoT devices to create an attack network of infected devices (also called zombies or bots) that can be used to direct huge volumes of data towards a target, performing a DDoS attack on the victim		Syed et al. (2018)
AA	Trusted orchestration management (TOM)	I, AuthN		To manage security (identity, origin, non-repudiation) in distributed autonomous clusters	It is challenging to ensure the identity of hardware devices and software applications, the origin and integrity of data and the contractual nature of orchestration	An architecture pattern based on blockchain		Pahl et al. (2018)
S	Hardware IoT security	C, I, AuthN		To allow even constrained devices to utilize state-of-the-art cryptographic functions	How to ensure that a IoT device can securely communicate through the internet by allowing the upgrade the device's cryptographic functions independent from its micro-controller	Use exchangeable cryptographic co-processors to secure IoT devices		Schulz et al. (2018)
S	Secure logger	C, Ac		To record and encrypt server events (Lee and Law 2017), or to securely maintain log on the gateway (Ur-Rehman and Zivic 2015)	Attackers can discover sensitive information through system logs (Dougherty et al. 2009)	The data is logged in a secure format, typically by encrypting the data (Dougherty et al. 2009)		Lee and Law (2017); Ur-Rehman and Zivic (2015)

Table 3 (continued)

Scope affect	Pattern name	Focus	Pattern properties			Notes	Paper #
			Intent	Problem	Solution		
S	Secure directory	I, AuthZ	To ensure that attackers cannot manipulate the files used during the execution of a program	Attackers can manipulate files used during the execution of a program	First, utilize the pathname canonicalization pattern to insure the file is valid. If the file is valid then check that it is secure (Dougherty et al. 2009)	Lee and Law (2017)	
S	Secure adapter pattern	AuthN, AuthZ	To verify the authorization of an IoT device before saving its data to database (Lee and Law 2017)	Improper saving of sensor data	Convert the interface of an existing class into a more convenient interface, while preserving the security of the adapted entities (Fernandez-Bugli- oni 2013)	Lee and Law (2017)	
S	Exception manager pattern	AV	To process all the exception in data communication with mobile phone	The system has a security exception while sending data to mobile phone application	The Security Exception Manager will wrap the exception	Lee and Law (2017)	
S	Input validation pattern	C, I, Av	To ensure all the data input by user is valid and without any malicious text	SQL injection and overflow attacks	Receive the user data and pass the data to Input-Validation for validating correctness of the user data	Lee and Law (2017)	
AA	Secure remote readout	C, I, P	A remote entity (e.g., a utility) needs to know the status of commodity consumption on regular basis	Measurements from the gateway to the remote entity need to be transmitted securely.	The gateway uses cryptographic mechanisms with the help of a dedicated hardware (Security Module). The security module provides cryptographic functionalities, such as, en-/decryption, digital signatures, key generation and secure key storage	Ur-Rehman and Zivic (2015)	
AD	Key manager	C	To perform the task of key management securely	NA	NA	Ur-Rehman and Zivic (2015)	

Table 3 (continued)

Scope affect	Pattern name	Focus	Pattern properties			Notes	Paper #
			Intent	Problem	Solution		
AD	Wakeup service	A	To react to the connection establishment from the remote readout center for pull readout operation	NA	NA	This pattern is only mentioned	Ur-Rehman and Zivic (2015)
AD	Transport layer security	C, I	For the transport layer security (TLS) operations	NA	NA	This pattern is only mentioned	Ur-Rehman and Zivic (2015)

* AA, App arch; AD, App design; S, system

NA, not available

[#]The paper number is referenced from Table 1

C, confidentiality; I, integrity; Av, availability; Ac, accountability; AuthN, authentication; AuthZ, authorization; P, privacy; SPD, security, privacy, dependability and interoperability

privacy. But, we only count for privacy if a primary study does mention privacy explicitly.

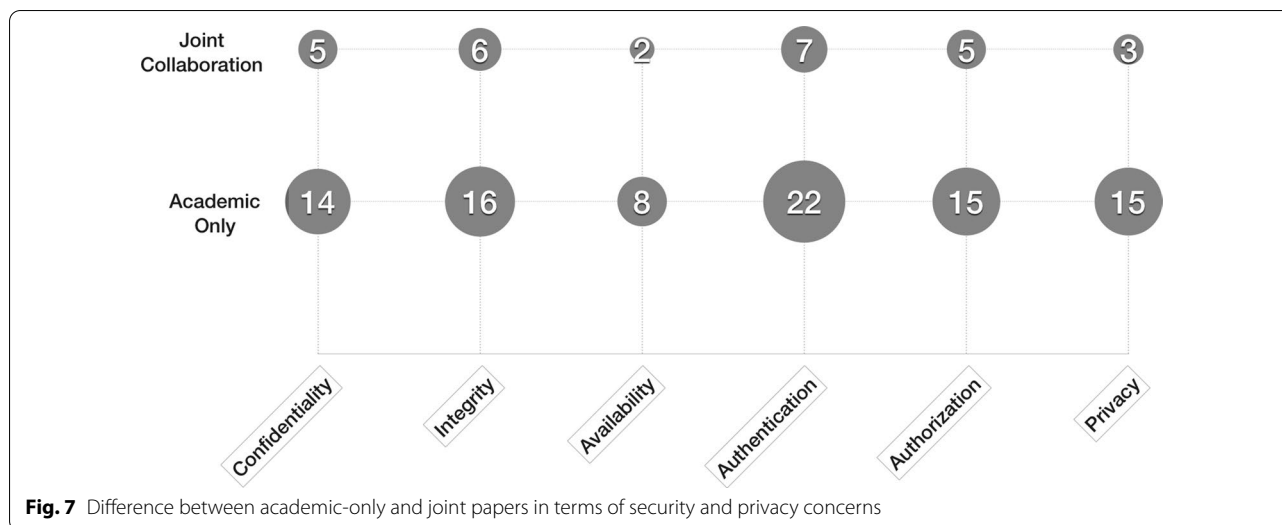
Table 3 shows the IoT security and privacy patterns that are presented in the primary studies. It is worth to note that there is one primary study (Pape and Rannenberg 2019) dedicated to IoT privacy patterns. There are seven patterns for IoT privacy presented in Pape and Rannenberg (2019), which describe different possibilities of privacy violation and the corresponding solutions. We summarize these patterns according to the main elements of security pattern in Table 3. There is another paper that even presents a misuse pattern (Syed et al. 2018). Paper Syed et al. (2018) shows a misuse pattern for Distributed Denial of Service (DDoS) in IoT. They specify appropriate countermeasures for mitigating it, contributing to a specific problem in many IoT systems. Paper Fysarakis et al. (2019) discusses a pattern-driven framework solution to encode dependencies between the security concerns mentioned in “Security and privacy concerns” section. More specifically, paper Fysarakis et al. (2019) presents orchestration models required for IoT and IIoT applications to guarantee quality properties including security, privacy. In the same direction but more on the trustfulness, paper Pahl et al. (2018) proposes an architecture pattern based on blockchain to ensure the identity of hardware devices and software applications, the origin and integrity of data and the contractual nature of orchestration. There is only one paper (Schuß et al. 2018) that proposes a pattern at the hardware layer for IoT security. Schuß et al. (2018) show a pattern to secure the device through hardware, by implementing exchangeable cryptographic co-processors. This paper provides security features that can be implemented to a general IoT system, but it requires changes or additions to the hardware. The hardware-based approach in Schuß et al. (2018) aims at allowing even constrained devices to utilize state-of-the-art cryptographic functions.

While the papers mentioned so far present IoT-specific patterns, the last two papers (Lee and Law 2017; Ur-Rehman and Zivic 2015) in Table 3 focus more on how generic security patterns can be applied for IoT. For example, both of them show how the well-known Secure Logger pattern can be used in IoT. Paper Lee and Law (2017) shows multiple patterns in which they describe and explain some usage areas, but they do not show results in these usage areas. It is more for cataloging purposes including other generic security patterns such as Secure Directory, Secure Adapter Pattern, Exception Manager Pattern, and Input Validation Pattern. Paper Ur-Rehman and Zivic (2015) presents the patterns that are adopted for smart metering systems. The Secure Remote Readout pattern is presented in details in Ur-Rehman

and Zivic (2015). The other patterns are name checked only such as Secure Logger, Key Manager, Wakeup Service, and Transport Layer Security.

As mentioned in the previous section, patterns target more specific parts of an IoT system, which also makes it easier to implement a pattern for that section of the system. In most cases, architectures are harder to implement/adopt because they propose a solution for multiple parts or the whole system but often lack security details for specific parts. We discuss some representative examples of the papers we found that explicitly address, propose, or use security architectures such as Vithya Vijayalakshmi and Arockiam (2020), Wittl and Konstantas (2018) and Pacheco et al. (2018). Paper Vithya Vijayalakshmi and Arockiam (2020) discusses an architecture that protects the data security at all the layers of data flow, the transmission of data is essential in this contribution. Paper Wittl and Konstantas (2018) shows architectures in use-cases where they apply and discuss how they are used and the results. Paper Wittl and Konstantas (2018) also explains how architecture can help securing a smart city while preserving citizens’ privacy in that city. A good example of security architecture can be found in paper Pacheco et al. (2018) by Pacheco et al. (2018), which proposes a security framework for a smart water system. That paper displays security issues at most of the IoT layers and proposes security algorithms for these issues to make developers consider security early rather than an ad-hoc or afterthought manner.

Answering RQ2.3 *What application domains have been addressed by the security patterns and architectures?* From Table 2 we see that nine primary studies have presented the application of IoT security patterns/architectures for some specific IoT application domains. The specific IoT application domains can help our analysis in the way they elaborate on the issues and how to mitigate them. Explicitly mentioning IoT application domain has the tendency to show that the patterns can be applied in the domain and can address the requirements in this IoT domain. Some patterns could be more important for some specific domains. For example, for smart city applications, patterns for scalability is important. For e-health, patterns for privacy are important. The primary studies that do explicitly present IoT application domains would address more clearly the IoT-specific requirements or challenges. The domain-specific solutions are created for the domains mentioned, but they may still be applicable in other domains. However, these domains usually take the initiative to incorporate IoT, which explains why these areas have specific solutions before others. We also saw that many of these domain-specific studies had graphical figures describing their contribution to show how they work or the different layers of their architectures.



We consider that domain-specific contributions may not necessarily have a more significant impact on IoT security, but it is better portrayed when having a real case scenario or issue. Both the generic and specific domain contributions cover approximately three security concerns per paper, so they both stand approximately equally strong in security concerns coverage. We believe these domain-specific contributions are getting more attention, but it may still not be a better solution than the general solutions that can apply to more systems or handle more generic issues. It is still good to see more security patterns and architectures in real cases to better grasp the contribution and the issues around these domains.

Table 2 can give us some ideas on any difference in terms of addressing security and privacy concerns between the papers by academic authors and the papers authored by both academia and industry. The joint papers on average cover $\sim 3, 2$ concerns per paper, while the “academic-only” papers on average cover $\sim 3, 3$ concerns per paper. We see that both types of paper cover at least over half of our security concerns on average. To better compare the difference between academic-only papers and joint papers in terms of addressing security and privacy concerns, we visualize the number of papers addressing each concern in Fig. 7. The first glance at Fig. 7 may give us an impression that the papers from academia have a broader coverage than the joint. This impression makes sense because academic-only papers are nearly three times more than joint papers. However, the number of academic-only papers addressing privacy (15) is five times the number of joint papers addressing privacy (three). Would this comparison imply that privacy (compared to other concerns) has gained more focus in academic-only papers than in industry-oriented papers?

On the other hand, the number of academic-only papers addressing availability (eight) is four times the number of joint papers addressing availability (two). Would this comparison imply that availability has also gained more focus in academic-only papers than industry-oriented papers? The data that we have so far is not significant to make any strong statement to answer these questions. As previously mentioned, we do, however, want to highlight joint papers as more practical for industry. If we compare the amounts of academic and joint papers, we see that the number of joint papers is still low. We hope the number of joint papers will grow in the years to come with the current trend.

In terms of validation, implementation and execution testing, five (Portal et al. 2020; Karaarslan et al. 2020; Koshy et al. 2020; Attia et al. 2019; Pacheco et al. 2016) out of the nine domain-specific contributions do testing to verify their contribution in some form, while the generic domain contributions have 16 out of 24 papers doing testing, or some form of validation or analysis of a case. These numbers can be found in Table 4 representing “[Categorization of security pattern research](#)” section and “[IoT architecture](#)” section and by “testing”; we are referring to item C3 (research implementation/validation). We also see from this table that there are limited number of papers that discuss their purpose with their contribution. Four papers from the domain-specific category and 12 from the general domain category specified their purpose (item C1). However for describing their work with figures and diagrams we found 30 contributions (10 specific, 20 general) where in average the domain-specific studies have a higher ratio of including figures (item C2).

Table 4 List of papers cross referenced from “Categorization of security pattern research” section and “IoT architecture” section

Primary study #	Categorization of security pattern research			IoT architecture							
	C1	C2	C3	Perception	Network		Application				
				L1	L2	L3	L4	L5	L6	L7	
Vijayakumaran et al. (2020)		✓	✓						✓	✓	✓
Vithya Vijayalakshmi and Arockiam (2020)		✓		✓	✓			✓	✓	✓	✓
Portal et al. (2020)		✓	✓	✓	✓	✓					
Karaarslan et al. (2020)		✓	✓	✓	✓					✓	
Perera et al. (2020)			✓							✓	
Dhieb et al. (2020)		✓	✓	✓	✓	✓					
Koo et al. (2020)		✓	✓	✓	✓	✓	✓	✓	✓		
Robles Enciso et al. (2020)		✓	✓	✓	✓	✓	✓				
Park (2020)			✓		✓	✓					
Koshy et al. (2020)		✓	✓	✓	✓	✓					
Attia et al. (2019)		✓	✓	✓	✓					✓	
Pape and Rannenber (2019)		✓	✓	✓	✓	✓	✓				
Fysarakis et al. (2019)	✓	✓		✓	✓					✓	
Tiburski et al. (2019)	✓	✓	✓	✓							
Zhang et al. (2019)		✓		✓	✓					✓	
Karmakar et al. (2019)		✓		✓	✓					✓	
Durresi et al. (2019)	✓	✓		✓	✓	✓					
Jerald et al. (2019)	✓	✓	✓	✓	✓			✓		✓	
Petroulakis et al. (2019)		✓		✓	✓					✓	
Syed et al. (2018)	✓	✓		✓	✓					✓	
Witti and Konstantas (2018)		✓	✓	✓	✓					✓	
Pahl et al. (2018)			✓		✓	✓					
Zhu and Badr (2018)	✓	✓	✓	✓	✓	✓					
Schuß et al. (2018)	✓			✓							
Alphand et al. (2018)	✓	✓	✓	✓	✓					✓	
Pacheco et al. (2019)		✓		✓	✓					✓	
Lee and Law (2017)	✓	✓		✓	✓		✓			✓	
Ye and Qian (2017)	✓	✓	✓		✓						
Pacheco et al. (2018)		✓		✓	✓					✓	
Ntuli and Abu-Mahfouz (2016)	✓	✓		✓	✓					✓	
Pacheco et al. (2016)	✓	✓	✓	✓	✓					✓	✓
Lessa dos Santos et al. (2015)	✓	✓	✓		✓						
Vučinić et al. (2015)	✓	✓	✓	✓	✓						
Ur-Rehman and Zivic (2015)	✓	✓		✓	✓	✓	✓			✓	
Garcia-Morchon et al. (2013)					✓						
Goncalves et al. (2013)	✓									✓	
Total (✓):	16	30	21	28	31	11	5	4	21	3	

*The paper number is referenced from Table 1

✓ = the contribution specifies the items from the taxonomy

Table 4 also shows where the primary studies operate in the different layers of the IoT architecture presented in “IoT architecture” section. If we look at the numbers from the three-layer IoT architecture point of view, all three layers perception, network, and application have

been almost completely covered by the different primary studies. However, the seven-layer IoT World Forum Reference Model of the IoT architecture can offer a closer view. We can see that the studies that explicitly address specific IoT application domains again have a higher

average (4,33 layers per contribution) when it comes to layer coverage while general papers display a lower number (2,96 layers per contribution). In total, we see the coverage of 3,3 layers per contribution, which seems a little low considering there are seven layers in the architecture from the World Forum Reference Model (Juxtology 2018). In particular, we found that most of the primary studies do not work in all the layers, but rather operate in the Physical Devices and Controller (L1), Connectivity (L2), and Application (L6) layers. There are four layers that have lower coverage in terms of the number of primary studies addressing IoT security challenges in those layers: Edge Computing (L3), and especially, Data Accumulation (L4), Data Abstraction (L5), Collaboration and Processes (L7).

Gaps and limitations (RQ3)

This section gives *our answers to the RQ3.1 and RQ3.2* that are supported by the findings presented above. **RQ3.1**—*What are the current limitations of the IoT security patterns and architectures research?* **RQ3.2**—*What research directions could be recommended for tackling the current limitations?* Although there is a spike in the number of primary studies on IoT security patterns and architectures recently as presented in our answer for RQ1.1, our analyses show that IoT security patterns and architectures research is still in its beginning stages. This topic is yet to bloom, both in the industrial and academic universes. There are fundamental gaps and open issues to be handled.

The last decade was only the beginning of research efforts

One of the main limitations is that research on security patterns is still relatively “young” for IoT domain and premature, e.g., in terms of addressing all the different levels of IoT architecture reference model as presented in Table 4, proper documentation and usage areas, as well as usage examples. Before conducting the review, we expected to see how existing security patterns being applied/adopted for IoT, and even more if new security patterns specific for IoT had emerged. But, based on the results of our review so far, we can say that the last decade has only marked the beginning of the research effort in this direction. The lack of evaluation in use cases or application in case studies as presented in our answer for RQ2.3 is one of the indicators of the premature work in most of the primary studies. Most of the contributions in the primary studies would only be ranked at the low levels (less than level five) in terms of the technology

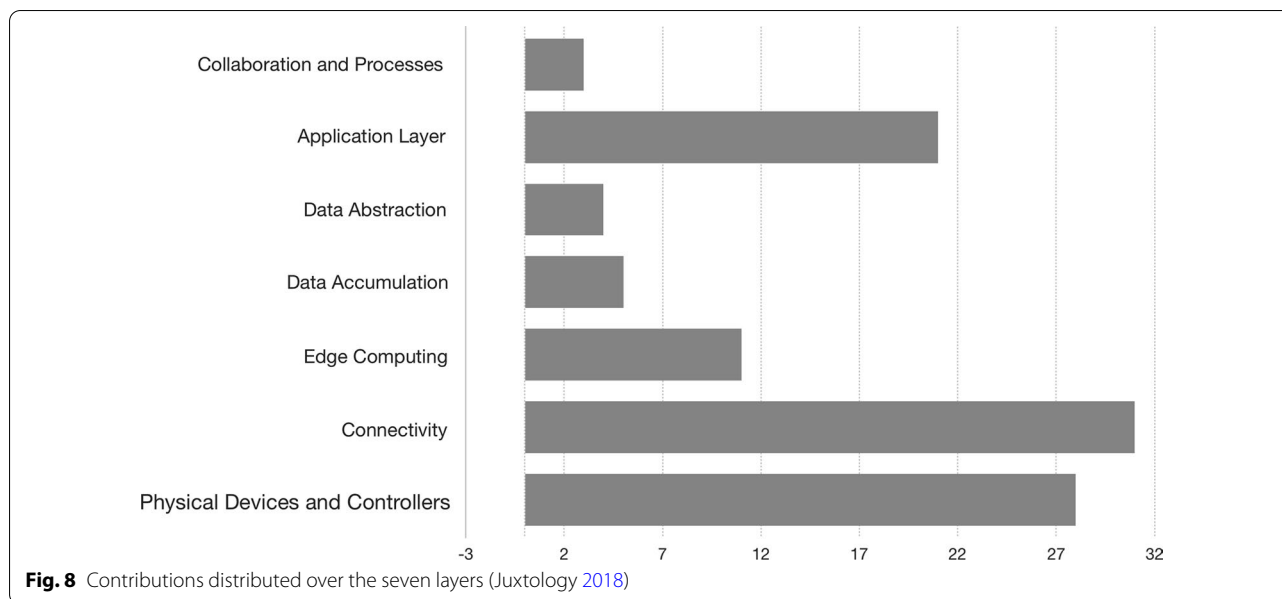
readiness levels (TRL).¹⁹ We believe that (empirical) evaluations on the application of security patterns in IoT can make a substantial positive impact if more contributed to this research area. Empirical studies can provide more insights for any potential adopters of patterns to create more secure systems, or at least find a proven solution for a common problem.

Security patterns have proven to be very valuable for practitioners, especially non-security experts to adopt and build secure (IT) systems (Schumacher et al. 2013; Fernandez-Buglioni 2013). We would expect a similar impact of using security patterns in building secure IoT systems. Security patterns can help to mitigate the lack of knowledge from developers without security expertise, who are often under time-to-market pressure and as a result may contribute to more breaches and malicious usage, leading to more catastrophic incidents. Because, security patterns consist of domain-independent time-proven security knowledge, and expertise, they should be helpful, especially for addressing such limitations early in the development of IoT systems. We believe that security patterns can continue to be very valuable for practitioners, especially non-security experts, in building secure IoT systems. It would be even more so with a systematic understanding of different security patterns for addressing the heterogeneity of the IoT domain that our study could be a starting point for more comprehensive IoT domains. In other words, new research efforts could aim at building a catalog of security (and privacy) patterns more specifically and systematically for IoT.

The lack of addressing IoT-specific security and privacy challenges

Compatibility and complexity issues in IoT are other limitations that make security patterns and architectures less practical. An IoT system often makes use of multiple devices connected to a system(s) via a network(s). For example, one device could use a of protocols to communicate between nearby networks and other protocols to communicate with the service provider via IP. The heterogeneity of various communication protocols often used in IoT raises more security issues, which even get worse for complex IoT systems. So far, we have found patterns and architectures for mostly general issues and some specific issues that should work for their stated purposes. However, we have not encountered research that fulfills both types of issues that security patterns and architectures handle. In other words, we have not seen any approach that proposes a (systematic) top-down

¹⁹ The use of TRLs in the Horizon 2020 Work Programmes (<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/faq/2890>).



application of security patterns, first at the architectural level, then to more low-level details for addressing specific challenges in the heterogeneity of IoT, for example sometimes ad-hoc network, and weak links caused by tiny IoT devices.

From the results (see Table 2), we found that the quantity of security pattern approaches is less than the number of security architectures for IoT, and way too few compared to the initial numbers of the search results displayed in Fig. 2. The quantity of existing papers that directly address security patterns for IoT is very low comparing to the explosion of the IoT as estimated by Gartner.²⁰ From the papers found, very few had characterized the patterns or architectures accordingly to the taxonomy categorization we constructed or characterized clearly in what layers of the IoT World Forum Reference Model²¹ the contribution tackles (Fig. 8). We would, therefore, recommend that further research that should address thoroughly and systematically security pattern aspects for IoT systems.

The status of addressing the top ten most common vulnerabilities within IoT

We also accumulated how the research contributions in the primary studies handle the different issues presented by the OWASP IoT top ten vulnerabilities list (OWASP

2018) as shown in Table 5. This extraction was done to highlight more of this topic's gaps to see how the existing contributions handle the top ten most common vulnerabilities within IoT (OWASP 2018). As we see from the extraction, vulnerabilities such as Insecure Network Services (I2), Insecure Ecosystem Interfaces (I3), and Insecure Data Transfer and Storage (I7) are the most covered vulnerabilities by the contributions. This spread of coverage is fair in terms of what the contributions present. Most of the solutions found are either in the communication part of the system or when interacting with multiple devices/systems. Most of the contributions are also descriptions proposing high-level architectural solutions and not detailing actual (physical) IoT products or devices. The other types of vulnerabilities, such as Weak, Guessable, or Hardcoded Passwords (I1), Insecure Default Settings (I9), Lack of Physical Hardening (I10), and so forth were not visible in the contributions of the primary studies. I2, I3, and I7 are appropriate vulnerabilities that these contributions should mitigate, however Insufficient Privacy Protection (I6) and Lack of Device Management (I8) should be more highlighted due to its natural occurrence within security patterns and architectures.

The need for new security patterns specifically for IoT

Other directions we recommend is to keep up the research on existing patterns and architectures, but also find out new security patterns specifically for IoT. The dominance of academia-only and a few joint collaboration in IoT security pattern research (see our answer to RQ1.3) suggests that there should be even

²⁰ Gartner, November 2018 (<https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends>).

²¹ Juxtology - IoT: Architecture (<https://www.m2mology.com/iot-transformation/iot-world-forum/>).

Table 5 List of issues compared to the OWASP IoT top ten

Primary study #	OWASP IoT top ten									
	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10
Vijayakumaran et al. (2020)		✓	✓	✓		✓	✓			
Vithya Vijayalakshmi and Arockiam (2020)		✓	✓			✓	✓			
Portal et al. (2020)		✓	✓			✓	✓			
Karaarslan et al. (2020)		✓	✓			X	✓			
Perera et al. (2020)			✓			✓	✓			
Dhieb et al. (2020)		✓	✓			✓	✓	✓		
Koo et al. (2020)	✓	X	✓			X	✓	✓		
Robles Enciso et al. (2020)		✓	✓			✓	✓			
Park (2020)		✓					✓			
Koshy et al. (2020)		✓	✓			✓	✓			
Attia et al. (2019)		✓	X		X	✓	X	✓		✓
Pape and Rannenber (2019)						✓	✓			
Fysarakis et al. (2019)		✓	✓			✓	✓	✓	✓	✓
Tiburski et al. (2019)	✓		✓	✓	✓			✓		✓
Zhang et al. (2019)		✓	✓			✓	✓			
Karmakar et al. (2019)		✓	✓				✓	✓		✓
Durresi et al. (2019)		✓	✓		X			✓		
Jerald et al. (2019)		✓	✓				✓			
Petroulakis et al. (2019)	✓	✓	✓		X	X		✓		
Syed et al. (2018)				X		✓		✓		✓
Witti and Konstantas (2018)	✓	✓				✓	✓			
Pahl et al. (2018)			✓				✓			
Zhu and Badr (2018)		✓	✓			X				
Schulz et al. (2018)	✓			✓		X				
Alphand et al. (2018)		✓	✓			✓				
Pacheco et al. (2019)		✓	✓	✓		✓	✓	✓		✓
Lee and Law (2017)	✓		✓			X	✓			
Ye and Qian (2017)		✓	✓				✓	✓		✓
Pacheco et al. (2018)		✓	✓			X	✓	✓		
Ntuli and Abu-Mahfouz (2016)		✓	✓	✓			✓			✓
Pacheco et al. (2016)			✓	✓		X	✓	✓	✓	✓
Lessa dos Santos et al. (2015)			✓			X				
Vučinić et al. (2015)		✓	✓		X		✓			
Ur-Rehman and Zivic (2015)				✓		✓	✓			
Garcia-Morchon et al. (2013)		✓	✓			X	✓			✓
Goncalves et al. (2013)	✓		✓			X	✓			✓
Total papers that handle the issue (✓):	7	24	29	7	1	16	27	13	2	11

* The paper number is referenced from Table 1

✓ = handles the issue

X = lack of description about how it is handled

= not mentioned

more collaboration between academia and industry. Especially since the IoT market is blossoming and making the industry more aware, there should be approaches that are more practical and closer to the needs in the industry. This research should be both of

research nature but should also aim to create an interest for industry and business owners. This way, we can get more test cases, gain more knowledge, and spread awareness around IoT security patterns in general. However, the ultimate goal of promoting IoT security

patterns is to make it easier to improve and implement security features early in the development of IoT systems.

Related work

There have been some recent surveys focusing on different aspects of IoT engineering, from the deployment support (Nguyen et al. 2019) to actuation conflict management (Lavirotte et al. 2020). In Nguyen et al. (2019), the authors present the state of the art of IoT deployment approaches in which most approaches do not properly support software deployment and orchestration at the tiny IoT device level. Besides, trustworthiness aspects including security were not addressed properly in the existing approaches for IoT systems deployment and orchestration. The new challenges in the IoT domain can also be seen in the physical layer of IoT actuators. The SMS in Lavirotte et al. (2020) brings attention to the risk of actuation effects to safety and trustworthiness, and analyzes approaches for actuation conflicts management. However, these two recent surveys do not focus on security patterns for IoT.

There exist some other surveys that have addressed IoT security and IoT patterns, but none has systematically, specifically investigated security pattern approaches for IoT. Oracevic et al. (2017) surveyed IoT security. They want to shed light on this topic and spread awareness, with examples of IoT security solutions. The authors provide different measures on different levels to secure the systems but do not go into details. They also do not offer any form of architectures or patterns to solve common recurring problems for IoT security. Nguyen et al. (2015) has also reviewed security patterns-based approaches for new systems design and development. However, the reviewed approaches are not specific for IoT systems, which the focus of this work.

Washizaki et al. (2020) present a collection of papers that either describe IoT architectures or design patterns, or both. They also classify the patterns that are being used in detail as well as in which paper. They present a security column and specify which papers from their study have patterns that cover security. We looked through these papers, but not all of the papers did meet our criteria described in “[Inclusion and exclusion criteria](#)” section. The papers from Washizaki et al. (2020) that we analyzed and included as primary studies are Pape and Rannenber (2019), Pahl et al. (2018), Lee and Law (2017) and Ntuli and Abu-Mahfouz (2016).

Reinfurt et al. (2016) give details of IoT patterns by investigating a large number of production-ready IoT offerings to extract recurring proven solution principles into patterns. These patterns show and describe how to

help other individuals to understand different aspects of IoT, and also make it easier.

Qanbari et al. (2016) elaborates on how to design, build, and engineer applications for IoT systems and have created patterns to do these steps in an IoT system. They do not highlight security as one of their focus points, which is our main concern for this paper.

In general, these studies' results not only address the functional aspects of IoT patterns but also some quality aspects, such as security and development, that we even considered in our work. However, they were not systematically and explicitly conducted to analyze the patterns and architectures for IoT security similar to our work. Note that we have clearly defined the scope of our SLR, which only considered peer-reviewed publications, not white papers from the industry. Thus, our SLR reports state of the art in IoT security pattern research, not including the state of practice in the industry.

Threats to validity

We mainly found the primary studies of this work from the database search process. The search features provided by the five online publication databases are very different from each other. We had to adapt our search string to make use of the provided search features of the publication databases. We tried to use the keywords and built search strings that were not too strict to obtain as many relevant papers as possible. However, it would be impossible to have perfect search strings for the database search process.

There is a possibility that we missed some studies that should have been included in the final set of primary studies. We have tried to mitigate possible missing primary studies of the database search process by the manual search process. While doing snowballing, we saw again some primary studies that we already found from the database search process. Removing the duplicates, we managed to get six more new primary studies that have not been found from the database search process. There were some other relevant papers from snowballing, but they finally did not pass our selection criteria. These few studies may have fulfilled our criteria but may have failed to detail what they did or did not detail enough to include them according to our criteria confidently. We ended our search and selection process in the beginning of December 2020, which means that our review does not completely cover all the publications in 2020, but a major part of them.

The primary studies that passed our selection criteria could still have limitations that make their contributions unreliable or flawed. Because many of the

contributions do not have test cases or examples, it can be hard to know if the patterns and architectures do what they are supposed to. It also creates uncertainty regarding how good the patterns preserve or contain the security in already existing systems. To mitigate this risk, we conducted cross-checks between at least two reviewers for some papers in doubt to remove any papers that do not have enough scientific contributions according to our selection criteria.

Conclusions

In this paper, we have presented our systematic review on patterns and architectures for IoT security. After systematically recognizing and reviewing 36 primary studies out of thousands of relevant papers in this domain, we have discovered that there is a slight rise in the number of publications addressing security patterns and architectures in the two recent years. However, our analysis has shown that security patterns are relatively “young” for the IoT domain and we have found more papers with main contributions categorized as architectures rather than patterns. This indicates that more efforts are needed in terms of formalization, proper documentation and adoption. We have not seen any approaches that combine architectural patterns or even IoT security reference architectures with other design patterns. Similarly, we have not seen architectural patterns or IoT security reference architectures referring to any design pattern they would be composed of. This includes patterns at the IoT “weak links”: the network and IoT devices levels. Most of the primary studies do not work in all the seven layers of the IoT World Forum Reference Model for IoT architecture. They mainly operate in the Physical Devices and Controller (L1), Connectivity (L2), and Application (L6) layers. There are four layers that have little coverage in terms of patterns and architectures for addressing IoT security challenges: Edge Computing (L3), Data Accumulation (L4), Data Abstraction (L5), Collaboration and Processes (L7). We also accumulated how the research contributions in the primary studies handle the different issues presented by the OWASP IoT top ten vulnerabilities list.

New IoT systems development should concentrate more on tending to security, which can be improved with progressively relevant security patterns to apply and reuse. In other words, we need to promote the utilization of patterns for IoT security (and privacy) by design. To make security patterns for IoT approaches more viable, we consider the research collaboration between academia and industry is key in this domain. Security patterns in literature can be researched and applied in developing secure IoT systems with

industrial context. Vice versa, experiences gained from securing industrial IoT systems can help to improve existing security patterns for IoT, or even new ones can emerge.

Abbreviations

IoT: Internet of Things; RQ: Research questions; SLR: Systematic literature review.

Acknowledgements

The research leading to these results has partially received funding from the European Commission's H2020 Programme under the grant agreement numbers 958363 (Dat4.ZERO), and 958357 (InterQ).

Author contributions

All authors contributed to all the steps of conducting this work and writing this manuscript. All the authors read and approved the final manuscript.

Availability of data and materials

All the data of our work is available in Google Drive <https://drive.google.com/drive/folders/19CbTTYauf4ijpcSSIN0yySZLz8QgscJ?usp=sharing>.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Author details

¹Capgemini, Oslo, Norway. ²SINTEF, Oslo, Norway. ³Université Côte d'Azur, I3S/INRIA Kairos, Sophia Antipolis, France.

Received: 30 April 2021 Accepted: 17 November 2021

Published online: 05 January 2022

References

- Alphand O, Amoretti M, Claeys T, Dall'Asta S, Duda A, Ferrari G, Rousseau F, Tourancheau B, Veltri L, Zanichelli F (2018) IoTChain: a blockchain security architecture for the Internet of Things, vol. 2018-April, pp 1–6. <https://doi.org/10.1109/WCNC.2018.8377385>
- Attia O, Khoufi I, Laouiti A, Adjih C (2019) An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application. In: 2019 10th IFIP international conference on new technologies, mobility and security (NTMS), pp 1–5. <https://doi.org/10.1109/NTMS.2019.8763849>
- Borgia E, Gomes DG, Lagesse B, Lea RJ, Puccinelli D (2016) Special issue on “internet of things: research challenges and solutions”. *Comput Commun* 89:1–4
- Ciccozzi F, Crnkovic I, Di Ruscio D, Malavolta I, Pelliccione P, Spalazzese R (2017) Model-driven engineering for mission-critical iot systems. *IEEE Softw* 34(1):46–53
- Covington MJ, Carskadden R (2013) Threat implications of the internet of things. In: 2013 5th international conference on cyber conflict (CYCON 2013), pp 1–12
- Create-IoT (2018) Deliverable D6.02—Recommendations for commonalities and interoperability profiles of IoT platforms. https://european-iot-pilots.eu/wp-content/uploads/2018/11/D06_02_WP06_H2020_CREATE-IoT_Final.pdf. Accessed 30 Sept 2021
- Dhieb N, Ghazzai H, Besbes H, Massoud Y (2020) Scalable and secure architecture for distributed iot systems. In: 2020 IEEE technology engineering

- management conference (TEMSCON), pp 1–6. <https://doi.org/10.1109/TEMSCON47658.2020.9140108>
- Dougherty C, Sayre K, Seacord RC, Svoboda D, Togashi K (2009) Secure design patterns. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst
- Durresi M, Subashi A, Durresi A, Barolli L, Uchida K (2019) Secure communication architecture for internet of things using smartphones and multi-access edge computing in environment monitoring. *J Ambient Intell Humaniz Comput* 10(4):1631–1640. <https://doi.org/10.1007/s12652-018-0759-6>
- Federal Trade Commission (1999) How to comply with the privacy of consumer financial information rule of the Gramm-Leach-Bliley Act. <https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm>. Accessed 29 Sept 2020
- Fernandez-Buglioni E (2013) Security patterns in practice: designing secure architectures using software patterns. Wiley, Hoboken
- Ferry N, Brataas G, Rossini A, Chauvel F, Solberg A (2014) Towards bridging the gap between scalability and elasticity. *CLOSER* 10:0004975307460751
- Fysarakis K, Spanoudakis G, Petroulakis N, Soulatos O, Broring A, Marktscheffel T (2019) Architectural patterns for secure iot orchestrations. In: 2019 Global IoT Summit (GIOTS), pp 1–6. <https://doi.org/10.1109/GIOTS.2019.8766425>
- Gamma E, Helm R, Johnson R, Vlissides JM (1994) Design patterns: elements of reusable object-oriented software, 1st edn. Addison-Wesley Professional, Boston
- Garcia-Morchon O, Keoh SL, Kumar S, Moreno-Sanchez P, Vidal-Meca F, Ziegeldorf JH (2013) Securing the ip-based internet of things with hip and dtls. In: Proceedings of the sixth ACM conference on security and privacy in wireless and mobile networks. *WiSec '13*. Association for Computing Machinery, New York, NY, USA, pp 119–124. <https://doi.org/10.1145/2462096.2462117>
- Goncalves F, Macedo J, Nicolau MJ, Santos A (2013) Security architecture for mobile e-health applications in medication control. In: 2013 21st international conference on software, telecommunications and computer networks—(SoftCOM 2013), pp 1–8. <https://doi.org/10.1109/SoftCOM.2013.6671901>
- IEEE SA, S.A. (2018) IEEE draft standard for an architectural framework for the internet of things (IoT). IEEE P2413/D0.4.5, December 2018, pp 1–264
- Jerald AV, Rabara SA, Arun Gnana Raj A (2019) Secured architecture for integrated iot enabled smart services. *Int J Recent Technol Eng* 8(3):7384–7393. <https://doi.org/10.35940/ijrte.C6145.098319>
- Juxtology (2018) IoT: architecture. <https://www.m2mology.com/iot-transformation/iot-world-forum/>. Accessed 27 July 2020
- Karaarslan E, Karabacak E, Cetinkaya C (2020) Design and implementation of sdn-based secure architecture for iot-lab. In: Hemanth DJ, Kose U (eds) *Artificial intelligence and applied mathematics in engineering problems*. Springer, Cham, pp 877–885
- Karmakar KK, Varadharajan V, Nepal S, Tupakula U (2019) SDN enabled secure IoT architecture, pp 581–585. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85066971444&partnerID=40&md5=c0f52e2ce49d38dad5d181190e28e795>
- Kitchenham BA, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report. <https://doi.org/10.1145/2372233.2372235>
- Kitchenham BA, Budgen D, Brereton OP (2011) Using mapping studies as the basis for further research—a participant-observer case study. *Inf Softw Technol* 53(6):638–651. <https://doi.org/10.1016/j.infsof.2010.12.011> (Special Section: Best papers from the APSEC)
- Koo J, Oh SR, Lee SH, Kim YG (2020) Security architecture for cloud-based command and control system in iot environment. *Appl Sci* 10:1035. <https://doi.org/10.3390/app10031035>
- Koshy P, Babu S, Manoj BS (2020) Sliding window blockchain architecture for internet of things. *IEEE Internet Things J* 7(4):3338–3348. <https://doi.org/10.1109/JIOT.2020.2967119>
- Kuhn DR, Hu VC, Polk WT, Chang S-J (2001) NIST SP 800-32, introduction to public key technology and the federal PKI infrastructure. National Institute of Standards & Technology, p 54. <https://doi.org/10.6028/NIST.SP800-32>
- Lavrotte S, Rocher G, Tigli J, Gonnin T (2020) IoT-based systems actuation conflicts management towards DevOps: a systematic mapping study. In: Proceedings of the 5th international conference on internet of things, big data and security, vol 1. *IoTBDSS*, pp 227–234. SciTePress. <https://doi.org/10.5220/0009355102270234>. INSTICC
- Lee W, Law P (2017) A case study in applying security design patterns for iot software system. In: 2017 international conference on applied system innovation (ICASI), pp 1162–1165. <https://doi.org/10.1109/ICASI.2017.7988402>
- Lessa dos Santos G, Guimaraes VT, da Cunha Rodrigues G, Granville LZ, Tarouco LMR (2015) A dtls-based security architecture for the internet of things. In: 2015 IEEE symposium on computers and communication (ISCC), pp 809–815. <https://doi.org/10.1109/ISCC.2015.7405613>
- Nguyen PH, Yskout K, Heyman T, Klein J, Scandariato R, Le Traon Y (2015) Sospa: a system of security design patterns for systematically engineering secure systems. In: 2015 ACM/IEEE 18th international conference on model driven engineering languages and systems (MODELS), pp 246–255. <https://doi.org/10.1109/MODELS.2015.7338255>
- Nguyen PH, Kramer M, Klein J, Traon YL (2015) An extensive systematic review on the model-driven development of secure systems. *Inf Softw Technol* 68:62–81. <https://doi.org/10.1016/j.infsof.2015.08.006>
- Nguyen PH, Ali S, Yue T (2017) Model-based security engineering for cyber-physical systems: a systematic mapping study. *Inf Softw Technol* 83:116–135. <https://doi.org/10.1016/j.infsof.2016.11.004>
- Nguyen P, Ferry N, Erdogan G, Song H, Lavrotte S, Tigli J, Solberg A (2019) Advances in deployment and orchestration approaches for IoT—a systematic review. In: 2019 IEEE international congress on Internet of Things (ICIOT), pp 53–60. <https://doi.org/10.1109/ICIOT.2019.00021>
- Ntuli N, Abu-Mahfouz A (2016) A simple security architecture for smart water management system. *Procedia Comput Sci* 83:1164–1169. <https://doi.org/10.1016/j.procs.2016.04.239>. The 7th international conference on ambient systems, networks and technologies (ANT 2016)/The 6th international conference on sustainable energy information technology (SEIT-2016)/Affiliated workshops
- Office for Civil Rights (2013) Summary of the HIPAA security rule. <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>. Accessed 29 Sept 2020
- Oravecic A, Dilek S, Ozdemir S (2017) Security in internet of things: a survey. In: 2017 international symposium on networks, computers and communications (ISNCC), pp 1–6. <https://doi.org/10.1109/ISNCC.2017.8072001>
- OWASP (2018) Internet of Things (IoT) Top 10 2018. <https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf>. Accessed 30 Sept 2020
- Pacheco J, Ibarra D, Vijay A, Hariri S (2018) IoT security framework for smart water system. In: 2017 IEEE/ACS 14th international conference on computer systems and applications (AICCSA), vol 2017-October, pp 1285–1292. <https://doi.org/10.1109/AICCSA.2017.85>
- Pacheco J, Satam S, Hariri S, Grijalva C, Berkenbrock H (2016) IoT security development framework for building trustworthy smart car services, pp 237–242. <https://doi.org/10.1109/ISI.2016.7745481>
- Pacheco J, Tunc C, Hariri S (2019) Security framework for IoT cloud services, vol 2018-November. <https://doi.org/10.1109/AICCSA.2018.8612808>
- Pahl C, Ioini NE, Helmer S, Lee B (2018) An architecture pattern for trusted orchestration in iot edge clouds. In: 2018 third international conference on fog and mobile edge computing (FMEC), pp 63–70. <https://doi.org/10.1109/FMEC.2018.8364046>
- Paillier P (1999) Public-key cryptosystems based on composite degree residuosity classes. In: Stern J (ed) *Advances in cryptology—EUROCRYPT '99*. Springer, Berlin, Heidelberg, pp 223–238
- Pape S, Rannenberg K (2019) Applying privacy patterns to the internet of things (iot) architecture. *Mobile Netw Appl* 24(3):925–933. <https://doi.org/10.1007/s11036-018-1148-2>
- Park C (2020) Security architecture for secure multicast coap applications. *IEEE Internet Things J* 7(4):3441–3452. <https://doi.org/10.1109/JIOT.2020.2970175>
- Perera C, Barhamji M, Bandara AK, Ajmal M, Price B, Nuseibeh B (2020) Designing privacy-aware internet of things applications. *Inf Sci* 512:238–257. <https://doi.org/10.1016/j.ins.2019.09.061>
- Petersen K, Vakkalanka S, Kuzniarz L (2015) Guidelines for conducting systematic mapping studies in software engineering: an update. *Inf Softw Technol* 64:1–18
- Petroulakis NE, Lakka E, Sakic E, Kulkarni V, Fysarakis K, Somarakis I, Serra J, Sanabria-Russo L, Pau D, Falchetto M, Presenza D, Marktscheffel T, Ramanatas K, Mekikis P, Ciechomski L, Waledzik K (2019) Semiotics architectural

- framework: End-to-end security, connectivity and interoperability for industrial iot. In: 2019 Global IoT Summit (GloTS), pp 1–6. <https://doi.org/10.1109/GIOTS.2019.8766399>
- Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV (2016) The quest for privacy in the internet of things. *IEEE Cloud Comput* 3(2):36–45
- Portal G, de Matos E, Hessel F (2020) An edge decentralized security architecture for industrial iot applications. In: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), pp 1–6. <https://doi.org/10.1109/WF-IoT48130.2020.9221176>
- Qanbari S, Pezeshki S, Raisi R, Mahdizadeh S, Rahimzadeh R, Behinaein N, Mahmoudi F, Ayoubzadeh S, Fazlali P, Roshani K, Yaghini A, Amiri M, Farivar-moheb A, Zamani A, Dustdar S (2016) IoT design patterns: computational constructs to design, build and engineer edge applications. In: 2016 IEEE first international conference on Internet-of-Things design and implementation (IoTDI), pp 277–282. <https://doi.org/10.1109/IoTDI.2015.18>
- Rajmohan T, Nguyen PH, Ferry N (2020) Research landscape of patterns and architectures for iot security: a systematic review. In: 2020 46th Euromicro conference on software engineering and advanced applications (SEAA), pp 463–470. <https://doi.org/10.1109/SEAA51224.2020.00079>
- Reinfurt L, Breitenbücher U, Falkenthal M, Leymann F, Riegg A (2016) Internet of things patterns. In: Proceedings of the 21st European conference on pattern languages of programs. EuroPlop '16. ACM, New York, NY, USA. <https://doi.org/10.1145/33011784.3011789>
- Richa E (2021) Iot: security issues and challenges. In: Senjyu T, Mahalle PN, Perumal T, Joshi A (eds) Information and communication technology for intelligent systems. Springer, Singapore, pp 87–96
- Robles Enciso A, Zarca A, Garcia Carrillo D, Hernandez-Ramos J, Bernal Bernabe J, Skarmeta A, Matheu Garcia SN (2020) Security architecture for defining and enforcing security profiles in dlt/sdn-based iot systems. *Sensors* 20:1882. <https://doi.org/10.3390/s20071882>
- Roman R, Najera P, Lopez J (2011) Securing the internet of things. *Computer* 44(9):51–58
- Ross R, McEvilley M, Oren J (2016) NIST SP 800-160, systems security engineering considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. National Institute of Standards & Technology, p 243. <https://doi.org/10.6028/NIST.SP.800-160v1>
- Schmidt DC, Buschmann F (2003) Patterns, frameworks, and middleware: their synergistic relationships. In: 25th international conference on software engineering, 2003. Proceedings, pp 694–704
- Schneier B (2017) Iot security: what's plan b? *IEEE Secur Privacy* 15(05):96. <https://doi.org/10.1109/MSP.2017.3681066>
- Schumacher M, Fernandez-Buglioni E, Hybertson D, Buschmann F, Sommerlad P (2013) Security patterns: integrating security and systems engineering. Wiley, Hoboken
- Schuß M, Iber J, Dobaj J, Kreiner C, Boano CA, Römer K (2018) Iot device security the hard(ware) way. In: Proceedings of the 23rd European conference on pattern languages of programs. EuroPlop '18. ACM, New York, NY, USA, pp 20–1204. <https://doi.org/10.1145/3282308.3282329>
- Steel C, Nagappan R (2006) Core security patterns: best practices and strategies for J2EE, web services, and identity management. Pearson Education, London
- Syed MH, Fernandez EB, Moreno J (2018) A misuse pattern for ddos in the iot. In: Proceedings of the 23rd European conference on pattern languages of programs. EuroPlop '18. ACM, New York, NY, USA, pp 34–1345. <https://doi.org/10.1145/3282308.3282343>
- Tiburski RT, Moratelli CR, Johann SF, Neves MV, Matos ED, Amaral LA, Hessel F (2019) Lightweight security architecture based on embedded virtualization and trust mechanisms for iot edge devices. *IEEE Commun Mag* 57(2):67–73. <https://doi.org/10.1109/MCOM.2018.1701047>
- Tran NK, Sheng QZ, Babar MA, Yao L (2017) Searching the web of things: state of the art, challenges, and solutions. *ACM Comput Surv (CSUR)* 50(4):55
- Ur-Rehman O, Zivic N (2015) Secure design patterns for security in smart metering systems. In: 2015 IEEE European modelling symposium (EMS), pp 278–283. <https://doi.org/10.1109/EMS.2015.49>
- Vijayakumaran C, Senthil M, Manickavasagam B (2020) A reliable next generation cyber security architecture for industrial internet of things environment. *Int J Electr Comput Eng: IJECE* 10:387. <https://doi.org/10.11591/ijece.v10i1.pp387-395>
- Vithya Vijayalakshmi A, Arockiam L (2020) A secured architecture for iot health-care system. In: Pandian AP, Senjyu T, Islam SMS, Wang H (eds) Proceeding of the international conference on computer networks, big data and IoT (ICCB-I-2018). Springer, Cham, pp 904–911
- Vučinić M, Tourancheau B, Rousseau F, Duda A, Damon L, Guizzetti R (2015) Oscar: object security architecture for the internet of things. *Ad Hoc Netw* 32:3–16. <https://doi.org/10.1016/j.adhoc.2014.12.005> (**Internet of Things security and privacy: design methods and optimization**)
- Washizaki H, Ogata S, Hazeyama A, Okubo T, Fernandez EB, Yoshioka N (2020) Landscape of architecture and design patterns for iot systems. In: IEEE Internet of Things Journal 2020 (early Access), p 1. <https://doi.org/10.1109/IJOT.2020.3003528>
- Washizaki H, Xia T, Kamata N, Fukazawa Y, Kanuka H, Yamaoto D, Yoshino M, Okubo T, Ogata S, Kaiya H, Kato T, Hazeyama A, Tanaka T, Yoshioka N, Priyalakshmi G (2018) Taxonomy and literature survey of security pattern research. In: 2018 IEEE conference on application, information and network security (AINS), pp 87–92. <https://doi.org/10.1109/AINS.2018.8631465>
- Williams-Grut O (2018) Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank. <https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4?r=US&IR=T>. Accessed 20 Aug 2020
- Witti M, Konstantas D (2018) A secure and privacy-preserving internet of things framework for smart city. In: Proceedings of the 6th international conference on information technology: IoT and smart city. ICIT 2018. Association for Computing Machinery, New York, NY, USA, pp 145–150. <https://doi.org/10.1145/3301551.3301607>
- Wohlin C (2014) Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th international conference on evaluation and assessment in software engineering. ACM, p 38
- Wright M (2020) Default passwords banned for smart devices as part of hacking crackdown. <https://www.telegraph.co.uk/news/2020/01/27/default-passwords-banned-smart-devices-part-hacking-crackdown/>. Accessed 20 June 2020
- Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J (2013) Taxonomy for description of cross-domain attacks on cps. In: Proceedings of the 2nd ACM international conference on high confidence networked systems. HiCoNS '13. Association for Computing Machinery, New York, NY, USA, pp 135–142. <https://doi.org/10.1145/2461446.2461465>
- Ye F, Qian Y (2017) A security architecture for networked Internet of Things devices, vol 2018-January, pp 1–6. <https://doi.org/10.1109/GLOCOM.2017.8254021>
- Yskout K, Heyman T, Scandariato R, Joosen W (2006) A system of security patterns. CW Reports. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.142.4538>
- Zhang J, Jin H, Gong L, Cao J, Gu Z (2019) Overview of IoT security architecture, pp 338–345. <https://doi.org/10.1109/DSC.2019.00058>
- Zhu X, Badr Y (2018) Fog computing security architecture for the internet of things using blockchain-based social networks. In: 2018 IEEE international conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp 1361–1366

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.