Privacy and Security in Requirements Engineering: Results from a Systematic Literature Mapping

Dorgival Netto[1,2], Mariana Peixoto[1], and Carla Silva[1]

[1] Centro de Informatica, Universidade Federal de Pernambuco, Pernambuco, Brazil
{dpsn2, mmp2, ctlls}@cin.ufpe.br
[2] Instituto Federal de Mato Grosso do Sul, Mato Grosso do Sul, Brazil

Abstract. Computing has been revolutionizing the way people communicate, share, and access information. Consequently, concerns about privacy and security are increasing. In this scenario, the literature reports that it is necessary to address privacy and security from the Requirements Engineering (RE) phase. This paper presents the results of a Systematic Literature Mapping, covers the period from 2000 to 2016, whose goal is to understand the current state of approaches concerning privacy and security in RE domain. We divided the results into research topics, research methods, types of study, research problems, and indications of future works regarding the field of privacy and security in RE.

Keywords: Privacy, Security, Requirements Engineering, Systematic Literature Mapping

1 Introduction

Privacy has become a top concern in software development, mainly due to incidents regarding unauthorized data exploration, misuse of information stored in social media websites, internet data, disclosure of personal information to third parties without users consent and many more[5]. This fact originated from the massive increase in computing power, data storage capacity, and data processing [17].

Digital data often reveal vast quantities of personal information, which are sometimes used for other purposes than initially intended, at times without the awareness and the agreement of users [17], [12]. Users may be unaware of when and for what purpose sensitive information about them collected, analyzed, or transmitted [10].

The exposure of such information in an unregulated way can threaten user privacy [10]. As a result, laws are being created to protect citizens' sensitive personal data and can impose severe sanctions for non-compliance, for example, the General Data Protection Regulation (GDPR) in the European Union [3]. The user's privacy can be defined as the right to determine when, how, and to what extent information about them communicated to others. In other words, users should be aware of the disclosure of their information [6].

Additionally, security concerns should also be considered [4], [15]. Security is about the prevention of harm caused by the actions of attackers. Attackers are people who gain by exploiting system failures, intentionally or accidentally provoked. This gain usually results in some harm to the system owner [4].

In this scenario, privacy and security issues need to be addressed from the early stages of system development rather than just in the implementation phase [6], [18]. Besides the industry, recognize that Requirements Engineering (RE) is critical to the success of any significant development project [9]. Consequently, new challenges arise in the RE field [6], [10].

Therefore, some research has already made efforts to understand privacy and security in RE. For example, Souag et al. [16] perform a systematic mapping study about Security Requirements Engineering (SRE) covering an interval from 2000 to 2013 identified 30 methods and categorized them in a set of five main types of knowledge forms of representation that were (re) used by SRE approaches: security patterns, taxonomies and ontologies, templates and profiles, catalogs and generic models and mixed. However, this systematic mapping takes into account only aspects of security.

Khan and Ikram [7] carried out systematic mapping of the literature in the field of SRE from 2010 to 2015. They present 15 problem cluster: domain security (74 papers, 29 %), methodologies (17 papers, 7 %), integration of security, lack of evaluation, architecture, documents, legal requirements, (eg, threats, human / environment not considered, automatic support, change, ontologies) and further divided into subcategories that comprise more specific related problems.

Abu-Nimeh and Mead [1] affirm that despite the overlap between Privacy Requirements Engineering (PRE) and SRE, each addresses a different set of problems. As a result, security risk assessment techniques used in SRE may be unsuitable for assessing privacy risks. Moreover, it is not yet evident how to achieve this systematically through the various stages of the RE process [18].

Motivated by this scenario, this paper intends to present a Systematic Literature Mapping (SLM), which aimed at understanding the state of the research on the privacy and security of Requirements Engineering. The SLM was chosen because it is the most appropriate method to provide a broad overview of a research area [8]. The SLM catch papers from the year 2000 to 2016.

The remainder of the paper is organized as follows. Section 2 presents a description of the research protocol. In Section 3, the results and discussion are exposed. In Section 4, data synthesis. Finally, Section 5 shows the final considerations.

2 Research Protocol

The SLM followed the procedures indicated by Kitchenham and Charters [8]. Two Ph.D. students conducted the SLM, and a graduate professor experienced researcher with expertise in Requirements Engineering validated.

2.1 Research Questions

Specifying the research questions are the most important part of any SLM [8]. Thus, this research answered the main question (RQ):

- **RQ:** What is the current state of privacy and security research in Requirements Engineering?

The following specific research questions (RQ) were used to guide the synthesis of results:

- **RQ1:** What research topics are investigated about privacy and security in requirements engineering?
- **RQ2:** What research methods are used for privacy and security in requirements engineering?
- **RQ3:** What types of study about privacy and security are in requirements engineering?
- **RQ4:** What is the research problem about privacy and security in requirements engineering?
- **RQ5:** What trends or future work about privacy and security in requirements engineering presented by primary studies?

2.2 Search Process

The rigor of the search process is a factor that distinguishes systematic literature review or mapping from other types of reviews [8]. The goal of an SLM is to find as many primary studies addressing the issue of possible research using an unbiased search strategy. The identification of the related research occurred in five automatic search engines: Ei COMPENDEX[1], IEEExplorer[2], ACM Digital library[3], Scopus[4], Science Direct[5]. We choose these search engines because they are relevant sources for the Software Engineering area.

We developed a search string, with relevant synonyms, for the identification of the related research through automatic search: (*privacy* OR *security*) AND (*"requirements engineering"* OR *"requirements approach"* OR *"requirements methodology"* OR *"requirements process"*).

We have thoroughly tested various combinations of terms and synonyms to get the search string used. It is important to clarify that for some search engines we apply the string to titles and abstracts, because when we perform different, we find many irrelevant works. Therefore, we adapted the search string according to the specific criteria of each search engine, as can be seen below.

[1] www.engineeringvillage2.org/
[2] ieeexplore.ieee.org/
[3] dl.acm.org
[4] www.scopus.com/
[5] www.sciencedirect.com/

- IEEE: (((*privacy*) OR (*security*)) AND ((“*requirements engineering*”) OR (“*requirements approach*”) OR (“*requirements methodology*”) OR (“*requirements process*”))). Obs: search for metadata.
- ACM: recordAbstract:(“*privacy*” OR “*security*”) AND (“*requirements engineering*” OR “*requirements approach*” OR “*requirements methodology*” OR ”*requirements process*”).
- SCOPUS: TITLE-ABS-KEY(*privacy*) OR TITLE-ABS-KEY(*security*) AND TITLE-ABS-KEY(“*requirements engineering*”) OR TITLE-ABS-KEY(“*requirements approach*”) OR TITLE-ABS-KEY(“*requirements methodology*”) OR TITLE-ABS-KEY(“*requirements process*”).
- ScienceDirect: TITLE-ABSTR-KEY((“*privacy*” or “*security*”)) and TITLE-ABSTR-KEY(“*requirements engineering*” or “*requirements approach*” or “*requirements methodology*” or “*requirements process*”).
- Ei COMPENDEX: (((((*privacy*)WN KY) OR ((*security*)WN KY)) AND (((“*requirements engineering*”)WN KY) OR ((“*requirements approach*”)WN KY) OR ((“*requirements methodology*”)WN KY) OR ((“*requirements process*”)WN KY)))).

2.3 Selection of Studies

Once we get only potentially relevant studies, they need to be evaluated, for which it is necessary to indicate some inclusion and exclusion criteria. These criteria are intended to identify primary studies that provide direct evidence on the research question [8]. We defined the inclusion and exclusion criteria, based on the RQ, to achieve consistent results: Inclusion Criteria: **I1** Peer-reviewed studies; **I2** Accessible studies; **I3** Original studies in the languages: English, Portuguese and Spanish. Exclusion Criteria: **E1** Duplicated studies (only one copy included); **E2** Gray literature (Short papers, presentations, reports, dissertations, theses, secondary and tertiary studies); **E3** Studies that do not focus on privacy or security; **E4** Studies that do not focus on RE; **E5** Publications whose text was not available (through search engines or by contacting the authors).

First, the studies have been checked using the exclusion criteria. If a paper could meet any of the exclusion criteria, in turn, if **E1** *OR* **E2** *OR* **E3** *OR* **E4** *OR* **E5** is true, then the paper must be removed. Another case for a duplicate **E1** is when a conference paper is followed by a journal article. In such cases, we select the higher-valued publication, i.e., journal over conference [13]. Subsequently, the inclusion criteria were observed. Thus, it was verified if **I1** *AND* **I2** *AND* **I3** could meet. If so, papers must be selected, if any criteria are not met, the article is excluded.

The selection process occurred in three different steps. **Step1:** reading titles, keywords, and abstract; considering the inclusion and exclusion criteria. **Step 2:** reading introduction and conclusion; considering the inclusion and exclusion criteria. **Step 3:** the studies included are thoroughly read; excluding irrelevant papers for the research questions.

2.4 Data Extraction

Data extraction should be designed to collect all the information needed to address the mapping issues [8]. We performed the data extraction with a spreadsheet and contained the following fields: Identifier, source, year, affiliations, list of authors, title, keywords, main subject (security or privacy), answers to research questions, subjective extraction.

2.5 Threats to Validity

The mapping protocol follows a few steps to ensure that the search is as accurate and objective as possible. However, potential limitations may arise. We used the categorization of threats presented by Wohlin et al. [20].

Construct validity is related to the generalization of the result to the concept or theory behind the study execution [20]. The search string used may not include all existing synonyms for the term "Privacy and Security in Requirements Engineering" and may be insufficient to capture all studies in the area. To minimize threats of this nature, we used synonyms for the key constructs.

Internal validity is related to a possible wrong conclusion about causal relationships between treatment and outcome [20]. To mitigate personal bias on the study, two Ph.D. students conducted the SLM, and a graduate professor, experienced research with expertise in RE validated.

External validity is concerned with the degree to which the primary studies are representative for the review topic [20]. In the case of a literature mapping, if the identified literature is not externally valid, neither is the synthesis of its content [19]. We excluded gray literature papers.

Conclusion validity [20] the research protocol was carefully designed and validated by the authors to minimize the risk of exclusion of relevant studies. Besides, we used many synonyms for the constructs of this paper to improve the high coverage of possibly relevant studies from automatic search.

3 Results and Discussion

Initially, through the automatic search, as shown in Table 1, we found 2658 papers. Excluding duplicate articles (1446), we get 1212 unique papers. Afterward, reading the title and the abstract. We excluded 630 studies, based on the exclusion criteria being: Gray literature (134 papers); Does not focus on privacy or security (245 articles); Does not present focus on RE (241 papers); Could not be accessed (08 papers), Non English, Spanish or Portuguese written papers (02 paper). In step 1, we selected 582 papers to be analyzed in the next step.

Of the 582 papers from the previous stage, 284 were excluded, resulting in 298 selected to participate in Step 3 (see Table 1). Of the excluded studies, it is possible to observe the following data: It was not peer-reviewed (2); Duplicates (19); Gray literature (28); Does not focus on privacy or security (78); Does not present focus on RE (97); Could not be accessed (60).

For the third stage (see Table 1), the studies resulting from the previous step were read, and those that presented answers to some of the research questions were selected. At the end of the process, we choose 267 papers after the exclusion of 31 studies. The complete list of the selected studies can be found in https://doi.org/10.6084/m9.figshare.7789637 Of the excluded studies, we observe the following data: Does not focus on privacy or security (21); Does not present focus on RE (10).

Table 1. Paper selection engines research

Search engines	Titles	Step 1	Step 2	Step3
ACM Digital library	76	36	30	26
Ei COMPENDEX	1002	12	06	04
IEEExplorer	425	183	114	95
Science Direct	33	22	14	14
Scopus	1122	329	134	128
Total	**2658**	**582**	**298**	**267**

We found papers were from the year 2000 to 2016. The pivotal year of publication was 2014 with a total of 36 papers (13.5%), followed by 2012 with 28 (10.5%), 2008 with 27 (10.1%) (see Figure 1). It is important to note that this research does not show the full effect of all the papers published in 2016 because the search and selection occurred between July and September of 2016.

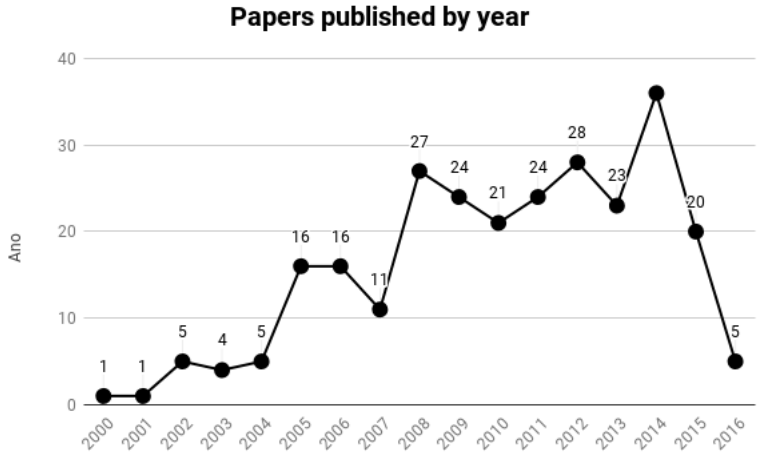

Fig. 1. Papers published by year

We categorize the papers according to the central theme, namely: security, privacy, or both (see Table 2). Security was the theme that presented the highest number, with 202 (75.7%) of papers.

Table 2. Central Theme

Main Theme	Frequency	Percentage
Privacy	44	16,5%
Security	202	75,7%
Privacy & Security	21	7,8%
Total	267	100%

4 Data Synthesis

This section presents the answers to each of the research questions.

First Research Question

The first question RQ1 asks what the research topics investigated about privacy and security in RE are. Based on the similarity of the problem and on how many studies reported the problem, we grouped the number of studies greater than four as a cluster. The studies which were stand alone in terms of the problem that they were reporting or problem reported by less than four studies were put into the "other" category. Table 3 shows the list of research topics and "other" category listed individually or together with other topics. Table 3 presents eight research topics identified from the classification that the authors show in their studies. The most prominent research topic was "Requirements Elicitation" in 84 (31.46%) papers. "Requirements Modeling" was the second most frequent topic in 39 (14.61%) of the papers. Followed by "Requirements Analysis" in 32 (11.99%) papers. We divide the papers into periods of years:

Table 3. Research Topics

Research Topics	**Frequency**	**Percentage**
Requirements Elicitation	128	47.94%
Requirements Modeling	41	15.35%
Requirements Analysis	30	11.24%
Requirements Specification	22	8.24%
Requirements Engineering Process	19	7.12%
Requirements Standards	08	3.00%
Requirements Design	06	2.24%
Other	13	4.87%
Total	**267**	**100.00%**

2000 - 2005: Thirty-two papers (privacy - 5, security - 25, both - 2). The main research topics were "Requirements Modeling" (10), "Requirements Elicitation" (5), and "Requirements Engineering Process" (5). In 2000 just one paper about Security Requirements Elicitation. The year with the highest number of publications was 2005, with 16 papers representing 50% of publications.

2006 - 2010: Ninety-nine papers (privacy - 22, security - 77). The main research topics were "Requirements Modeling" (22), "Requirements Elicitation" (15), and "Requirements Analysis" (14). In this period, the year with the highest number of publications was 2008, with 27 papers representing 27% of published papers.

2011 - 2016: 136 papers are in this range (privacy -18, security - 104, and both - 14). The main research topics were "Requirements Elicitation" (61), "Requirements Identification" (18), and "Requirements Analysis" (13). In this period, the year with the highest number of publications was 2014, with 36 papers, which represented 26.47% of the published papers. In the first six months of 2016, we identified five published papers whose research topics are Requirements Elicitation and Specification.

Second Research Question

The second question RQ2 asks what research methods used for privacy and security in RE are. Table 4 shows the list of research methods listed individually or in combination with other methods.

The most prominent research method was "Applying the method to an example or simulation with 115 papers, 17 in the privacy field, 88 in security, and 10 in papers that addressed privacy and security together. "Case Study / Focus Group" also presented good results with a total of 70 papers, 15 in the privacy area, 49 in security and 6 in papers addressing both areas. Some methods have only one occurrence. They are: "Experts evaluation" (security), "Interview" (security), "Literature study, structured analysis" and, "brainstorming" (security).

Third Research Question

The third question RQ3 asks what types of study about privacy and security in RE are. Table 5 shown the types of studies. The variable type of study was based on Petersen et al. [14]:

Evaluation Research: Techniques implemented (applied) in practice, and an evaluation of the method conducted (solution implementation).

Opinion Papers: These papers express the opinion of somebody whether a specific technique is right or wrong, or how things should have been done.

Philosophical Papers: These papers sketch a new way of looking at existing things by structuring the field in the form of taxonomy or conceptual framework.

Solution Proposal: A solution to a problem can be either novel or a significant extension of an existing technique. A small example or a good line of argumentation shows the potential benefits and the applicability of the solution (but no empirical data).

Validation Research: Techniques investigated are novel and have not yet been implemented in practice. Techniques used are, for example, experiments.

Table 4. Research Methods

Research Methods	**Privacy**	**Security**	**Privacy & Security**	**Total**
Study/comparative analysis of models or approaches	1	2	0	3
Applying the method to an example or simulation	17	88	10	115
Experts evaluation	0	1	0	1
Interview	0	1	0	1
Case Study / Focus Group	15	49	6	70
Literature study, structured analysis	0	1	0	1
Usability study or user study	0	2	0	2
Observational study	0	0	2	2
Experiment	1	7	0	8
Does not present a formal method or did not make clear the used method	9	47	2	58
Survey	1	4	1	6
Total	**44**	**202**	**21**	**267**

Solution Proposal with 204 papers was the type of study that presented the highest number of results, followed by Evaluation Research with 28 articles and Validation Research with 14 papers. The fact that the Solution Proposal has been the type of study with the highest number of results can demonstrate a lack of studies that carry out validation with formal methods, such as controlled experiments.

Table 5. Type of Study

Type of Study	**Privacy**	**Security**	**Privacy & Security**	**Total**
Evaluation Research	6	20	2	28
Experience Papers	2	7	0	9
Opinion Papers	4	3	0	7
Philosophical Papers	2	3	0	5
Solution Proposal	29	158	17	204
Validation Research	1	11	2	14
Total	**44**	**202**	**21**	**267**

Fourth Research Question

The fourth question RQ4 asks what the research problem about privacy and security in RE. We grouped the papers according to the research topic (Table 3), covered in RQ1, and we performed a characterization of the research problems of this research topic.

Requirements Elicitation is the most cited research topic. These papers aim to derive privacy and security requirements and guidelines for specific con-

texts, such as mobile technologies, goal-oriented approaches and legal requirements, contributing to security and privacy users' data protection. In this category, the study proposes a methodology to determine the software requirements by analyzing the natural language of privacy policies [SC0178][1]. Define a Goal-Oriented approach to elicitation and formal description of security requirements and incorporates fault tolerance into system requirements models through the partial satisfaction of security objectives [SC0327][1]. Define a method for eliciting security objectives and then make suggestions on how to compose these goals into consistent security requirements [SC0205][1].

Requirements Elicitation and Legal Requirements is a broad field of research. Secure Tropos framework allows to obtain high-level security requirements, automatic verification of system requirements specified in the formal modeling language [SD021][1]. A paper present a framework called "Water Marking Requirements" that business analysts can use to align the requirements of various jurisdictions [IEEE198][1]. Other papers define a methodology for directly extracting access rights and obligations from regulatory texts [SCOPUS144][1]. A paper aims to define an approach that identifies software requirements through an analysis of privileged documents, appointments, and online rights [IEEE007][1].

Requirements Modeling is the second most identified research topics in the papers captured in this mapping. In this category, the existing approaches to specifying and enforcing access control policies do not provide methodological support during the process of determining these policies. Therefore, [EI001][1] define a modeling language to specify and analyze access control policies about the organization and security and permission requirements of system administrators. Derive semantic goals models extracted from privacy policy documents [IEEE030][1]. Presenting a methodology that incorporates basic privacy requirements into the design process also describes a systematic way of analyzing the impact of privacy objectives on the organizational process and the systems that support the process [IEEE067][1]. Present an approach that assists navigation, indexing, and modeling of security goals formulated in Natural Language (NL) and provides a valuable tool for critically assessing and refining NL text [ACM033][1].

Requirements analysis is one of the most identified research topics in the papers captured in this mapping. In this category, the research problems addressed are identified the assets, threats, and vulnerabilities of a system, helping developers to analyze and extract the requirements at the early stage of development. Applying the principles and best practices of RE offer privacy policy analysis to analyze the relationship between the various participants, possible attacks, threats, and vulnerabilities; and use the techniques of misuse cases, tree attack and risk assessment to obtain the elements [IEEE283][1]. Use privacy arguments as a means of generally reviewing privacy requirements to allow the system to adapt at runtime to privacy requirements [IEEE194][1].

Papers in the research topic **Requirement Specification** identify the issues, types, and methods of security requirements. Such as [SC0615][1] who use a framework to derive a set of requirements specifications. [SCOPUS020][1] Auto-

[1] Selected Studies List: https://doi.org/10.6084/m9.figshare.7789637

matically generates a security policy from a more structured specification of the system objectives.

Requirements Engineering has an activity called **Requirements Management** that seeks to control evolution and changes, as well as enable the tracking of requirements throughout the development process. One of the paper that treats this topic aims to define a metamodel for tracking compliance between different models of User Requirements Notation (URN) models of the HIC (Health Information Custodians) and privacy legislation [SC0712][1]. Another paper presents a tool (SecMER) that can automatically detect changes in requirements and violations of security properties [SCOPUS085][1].

At the level of **Requirements Design**, the papers have as research problems to use approaches of the RE to define and evaluate models of access control about the security requirements of the organization and to analyze the impact of the privacy requirements of the organizational objectives [ACM010][1], [EI001][1], [IEEE095][1].

One of the papers whose theme is **Requirements Reuse** aims to develop a repository with all sources of relevant security requirements for the organization to avoid unnecessary efforts to identify, understand and relate security aspects to requirements sources [IEEE134][1].

Using **Requirements Standards** can significantly reduce the time spent in the requirements elicitation phase. Some papers use requirements standards to support the Security Requirements Specification process [IEEE152][1]. Legal Requirements also appears related to requirements standards. In the paper that presents an organizational-level security standard to assist legal and security experts in capturing, modeling, and setting security standards [SC0355][1].

Papers whose research topic is **RE Process** aims to integrate existing tools and techniques (i* (*i star*), NFR framework, misuse case, abuse case) with risk analysis to improve the process of RE for Privacy and Security [SC0715][1]. Extend RUP as security requirements in elicitation, analysis, and specification activities [ACM047][1].

Papers dealing with Privacy and Security **Requirements Evolution** aim to investigate the challenges of analyzing the impact of evolutionary changes on system security. The international standard for secure application development, **Common Criteria (CC)**, is regularly cited in the papers either as a certification parameter or as a guide that can be used to verify security requirements. A paper aims to integrate CC into the RE Process for requirements security through the definition of a tool that allows applying the SREPPLine approach systematically and intuitively, as well as compliance with standards (CC, ISO / IEC 270001 and IEEE 830: 1998) without the need to know these standards, reducing the participation of specialists [SC0164][1].

Misuse cases technique is used in the field of security to determine the actions that can be performed by any actor to harm the system. Papers establish a framework (MOSRE) consisting of use cases and misuse cases to identify security requirements [SC0618]. Misuse cases are used to define a framework to

[1] Selected Studies List: https://doi.org/10.6084/m9.figshare.7789637

detect threats such as risk assessments that arise from misuse of stakeholder permissions over resources [SC0192]. In this paper, the authors propose translating Tropos models into Misuse Cases diagrams enable to integrate security analysis from the earliest stages into all stages of the process development [ACM057].

Ontologies is used in Software Engineering to represent a set of concepts within a domain and its relationships. Ontologies can be used as a source to specify knowledge of security requirements efficiently [SC0475][1]. Other paper proposes to include it in the elicitation, analysis, and validation process to the engineering of security requirements [SC0714]. Some papers relate Common Criteria to ontologies to defining a Goal-Oriented ontology model for CC requirements [SC0271][1]. This paper proposes to use Object Constraint Language (OCL) to formalize security requirements in a model-driven approach to critical applications [IEEE241][1].

Fifth Research Question

The fifth question RQ5 asks what trends or future work about Privacy and Security in RE. Many papers also present the need for tool development that supports the proposed methodology. When they already have tools, the papers present the need for usability improvements for a better user experience [SCOPUS085][1] [IEEE213][1]. Some papers also claim that it is possible to use an approach to other types of requirements that are not about privacy or security [ACM011][1], or indicated the need to extend the work to support other security standards [ACM012][1], or to apply the method different types of security [IEEE326][1]. Other paper will discuss how security research can be extended or also adapted to support privacy [IEEE131][1].

One paper address Requirements Reuse, with the need to develop a framework that addresses the adequacy of reusable requirements presented in a requirements catalogs [IEEE144][1].

Requirements Modeling address to extend modeling activities to the design, coding, and testing phase [SC0637][1]. A paper provides to investigate modeling techniques to conduct a RE process in a planned way in a framework that uses the models created to identify functional requirements [ACM013][1].

As a future works, Requirements Specification says that it is necessary to evaluate the efficient use of Security Requirements in the final stages of the software development life cycle. Integrate approaches to measures to ensure compliance with security quality policies and the profile of the attacker [IEEE023][1].

The papers of Requirements Elicitation notes that a future direction is to analyze the priority of requirements and builds a system of compatible privacy legislation, in addition to developing standards of security requirements. Address need to define a complete list of security requirements to address vulnerabilities [IEEE251][1]. Identify more complex threat patterns that lead to the violation of security properties [SC0192][1]. Develop a method to identify criteria for assessing functional requirements derived from non-functional legislation [SCOPUS143][1].

[1] Selected Studies List: https://doi.org/10.6084/m9.figshare.7789637

Develop a support tool to extract legal requirements related to privacy and security from the specification expressed in natural language [SC0355][1].

5 Conclusions

This paper, in particular, presented the results of a Systematic Literature Mapping whose goal is to understand the state-of-the-art of Privacy and Security in RE. We identified 267 studies from several domains, selected from a set of 2658, following guidelines for performing SLM. Although this SLM presents data of articles published until September 2016, its results are relevant and allow future research to update this mapping to be performed considering articles published as of the second half of 2016. The most relevant findings of this mapping and its implications for further research are:

Several papers on different research topics address **legal requirements** and verification of **compliance** with legislation. We have identified some systematic reviews of the literature dealing with RE for legal compliance [11],[2].

The terminology used in Requirements Engineering is very different from those used in the legal domain, and there is a lack of appropriate **modeling techniques** and **languages** to support the requirements specification activities.

Investigate the **ambiguity** present in the regulatory requirements, and the specification of legal requirements.

Investigate the absence of an approach to elicitation and specification of privacy and security requirements.

Due to potential privacy risks **Internet of Things (IoT)** domain deserves attention concerning requirements elicitation and specification activities.

We note that few papers, in most topics of RE, carry out an empirical evaluation with experts or application to real problems. The studies present the future work the need for more validation of the proposals with the accomplishment of case studies, controlled experiments, refinement of methodology, comparisons with other approaches.

Based on this SLM, we intend to explore how to elicit and specify privacy requirements in agile software development. Moreover, to define a set of guidelines, based on the best practices of academia and industry, to assist the requirements analyst, with the participation of a legal expert, in the elaboration of a requirements specification with reduced ambiguity and compliance with the legislation.

References

1. Abu-Nimeh, S., Mead, N.R.: Privacy risk assessment in privacy requirements engineering. In: 2009 Second International Workshop on Requirements Engineering and Law. pp. 17–18. IEEE (2009)
2. Akhigbe, O., Amyot, D., Richards, G.: A systematic literature mapping of goal and non-goal modelling methods for legal and regulatory compliance. Requirements Engineering pp. 1–23 (2018)

[1] Selected Studies List: https://doi.org/10.6084/m9.figshare.7789637

3. Ayala-Rivera, V., Pasquale, L.: The grace period has ended: An approach to operationalize gdpr requirements. In: 2018 IEEE 26th International Requirements Engineering Conference (RE). pp. 136–146. IEEE (2018)
4. Haley, C.B., Moffett, J.D., Laney, R., Nuseibeh, B.: A framework for security requirements engineering. In: Proceedings of the 2006 international workshop on Software engineering for secure systems. pp. 35–42. ACM (2006)
5. Kalloniatis, C.: Incorporating privacy in the design of cloud-based systems: a conceptual meta-model. Information & Computer Security **25**(5), 614–633 (2017)
6. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: the pris method. Requirements Engineering **13**(3), 241–255 (2008)
7. Khan, N.F., Ikram, N.: Security requirements engineering: A systematic mapping (2010-2015). In: 2016 International Conference on Software Security and Assurance (ICSSA). pp. 31–36. IEEE (2016)
8. Kitchenham, B., Charters, S.: Guidelines for performing systematic literature reviews in software engineering (2007)
9. Mead, N.R., Stehney, T.: Security quality requirements engineering (SQUARE) methodology, vol. 30. ACM (2005)
10. Omoronyia, I., Cavallaro, L., Salehie, M., Pasquale, L., Nuseibeh, B.: Engineering adaptive privacy: on the role of privacy awareness requirements. In: Proceedings of the 2013 International Conference on Software Engineering. pp. 632–641. IEEE Press (2013)
11. Otto, P.N., Antón, A.I.: Addressing legal requirements in requirements engineering. In: 15th IEEE International Requirements Engineering Conference (RE 2007). pp. 5–14. IEEE (2007)
12. Party, W.: Article 29 data protection working party-opinion 5/2010 on the industry proposal for a privacy and data protection impact assessment framework for rfid applications. Brussels, Belgium, Working Party **11** (2013)
13. Paternoster, N., Giardino, C., Unterkalmsteiner, M., Gorschek, T., Abrahamsson, P.: Software development in startup companies: A systematic mapping study. Information and Software Technology **56**(10), 1200–1218 (2014)
14. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering. In: Ease. vol. 8, pp. 68–77 (2008)
15. Salehie, M., Pasquale, L., Omoronyia, I., Nuseibeh, B.: Adaptive security and privacy in smart grids: A software engineering vision. In: Proceedings of the First International Workshop on Software Engineering Challenges for the Smart Grid. pp. 46–49. IEEE Press (2012)
16. Souag, A., Mazo, R., Salinesi, C., Comyn-Wattiau, I.: Reusable knowledge in security requirements engineering: a systematic mapping study. Requirements Engineering **21**(2), 251–283 (2016)
17. Van Der Sype, Y.S., Maalej, W.: On lawful disclosure of personal user data: What should app developers do? In: 2014 IEEE 7th International Workshop on Requirements Engineering and Law (RELAW). pp. 25–34. IEEE (2014)
18. Van Lamsweerde, A.: Elaborating security requirements by construction of intentional anti-models. In: Proceedings of the 26th International Conference on Software Engineering. pp. 148–157. IEEE Computer Society (2004)
19. Vilela, J., Castro, J., Martins, L.E.G., Gorschek, T.: Integration between requirements engineering and safety analysis: A systematic literature review. Journal of Systems and Software **125**, 68–92 (2017)
20. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A.: Experimentation in software engineering. Springer Science & Business Media (2012)