SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Comprehensive Analysis of Security Requirements Engineering Approaches with Assurance Perspective

Aftab Alam Janisar[1,*], Khairul Shafee Kalid[1], Aliza Sarlan[1], Anas Abdelsatar Mohammad Salameh[2]

[1] Department of Computer and Information Science Universiti Teknologi Petronas, 32610 Seri Iskandar Perak Malaysia
[2] Department of Management Information Systems, College of Business Administration, Prince Sattam bin Abdulaziz University, 165 Al-Kharj 11942, Saudi Arabia

ABSTRACT

Given the wide distribution of software and its current growth, security is inevitable, and software systems have become more complex. To avoid the complexity and protect valuable assets of software systems, researchers, and practitioners in the fields of security requirement engineering (SRE) and security assurance advise incorporating security requirements early in software development life cycle (SDLC). Nowadays, security requirements specification and identification are an active research area for ensuring the effectiveness of software systems. However, security requirement identification is a challenging task due to sheer numbers of threats and attacks to a software system. Previous researchers have identified different SRE techniques, each looking at the same problem from a different perspective. Therefore, a literature review conducted on SRE techniques. We compared and analyzed different SRE techniques to find the most suitable SRE techniques for researchers and practitioners. Selected SRE techniques compared based on various parameters, such as different attributes, requirement elicitation, requirement analysis, project size, and integration of standards. The literature also indicates that among SRE approaches, security quality requirements engineering (SQAURE), secure tropos, security requirements engineering process (SREP), and comprehensive lightweight application security process (CLASP) are the most used SRE approaches that focus on activities such as threats, security requirements identification, and security objectives identification. Unfortunately, several SRE approaches fail to explicitly integrate the security standard and security assurance perspective. Three questions developed for this study: Question 1 is based on comparison of existing SRE approaches, Question 2 is based on SRE with security requirements elicitation and analysis, and Question 3 highlights the incorporation of security requirements assurance by SRE approaches implicitly or explicitly. The researcher must work with the developer to easily adopt SRE approaches to elicit and ensure security requirements for the software system.

Keywords:
Security requirement engineering;
security requirement elicitation;
security requirement analysis;
requirement engineering;
software security

[*] *Corresponding author.*
E-mail address: aftab_22001362@utp.edu.my

https://doi.org/10.37934/araset.54.2.104119

1. Introduction

Nowadays, security is an inevitable concern for software systems [1]. As software has become a critical part of every domain of human society such as telecommunications, financial services, healthcare, nuclear power plants and electronics and many more [2, 3]. Machine learning (ML) and artificial intelligence (AI) have indeed emerged as powerful tools in the energy sector, including oil and gas, to enhance various aspects of operations and decision-making, thereby contributing to energy security [4-6]. In recent times, security in software systems is a must feature, because the developed software should function properly under any malicious circumstances [2, 7]. Security awareness is essential in all stages of software development life cycle in building secure software [8, 9]. The growing amount of software security risks, with increased security awareness, means that software security is no longer an optional feature [10-12]. With the enhancement in technology, security flaws and security threats raised, that has bad impact on organization's integrity and financial status [13, 14]. Using security measures in development process, some authors are focused on the requirement and design phase, while others concentrated using security in coding and testing stage [15]. Normally, security is considered as non-functional requirement, with this reason security measures are utilized at the final stages of SDLC [16]. Requirement engineering is the critical stage where security awareness is must for building secure software [17]. Nevertheless, attention to software security must be paid at the early stage of SDLC [2, 10]. It is observed that requirement engineers got low awareness about elicitation of security requirement, by paying close attention to security requirement, requirement engineer can aid in building a secure software system [18, 19]. Security requirements are constraints on software system functionalities such ass authentications, authorization, confidentiality, availability, and integrity etc. Most requirement engineers had trouble getting security requirements from their clients' key stakeholders because the security terms they used didn't always match up with what was really needed [20, 21]. likelihood of security vulnerabilities increases because of incorporating security requirements late in the software development process [22].

In 2016, California data breach report stated, in the last couple of years the Attorney General received 657 data breached reports involving records of 49 million Californians. In 2012, there were 131 breaches, compromising 2.6 million records of individuals from California. Moving forward to 2015, a total of 178 breaches exposed over 24 million records to potential risk. This implies that nearly 60% of Californians encountered a data breach in the single year of 2015, primarily due to security failure [23]. Some other instances occurred regarding security threats, cost on repairing vulnerabilities [24], and Gartner, Inc has spent $96.3 billion in 2018 on security consequences [25] etc. These threats and vulnerabilities occur because of security failure and not thoroughly coping the security requirements in elicitation and analysis phase [1, 10, 26-28]. Poorly written security requirements can impact negatively the software system in terms of cost, time, rework and change in requirements [29-31].

In order to prevent security issues in software systems, security requirement engineering has a significant role in requirement elicitation and analysis to avoid such problems [32]. Over the past few years, security requirements engineering (SRE) has experienced significant growth, with the academic and scientific communities presenting various security frameworks [10]. Today, several methodologies exist for conducting security requirements engineering, such as secure quality requirements engineering (SQUARE), abuse frames, CLASP, misuse case, SREP, secure tropos, MORSE, secureUML and UMLsec, etc. Each framework comes with its own strengths and weaknesses and is particularly suited for specific purposes [1].

However, these approaches still lack comprehensive security requirements process and rely heavily on the expertise of security specialists [33, 34]. Unfortunately, to address security requirements within the realm of requirement engineering remains a challenge [35]. Therefore, attacks and threats occur because of insufficient emphasis on elicitation and analysis of security requirements [26], as well as the assurance of these security requirements [32, 36]. Security requirement assurance serve the purpose of confirming that a system aligns with security requirements and possesses resilience against potential security risks and threats, and it can be no longer neglected [10, 37]. Given the escalating count of software security threats and security awareness, implies that security requirement assurance is no longer a choice but a requirement [38]. Therefore, the objective of this study is to identify various prominent activities of SRE approaches and assurance of security requirements, which must be followed to overcome the security flaws and threats early in development process by industry practitioners for secure software development [39].

The remainder of this paper is structured as follows: In Section 2, we discuss relevant work in the fields of security requirements engineering. Research methodology described in Section 3. Section 4 is about results and discusses. Section 5 describes the conclusion.

2. Literature Review

Software systems are secure when their data and information is protected from threats, attacks and vulnerabilities, by applying efficiently the CIA Trio (confidentiality, integrity, and availability) [40]. In recent years, concern about security is the top priority [1], and security must be a part of SDLC from the beginning [41, 42]. Therefore, security requirements must be incorporated in requirement engineering phase [43], several models and frameworks have been reported in the literature [1]. Security requirements are constraints on systems functional requirements and most of the researcher considered security requirements non-functional requirements because of no clear-cut view about their criteria [1, 43].

2.1 Overview of SRE Methods

Security requirements engineering step is performed during software development [8]. Primary activities of SRE include eliciting, assessing, and specifying security requirements [10]. Security requirement engineering frameworks are required to facilitate and satisfy the security requirements of software systems, several well-studied SRE frameworks has been developed, though, the standard framework for security requirements is still yet to be developed [1]. Practitioners and organizational experts indicate that, in any SDLC process the security requirement frameworks should be incorporated in the processes to enhance the development methodology. There are several published SRE methods in real software development. Some of these are SQUARE [1, 34, 17], CLASP [34, 17], secure i* , UMLsec [1], SREP [17], secure tropos [1], MORSE [44, 17], STORE [25], P-STORE [45], BPMN [14], case-based problem domain ontology [46] , scenarios and user stories [47], secure development ontology [19], (FSSPM) in formal methods [27], SOFL formal specifications [48, 49], security requirements specification using formal methods [50, 51], identify threats related to MLBSs using DFDs and STRID [52], and many more. These techniques can be used to figure out security requirements and evaluate them according to their significance and cost [14].

Additionally, security requirements are represented using overly general and information-specific security goals. The importance of security threats is discussed in certain security requirements processes. Security requirements engineering frameworks consist of two levels of modelling namely object-level and meta-level modelling [53]. There are various techniques and methods developed in

SRE i.e., SQAURE, secure tropos, abuse frames, SREP, misuse-cases, UMLsec, MORSE, and secureUML [34, 1, 44, 54-56]. One common challenge in SRE approaches is capturing security requirements during the initial stages [43, 1]. Security requirements “selection and assessment conceptual frameworks” and “requirements models” are two methods for eliciting and documenting security requirements [57]. Researchers have also come up with methods to systematically elicit security requirements by considering potential problems and abuses frames [19, 58]. To enhance the process of eliciting security requirements, techniques like abuse frames, problem frames, and misuse case instances have been used to identify threats and vulnerabilities [25, 17, 59]. Some studies even explain how to elicit security requirements from business process models [14]. In certain cases, a technique called model-oriented security requirements engineering (MORSE) has been used, particularly in web-based healthcare applications for eliciting security requirements, it helps identify and prioritize risks posed by security threats [58, 60, 61]. Another approach is using misuse cases to elicit security threats and requirements effectively [1].

2.2 Security Requirement Assurance

Security assurance ensures the system meets security requirements and can resist security threats and failures [38]. Existing security assurance tools, methodologies, and procedures may not account for growing issues due to insufficient requirement specifications, static nature, and poor development processes [32]. Traditional security assurance approaches have limitations due to their static nature, inadequate security requirements specifications and design, etc. [37]. Current security assurance methodologies are effective at identifying anomalies but fall short when it comes to measuring their impact and potential risks. Software security assurance measures the beneficial effects of security requirement fulfilment on the security assurance score using several metrics. Knowing the impact will help stakeholders maximize the positive effects to meet security goals [62]. There are several security requirement assurance methods exist such as common criteria (CC) [32], security metrics [37], security assurance cases (SAC) [63], threat modelling [64], and formal methods etc. Table 1 SLR has focused on security requirements engineering.

2.3 Analysis of SRE Methods

This section explains the analyses of security requirements engineering (SRE) approaches. Table 1 explains the extensive studies conducted on security requirement in literature. While Table 4 checks whether the SRE approaches perform the critical activities in requirement engineering elicitation and analysis phase which is given in section 4. Some of the SRE approaches focuses on the early stages of software development [33]. Authors in Table 1 have explained strong arguments about the SRE approaches, relevant critical activities, and security requirements.

From Table 1, all studies performed comparative analysis of SRE approaches. Fabian *et al.*, [65] presented a conceptual framework with focus on elicitation and analysis, later the framework was compared with SRE approaches. Anwar *et al.,* [1], Salini and Kanmani [66] compared the SRE approaches on based on the threat modelling, risk analysis in RE subphases and SDLC. While Silva *et al.,* [67] presented overall 30 sources have been identified from integration two systematic mapping studies, out of 19, 17 covering threat identification and 14 covering mitigation of threats in SDLC. Similarly, Salini and Kanmani [66], and Muñante *et al.,* [68] comparison and compatibility of SRE approaches have been made using the criteria of risk analysis. Each study has its strength and weaknesses discussed in Table 1. The analysis of these studies is based on the research questions defined by each study. Most of the studies are focusing on the comparison of SRE approaches in SDLC and RE. However, security requirement assurance is major concern of SRE approaches, and the studies in Table 1 are lacking in defining the assurance perspective. For assurance this study has observed that SRE approaches are compared based on different actives and criteria but lacking in describing the right course of security requirements assurance. Comparatively in our study we have designed a question for assurance of security requirement that which SRE methodologies implicitly or explicitly incorporate the assurance perspective.

Table 1
SLR studies on security requirement

S.No	References	SR extensive studies
1	[1]	A SLR is conducted on the security requirement engineering approaches providing detailed discussion on the 20 most used SRE approaches. Analytical evaluation is carried out based on some technical parameters. Later, compared SRE approaches based on different criteria like threat modeling and risk analysis and sub-phases. To supply the comprehensive best SRE practices to researchers and practitioners in the domain of requirement engineering. However, some of the approaches discussed in this study is focused on design phase, but Scope of the study was only limited to RE sub-phase.
2	[66]	A view is presented on security requirement types, issues and security requirements engineering methods. In this study 11 SRE methods are compared based on Threat modeling, risk analysis, and sub phases of SDLC. Moreover, this study lacks in providing systematic literature, and the comparison of SRE approaches were based on only two critical activities.
3	[65]	This study presented a conceptual framework with a focus on security elicitation and analysis. The SRE methods were assessed on different criteria such as scope of the methods, their validation and quality assurance capabilities. This framework was compared with the SRE approaches to review how the SRE methods are related to this conceptual framework. However, the study lacks in providing SRE approaches systematic literature review, as well as comparing the SRE approaches was based on quite rigorous criteria in software engineering discipline.
4	[68]	In this study a comparative analysis has been conducted including 13 SRE approaches review. Further this study evaluated the SRE methods compatibility with Risk Analysis and Model driven engineering. Compatibility and integration of SRE approaches in MDE is based on only Risk analysis, but other critical activities are not considered. This study review is only based on SRE approaches identification from previously conducted studies [66] [65] [1].
5	[67]	In this study 2 systematic mapping studies are conducted. Overall, 19 methods have been identified out of 19, 17 covering threat identification and 14 covering mitigation of threats in SDLC. Outlining the important other techniques are overlooked and focused area of this study is not concentrated to the early stage od SDLC.

To avoid rework and difficulties later, practitioners and researchers recommend incorporating security into requirements [34]. However, security concerns in requirement engineering are still imprecise [35]. Unfortunately, to address security requirements within the realm of requirement engineering remains a challenge [35]. However, attacks and threats occur because of insufficient emphasis on elicitation and analysis of security requirements [26], as well as the assurance of these security requirements [32, 36]. Thus, an in-depth literature is needed to complement security requirements engineering approaches to verify the assurance of security requirements in development [37]. However, clarification and verification of the security requirements and security requirements assurance is a possible research gap [32]. Moreover, there is no standard process available to measure the security assurance of software security requirements [69].

3. Review Methods

The focus of this study is to identify the existing literature on security requirement engineering and security requirements assurance during software development in a synthesized and formal way. A well-defined sequential process is followed, for comparison and evaluation of the SRE approaches and their activities. So, this is a literature review study, as the objective of the study is to capture SRE broad overview. In contrast, we queried several digital libraries such as ACM, google scholar, Scopus, IEEE, and other to obtain the required research articles.

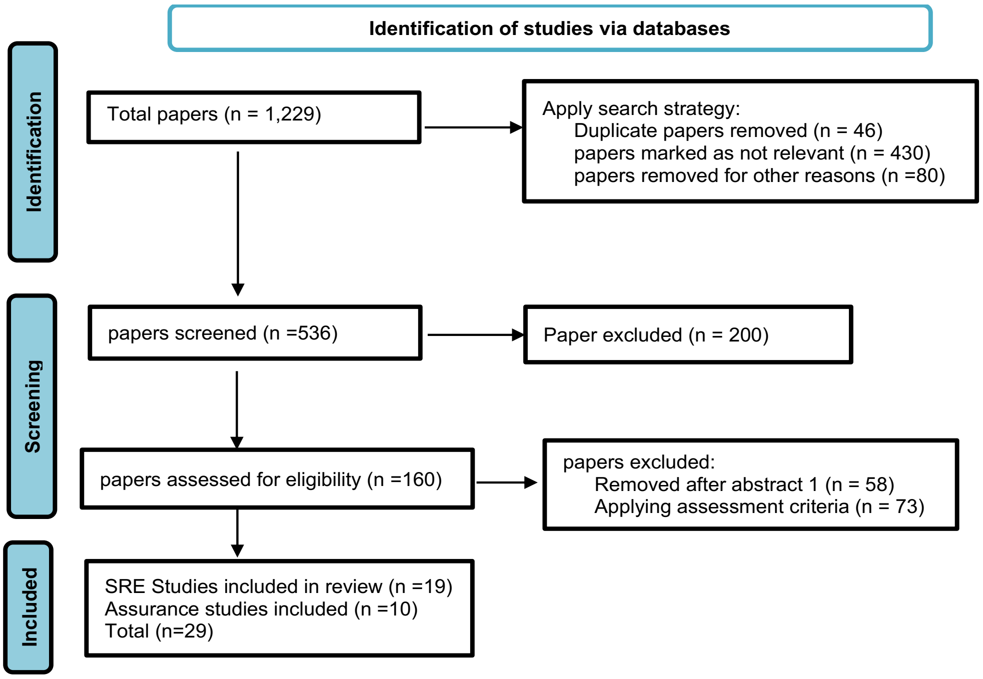
Identification of studies via databases
Identification
Total papers (n = 1,229)
Apply search strategy:
Duplicate papers removed (n = 46)
papers marked as not relevant (n = 430)
papers removed for other reasons (n =80)
Screening
papers screened (n =536)
Paper excluded (n = 200)
papers assessed for eligibility (n =160)
papers excluded:
Removed after abstract 1 (n = 58)
Applying assessment criteria (n = 73)
Included
SRE Studies included in review (n =19)
Assurance studies included (n =10)
Total (n=29)

Fig. 1. Research paper selection criteria

3.1 Research Questions

A literature review conducted to search for initiatives for security requirement engineering and security requirements assurance. According to the objective of the study, and after gathering the required information from the digital libraries, we elaborated the following research questions.

1. Which SRE methodologies have been proposed by researchers in the literature for identification of security requirements?
2. Which techniques for security requirement elicitation and analysis have been prominently utilized by established SRE methodologies?
3. To what extent the assurance of security requirements provided by the SRE methodologies explicitly or implicitly?

Research question 1 [1, 70], searched for the available literature on existing SRE approaches for extensive study, which is published during 2016-2023. Only three SLR papers were selected from 2009 [65], 2012 [66] and 2014 [68] for comparative analysis among SRE approaches. Research question 2 formulated in a way to examine the elicitation and analysis techniques in terms of SRE approaches [1, 58]. Research question 3, which is the primary question of this study. How implicitly or explicitly the SRE approaches utilizes the assurance perspective in development of security requirements.

3.2 Data Sources and Search Strategy

This study is based on the literature review, search strategy for this study generally suggested the use and identification of population and intervention. While searching for keywords in search engines, we identified some of the relevant keywords mentioned below in Table 2 with search string.

Table 2
Data source and search strategy

Population	Security requirement engineering, security requirements or assurance.
Intervention	Existing approaches for security requirements engineering and security requirement assurance.
Search String	“security” AND “requirement” AND “engineering” OR “approaches” OR “techniques” OR “methods” OR “frameworks”, “security” AND “requirement engineering” OR “requirements”, “security” AND “requirement” AND “assurance”, “security” AND “assurance”.

Table 2 provide the brief description of population and intervention with search string. Later, the retrieved studies were assessed according to the search string, overall, 160 paper relevant to security requirement engineering and assurance were filtered. In the second stage of filtration with inclusion and exclusion criteria, we found only 29 specific research manuscripts according to our need. Out of 29, 19 papers were relevant to security requirement engineering and 10 were related the assurance. Moreover, the quality assessment criteria were done on filtered research papers. The quality assessment questions were “does these studies consider SRE approaches and security requirement assurance?”, and “does the purpose and aim of the research papers is described fully?”

4. Results and Discussion

This section discusses the comparative analysis among SRE approaches, their activities, and presents answers to the research questions. From the selected 29 research papers, we have noted 9 specific SRE approaches that are used for security requirement identification in elicitation and analysis phase. Based on the identified overall 20 activities, 11 activities were identified for SRE methods, 5 were identified for security requirement elicitation, and the rest 4 for security requirement analysis. We compared and evaluated SRE approaches based on these 20 identified activities.

Table 3
Description of SRE methods and requirement phase activities

Activities	Description of SRE Methods Activities
Flexibility	Flexibility refers to how flexible the framework is in adapting to different settings.
Scalability	Scalability in software refers to the ability of a system to grow in features and capabilities in response to rising demand.
Threats	Any situation or occurrence that has the potential to negatively affect organizational / software / system operations.
Validation of requirements	Validation of requirements is the process of ensuring that a system satisfies its objectives and operates as intended.
Risk analysis	recognizing and analyzing potential concerns that could have a negative effect on highly influenced activities or projects.
vulnerability	Analyses weaknesses in a system.
Consistency	Requirements which are compatible with your strategic objectives, vision, and corporate ambitions.
Integration of security requirements	Integration of requirements with security.
Assets identification	Takes into consideration the value of stakeholder’s assets.

Misuse modeling	Utilizes the misuse case technique to analyze threats.
Domain knowledge	Knowledge about which environment the system would operate in.
Activities	Description of Security Requirement Elicitation Activities
Elicitation and analysis phase	interaction with clients and end-users to determine domain requirements, system services, and system limits.
Identify stakeholders	Taking the opinion of all stakeholders.
Security goals	It fulfils the concepts of: (i.e., confidentiality, integrity, availability etc.).
Other non-functional requirements	It provides support to other non-functional requirements such as (performance, security, useability etc.)
Support during requirement elicitation	This attribute provides engaging, and understanding stakeholders needs and translating them into requirements.
Activities	Description of Security Requirement Analysis Activities
Complete security requirement can be produced	Collaboration among stakeholders, security experts, designers, and developers are key to achieving a well-rounded and effective set of security requirements.
Missed security requirements can be added	It allows for the inclusion of missed requirements as they are recognized, ensuring that security concerns are adequately addressed throughout the development lifecycle.
Security requirement conflict can be resolved	Addressing security requirement conflicts, it reduces the chances of misunderstandings, delays, or costly revisions later in the development process.
Identify business objectives	By aligning the project with business goals early on, the development process becomes more focused and efficient.
Criteria	Other attributes
Project size	The scope and complexity of work involved in terms of effort, resources, and deliverables.
Integration of standards	Aligning identified security requirements with established industry best practices and regulatory guidelines.

Table 3 describes the overall SRE, and requirement elicitation and analysis activities selected from literature. These activities are divided into four sections i.e., SRE, security requirement elicitation, security requirement analysis and other attributes. In section 1, the most adopted and popular 9 SRE approaches are selected, and 11 most important activities relevant to those SRE approaches are identified for comparative analysis. In section 2, several security elicitation approaches are developed for eliciting security requirements in the past, but in this study, we have selected 5 specific activities which are utilized by SRE approaches for security requirement elicitation. In section 3, among the developed and proposed security requirement analysis approaches and their activities for identification of security requirement in the past, regarding that we selected 4 specific activities which is utilized by SRE approaches for security requirement analysis. The last 4th section is based on other attributes such as project size and the security standard followed by the SRE approaches.

Table 4 refers to the results of research question 1, in which SRE approaches have been adopted and proposed by the researcher in literature. Critically analysed the existing literature for comparative analysis of SRE approaches. SRE approaches are compared based on three level Likert scale i.e., (“√”,” •”,” ‐ ”), for project size, (“Large = L”, “Medium -= M”, “Small = s”). Three level Likert scale sign “√” indicates that the specific activity is supported within the approach,” •” this indicates that the available is not supported by the approach and” ‐ ” suggested that the available activity is not found in the literature for SRE approach. Approaches are regarded as comprehensive if they achieve (70%-100% of the 20 activities, average if it achieves (55%-70%) and limited if it achieves below 50%.

Table 4
SRE methods and requirement phase activities comparison

SRE Methods Activities									Security Requirement Elicitation Activities						Security Requirement Analysis Activities						Project Size	Integration of Standards
SRE Methods	Flexibility	scalability	Threats,	Validation of Requirements	Risk analysis	vulnerability	Consistency	Integration of security requirements	Assets identification	Misuse Modeling	Domain Knowledge	Elicit security Requirements	Identify stakeholders	Support Requirement elicitation process	Identify security goals	Other non-functional requirements	Complete SR can be produced.	identify business objectives.	Missed SR can be included	SR conflict can be resolved		
SQUARE [1, 34, 17]	✓	✓	✓	✓	✓	•	✓	•	•	✓	•	✓	•	✓	✓	✓	✓	•	✓	✓	-	-
Secure Tropos [1, 68]	✓	✓	✓	✓	•	✓	•	✓	•	-	-	✓	✓	✓	✓	✓	✓	✓	•	✓	L	ISO/IEC 17799
Abuse Frames [1, 67]	-	✓	✓	✓	•	✓	-	•	✓	-	-	✓	•	•	✓	•	✓	✓	✓	•	M	ISO13 335
SREP [1, 17]	✓	✓	✓	✓	✓	✓	✓	•	✓	•	•	✓	•	•	✓	•	✓	✓	✓	✓	-	cc
Misuse-cases [1, 67]	✓	•	✓	•	•	✓	•	✓	•	✓	•	✓	✓	✓	✓	✓	✓	•	✓	✓	S	-
UMLsec [1, 65]	-	-	✓	•	✓	✓	-	-	•	✓	-	✓	•	•	✓	•	-	✓	✓	•	M	ISO/IEC 15408, 27001, IEEE 830-1998
MORSE [1, 25]	✓	•	✓	•	•	✓	•	✓	•	•	•	✓	✓	✓	✓	•	✓	✓	✓	✓	M	-
SecureUML [1]	-	-	•	•	•	•	-	-	•	-	-	✓	•	•	✓	•	-	✓	✓	✓	M	-
CLASP [34, 17]	✓	-	✓	✓	✓	✓	•	✓	✓	•	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	L	-

(RQ$_1$) Which SRE methodologies have been proposed by researchers in the literature for identification of security requirements?

Research question 1, based on the existing SRE approaches available in literature which is published during 2016-2023. Only three SLR research papers were selected from 2009, 2012 and 2014 for comparative analysis among SRE approaches. Table 3 summarizes the found critical activities of SRE approaches. It is important that we should know about the systems' threats, vulnerabilities and security goals, without these activities and attributes we are unable to design the requirement for the secure system. It is to make sure that while eliciting the requirements, security concerns need to be incorporated for developing the security artifact. From Table 4, 9 security requirement engineering approaches are proposed but SQUARE [1, 34, 17], secure Tropos [1, 68], SREP [1, 12] and CLASP [34, 17] are the most comprehensive approaches as they cover more than 13 out of the 20 activities. The rest of the SRE approaches placed under the average and limited section.

Table 4 also expresses the limitations in each framework. The SQUARE framework is primarily designed for the phase of security requirements engineering. The approach does not emphasize domain knowledge, asset, integration of security requirements and vulnerability openly or implicitly. Project size and integration of standards are not specified for SQAURE methodology Alternatively, SREP is quite like SQUARE, SREP does not emphasize integration of security requirement, misuse case modelling, and domain knowledge. SREP the project size is not defined but it supports common criteria security standards. CLASP has also some limitations such as scalability, consistency in the security requirements, and misuse case modelling. CLASP supports the large project size, but no security standards are defined for it. Secure Tropos does not emphasize risk analysis, consistency in security requirements, and asset identification openly or implicitly. Secure Tropos follows the ISO/IEC 17799 standards, and it is supported for large project sizes. Clearly, each approach has advantages and limitations and is best suited for a certain function. In addition, there is no standard approach for security criteria that meets the demands of every enterprise for software systems. Therefore, requirement engineers and requirement analysts are faced with a difficult decision when selecting an acceptable security requirements engineering approach based on their demands and expectations. When selecting an SRE methodology, consider the project's specific requirements, team expertise, and the nature of security concerns. Each methodology has its strengths and weaknesses and adapting them to suit the project's context is essential for successful security requirement identification. When selecting techniques, models, and security standards, consider the project's goals, complexity, team capabilities, and stakeholder expectations. A balanced approach that combines various elements while considering their justifications, possible solutions, and drawbacks will help in effectively identifying and addressing security requirements.

(RQ$_2$) Which approaches for security requirement elicitation and analysis have been prominently utilized by established SRE methodologies?

Research question 2 formulated in a way to examine the elicitation and analysis techniques in terms of SRE approaches [1, 58]. Table 3 summarizes the found critical activities of SRE approaches. Table 4 refers to the results of research question 1, in which SRE approaches have been adopted and proposed by the researcher in literature. Critically analysed the existing literature for comparative analysis of SRE approaches.

There is no one-size-fits-all answer to determine the "best" Security Requirements Engineering (SRE) approach for security requirements elicitation and analysis. The effectiveness of an approach depends on various factors including project context, goals, team expertise, and the specific security concerns involved. The combination of these techniques ensures a comprehensive approach to security requirement elicitation and analysis. From table 4 by employing threat modelling, risk assessment, and use case/misuse case modelling in SRE methodologies can systematically identify, analyse, and prioritize security requirements [1, 34, 17]. The justification for using these techniques stems from their ability to provide a structured and systematic way to uncover security concerns early in the software development process [26, 34, 71]. Threat modelling and risk assessment offer a proactive approach to identifying vulnerabilities and prioritizing actions [25]. Use case/misuse case modelling helps visualize potential security threats in context, while security patterns offer reusable solutions that align with established best practices. Overall, these techniques contribute to a more robust understanding of security requirements, ensuring that software systems are designed and developed with adequate security measures in place to mitigate potential threats.

(RQ3) To what extent the assurance of security requirements provided by the SRE methodologies explicitly or implicitly?

Research question 3, which is the primary question of this study. In requirement elicitation and analysis phase which SRE methodologies investigate and provide support for security requirement assurance. SRE methodologies are designed to enhance security consideration throughout the software development lifecycle. SRE methodologies emphasize validating security requirements against identified threats, vulnerabilities, and industry standards using assurance perspective.

However, SRE approaches contribute to the security requirements assurance, some approaches have strong emphasis while others have not explicitly highlighted it as a distinct phase. Among the SRE approaches STRIDE threat modelling [25], secure tropos, abuse frames, SecureUML, UMLsec, misuse case modelling, and CLASP all are focusing on security concerns but does not highlight assurance explicitly as distinct phase [1, 34, 17]. While SQUARE, SREP, MORSE, SecReq, ISO/IEC 27001, and NIST security standard documents explicitly highlight the assurance as distinct phase. While most security requirements engineering (SRE) methodologies inherently involve some level of assurance for security requirements, it's important to note that the term "assurance" might not always be explicitly used in all methodologies. However, the concepts of validation, verification, testing, and implementation oversight often align with the idea of ensuring security requirements are effectively implemented. As such, it's challenging to identify methodologies that completely exclude assurance altogether. In essence, SRE approaches might not all explicitly label a "security requirement assurance" phase, but the core principles of these methodologies inherently contribute to the assurance of security requirements.

5. Conclusion

In SDLC, SRE role is very crucial, because security issues required to be addressed at the very beginning of development. In last couple of years, systematic reviews are conducted on SRE, but unfortunately, they were not addressing the assurance perspective of security requirements. To address this gap a modest review study was conducted with the total 160 research articles. Out of identified research papers, 29 specific research papers were found relevant. Out of 29, 19 papers were relevant to security requirement engineering and 10 were related the assurance. Moreover, the quality assessment criteria were done on filtered research papers. Therefore, after the final selection of papers, SRE approaches were compared on 20 different activities/attributes. Three research questions were designed for this study, questions were answered from literature. From question 1, it was observed that SQAURE, secure tropos, SREP and CLASP are the most used SRE approaches with focus on activities such as Threats, elicit security Requirements, and Identification security goals. From question 2, it is noticed that it is difficult to answer which SRE approach is best fits for security requirements elicitation and analysis, because the effectiveness of an approach depends on various factors including project context, goals, team expertise, and the specific security concerns involved. From question 3, it is identified that among the SRE approaches STRIDE threat modelling, secure tropos, abuse frames, SecureUML, UMLsec, misuse case modelling, security patterns, agile and develops approaches, and CLASP all are focusing on security concerns but does not highlight assurance explicitly as distinct phase. While SQUARE, SREP, MORSE, SecReq, ISO/IEC 27001, and NIST security standard documents explicitly highlight the assurance as distinct phase. The assurance of security requirements is a fundamental aspect of SRE methodologies whether it is explicit or implicit. It is required that security requirement assurance phase must beaded and highlighted in the SRE approaches. The contribution of this study is to provide the existing SRE approaches comparison to researcher as well as to the industry practitioners for selecting the best fit approach in assurance perspective.

Acknowledgement

This research was funded by YUTP-FRG (015LC0-514).

Reference

[1] Anwar Mohammad, Malik Nadeem, Mohammed Nazir, and Khurram Mustafa. "A systematic review and analytical evaluation of security requirements engineering approaches." *Arabian Journal for Science and Engineering* 44 (2019): 8963-8987. https://doi.org/10.1007/s13369-019-04067-3

[2] Khan, Rafiq Ahmad, and Siffat Ullah Khan. "A preliminary structure of software security assurance model." In *Proceedings of the 13th International Conference on Global Software Engineering*, pp. 137-140. 2018. https://doi.org/10.1145/3196369.3196385

[3] Khattak, Muhammad Adil, Muhammad Khairy Harmaini Shaharuddin, Muhammad Saiful Islam Haris, Muhammad Zuhaili Mohammad Aminuddin, Nik Mohamad Amirul Nik Azhar, and Nik Muhammad Hakimi Nik Ahmad. "Review of cyber security applications in nuclear power plants." *Journal of Advanced Research in Applied Sciences and Engineering Technology* 7, no. 1 (2017): 43-54.

[4] Yagoub, Sami Abdelrahman Musa, Gregorius Eldwin Pradipta, and Ebrahim Mohammed Yahya. "Prediction of bubble point pressure for Sudan crude oil using Artificial Neural Network (ANN) technique." *Progress in Energy and Environment* (2021): 31-39.

[5] Khattak, Muhammad Adil, Jun Keat Lee, Khairul Anwar Bapujee, Xin Hui Tan, Amirul Syafiq Othman, Afiq Danial Abd Rasid, Lailatul Fitriyah Ahmad Shafii, and Suhail Kazi. "Global energy security and Malaysian perspective: A review." *Progress in Energy and Environment* (2018): 1-18.

[6] Suresh, Sachin Dev, Ali Qasim, Bhajan Lal, Syed Muhammad Imran, and Khor Siak Foo. "Application of Gaussian process regression (GPR) in gas hydrate mitigation." *Journal of Advanced Research in Fluid Mechanics and Thermal Sciences* 88, no. 2 (2021): 27-37. https://doi.org/10.37934/arfmts.88.2.2737

[7] Othman, Intan Safina, Abdul Samad Shibgatullah, Abd Samad Hassan Basari, Zul Azri, and Muhammad Noh. "The awareness of security breach among IT users in Kolej PolyTech MARA, Batu Pahat."

[8] Niazi, Mahmood, Ashraf Mohammed Saeed, Mohammad Alshayeb, Sajjad Mahmood, and Saad Zafar. "A maturity model for secure requirements engineering." *Computers & Security* 95 (2020): 101852. https://doi.org/10.1016/j.cose.2020.101852

[9] Janisar, Aftab Alam, Khairul Shafee bin Kalid, Aliza Bt Sarlan, and Abdul Rehman Gilal. "Security Requirements Assurance: An Assurance Case Perspective." In *2023 IEEE 8th International Conference On Software Engineering and Computer Systems (ICSECS)*, pp. 78-83. IEEE, 2023. https://doi.org/10.1109/ICSECS58457.2023.10256374

[10] Ur Rehman, Shafiq, Christopher Allgaier, and Volker Gruhn. "Security requirements engineering: A framework for cyber-physical systems." In *2018 International conference on frontiers of information technology (FIT)*, pp. 315-320. IEEE, 2018. https://doi.org/10.1109/FIT.2018.00062

[11] Boutahar, Jaouad, Ilham Maskani, and Souhail El Ghazi El Houssaini. "Experimental evaluation of security requirements engineering benefits." *Int. J. Adv. Comput. Sci. Appl.(IJACSA)* 9, no. 11 (2018): 411-415. https://doi.org/10.14569/IJACSA.2018.091158

[12] Assal, Hala, and Sonia Chiasson. "Security in the software development lifecycle." In *Fourteenth symposium on usable privacy and security (SOUPS 2018)*, pp. 281-296. 2018.

[13] Khan, Rafiq Ahmad, Siffat Ullah Khan, Habib Ullah Khan, and Muhammad Ilyas. "Systematic mapping study on security approaches in secure software engineering." *Ieee Access* 9 (2021): 19139-19160. https://doi.org/10.1109/ACCESS.2021.3052311

[14] Zareen, Saima, Adeel Akram, and Shoab Ahmad Khan. "Security requirements engineering framework with BPMN 2.0. 2 extension model for development of information systems." *Applied Sciences* 10, no. 14 (2020): 4981. https://doi.org/10.3390/app10144981

[15] Sharma, Anuradha, and Praveen Kumar Misra. "Aspects of enhancing security in software development life cycle." *Advances in Computational Sciences and Technology* 10, no. 2 (2017): 203-210.

[16] Karim, Nor Shahriza Abdul, Arwa Albuolayan, Tanzila Saba, and Amjad Rehman. "The practice of secure software development in SDLC: an investigation through existing model and a case study." *Security and Communication Networks* 9, no. 18 (2016): 5333-5345. https://doi.org/10.1002/sec.1700

[17] Mufti, Yusuf, Mahmood Niazi, Mohammad Alshayeb, and Sajjad Mahmood. "A readiness model for security requirements engineering." *IEEE Access* 6 (2018): 28611-28631. https://doi.org/10.1109/ACCESS.2018.2840322

[18] Kouraogo, Yacouba, Ghizlane Orhanou, and Said Elhajji. "Advanced security of two-factor authentication system using stego QR code." *International Journal of Information and Computer Security* 12, no. 4 (2020): 436-449. https://doi.org/10.1504/IJICS.2020.107451

[19] Steinmann, Jessica, and Omar Ochoa. "Supporting Security Requirements Engineering through the Development of The Secure Development Ontology." In *2022 IEEE 16th International Conference on Semantic Computing (ICSC)*, pp. 151-158. IEEE, 2022. https://doi.org/10.1109/ICSC52841.2022.00031

[20] Kamalrudin, Massila, Nuridawati Mustafa, and Safiah Sidek. "A template for writing security requirements." In *Requirements Engineering for Internet of Things: 4th Asia-Pacific Symposium, APRES 2017, Melaka, Malaysia, November 9–10, 2017, Proceedings 4*, pp. 73-86. Springer Singapore, 2018. https://doi.org/10.1007/978-981-10-7796-8_6

[21] Sadiq, Mohd. "A fuzzy set-based approach for the prioritization of stakeholders on the basis of the importance of software requirements." *IETE Journal of Research* 63, no. 5 (2017): 616-629. https://doi.org/10.1080/03772063.2017.1313140

[22] Sánchez-Gordón, Mary-Luz, Ricardo Colomo-Palacios, Alex Sánchez, Antonio de Amescua Seco, and Xabier Larrucea. "Towards the integration of security practices in the software implementation process of ISO/IEC 29110: a mapping." In *Systems, Software and Services Process Improvement: 24th European Conference, EuroSPI 2017, Ostrava, Czech Republic, September 6–8, 2017, Proceedings 24*, pp. 3-14. Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-64218-5_1

[23] Harris, Kamala D., and Attorney General. "California data breach report." *Retrieved August* 7 (2016): 2016.

[24] Worakitpreeda, Natchapol, and Monvarath Pongpaibul. "Framework for Eliciting Security Requirements of Web Application from Business Users." In *2021 25th International Computer Science and Engineering Conference (ICSEC)*, pp. 216-221. IEEE, 2021. https://doi.org/10.1109/ICSEC53205.2021.9684600

[25] Ansari, Md Tarique Jamal, Dhirendra Pandey, and Mamdouh Alenezi. "STORE: Security threat oriented requirements engineering methodology." *Journal of King Saud University-Computer and Information Sciences* 34, no. 2 (2022): 191-203. https://doi.org/10.1016/j.jksuci.2018.12.005

[26] Anderson, Ross. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 2020. https://doi.org/10.1002/9781119644682

[27] Mishra, Aditya Dev, and Khurram Mustafa. "A Survey on Formal Specification of Security Requirements." In *2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pp. 1453-1456. IEEE, 2021. https://doi.org/10.1109/ICAC3N53548.2021.9725779

[28] Lal, Bechoo, and Chandrahauns R. Chavan. "Analysis Report on Attacks and Defence Modeling Approach to Cyber Security." *International Journal of Scientific Research in Science and Technology* (2019): 52-60. https://doi.org/10.32628/IJSRST196215

[29] Lal, Bechoo, and Chandrahauns R. Chavan. "Analysis Report on Attacks and Defence Modeling Approach to Cyber Security." *International Journal of Scientific Research in Science and Technology* (2019): 52-60. https://doi.org/10.32628/IJSRST196215

[30] Mustafa, N. U. R. I. D. A. W. A. T. I., M. A. S. S. I. L. A. Kamalrudin, S. A. F. I. A. H. Sidek, ANGGRAINI JUNIA, LA MANI, Y. ALZYOUD FAISAL, NISREEN ALSHARMAN et al. "Security requirements template-based approach to improve the writing of complete security requirements." *Journal of Theoretical and Applied Information Technology* 99, no. 1 (2021): 1-12.

[31] MUSTAFA, NURIDAWATI, MASSILA KAMALRUDIN, and SAFIAH SIDEK. "SECURITY REQUIREMENTS ELICITATION AND CONSISTENCY VALIDATION: A SYSTEMATIC." *Journal of Theoretical and Applied Information Technology* 96, no. 16 (2018).

[32] Shukla, Ankur, Basel Katt, Livinus Obiora Nweke, Prosper Kandabongee Yeng, and Goitom Kahsay Weldehawaryat. "System security assurance: A systematic literature review." *Computer Science Review* 45 (2022): 100496. https://doi.org/10.1016/j.cosrev.2022.100496

[33] Li, Hongbo, Xiaohong Li, Jianye Hao, Guangquan Xu, Zhiyong Feng, and Xiaofei Xie. "Fesr: A framework for eliciting security requirements based on integration of common criteria and weakness detection formal model." In *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pp. 352-363. IEEE, 2017. https://doi.org/10.1109/QRS.2017.45

[34] Qadir, Nuzhat, and Rodina Ahmad. "SecRS template to aid novice developers in security requirements identification and documentation." *International Journal of Software Engineering and Computer Systems* 8, no. 1 (2022): 45-52. https://doi.org/10.15282/ijsecs.8.1.2022.5.0095

[35] Villamizar, Hugo, Marcos Kalinowski, Marx Viana, and Daniel Méndez Fernández. "A systematic mapping study on security in agile requirements engineering." In *2018 44th Euromicro conference on software engineering and advanced applications (SEAA)*, pp. 454-461. IEEE, 2018. https://doi.org/10.1109/SEAA.2018.00080

[36] Jahan, Sharmin, Matthew Pasco, Rose Gamble, Philip McKinley, and Betty Cheng. "MAPE-SAC: A framework to dynamically manage security assurance cases." In *2019 IEEE 4th International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, pp. 146-151. IEEE, 2019. https://doi.org/10.1109/FAS-W.2019.00045

[37] Shukla, Ankur, Basel Katt, Livinus Obiora Nweke, Prosper Kandabongee Yeng, and Goitom Kahsay Weldehawaryat. "System security assurance: A systematic literature review." *Computer Science Review* 45 (2022): 100496. https://doi.org/10.1016/j.cosrev.2022.100496

[38] Khan, Rafiq Ahmad, and Siffat Ullah Khan. "A preliminary structure of software security assurance model." In *Proceedings of the 13th International Conference on Global Software Engineering*, pp. 137-140. 2018.. https://doi.org/10.1145/3196369.3196385

[39] Wirtz, Roman, and Maritta Heisel. "Systematic Treatment of Security Risks during Requirements Engineering." In *ENASE*, pp. 132-143. 2020. https://doi.org/10.5220/0009397001320143

[40] Flores, Fabiana Figueira Sanches, and Silvio Romero de Lemos Meira. "Ethical software engineering: a critical review about software engineering in face of security requirements in the IoT/IoE society." In *2021 IEEE International Systems Conference (SysCon)*, pp. 1-8. IEEE, 2021. https://doi.org/10.1109/SysCon48628.2021.9447113

[41] Mahmood, Waqas, Syed Shaharyar Rizvi, and Siraj Munir. "Hindrance to Requirements Engineering During Software Development with Globally Distributed Teams." *International Journal of Information Engineering and Electronic Business* 13, no. 2 (2022): 39. https://doi.org/10.5815/ijieeb.2022.02.03

[42] Sonmez, F. F., and B. Günel Kılıç. "Reusable security requirements repository implementation based on application/system components." Institute of Electrical and Electronics Engineers, 2021. https://doi.org/10.1109/ACCESS.2021.3133020

[43] Amin, Md Rayhan, and Tanmay Bhowmik. "Existing Vulnerability Information in Security Requirements Elicitation." In *2022 IEEE 30th International Requirements Engineering Conference Workshops (REW)*, pp. 220-225. IEEE, 2022. https://doi.org/10.1109/REW56159.2022.00049

[44] Prabhakaran, Salini, and Kanmani Selvadurai. "Performance analysis of security requirements engineering framework by measuring the vulnerabilities." *Int. Arab J. Inf. Technol.* 15, no. 3 (2018): 435-444.

[45] Ansari, Md Tarique Jamal, Abdullah Baz, Hosam Alhakami, Wajdi Alhakami, Rajeev Kumar, and Raees Ahmad Khan. "P-STORE: Extension of STORE methodology to elicit privacy requirements." *Arabian Journal for Science and Engineering* 46 (2021): 8287-8310. https://doi.org/10.1007/s13369-021-05476-z

[46] Jung, Ji-Wook, Sihn-Hye Park, and Seok-Won Lee. "A Tool for Security Requirements Recommendation using Case-Based Problem Domain Ontology." In *2021 IEEE 29th International Requirements Engineering Conference (RE)*, pp. 438-439. IEEE, 2021. https://doi.org/10.1109/RE51729.2021.00059

[47] Hibshi, Hanan, Stephanie T. Jones, and Travis D. Breaux. "A Systemic Approach for Natural Language Scenario Elicitation of Security Requirements." *IEEE Transactions on Dependable and Secure Computing* 19, no. 6 (2021): 3579-3591. https://doi.org/10.1109/TDSC.2021.3103109

[48] Emeka, Busalire Onesmus, and Shaoying Liu. "Assessing and extracting software security vulnerabilities in SOFL formal specifications." In *2018 International Conference on Electronics, Information, and Communication (ICEIC)*, pp. 1-4. IEEE, 2018. https://doi.org/10.23919/ELINFOCOM.2018.8330613

[49] Emeka, Busalire Onesmus, and Shaoying Liu. "Security requirement engineering using structured object-oriented formal language for m-banking applications." In *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pp. 176-183. IEEE, 2017. https://doi.org/10.1109/QRS.2017.28

[50] Mishra, Aditya Dev, and K. Mustafa. "Security requirements specification: A formal method perspective." In *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 113-117. IEEE, 2020. https://doi.org/10.23919/INDIACom49435.2020.9083691

[51] Mishra, Aditya Dev, and K. Mustafa. "Formalization of Security Requirements-A Case Study on a Web-Based Application." *Journal of Scientific Research* 66, no. 2 (2022). https://doi.org/10.37398/JSR.2022.660214

[52] Wilhjelm, Carl, and Awad A. Younis. "A threat analysis methodology for security requirements elicitation in machine learning based systems." In *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 426-433. IEEE, 2020. https://doi.org/10.1109/QRS-C51114.2020.00078

[53] Alkubaisy, Duaa, Luca Piras, Mohammed Al-Obeidallah, Karl Cox, and Haralambos Mouratidis. "ConfIs: a tool for privacy and security analysis and conflict resolution for supporting GDPR compliance through privacy-by-design." (2021). https://doi.org/10.5220/0010406100800091

[54] Ansari, Md Tarique Jamal, Fahad Ahmed Al-Zahrani, Dhirendra Pandey, and Alka Agrawal. "A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development." *BMC Medical Informatics and Decision Making* 20, no. 1 (2020): 1-13. https://doi.org/10.1186/s12911-020-01209-8

[55] Sadiq, Mohd, V. Susheela Devi, Javed Ahmad, and Chaudhary Wali Mohammad. "Fuzzy logic driven security requirements engineering process." *Journal of Information and Optimization Sciences* 42, no. 7 (2021): 1685-1707. https://doi.org/10.1080/02522667.2021.1972618

[56] Martínez, Andrés, Marcelo Jenkins, and Christian Quesada-López. "Identifying implied security requirements from functional requirements." In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-7. IEEE, 2019. https://doi.org/10.23919/CISTI.2019.8760631

[57] Riaz, Maria, Jason King, John Slankas, Laurie Williams, Fabio Massacci, Christian Quesada-López, and Marcelo Jenkins. "Identifying the implied: Findings from three differentiated replications on the use of security requirements templates." *Empirical software engineering* 22 (2017): 2127-2178. https://doi.org/10.1007/s10664-016-9481-1

[58] Almadani, Batoul. "STRUCTURE OF SECURITY REQUIREMENTS: INSIGHTS FROM REQUIREMENTS ELICITATION." (2022).

[59] El-Hadary, Hassan, and Sherif El-Kassas. "Capturing security requirements for software systems." *Journal of advanced research* 5, no. 4 (2014): 463-472. https://doi.org/10.1016/j.jare.2014.03.001

[60] Mai, Phu X., Arda Goknil, Lwin Khin Shar, Fabrizio Pastore, Lionel C. Briand, and Shaban Shaame. "Modeling security and privacy requirements: a use case-driven approach." *Information and Software Technology* 100 (2018): 165-182. https://doi.org/10.1016/j.infsof.2018.04.007

[61] Bulusu, Sravani Teja, Romain Laborde, Ahmad Samer Wazan, Francois Barrère, and Abdelmalek Benzekri. "Which security requirements engineering methodology should I choose? Towards a requirements engineering-based evaluation approach." In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pp. 1-6. 2017. https://doi.org/10.1145/3098954.3098996

[62] Katt, Basel, and Nishu Prasher. "Quantitative security assurance metrics: REST API case studies." In *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*, pp. 1-7. 2018. https://doi.org/10.1145/3241403.3241464

[63] Mohamad, Mazen, Jan-Philipp Steghöfer, and Riccardo Scandariato. "Security assurance cases—state of the art of an emerging approach." *Empirical Software Engineering* 26, no. 4 (2021): 70. https://doi.org/10.1007/s10664-021-09971-7

[64] Xiong, Wenjun, and Robert Lagerström. "Threat modeling–A systematic literature review." *Computers & security* 84 (2019): 53-69. https://doi.org/10.1016/j.cose.2019.03.010

[65] Fabian, Benjamin, Seda Gürses, Maritta Heisel, Thomas Santen, and Holger Schmidt. "A comparison of security requirements engineering methods." *Requirements engineering* 15 (2010): 7-40. https://doi.org/10.1007/s00766-009-0092-x

[66] Salini, P., and S. Kanmani. "Survey and analysis on security requirements engineering." *Computers & Electrical Engineering* 38, no. 6 (2012): 1785-1797. https://doi.org/10.1016/j.compeleceng.2012.08.008

[67] Silva, Paulina, René Noël, Santiago Matalonga, Hernán Astudillo, Diego Gatica, and Gastón Marquez. "Methodologies to identify and mitigate security threats in software development: two systematic reviews." *CLEI Electronic Journal* 19, no. 3 (2016): 5. https://doi.org/10.19153/cleiej.19.3.5

[68] Muñante, Denisse, Vanea Chiprianov, Laurent Gallon, and Philippe Aniorté. "A review of security requirements engineering methods with respect to risk analysis and model-driven engineering." In *Availability, Reliability, and Security in Information Systems: IFIP WG 8.4, 8.9, TC 5 International Cross-Domain Conference, CD-ARES 2014 and 4th International Workshop on Security and Cognitive Informatics for Homeland Defense, SeCIHD 2014, Fribourg, Switzerland, September 8-12, 2014. Proceedings 9*, pp. 79-93. Springer International Publishing, 2014. https://doi.org/10.1007/978-3-319-10975-6_6

[69] Joshi, Chanchala, and Umesh Kumar Singh. "Information security risks management framework–A step towards mitigating security risks in university network." *Journal of Information Security and Applications* 35 (2017): 128-137. https://doi.org/10.1016/j.jisa.2017.06.006

[70] Mohammed, Nabil M., Mahmood Niazi, Mohammad Alshayeb, and Sajjad Mahmood. "Exploring software security approaches in software development lifecycle: A systematic mapping study." *Computer Standards & Interfaces* 50 (2017): 107-115. https://doi.org/10.1016/j.csi.2016.10.001

[71] Pacheco, Carla, Ivan García, and Miryam Reyes. "Requirements elicitation techniques: a systematic literature review based on the maturity of the techniques." *IET Software* 12, no. 4 (2018): 365-378. https://doi.org/10.1049/iet-sen.2017.0144