A Systematic Mapping of Patterns and Architectures for IoT Security

Tanusan Rajmohan[1], Phu H. Nguyen[2] and Nicolas Ferry[2]
[1]*University of Oslo (UiO), Oslo, Norway*
[2]*SINTEF, Oslo, Norway*

Keywords: IoT, Security, Privacy, Architecture, Patterns, Review, Survey.

Abstract: We have entered a vast digital revolution of the IoT era when everything is connected. The popularity of IoT applications makes security for IoT of paramount importance. Security patterns are based on domain-independent time-proven security knowledge and expertise. Can they be applied to IoT? We aim to draw a research landscape of patterns and architectures for IoT security by conducting a systematic mapping study. From more than a thousand of relevant papers, we have systematically identified and analyzed 24 papers that have been published around patterns for IoT security (and privacy). Our analysis shows that there is a rise in the number of publications addressing security patterns in the two recent years. However, there are gaps in this research area that can be filled in to promote the use of patterns for IoT security and privacy.

1 INTRODUCTION

The Internet of Things (IoT) is becoming increasingly popular. We can see that every "thing" is getting smarter and connected, from smartphones, smart cars, to smart energy grids, smart cities. According to Gartner, 25 billion connected things will be in use by 2021, producing immense volumes of data[1]. 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)

Most of the critical infrastructures, such as energy, water, transport, and healthcare, have already been or will be IoT-empowered. IoT security issues will "affect not only bits and bytes" but also "flesh and blood" (Schneier, 2017). Without reliable security in place, users will not trust IoT devices and related services as discussed in (Nguyen et al., 2018; Nguyen et al., 2019) because attacks and malfunctions in IoT-based critical infrastructures may outweigh any of their benefits (Roman et al., 2011), (Hany and Wills, 2020). Security design patterns could be considered as reusable security design bricks upon which sound and secure systems can be built. From security engineering's point of view, one of the best practices is using patterns to guide security at each stage of the development process (Schumacher et al., 2013). Security patterns are based on domain-independent, time-proven security knowledge, and expertise. Books and catalogs of security patterns such as (Schumacher et al., 2013), (Fernandez-Buglioni, 2013), (Nguyen et al., 2015), (Steel and Nagappan, 2006) are supposed to be helpful for users to solve security challenges by using time-proven security knowledge and expertise. However, the IoT age may introduce new security challenges that existing approaches and methods cannot address. Have security patterns been researched and applied to IoT?

To figure out a research landscape of existing approaches around patterns for security in IoT, we have conducted a Systematic Mapping Study (SMS). Our SMS has three main objectives. First, we want to give a summary of the existing publications around patterns for IoT security (and privacy). Second, by examining the current patterns and approaches, we can recognize gaps in the state-of-the-art. Also, we want to explore which developmental level the existing patterns for IoT are describing. We are particularly interested in their method and how advanced the patterns are, especially in addressing IoT security. Third, based on the results, we propose new research activities to fill the gaps for supporting security in modern IoT systems. We conducted our SMS following

[1]https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends, November 2018

Rajmohan, T., Nguyen, P. and Ferry, N.
A Systematic Mapping of Patterns and Architectures for IoT Security.
DOI: 10.5220/0009583001380149
In *Proceedings of the 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020)*, pages 138-149
ISBN: 978-989-758-426-8

the latest guidelines from (Petersen et al., 2015). The main contributions of this work are our answers to the following *Research Questions* (RQs).

- **RQ1:** *What are the publication trends of the research on patterns and architecture for IoT security?*
- **RQ2:** *What is the existing research on patterns for IoT security, and how advanced is it?*
- **RQ3:** *What are the open issues to be further investigated in this field?*

We have systematically filtered a large number of relevant papers from five central online publication databases, and a manual search process, to finally obtain a set of *twenty-four* (24) primary studies. We extracted and synthesized data from the primary studies to answer our RQs. The results show that there is a rise in the number of publications addressing security patterns and architectures for IoT in the two recent years. However, there are gaps in this research area that can be filled to promote the use of patterns for IoT security and privacy.

In the remainder of this paper: Section 2 gives some background definitions. In Section 3, we present our SMS approach. To facilitate data extraction and comparison, Section 4 describes our classification schemes for the primary studies. We present the results of our SMS in Section 5. Related work is discussed in Section 6. Finally, we conclude the paper with summarizing the main findings in Section 7.

2 BACKGROUND

In this section, we give the definitions of SMS (2.1), design patterns (2.2), security design patterns (2.3), and security architecture (2.4) that were used to define the scope of this work.

2.1 Systematic Mapping Study

An SMS is a kind of secondary research, which is "a study that reviews all the primary studies relating to a specific research question to integrate/synthesize evidence related to a specific research question." More specifically, an SMS gives "a broad review of primary studies in a specific topic area that aims to identify what evidence is available on the topic." (Kitchenham et al., 2011)

2.2 Design Pattern

The conventional explanation for a design pattern is that it is a reusable solution to a standard reoccurring problem in software design. A pattern is usually general so that it can be reused, and it is a proven solution to solve a design problem. A design pattern is not a finished implementation that can be directly used, but more a strategy or a template for how to solve a problem that can serve in different situations. (Gamma et al., 1994) (Fernandez-Buglioni, 2013).

2.3 Security Design Pattern

A Security Design Pattern (aka. security pattern) is defined as: "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." (Schumacher et al., 2013).

Because security patterns and design patterns mostly impact a specific part of an IoT system, we also want to look at a reusable solution for a high-level perspective. This is why we include security architecture because architectures will concern large-scale components and global properties and mechanisms of a system.

2.4 Security Architecture

National Institute of Standards and Technology (NIST) describes security architecture as "the design artifact that describes how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose of maintaining the system's quality attributes: confidentiality, integrity, availability, accountability, and assurance services." (Ron Ross, 2016)

In this paper, we include framework as a prebuilt general or special purpose architecture that is designed to be extended. This is why we would say that the architecture is the design of a structure. In contrast, a framework is the architecture foundation. We, therefore, include framework as a "sub-part" of the architecture and suggest that framework solutions are similar to an architecture solution.

3 OUR SYSTEMATIC MAPPING APPROACH

We conducted our SMS by following the most recent principles (Petersen et al., 2015), and other guidelines from (Kitchenham, 2004). With the specific context and motivation exhibited in Section 1, we describe

our RQs for this paper in Section 3.1. We clarify the inclusion criteria for selecting primary studies by explicitly characterizing the extent of our SMS and lessen possible bias in our selection process, in Section 3.2. Section 3.3 shows our search strategy to find the primary studies for answering the RQs.

3.1 Research Questions

This SMS aims to answer the three RQs presented in Section **1**. Each is extended with sub-questions.

RQ1 includes three sub-RQs. **RQ1.1 -** *In which years were the primary studies published?* Answering this question allows us to know when this research topic started to get attention as well as how recent the research on this topic is. The publication trend can give an indicator of how much attention security patterns and architectures for IoT get from the research community. **RQ1.2 -** *What are the targeted domains (e.g., IoT, Network, Cloud, and Software Engineering(SE)) and which venue type (i.e., Journal, Conference/Workshop) were the primary studies published as?* Answering this question allows us to know what the target domain was for each paper. This is especially important when security patterns are something that can crossover several related research areas. The type of paper can give some clues on the maturity of the primary study. Journal papers normally report progressively mature studies compared to papers published at conferences. **RQ1.3 -** *How is the collaboration between industry and academia on this topic?* We classify a paper as *academic* if all the authors are affiliated with a university or a research institute. Likewise, we classify papers as *industrial* if all the associated authors are with a company, and sort the papers as *both* if there is a collaboration. Answering RQ1.3 will show the collaboration level between the industry and academia. It also indicates the interest and needs of security patterns in industry.

RQ2 has two sub-RQs. **RQ2.1 -** *Are there any papers explicitly addressing, proposing, describing, or using security patterns or architectures for IoT systems?* Answering this RQs allows us to examine the support of security pattern and architecture approaches towards secure IoT systems. **RQ2.2 -** *How do the patterns/architectures in the primary studies support IoT security?* Answering RQ2.2 shows us how the primary studies use patterns and architectures, and for what purpose. It also allows us to assess the characteristics of the primary studies in security patterns and architectures for IoT.

RQ3 also has two sub-RQs. **RQ3.1 -** *What are the open issues of IoT security pattern research?* **RQ3.2 -** *What research directions could be recommended for tackling the open issues?* These RQs help to suggest potential directions for future work.

3.2 Inclusion and Exclusion Criteria

In light of the RQs and the extent of our study presented in Section 1, we predefined the inclusion and exclusion criteria to reduce bias in our procedure of search and selection of primary studies. The primary studies must meet ALL the following inclusion criteria (IC):

1. (IC1) A primary study must contain security patterns (one or more) or architectures in some form relevant for an IoT system.
2. (IC2) A primary study must be specifically within the area of IoT, either in a generally applicable domain or in a specific application domain of IoT.
3. (IC3) The paper presents security concerns in system design, architecture, or infrastructure.
4. (IC4) The paper discusses some form of a pattern or architecture (/reusable method) that can be applied to IoT.

We excluded and filtered out papers that are not written in English, as well as papers that only are available as extended abstracts, posters, or presentations (not full version).

3.3 Search and Selection Strategy

The search strategy used in this thesis is a mix of automatic and manual search as well as snowballing as shown by (Nguyen et al., 2015), to exhaustively search for IoT security pattern papers. Where the goal is to find the most relevant papers and, therefore, to find as many primary IoT security pattern papers as possible. Fig. 1 shows an overview of the search and selection process with the results for each step, which we describe in the following sections.

3.3.1 Database Search

Utilizing the online inquiry elements of accessible publication databases is the most well-known approach to scan for essential primary studies when directing auxiliary studies (Petersen et al., 2015). We used five of the accessible publication databases IEEE Xplore[2], ACM Digital Library[3], ScienceDirect[4], Web of Knowledge (ISI)[5], and Scopus[6] to

[2]https://ieeexplore.ieee.org
[3]https://dlnext.acm.org
[4]https://sciencedirect.com/
[5]http://apps.webofknowledge.com
[6]https://scopus.com

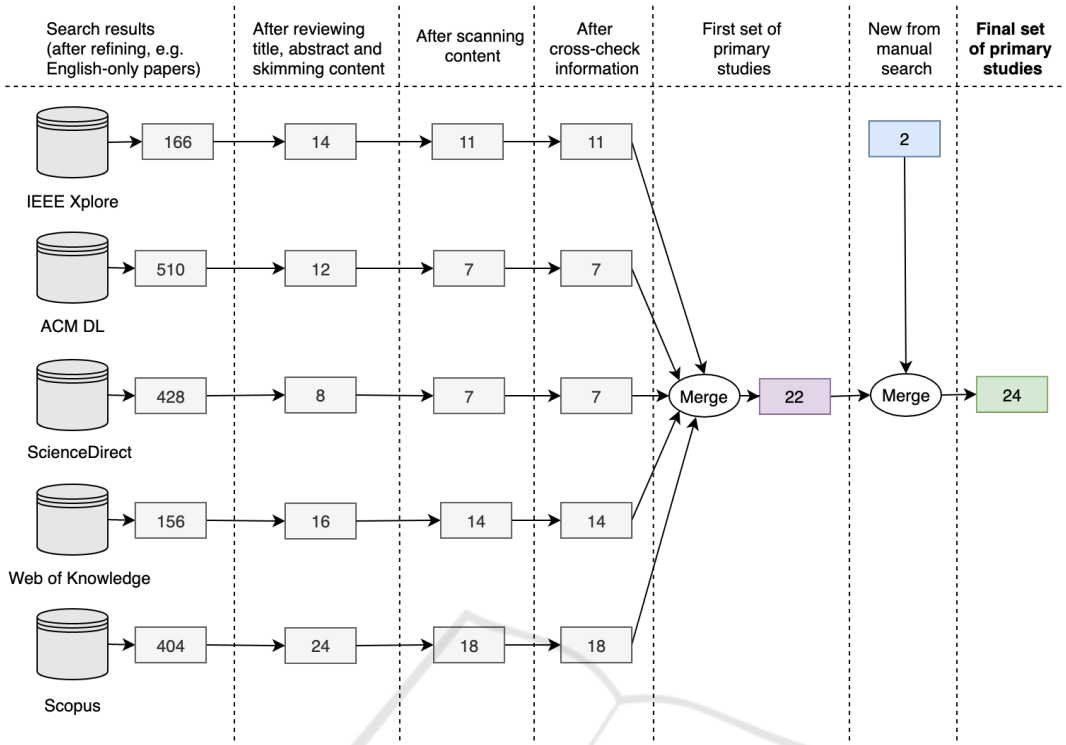

Figure 1: Overview of the search and selection steps.

search for potential primary studies. We did not use Google Scholar, Researchgate, or SpringerLink. Scopus and ACM DL already index SpringerLink[7] (Tran et al., 2017). Google Scholar and ResearchGate return all kinds of papers, in which our five chosen databases should have covered peer-reviewed articles. Google Scholar also returns many non-peer-reviewed and non-English papers. The five selected databases contain peer-reviewed articles, which provide advanced search functions. Following the guidelines from (Kitchenham, 2004), based on the research questions and keywords used in some related articles, we have created the search keywords. The following keywords are the final set used as a search query. The query was tweaked to fit all search engines.

(*"Internet of Things"* **OR** *"IoT"* **OR**
"Cyber Physical Systems" **OR** *"CPS"* **OR**
"Web of things" **OR** *"WOT"*)
AND
(*"Security Pattern"* **OR** *"Design Pattern"* **OR**
"Security Design Pattern" **OR** *"Security Architecture"*)

[7]https://www.springer.com/gp/computer-science/lncs/information-on-abstracting-and-indexing/799288

For each candidate paper, we first reviewed the paper's title and abstract, followed by skimming through the contents. If a candidate paper appears in more than one database, we list them in the other database results. When merging to the first set of primary studies, we combine the results, so we get the correct number of papers without duplicates.

3.3.2 Manual Search

It is unrealistic to ensure the database search results can cover all the relevant papers in our study. We have, therefore, tried to complement the database search by doing a manual search. We began our manual search by initiating a set of IoT security and security pattern studies from published journals and conferences. The conferences and journals we went through to find papers were: The International Conference on the Internet of Things[8], IEEE ICIOT[9], ACM Transactions on Internet of Things (TIOT)[10], and IEEE Internet of Things Journal[11]. After searching through these journals and conferences, we concluded that the papers posted were already found in

[8]https://iot-conference.org/iot2020/
[9]https://conferences.computer.org/iciot/2019/
[10]https://dl.acm.org/journal/tiot
[11]https://ieee-iotj.org/

the database search, or they did not fulfill the inclusion criteria set. Therefore we only found two extra papers that supplemented our primary set with papers from the manual search and increased with two. The manual search also included a snowballing process, but no new primary studies found.

Note that, at every stage of our search and selection process, any candidate papers in doubt were kept to be thoroughly reviewed and crosschecked among the reviewers. Our group discussions have finally yielded a set of 24 primary studies for data extraction and synthesis to answer the RQs[12].

4 TAXONOMY OF THE RESEARCH AREA

In this section, we define a taxonomy of IoT security patterns. The primary purpose of the taxonomy is to extract and compare data from the primary studies so that they can help to answer the RQs. This taxonomy is defined by a *top-down* and *bottom-up* approach. These approaches are strategies commonly used for information processing and knowledge ordering. We have used the top-down method to process information from the literature around IoT, security patterns, IoT architecture, design patterns, and so forth. The bottom-up approach is for extracting data from a test set of primary studies. This test set is the first ten primary studies selected. It helped us to classify and specify the essential techniques and terminology used in the primary studies.

4.1 Domain Specificity

We characterize the Domain Specificity in the same manner as (Washizaki et al., 2019) with minor adjustments. It is essential to examine the applicability and reusability of each IoT security pattern. We divide this into three types: any, general IoT, and specific IoT.

1. **Any.** General systems and software security patterns, as well as design patterns and security architectures that can be adapted to design IoT systems and software if their contexts and problems match the patterns' contexts and challenges.
2. **General IoT.** IoT security and design patterns, as well as security architectures, which apply to any IoT system and software.
3. **Specific IoT.** IoT security and design patterns, as well as security architectures that address specific problem domains (e.g., healthcare) and technical domains (e.g., brain-computer interaction).

[12]Our search and selection process for the primary studies ended late December 2019

4.2 Categorization of Security Pattern and Architecture Research

To specify the domain, security concerns, implementation and modeling, we list some features to sort out the different security patterns and architectures quickly. In such a way that we can see the patterns' or architectures' *purpose*, *quality*, *method*, and *research implementation* as defined in (Washizaki et al., 2018).

- **Purpose.** This includes intended users, and phases of the targeted system and software lifecycle.
- **Quality.** This refers to security characteristics: confidentiality, integrity, availability, authentication, and authorization.
- **Method.** This includes methodology and modeling methods to identify the structure and design of the pattern or architecture.
- **Research Implementation.** This consists of the platform to realize the results of security pattern research, whether the results are automated and encapsulated as a tool, and whether case studies or experiments are conducted to evaluate the results relevant to the original research purpose.

4.3 Design Pattern

Design patterns are similar to security patterns in the way of their structure. Therefore, we will show the core parts that will be in a design pattern, so that the pattern structure is familiar and makes it easier to look for patterns in the primary studies. The following elements often express a design pattern (Joshi, 2014):

- **Name.** Representation of its purpose in a nutshell.
- **Intent.** What the pattern does, short statement to capture essence of the pattern.
- **Problem.** A software design problem under a given system environment.
- **Solution.** A solution to the problem mentioned above.
- **Consequences.** Trade-offs of using a design pattern.

4.4 IoT Architecture

In our taxonomy, we reuse the IoT World Forum Reference Model[13] with minimal modifications. The IoT World Forum Reference Model consists of seven layers:

- **Physical Devices and Controllers.** This layer as the title describes is the physical layer consisting of devices or "things" of the internet of things. The "things", sensors and Edge Node devices are classified within this layer.
- **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.
- **Edge Computing.** This layer is referred to as the layer that brings computation and data storage closer to the location it is needed. "Protocol conversion, routing to higher-layer software functions, and even "fast path" logic for low latency decision making will be implemented at this layer."
- **Data Accumulation.** This layer serves as 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.
- **Data Abstraction.** This is the layer where data is made clear and understandable. This layer 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.
- **Application Layer.** This is the layer where 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.
- **Collaboration and Processes.** This layer presents the 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.

[13] Juxtology - IoT: Architecture

5 RESULTS

Table 1 shows an overview of the primary IoT security pattern and architecture studies. Based on the taxonomy, we have extracted and synthesized the data from the primary studies to answer the RQs.

Table 1: Overview of the primary IoT security pattern studies (sorted by year of publication).

#	*Year*	*Title (click to open the corresponding publication)*	v	f
1	2019	Applying Privacy Patterns to the Internet of Things' (IoT) Architecture	J	P
2	2019	Architectural Patterns for Secure IoT Orchestrations	C	P
3	2019	From internet of threats to internet of things: A cyber security architecture for smart homes	C	A
4	2019	BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network	J	A
5	2019	Lightweight security architecture based on embedded virtualization and trust mechanisms for IoT edge devices	J	A
6	2018	A blockchain-based decentralized security architecture for Iot	C	A
7	2018	A misuse Pattern for DDoS in the IoT	C	P
8	2018	A Secure and Privacy-preserving Internet of Things Framework for Smart City	C	A
9	2018	Applying Security Patterns for authorization of users in IoT Based Applications	C	P
10	2018	Cataloging design patterns for internet of things artifact integration	C	P
11	2018	Design patterns for the industrial Internet of Things	C	P
12	2018	IoT device security the hard(ware) way	C	P
13	2017	A Case Study in Applying Security Design Patterns for IoT Software System	C	P
14	2016	A Simple Security Architecture for Smart Water Management System	J	A
15	2016	A survey on Internet of Things architectures	J	A
16	2015	New Security Architecture for IoT Network	C	A
17	2015	OSCAR: Object security architecture for the Internet of Things	J	A
18	2015	Secure Design Patterns for Security in Smart Metering Systems	C	P
19	2015	Software-security patterns: degree of maturity	C	P
20	2014	A security engineering process for systems of systems using security patterns	C	P
21	2013	HIP Security Architecture for the IP-Based Internet of Things	C	A
22	2013	Securing the IP-based internet of things with HIP and DTLS	C	A
23	2013	Using security patterns to model and analyze security requirements	J	P
24	2011	A natural classification scheme for software security patterns	C	P

[v] Venue type: J = Journal (7), C = Conference (17).
[f] Focus: P = pattern, A = Architecture.

5.1 Publication Trends

In this section, we address the sub-RQs 1.1, 1.2 and 1.3 correspondingly in the following subsections 5.1.1, 5.1.2, and 5.1.3.

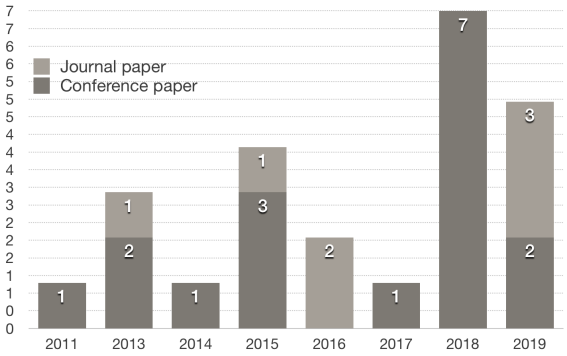

Figure 2: Publications per year, per venue type.

5.1.1 Publication Trend

Fig. 2 displays paper publications within the domain of security patterns and architectures for IoT systems in the last 10 years. As Fig. 2 shows, we can see a rise in the number of IoT security patterns and architectures related publications in the last two years (2018: 7C and 2019: 2C, 3J). The trend in recent years indicates that there is a need for IoT security pattern and architecture research, and more attention to these research areas. The results are a bit lower than expected, but we hope that this trend will keep increasing. Our search process ended in December 2019, and we found five primary studies with our search query that were published in 2019 (2C, 3J).

5.1.2 Publication Venue Types and Target Domains

IoT, with its heterogeneous nature, traverses through different relevant research domains, among which we recognized Software Engineering (SE), Cloud , Network, and recently specialized IoT research domain. (Borgia et al., 2016)

Fig. 3 displays the occurrence of each research domain appearance in the primary studies (SE:4, IoT: 20, Cloud: 4, Network: 6). Note that the publication venues can have several research domains in their calls for papers. Some of the papers overlap in their research domain, *i.e.* almost all the papers fall under the IoT domain and might include another domain. Since we are looking for security patterns and architectures for IoT systems, this may be patterns for specific parts within an IoT system. It can also include patterns and architectures for software that can be applied for IoT systems, which is why we have several domains and why these can overlap considering the numbers in Fig. 3. These numbers do mirror the different ideas of IoT research, with IoT research domain is getting progressively visible. We see the trends of conference papers within each research area is higher

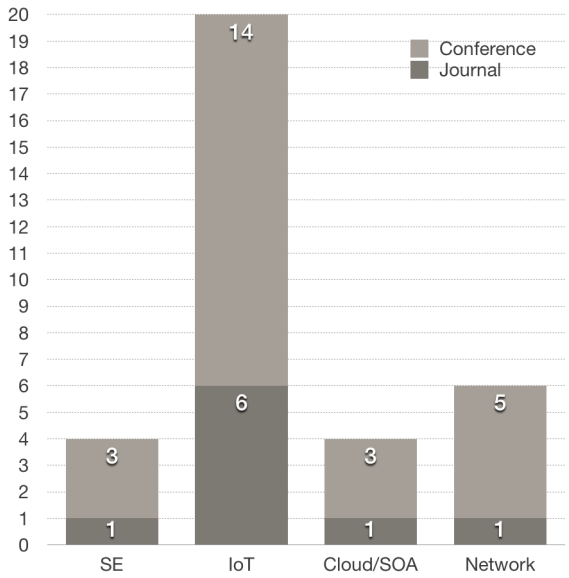

Figure 3: Research topics per publication venue.

than in journals, which is expected. Conference papers tend to gain quick feedback and visibility within the research field. In comparison, it can take years for a journal publication to appear, and the research topic may become outdated. Which explains the numbers in Fig. 2 and Fig. 3. Even though the numbers are low for journal papers, we still hope to see more journal papers, which normally have a more in-depth analysis of the domain.

5.1.3 Author Affiliation Impact

Because IoT systems and devices are widely used and growing in the industry and consumer market, we took a closer look at how the affiliations of the authors are distributed from the primary studies. Fig. 4 shows that a majority of the authors who have published results on IoT security pattern or architecture are from academia ($\sim$ 58%), as expected. While there are no contributions solely from industry, this number is not surprising, considering that industry rarely publishes papers alone. Industry occasionally publishes with the collaboration of academia. We found some papers of this type ($\sim$ 42%). These papers have more implementation examples and testing compared to papers purely from academia, in accordance with *research implementation* from Section 4.2. Almost half of the primary studies are joint papers between academia and industry, which show a promising collaboration level. This is a trend we want to see grow as well as real implementations of the research to show how it is implemented and distributed. We do not expect the industry to publish on their own, which is why we think

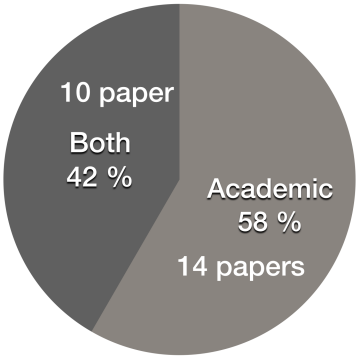

Figure 4: Affiliation trend of authors.

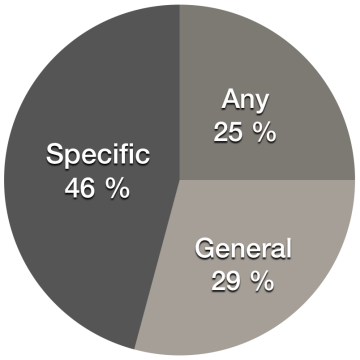

Figure 5: IoT specificity, Section 4.1.

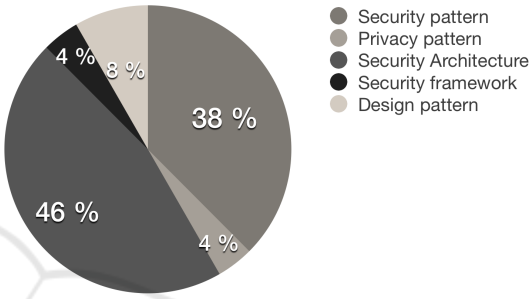

Figure 6: Pattern/architecture categorization.

the numbers for joint papers are reasonably good. We hope that this number keeps growing as well as that they use the patterns and architectures proposed to improve their products, production process, and internal processes that use IoT devices or systems further. We would be interested to see some real implementations or examples of security patterns or architectures usage in the industry in the future.

5.2 The Primary Approaches

We will address the sub-RQs 2.1 and 2.2 correspondingly in the subsections 5.2.1, and 5.2.2. These subsections detail the primary approaches and how advanced they are, especially in addressing security aspects in this section. We outline and depict the illustrations to show findings clearly and understandably, as well as highlight some of the trends within security.

5.2.1 Security Pattern Usage

Fig. 5 illustrates the distribution of papers with regards to the domain specificity of the papers, elaborated in Section 4.1. We see that most of the papers found were in *specific* domains, *i.e.* healthcare, water systems, network communication, manufacturing factories, smart metering, etc. The *general* cases have security patterns for IoT systems, but not a specific or detailed use case. In contrast, *any* cases are just security patterns in general that we think can be applied for any IoT systems.

Out of all the papers we review, we found that 46% of the papers were explicitly discussing or using security patterns for IoT. The other papers either discussed security architectures (38%), privacy pattern (4%), security framework (4%), or design patterns (8%). Fig. 6 shows that out of all the papers found, over half (84% / 88% when framework is included) of the papers use or propose how to use security patterns or architectures either in general or in specific usage areas. This tells us that out of all the papers found (24) there is already a good amount of papers regarding the topic we want to highlight. When we look directly at numbers and compare this to how many papers we initially found when doing the automatic search it is a low number. We still believe this a good amount, but it should be higher so that security patterns become more frequent and accessible for industry and users who want to develop IoT systems (software, hardware, or Cloud).

The papers such as 10, 7, 12, 9, 13, and 18 from Table. 1 are examples of papers we found that explicitly address, propose, or use security patterns. Papers 7, 12, 13, and 18 show patterns in a use case where they apply the pattern and discuss how it is used and what the results are. While papers 9 and 10 show multiple security patterns and explain their usage area, name, intent, problem, solution, and consequence in accordance with design pattern description in Section 4.3. Papers 9 and 10 do not explicitly use the patterns in any way, it is mostly for illustration and cataloging. All these patterns contribute with one or several patterns that have a specific usage area or a generic area.

5.2.2 Supporting IoT Security

To answer this sub-RQ, we look at Fig. 7, where we see that out of all the papers found, 66% discuss security in some form, either by using a security pattern

or suggesting how security can be improved. The remaining 34% discuss privacy, which security helps to improve. Some primary studies give a clear solution, while others propose a possible solution, and some papers have overlapping concerns regarding both security and privacy. To get an elaborate statistic, we look at Fig. 8, which is a figure that crosses results with the help of Sections 4.2 and 4.4. This diagram illustrates how many papers fall into each IoT architecture layer and how many of them concern security and privacy. The security categorization is based on the quality aspect from Section 4.2, where we categorize papers that focus on security characteristics, such as confidentiality, integrity, availability, authentication, and authorization within the security category.

The patterns shown in the papers either propose patterns or architectures that can increase the security of IoT, software, or the Cloud fragment. Some essential papers (7, 12, 13, and 18) from Table. 1 discuss how they keep the security intact by securing the confidentiality, integrity, and availability (CIA). Paper 12 proposes a security pattern for the hardware level that ensures the integrity and confidentiality of the device. While paper 7 shows a misuse pattern that attacks the availability, but they list countermeasures on how to prevent this and maintain the availability. Paper 18 discusses smart metering systems and propose a pattern that especially secures integrity and confidentiality by digitally signing and encrypting the data in transit to ensure security and privacy. Paper 13 shows five patterns that help to provide security through the CIA for different application areas of an IoT system. They propose patterns for input validation, secure logging, secure exception handling, etc.

The data from the papers have been extracted accordingly to the taxonomy to give us meaningful information as well as pinpoint how the papers are relevant and where they contribute. From the IoT architecture, we also saw that most of the papers added to the Physical Devices and Controllers, Connectivity, Edge Computing, and Application layer, which is illustrated in Fig. 8. From the figures referenced through this section, we see that the patterns and architectures help to secure different levels of the architecture as well as the system in itself by focusing on the characteristics mentioned. With the help of our taxonomy, we found 14 papers out of 24 that had both implementation or example and model or methodology description of their architecture or pattern.

5.3 Ideas for Future Research

Here we address the open issues that we believe should be further investigated. We try to illustrate some of the issues and suggest research directions to further improve this domain.

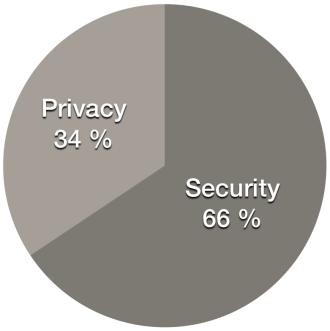

Figure 7: Pattern topic of the papers.

5.3.1 Open Issues

To illustrate the open issues, we crossed the taxonomy criteria of quality to find papers that handle the security characteristics to improve the security with the contribution of the different papers. This gave us the results we can see in Fig. 9, where the main contributions of architectures and patterns from the several patterns show that they mostly propose security related contributions. The reason we still keep the three contributions that do not handle the security characteristics is that they discuss how to improve security patterns in general, securing systems, or do not contribute but rather evaluate patterns or architectures.

We found that the number of security pattern approaches is nearly the same as the number of security architecture patterns for IoT. The number of existing papers that directly address security patterns for IoT is not as high as it should be when considering the estimates of growth, according to Gartner (van der Meulen, 2017). Even among those studies, we have not found any that explicitly and systematically list or show patterns that apply to IoT security.

The open issues of IoT security pattern research, in our opinion, would be the lack of research on the topic already. Even though most of the papers we found discuss security or improves it. This is only a small fraction of what we expected after looking through thousands of papers to find relevant primary studies. We saw that there is a spike in the number of publications within this domain for the last couple of years, and our analysis shows that IoT security pattern research is still in its early stages. In addition to a lack of research, it is harder to produce good quality patterns that are tested and used in the industry. The lack of research may lead to mistakes in the production of these systems that consumers might buy and may end up in catastrophic consequences. This is why we want to promote this type of study to highlight the security

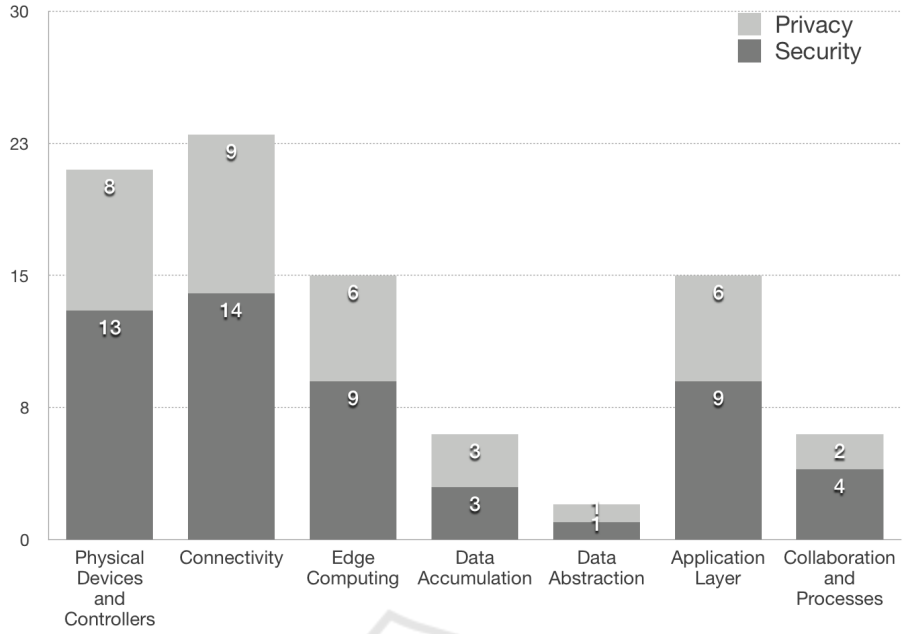

Figure 8: Security and privacy with relation to the IoT architecture from Section 4.4.

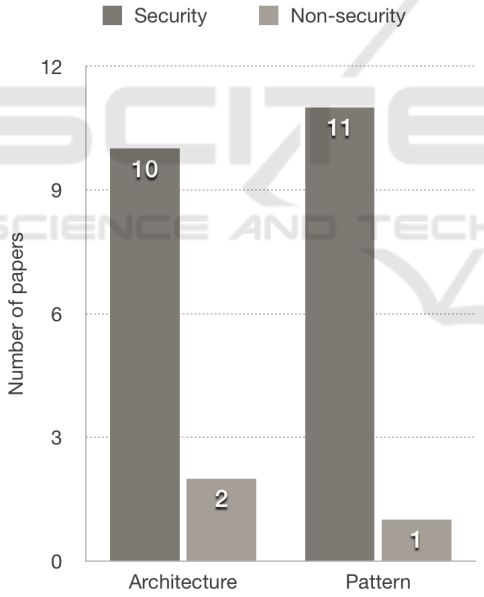

Figure 9: Patterns and architectures in relation to the quality from categorization, Section 4.2.

aspects and make it easier to implement and use security from the beginning, also known as *security by design*. Promoting the use of patterns and architecture for IoT security (and privacy) early and in combination with continuous deployment of security and privacy mechanisms together with IoT applications as presented by (Ferry et al., 2019; Ferry and Nguyen, 2019) is a way forward.

5.3.2 Potential Directions for Future Work

From the papers found, not many had defined the patterns or architecture accordingly to the taxonomy we built or defined clearly in which layers of the IoT architecture the patterns work. We would hope that this research domain grows as well as the contributions to ensure the security and privacy in IoT systems. To make it safe would be more comfortable if there were more security patterns that developers could use with proper testing and documentation. We would, therefore, propose that further research should address more thoroughly and systematically security pattern aspects for IoT systems. This can further highlight and bring forth research, while systematically listing it and giving a reference for either future research, production, or development.

Finally, the dominance of academia-only and joint collaboration in IoT security pattern research suggests that there should be even 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 topic is yet to blossom, both in the industrial and academic worlds.

6 RELATED WORK

There exist some 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 detail. They also do not offer any form of architecture or pattern to solve common recurring problems for IoT security. Security patterns-based approaches for new systems design and development have also been reviewed by (Lúcio et al., 2014; Nguyen et al., 2015). However, the reviewed approaches are not specific for IoT systems, which is what we focus on.

(Washizaki et al., 2019) present a collection of papers that either describe IoT architecture 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 that have patterns that cover security. We looked through these papers, but not all of the papers did meet our criteria described in Section 3.2. The papers from (Washizaki et al., 2019) that we analyzed and included as primary studies are the papers 10 and 14 in Table. 1.

(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) elaborate on how to design, build, and engineer applications for IoT systems and have created patterns to do this. They do not highlight security as one of their focus points, which is our main concern for this paper.

(Nguyen et al., 2019a; Nguyen et al., 2019b) surveyed deployment and orchestration approach for IoT but neither about security nor patterns. The approach used in their study is similar to ours, an SMS.

In general, the results of these studies do address not only 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 conducted systematically and explicitly for analyzing the patterns and architectures for IoT security similar to our work. Note that we have clearly defined the scope of our SMS, which only considered peer-reviewed publications, not white papers from the industry. Thus, our SMS reports the state of the art in IoT security pattern research, not including the state of practice in the industry.

7 CONCLUSION

In this paper, we have examined a research landscape of patterns and architectures for IoT security by conducting a systematic mapping study. After systematically recognizing and reviewing 24 primary studies out of thousand of relevant papers in this field, we have found out that 1) there is a rise in the number of publications addressing security patterns in the two recent years; 2) however, there are still gaps in the research that does not focus on security patterns, security architectures or security in general; 3) new IoT systems development should focus more on addressing security, which can be improved with more relevant security patterns to apply and reuse. In other words, we want to promote the use of patterns and architectures for IoT security (and privacy) by design. To make security patterns for IoT approaches more practical, research collaborations between academia and industry should be increased.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Commission's H2020 Programme under the grant agreement number 780351 (ENACT), and from the Research Council of Norway's Pilot-T Programme under the grant agreement number 296651 (ASAM).

REFERENCES

Borgia, E., Gomes, D. G., Lagesse, B., Lea, R. J., and Puccinelli, D. (2016). Special issue on "internet of things: Research challenges and solutions". *Computer Communications*, 89:1–4.

Fernandez-Buglioni, E. (2013). *Security patterns in practice: designing secure architectures using software patterns*. John Wiley & Sons.

Ferry, N., Nguyen, P., Song, H., Novac, P., Lavirotte, S., Tigli, J., and Solberg, A. (2019). Genesis: Continuous orchestration and deployment of smart IoT systems. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 870–875.

Ferry, N. and Nguyen, P. H. (2019). Towards model-based continuous deployment of secure IoT systems. In *2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C)*, pages 613–618.

Gamma, E., Helm, R., Johnson, R., and Vlissides, J. M. (1994). *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional, 1 edition.

Hany, F. A. and Wills, G. (2020). IoT security, privacy, safety and ethics. In Farsi, M., Daneshkhah, A., Hosseinian-Far, A., and Jahankhani, H., editors, *Digital Twin Technologies and Smart Cities*, pages 1–27. Springer International Publishing.

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*, pages 1–264.

Joshi, B. (2014). Overview of design patterns for beginners.

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele university. technical report tr/se-0401, Research community, Department of Computer Science, Keele University, UK.

Kitchenham, B. A., Budgen, D., and Brereton, O. P. (2011). Using mapping studies as the basis for further research – a participant-observer case study. *Information and Software Technology*, 53(6):638 – 651. Special Section: Best papers from the APSEC.

Lúcio, L., Zhang, Q., Nguyen, P. H., Amrani, M., Klein, J., Vangheluwe, H., and Traon, Y. L. (2014). Chapter 3 - advances in model-driven security. In Memon, A., editor, *Advances in Computers*, volume 93 of *Advances in Computers*, pages 103 – 152. Elsevier.

Nguyen, P., Ferry, N., Erdogan, G., Song, H., Lavirotte, S., Tigli, J., and Solberg, A. (2019). Advances in deployment and orchestration approaches for IoT - a systematic review. In *2019 IEEE International Congress on Internet of Things (ICIOT)*, pages 53–60.

Nguyen, P. H., Ferry, N., Erdogan, G., Song, H., Lavirotte, S., Tigli, J.-Y., and Solberg, A. (2019a). The preliminary results of a mapping study of deployment and orchestration for IoT. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, SAC '19, page 2040–2043, New York, NY, USA. Association for Computing Machinery.

Nguyen, P. H., Ferry, N., Gencer Erdogan, H. S., Lavirotte, S., Tigli, J.-Y., and Solberg, A. (2019b). A systematic mapping study of deployment and orchestration approaches for IoT. In *International Conference on Internet of Things, Big Data and Security (IoTBDS)*.

Nguyen, P. H., Kramer, M., Klein, J., and Traon, Y. L. (2015). An extensive systematic review on the model-driven development of secure systems. *Information and Software Technology*, 68:62 – 81.

Nguyen, P. H., Phung, P. H., and Truong, H.-L. (2018). A security policy enforcement framework for controlling iot tenant applications in the edge. In *Proceedings of the 8th International Conference on the Internet of Things*, IOT '18, New York, NY, USA. Association for Computing Machinery.

Nguyen, P. H., Yskout, K., Heyman, T., Klein, J., Scandariato, R., and 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)*, pages 246–255.

Oracevic, A., Dilek, S., and Ozdemir, S. (2017). Security in internet of things: A survey. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6.

Petersen, K., Vakkalanka, S., and Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and Software Technology*, 64:1–18.

Qanbari, S., Pezeshki, S., Raisi, R., Mahdizadeh, S., Rahimzadeh, R., Behinaein, N., Mahmoudi, F., Ayoubzadeh, S., Fazlali, P., Roshani, K., Yaghini, A., Amiri, M., Farivarmoheb, A., Zamani, A., and 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)*, pages 277–282.

Reinfurt, L., Breitenbücher, U., Falkenthal, M., Leymann, F., and Riegg, A. (2016). Internet of things patterns. In *Proceedings of the 21st European Conference on Pattern Languages of Programs*, EuroPlop '16, New York, NY, USA. ACM.

Roman, R., Najera, P., and Lopez, J. (2011). Securing the internet of things. *Computer*, 44(9):51–58.

Ron Ross, Michael McEvilley, J. C. O. (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.

Schneier, B. (2017). IoT security: What's plan b? *IEEE Security Privacy*, 15(5):96–96.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., and Sommerlad, P. (2013). *Security Patterns: Integrating security and systems engineering*. John Wiley & Sons.

Steel, C. and Nagappan, R. (2006). *Core Security Patterns: Best Practices and Strategies for J2EE", Web Services, and Identity Management*. Pearson Education.

Tran, N. K., Sheng, Q. Z., Babar, M. A., and Yao, L. (2017). Searching the web of things: state of the art, challenges, and solutions. *ACM Computing Surveys (CSUR)*, 50(4):55.

van der Meulen, R. G. (2017). Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016. Technical report, Consulting community.

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., and Priyalakshmi, G. (2018). Taxonomy and literature survey of security pattern research. In *2018 IEEE Conference on Application, Information and Network Security (AINS)*, pages 87–92.

Washizaki, H., Yoshioka, N., Hazeyama, A., Kato, T., Kaiya, H., Ogata, S., Okubo, T., and Fernandez, E. B. (2019). Landscape of IoT patterns. In *2019 IEEE/ACM 1st International Workshop on Software Engineering Research Practices for the Internet of Things (SERP4IoT)*, pages 57–60.