SECURITY REQUIREMENTS ELICITATION AND CONSISTENCY VALIDATION: A SYSTEMATIC LITERATURE REVIEW

[1] NURIDAWATI MUSTAFA, [2] MASSILA KAMALRUDIN, [3] SAFIAH SIDEK
[1] Postgraduate Student, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
[2,3] Associate Professor, Innovative Software System and Service Group (IS^3), Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.
Email: [1]nuridawati@gmail.com, [2]massila@utem.edu.my, [3]safiahsidek@utem.edu.my

ABSTRACT

Security requirements are important in developing secure software development. **Objectives**: This study plans to identify properties of security requirements for developing secure software as well as to analyse the existing works for requirements validation. The gaps and limitations of each approach was discussed in this study. **Method**: A systematic literature review is conducted to identify and analyse related literature on elicitation of security requirements for developing secure software. **Findings**: There are four results: (1) the security properties highly considered for developing secure software are “Confidentiality”, “Integrity” “Identification & Authentication”, and “Availability”; (2) the approaches in validating security requirements are controlled user experiments, tools and manual checklist; (3) the security references used are the NIST, the Common Criteria and the ISO/IEC; and (4) security requirements template and consistency checking. Finally, the gaps and limitations of the existing works were also discussed. **Conclusion**: The primary challenge of security requirements during elicitation is to write the correct security requirements and validating the consistency of security requirements. As such, requirements engineers should consider the challenges posed by security requirements in eliciting and validating security requirements.

Keywords: *Security Requirements, Consistency Management, Security Requirements Validation, Security Requirement Engineering, Secure Software*

1. INTRODUCTION

Building secure software is becoming essential considering security is a crucial aspect of software in today’s world. In the last decade, software system security has become an increasingly growing concern due to the large number of incidents and attacks targeting software systems. Attackers exploit software vulnerabilities and cause threats to the systems such as stealing sensitive information and manipulating data, resulting in denial of service [1]. According to [2], the US National Institute of Standards and Technology (NIST) estimates that the US economy loses $60 billion each year in costs associated with developing and distributing software patches and reinstalling systems that have been infected, as well as costs from the loss of productivity due to computer malware and other problems enabled by software errors.

Security requirements is defined as a system specification of its required security, such as the specification towards types and levels of protection necessary for the data, information, and application of the systems. The examples of security requirements are authentication requirements, authorization requirements, intrusion detection requirements, and others [6]. Security requirements are likewise separated into two sections which are the functional and non-functional requirements.

Capturing accurate functional security requirements is important for the development of secure software. It needs to be accurately defined because poor elicited functional security requirements could cause failure to the development and consume higher cost [7]. Furthermore, inaccurate functional security requirements could lead to incorrect generation of non-functional security requirements. In addition, the process of

Journal of Theoretical and Applied Information Technology
31st August 2018. Vol.96. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

eliciting security requirements is complicated and requires the requirement engineers to have security experience in the process of eliciting consistent security requirements for the clients-stakeholders.

Drawn from the above mentioned scenario, we believe that it is important to have a mean that could elicit and validate security requirements at the early stage of the secure software development. Yet, a proper elicitation mechanism of security requirements elicitation is found to be lacking especially in writing consistent security requirement.

Motivations from these constraints, this study presents a Systematic Literature Review (SLR) that provides two findings: 1) reveals the most needed properties of security requirements for software development and the validation method used. 2) identification of the gaps and limitations of the current approach for security requirements elicitation and consistency validation.

This paper is organized in six sections. After this section, Section 2 will explained the reviewing method activities that addresses our research questions. Then, in Section 3, the review result is being discussed. The overall findings for each research questions are presented in Section 4. Next, the limitations of this study is explained in Section 5. Finally, the conclusion and the future works of this study is presented in Section 6.

2. REVIEW METHOD

This study used the SLR method proposed by [9]. This SLR consists of three main activities, which are firstly the Planning Phase that consists of the Review Method activities. Secondly, the Conducting phase that involved the execution of reviewing activities and finally the Reporting review result phase. Figure 1 summarizes the activities carried out within the three steps. The following are the description of the tasks performed in each phase.

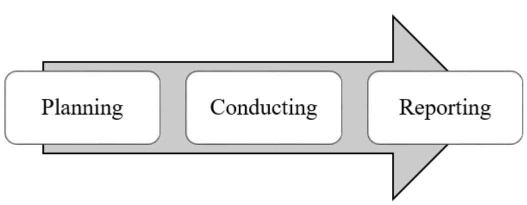

Figure 1: The three phases in systematic literature review

2.1 Planning The Review

2.1.1 Research questions

Research questions (RQ) were specified to keep the review focused. Table 1 shows the use of PICOC [10] for the structuring of the research questions.

Table 1: Summary of PICOC

Population	Security Requirements Elicitation, Security Requirement Engineering
Intervention	Security Requirements Elicitation Problems", Model, Methods, Techniques, Best-Practice Template
Comparison	Existing model, methods and techniques
Outcomes	Security Requirements Best-Practice Template, A New Validation Approach For Validating Consistency of Functional Security Requirements
Context	Empirical Studies in Academia and Industry

In planning phase, we designed the following questions in Table 2 for data extractions. As overall, this SLR was conducted to address two main objectives. Firstly, is to identify the essential security requirements properties for secure software development. Secondly, is to identify the gaps and limitations of existing techniques and approaches used for validating the consistency of security requirements.

Table 2: Research Questions

ID	Research Question	Motivation
RQ1	1.1 What are the security properties considered for developing secure software?	Identify the security properties considered for developing secure software.
	1.2 What are the approaches used to validate security requirements?	Identify the existing approaches used in security requirement validation.
RQ2	2.1 What are security references used as guidance for secure development?	Identify the existing security references used in secure development.
	2.2 What are the existing work in secure requirements template which includes consistency checking?	Identify the existing security template including consistency checking used for secure development.

2.1.2 Review protocol formulation and validation

The goal of this review was to thoroughly reviewing the existing literatures on validating the consistency of security requirements. Next, we specifies our review protocol for the selection of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

source, selection procedure, quality assessment checklist and strategy for data extraction.

2.1.2.1 Selection of source

After finalising the research questions, we conducted the search process. The related digital databases with our study is shown in Table 3.

Table 3: Digital Database Library

Source	Links
ACM DL	https://dl.acm.org/
Elsevier	https://www.elsevier.com/solutions/scopus
Google Scholar	https://scholar.google.com/
IEEEXplore	https://ieeexplore.ieee.org/Xplore/home.jsp
Science Direct	https://www.sciencedirect.com/
Scopus	https://www.scopus.com/search/form.uri?display=basic
Springer	https://link.springer.com/

2.1.2.2 Procedure of study selection

The selection process following steps in Figure 2 was conducted systematically.

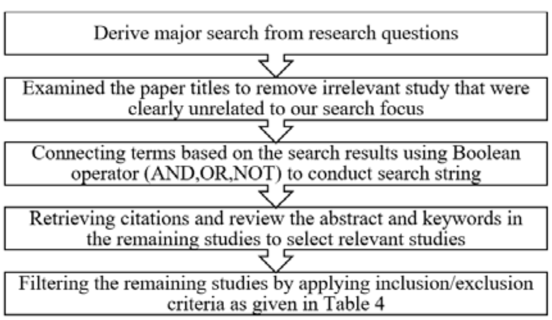

Figure 2: Selection Process[10]

Table 4: Inclusion and Exclusion criteria

Inclusion Criteria	Exclusion Criteria
1. Papers on security properties for secure software development. 2. Papers on consistency management for security requirements. 3. Papers on consistency validation for security requirements. 4. Papers on Security Requirement Engineering.	1. Papers presented but not subject to peer review. 2. Papers presenting results without supporting evidence. 3. Papers not related to the research questions. 4. Papers that are unclear or duplicated reports of the same study.

2.1.2.3 Quality assessment checklist

Each SLR is selected based on quality checklists provided by Kitchenham and Charters [10]. The assessment is based on four quality assessments as in Table 5 below:-

Table 5: Quality Assessments (QA) [10]

ID	QA Questions
QA1	Are the reviews on the inclusion and exclusion criteria have been well described and appropriate for the study?
QA2	Is the literature search liable to cover every single relevant studies?
QA3	Did the reviewers assess the quality or validity of included studies?
QA4	Were the essential information or studies sufficiently depicted?

Three possible answers to the questions are Yes=1, Partly=0.5 and No=0. Criteria that is not applicable to any study was excluded from the evaluation. Studies that scored less than 50% in quality assessment were rejected as they do not provide basic information of their research methodology, as shown in Table 6.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 6: Question scores [10]

ID	Y (Yes)	P (Partly)	N (No)
QA 1	The inclusion criteria are explicitly defined in the study	The inclusion criteria are implicit.	The inclusion criteria are not defined and cannot be readily inferred.
QA 2	The authors have either searched 4 or more digital libraries and included additional search strategies or identified and referenced all journals addressing the topic of interest	The authors have search ¾ digital libraries with no extra search strategies or search a defined but restricted set of journals and conference proceedings	The authors have search up to 2 digital libraries or an extremely restricted set of journals
QA 3	The authors have explicitly defined quality criteria and extracted them from each primary study	The research question involves quality issues that are addressed by the study	No explicit quality assessment of individual primary studies has been attempted.
QA 4	Information is presented about each study	Only the summary of information about primary studies is presented	The results of the individual primary studies are not specified

2.1.2.4 Strategy of data extraction

The relevant information for answering the research questions required to be extracted from selected primary studies are shown in Table 7. Data extraction form was used to make sure that the task was carried out in an accurate, consistent and complete manner.

Table 7: Data extraction

Search focus	Data item	Description
General	Bibliography	Author, year, title, source
	Type of article	Journal/conference paper/technical report
	Study aims	The aim or goals of primary study
	Study design	Controlled experiments/survey
RQ1	Comparison	Define the attributes for secure software
	Examples	Examples of consistency validation for security requirements
RQ2	Testing method	Description of method used
	Validation method	Describe the validation of method used
	Existing/new/extension	Whether testing and validation method is new, existing from existing method

2.2 Conducting The Review

2.2.1 Identifying relevant studies and primary studies

To identify relevant studies, firstly, we examined the title of the papers and remove any studies that are not clearly related to the research focus. Secondly, we examine the abstract, key words and the conclusion of the papers to eliminate additional unrelated studies. After these two steps, only 87 studies remained. Next, we examined these 87 papers based on inclusion/exclusion criteria in Table 4 to select the primary studies for this SLR.

2.2.2 Data extraction and quality assessments

Data extraction form in Table 7 was used to extract important information from the primary studies. Many primary studies did not answer all the questions in the data extraction form. Next, quality assessment questions were used based on the type of study in Table 5 or Table 6 to each primary study. 'Yes' and 'No' answer were used for quality assessment questions. Binary scale was used since the study did not provide quality score data.

3. REVIEW RESULTS

Section 3 presents the synthesized evidence from previous section. Additionally, we used the selected primary papers to provide answers to the research questions. Table 8 shows the number of studies for quality assessment through level of layers in SLR. As final, out of 77 papers, only 35 primary studies were accepted and 42 primary studies were rejected.

Table 8: Paper Study for Quality Assessment

Criteria	Paper Study
Before Quality Assessment	87
Duplicate	2
Exclusion	8
After Quality Assessment	77
Accepted	35
Rejected	42

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Quality Assurances

Table 9 below shows the details of accepted and rejected papers based on the quality assessments conducted during the searching process. For this purpose, papers that received 50% and above are considered as accepted papers, while papers that received less than 50% are rejected.. Thus, out of 77 papers, the final result shows that 35 primary studies were accepted, while 42 primary studies were rejected.

Table 9: Quality Assurance

PID	QA1	QA2	QA3	QA4	R (%)	Status
PS1	0.5	0.5	0.5	0.5	50	Accepted
PS2	0	0.5	0.5	0.5	37.5	Rejected
PS3	0.5	0.5	0.5	0.5	50	Accepted
PS4	0.5	0.5	1	0.5	62.5	Accepted
PS5	0	0.5	0.5	0.5	37.5	Rejected
PS6	1	0.5	0.5	0.5	62.5	Accepted
PS7	0.5	0.5	0.5	0.5	50	Accepted
PS8	0	0.5	0.5	0.5	37.5	Rejected
PS9	0.5	0.5	0.5	0.5	50	Accepted
PS10	0.5	0.5	0.5	0.5	50	Accepted
PS11	0	0.5	0.5	0.5	37.5	Rejected
PS12	0.5	0.5	0.5	0.5	50	Accepted
PS13	0	0.5	0.5	0.5	37.5	Rejected
PS14	0.5	0.5	0.5	0.5	50	Accepted
PS15	0	0.5	0.5	0.5	37.5	Rejected
PS16	0.5	0.5	0.5	0.5	50	Accepted
PS17	1	0.5	0.5	0.5	62.5	Accepted
PS18	1	0.5	0.5	0.5	62.5	Accepted
PS19	0.5	0	0.5	0.5	37.5	Rejected
PS20	0	0.5	0.5	0.5	37.5	Rejected
PS21	0	0.5	0.5	0.5	37.5	Rejected
PS22	0.5	0.5	0.5	0.5	50	Accepted
PS23	0	0.5	0.5	0.5	37.5	Rejected
PS24	0	0.5	0.5	0.5	37.5	Rejected
PS25	0	0.5	0.5	0.5	37.5	Rejected
PS26	1	0.5	0.5	0.5	62.5	Accepted
PS27	1	0.5	0.5	0.5	62.5	Accepted
PS28	0.5	0	0.5	0	25	Rejected
PS29	0	0.5	0.5	0	25	Rejected
PS30	0	0.5	0.5	0	25	Rejected
PS31	0.5	0.5	0.5	0.5	50	Accepted
PS32	0.5	0.5	0.5	0	37.5	Rejected
PS33	0.5	0.5	0.5	0	37.5	Rejected
PS34	0	0.5	0.5	0	25	Rejected
PS35	0.5	0.5	0.5	0.5	50	Accepted
PS36	0	0.5	0.5	0	25	Rejected
PS37	0	0.5	0.5	0	25	Rejected
PS38	0.5	0	0.5	0	25	Rejected
PS39	0	0.5	0.5	0	25	Rejected
PS40	0.5	0	0.5	0	25	Rejected
PS41	0.5	0.5	0.5	0.5	50	Accepted
PS42	0	0.5	0.5	0.5	37.5	Rejected
PS43	0.5	0.5	0.5	0.5	50	Accepted
PS44	0.5	0.5	0.5	0.5	37.5	Accepted
PS45	0	0.5	0.5	0.5	37.5	Rejected
PS46	0	0.5	0.5	0.5	37.5	Rejected
PS47	0	0.5	0.5	0.5	37.5	Rejected
PS48	0.5	0	0.5	0	25	Rejected
PS49	0.5	0	0.5	0	25	Rejected
PS50	0.5	0.5	0.5	0.5	50	Accepted
PS51	0.5	0	0.5	0	25	Rejected
PS52	0.5	0	0.5	0	25	Rejected
PS53	0.5	0	0.5	0	25	Rejected
PS54	0	0.5	0.5	0.5	37.5	Rejected
PS55	0.5	0.5	0.5	0.5	25	Accepted
PS56	0	0.5	0.5	0.5	37.5	Rejected
PS57	0.5	0	0.5	0	25	Rejected
PS58	0.5	0.5	0.5	0.5	50	Accepted
PS59	0.5	0	0.5	0	25	Rejected
PS60	0.5	0	0.5	0	25	Rejected
PS61	0.5	0.5	0.5	0	37.5	Rejected
PS62	0.5	0.5	0.5	0.5	50	Accepted
PS63	0.5	0.5	0.5	0	37.5	Rejected
PS64	0.5	0	0.5	0	25	Rejected
PS65	0.5	0.5	0.5	0	37.5	Rejected
PS66	0.5	0.5	0.5	0.5	50	Accepted
PS67	0.5	0.5	0.5	0.5	50	Accepted
PS68	0.5	0	0.5	0	25	Rejected
PS69	1	0.5	0.5	0.5	62.5	Accepted
PS70	0.5	0.5	0.5	0.5	50	Accepted
PS71	0	0.5	0.5	0.5	37.5	Rejected
PS72	0.5	0.5	0.5	0.5	50	Accepted
PS73	0.5	0.5	0.5	0.5	50	Accepted
PS74	0.5	0.5	0.5	0.5	50	Accepted
PS75	0.5	0.5	0.5	0.5	50	Accepted
PS76	0.5	0.5	0.5	0.5	50	Accepted
PS77	0.5	0.5	0.5	0.5	50	Accepted
PS78	0.5	0.5	0.5	0.5	50	Accepted

3.2 Quality Extractions

Based on Table 10, 35 papers related to research questions were sorted out. The study identified that

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

several studies were appointed to single and multiple studies.

Table 10: Quality Extractions

Paper ID	Ref	RQ1.1	RQ1.2	RQ2.1	RQ2.2
PS1	[11]	/	/	/	
PS3	[12]	/	/		
PS4	[13]	/		/	
PS6	[14]	/	/		/
PS7	[15]	/	/	/	
PS9	[16]	/			
PS10	[17]	/			
PS12	[1]	/	/		/
PS14	[18]	/	/	/	
PS16	[19]	/	/	/	
PS17	[20]	/		/	/
PS18	[21]	/	/		
PS22	[22]	/			
PS26	[23]	/			
PS27	[4]	/			
PS31	[24]	/	/		
PS35	[25]	/			
PS41	[26]	/	/	/	
PS43	[27]	/	/		
PS44	[28]	/	/		
PS50	[29]	/	/		
PS55	[30]	/	/		
PS58	[31]	/	/		
PS62	[32]	/			
PS65	[33]	/	/		
PS66	[34]	/			
PS67	[35]	/			
PS69	[36]	/			
PS70	[37]	/			
PS72	[38]	/			
PS73	[39]	/			
PS74	[40]	/			
PS75	[41]	/			
PS76	[42]	/			
PS77	[43]		/		
PS78	[44]			/	

Table 7 shows that Google Scholar provided 12 relevant studies to the research questions, followed by ACM Digital Library with 8 studies.

Table 11: Digital library of Paper Study

Database Library	No. Paper Study	Detail
IEEE Xplore	7	PS17, PS31, PS35, PS58, PS66, PS76, PS77, PS78
ScienceDirect	3	PS10, PS12, PS41
Springer	5	PS26, PS27, PS72, PS74, PS75
Google Scholar	12	PS3, PS4, PS6, PS9, PS16, PS43, PS44, PS62 PS65, PS67, PS70, PS73
ACM Digital Library	8	PS1, PS7, PS14, PS18, PS22, PS50, PS55, PS69

Table 12 shows type of papers that we investigated based on their effectiveness for this study. As summary, we found that the conference proceedings and journals article contributed the highest with 22 and 11 studies. Furthermore, this study also includes book sections and thesis.

Table 12: Type of Paper Study

Type of Study	No. Paper Study	Detail
Conference Proceedings	22	PS1, PS3, PS4, PS6, PS7, PS9, PS14, PS16, PS17, PS18, PS22, PS35, PS50, PS55, PS65, PS66, PS67, PS69, PS70, PS76, PS77, PS78
Journal	11	PS10, PS12, PS26, PS27, PS31, PS41, PS43, PS58, PS62, PS73, PS74
Book Section	1	PS72, PS75
Thesis	1	PS44

3.2.1 RQ1.1 What are the security properties being considered for developing secured software?

Based on the list of the most used security properties in Table 13, the study found that "Confidentiality" and "Integrity" are the highly considered, which accounts for 20 studies. This is followed by "Identification & Authentication" with 18 studies, "Availability" with 17 and "Privacy" with 13 studies.

Table 13: Security Properties

Security Attributes	Quantity	Paper ID
Confidentiality	20	PS1, PS3, PS6, PS7, PS12, PS14, PS16, PS17, PS18, PS22, PS24, PS31, PS41, PS44, PS35, PS50, PS55, PS58, PS69, PS76
Integrity	20	PS1, PS3, PS4, PS12, PS14, PS16, PS17, PS18, P22, PS24, PS31, PS35, PS41, PS43, PS44, PS50,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Security Attributes	Quantity	Paper ID
		PS55, PS62, PS65, PS69, PS76
Identification & Authentication	18	PS1, PS3, PS4, PS6, PS7, PS9, PS12, PS14, PS16, PS17, PS18, PS22, PS24, PS43, PS44, PS62, PS65, PS69, PS76
Availability	17	PS1, PS3, PS7, PS12, PS14, PS16, PS17, PS18, P22, PS24, PS31, PS35, PS41, PS43, PS44, PS69, PS76
Privacy	13	PS1, PS3, PS6, PS14, PS16, PS17, PS18, PS24, PS43, PS44, PS58, PS62, PS65, PS69
Accountability	11	PS1, PS3, PS12, PS16, PS17, PS18, PS24, PS35, PS44, PS50, PS69
Authorization	11	PS4, PS9, PS16, P22, PS24, PS41, PS43, PS44, PS62, PS65, PS69, PS76
Non-Repudiation	7	PS7, PS14, PS16, PS44, PS62, PS65, PS69, PS76
Access Control	3	PS4, PS9, PS24
Compliance	2	PS14, PS24
Intrusion Detection and Response	2	PS44, PS62, PS65
Accessibility	1	PS50
Auditability	1	P22
Configurability	1	PS76
Cryptography-Encryption	1	PS4
Data at Rest Security	1	PS9
Immunity	1	PS62, PS65
Physical Protection	1	PS62, PS65
Recoverability	1	PS44
Scalability	1	PS76
Security Auditing	1	PS62, PS65
Security Management	1	PS14, PS44
Session Management	1	PS9
Survivability Requirements	1	PS62, PS65
System Maintenance	1	PS62, PS65
Timeliness	1	PS76
Transparency	1	PS14
Usage Frequency	1	PS76

a) Confidentiality

Most of the studies focus on confidentiality. As in [45], confidentiality refers to requirements containing private or confidential information that must not be disclosed to unauthorized individuals. Besides, it is use to express the security objectives of an Information System. Additionally, it helps to perform search in the repository that leads to the identification of the security pattern virtual private network (VPN) [15]. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can receive it. Access is restricted to those authorized to view the data. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands [46].

b) Integrity

Integrity is important when performing ‘create, update, delete’ and ‘transfer’ actions [11]. In banking, finance, and business-related computing, the security emphasis is on the protection of assets. While disclosure is an important risk, the far greater risk is the unauthorized modification of information. Since protecting the integrity of information produces trust from the customers, it builds confidence for organizations responsible for maintaining these data and processes [47]. In [13], integrity is one of the important element that cannot be checked directly using their tool.

c) Identification and Authentication

The properties of “Identification and& Authentication” property perform the mapping between the user’s identity within the system or application and the person or system accessing the system. This service is essential for many of the concerns in security, as most of the internal security decisions rely on correct auditing and analysis, correctly identifying and authenticating the user or system. There are many types of authentication, including password, bio-metric, third-party, and capability-based [47].

d) Availability

According to ISO/IEC 27000 [48], availability is a property of being accessible and usable upon demand by an authorized entity. Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts [46].

3.3.2 RQ1.2 What are the approaches used to validate security requirements?

Based on Table 14, most of the research validates security requirements using control user experiment. The validation approach can be categorized using manual checklist, user experiment, expert validation and using tool. Based on [1], they adopt a checklist

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

from Information Assurance Technology Analysis Center (IATAC) to evaluate the resulting security requirements that aim for providing good security requirements that are feasible, unambiguous and non-conflicting with other requirements. Meanwhile [21], conducted a controlled experiment involving 50 graduate students enrolled in a software security course to evaluate implied security requirements. Similarly in [11], 28 students agreed to participate on validating the overall DIGS framework. In [18], they validated requirements patterns in cooperation with industrial partners of the ClouDAT project. [19] on the other hand, used the experts from IBM Corporation from India, Austria, France and Malaysia to evaluate their security patterns. Likewise, validation tool, specifically ProVerif was used by [14] to perform consistency checks and to allow the verification of a broad range of properties of the system model.

Table 14: Security Requirements Validation Approach

Type Selection	Quantity	Paper ID
Control User Experiments	3	PS1, PS18, PS76
Security Checklist / Data and Analysis	1	PS12
Industrial partners discussion	1	PS14
Experts in security requirements from IBM Corporation from India, Austria, France and Malaysia.	1	PS16
Model and Design Validation	1	PS43
Pattern Mapping Effectiveness	1	PS44
Peer review log	1	PS55
ProVerif Tool	1	PS6
Random Test Training set-based	1	PS3
Satisfaction Argument	1	PS73
Structured Informal and Formal Argumentation	1	PS50
Supervisory Control And Data Acquisition (SCADA)	1	PS7
Validation Report	1	PS41

3.3.3 RQ2.1 What are security references used as guidance?

Based on findings in Table 15, there are several types of references used as guideline for security requirements which are the NIST Special Publication 800-53, SRS, ISO/IEC 27005, ISO 27001, NIST and Common Criteria. There are also studies, such as [20] that used combinations of this reference for identifying the security objectives in their templates.

Table 15: Security Guidelines

Type Selection	Quantity	Paper ID
Common Criteria	3	PS16, PS44, PS78
Common Criteria & ECMA Protection Profile	1	PS58
Common Criteria & NIST	1	PS17
IEEE 830-1998	1	PS41
ISO 27001	1	PS14
ISO/IEC 27005	1	PS7
NIST Special Publication 800-53	1	PS1
SRS	1	PS4

3.3.4 RQ2.2 What are the existing work in security requirements template which including consistency checking?

Based on Tale 16, [14], only utilized the consistency checking using anonymous functions, like lambda functions in C++ 11 or Java8. This approach returns a string resulting from the rule check or a more complex object, which could be executed automatically without the provision of a security template. In [1], checking conflict between requirements is manually done. While in [20], the researchers provided semi-automated security template without consistency management.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 16: Security Requirements Template vs. Consistency Checking

PID	Security Requirements Template			Consistency Checking		
	M	SM	FA	M	SM	FA
PS1	X	X	X	X	X	X
PS3	X	X	X	X	X	X
PS4	X	X	X	X	X	X
PS6	X	X	X	X	√	X
PS7	X	X	X	X	X	X
PS9	X	X	X	X	X	X
PS12	X	X	X	√	X	X
PS14	X	X	X	X	X	X
PS16	X	X	X	X	X	X
PS17	X	√	X	X	X	X
PS18	X	X	X	X	X	X
PS22	X	X	X	X	X	X
PS31	X	X	X	X	X	X
PS35	X	X	X	X	X	X
PS41	X	X	X	X	X	X
PS43	X	X	X	X	√	X
PS44	X	X	X	X	X	X
PS50	X	X	X	X	X	X
PS65	X	X	X	X	X	X

M-Manual, SA- Semi-Automated, FA- Fully-Automated

4. FINDINGS

The findings have addressed the following four research questions of this study:

QA 1.1 What are the security properties being considered for developing secure software?

QA 1.2 What are the approaches used to validate security requirement?

QA 2.1 What are security references used as guidance for secure development?

QA 2.2 What are the existing work in security requirement template which including consistency checking?

The following are the summary of the main findings from the SLR. These findings are considered as the challenges in consistency management for security requirements.

4.1 The Most Security Properties Being Considered For Developing Secure Software

The study discovered the important security properties being considered for developing secure software are Confidentiality, Integrity, Identification & Authentication and Availability. Based on the result, Confidentiality is the most highly considered for developing secure software and it is known as a set of rules that limits the access to the information. Additionally, is not made available or disclosed to unauthorized individuals, entities, or processes.The study discovered the important security properties being considered for developing secure software are Confidentiality, Integrity, Identification & Authentication and Availability. Based on the result, Confidentiality is the most highly considered for developing secure software and it is known as a set of rules that limits the access to the information. Additionally, is not made available or disclosed to unauthorized individuals, entities, or processes.

4.2 The Most Commonly Used Approach To Validate Security Requirements

The validation approach can be categorized into four approaches, which are validating user experiment, using manual checklist, expert validation and tool validation. The results show that the widely used validation methods are user experiments and expert validations.

4.3 The Most Commonly Used Security References

There are several types of references used as guideline for security requirements, which are the NIST Special Publication 800-53, the SRS, ISO/IEC 27005 and the combination of ISO 27001 and Common Criteria.

4.4 The Existing Security Requirements Templates

There are limited solutions that cater for writing security requirements. Although writ-ing templates has been proposed, the template has been drawn from a particular standard; hence covering limited security properties in healthcare domain that as been proposed by [14] and [1] in Table 16. The existing works also does not cater the consistency checking for security requirements.

5. LIMITATIONS

The weakness of this SLR is that it fails to ensure that the search facilities return a set of papers similar to a search process conducted independently. Therefore, there may be other solutions provided by the security requirement elicitations and validations methods due to the failure to capture some of the methods proposed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In security requirements elicitation, there are limited solutions that cater for writing security requirements. The existing initiatives has been drawn from a particular standard; hence covering limited security properties that only applicable in limited domain. Limited research provides full end-to-end writing template with consistency checking support, which means from the natural language requirement to models and then to the prototype. Whereas, in security requirements validation, the consistency checking is still lacking to support confirming consistency and validating requirements.

6. CONCLUSIONS AND FUTURE WORKS

Our research work contributes to minimise the research efforts on security requirements elicitation and validation for developing a secure software. The findings of this paper could help requirement engineers and client-stakeholders to analyze and identify the appropriate security requirement properties and to improve the quality of security requirements. In addition, there are advantages for requirement engineering researchers to find solution, awareness on the process and method and identify an approach to solve the challenges identified in security requirements elicitation and validation area.

This paper described a SLR targeted at empirical studies of security requirements attributes, and for this purpose a total of 35 primary studies were selected. The study found four properties, namely i) confidentiality, ii) integrity, iii) identification & authentication and iv) availability, are essential for secure software development. However, the most important security requirements property is confidentiality, which is necessary for the use of secure software development such as the Internet banking, Flight booking and many others. The findings also highlighted that security requirements properties are the major concern in the study. There were various methods employed to elicit security requirements for software development, and the most commonly used methods of validating the security requirements are user experiments and experts. Most of the studies reported that a variety of approaches are the common method used for security requirements elicitation. This study concludes that analyzing security requirements elicitation is rarely employed in the software development. It is crucially needed at the early stage of development, considering that software products are highly exposed to vulnerabilities and privacy issue.

ACKNOWLEDGEMENT

We would like to thank Universiti Teknikal Malaysia Melaka (UTeM) and Ministry of Higher Education (MoHE) for the funding research: FRGS/1/2016/ICT01/FTMK-CACT/F00325

REFERENCES:

[1] H. El-Hadary and S. El-Kassas, "Capturing Security Requirements For Software Systems," *J. Adv. Res.*, vol. 5, no. 4, pp. 463–472, Jul. 2014.

[2] M. Zhivich and R. K. Cunningham, "The Real Cost of Software Errors," *IEEE Secur. Priv.*, vol. 2, no. 2, pp. 87–90, 2009.

[3] G. S. Walia and J. C. Carver, "A Systematic Literature Review To Identify And Classify Software Requirement Errors," *Inf. Softw. Technol.*, vol. 51, no. 7, pp. 1087–1109, 2009.

[4] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens, and K. Schneider, "Eliciting Security Requirements And Tracing Them To Design: An Integration Of Common Criteria, Heuristics, and UMLsec," *Springer Requir. Eng.*, vol. 15, no. 1, pp. 63–93, Mar. 2010.

[5] A. Banerjee, M. Sharma, C. Banerjee, and S. K. Pandey, "Research On Security Requirements Engineering: Problems And Prospects," *MATRIX Acad. Int. Online J. Eng. Technol.*, vol. III, no. 1, pp. 32–35, 2015.

[6] D. G. Firesmith, "Analyzing and Specifying Reusable Security Requirements," in *IEEE 11th International Conference on Requirements Engineering, RHAS 2003*, 2003, pp. 507–514.

[7] K. Schneider, E. Knauss, S. Houmb, S. Islam, and J. Jürjens, "Enhancing Security Requirements Engineering by Organizational Learning," in *Requirements Engineering*, vol. 17, no. 1, 2012, pp. 35–56.

[8] M. Kamalrudin, N. Mustafa, and S. Sidek, "A Preliminary Study: Challenges In Capturing Security Requirements And Consistency Checking By Requirement Engineers," *J. Telecommun. Electron. Comput. Eng.*, vol. 10, no. (1-7), pp. 5–9, 2017.

[9] B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, and S. Linkman, "Systematic literature reviews in software engineering – A tertiary study," *Inf. Softw. Technol.*, vol. 52, pp. 792–805, 2010.

[10] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review,"

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Inf. Softw. Technol., vol. 51, no. 1, pp. 7–15, 2009.

[11] M. Riaz, J. Stallings, M. P. Singh, J. Slankas, and L. Williams, "DIGS – A Framework for Discovering Goals for Security Requirements Engineering," in *ACM International Symposium on Empirical Software Engineering and Measurement (ESEM 2016)*, 2016, p. 35.

[12] M. Riaz, S. Elder, and L. Williams, "Systematically Developing Prevention, Detection, and Response Patterns for Security Requirements," in *Requirements Engineering Conference Workshops (REW)*, 2016, pp. 62–67.

[13] R. Jindal, R. Malhotra, and A. Jain, "Automated Classification of Security Requirements," in *International Conference on Advances in Computing, Communications and Informatics (ICACCI 2016)*, 2016, pp. 2027–2033.

[14] H. Decke and J.-P. Seifert, "Checking And Verifying Security Requirements With The Security Engineering System Model Core," in *The Fourth International Conference on Advances in Vehicular Systems, Technologies and Applications, VEHICULAR 2015*, 2015, no. c, pp. 26–35.

[15] A. Motil, B. Hamid, A. Lanusse, J.-M. Bruel, A. Motii, B. Hamid, A. Lanusse, and B. Jean-Michel, "Guiding The Selection Of Security Patterns Based On Security Requirements And Pattern Classification," in *ACM The 20th European Conference on Pattern Languages of Programs, EuroPLoP 2015*, 2015, p. 10.

[16] C. Schmitt and P. Liggesmeyer, "A Model for Structuring And Reusing Security Requirements Sources and Security Requirements," in *21st International Working Conference on Requirement Engineering: Foundation For Software Quality (REFSQ 2015)*, 2015, pp. 34–43.

[17] E. Paja, F. Dalpiaz, and P. Giorgini, "Modelling And Reasoning About Security Requirements In Socio-Technical Systems," *Data Knowl. Eng.*, vol. 98, pp. 123–143, 2015.

[18] K. Beckers, I. Côté, and L. Goeke, "A Catalog of Security Requirements Patterns For The Domain of Cloud Computing Systems," in *ACM The 29th Symposium On Applied Computing*, 2014, pp. 337–342.

[19] S. Yahya, M. Kamalrudin, S. Sidek, and J. Grundy, "Capturing Security Requirements Using Essential Use Cases (EUCs)," in *The First Asia Pacific Requirements Engineering Symposium, APRES 2014*, 2014, vol. 432 CCIS, pp. 16–30.

[20] M. Riaz, J. King, J. Slankas, and L. Williams, "Hidden In Plain Sight: Automatically Identifying Security Requirements From Natural Language Artifacts," in *IEEE 22nd International Requirements Engineering Conference, RE 2014*, 2014, pp. 183–192.

[21] M. Riaz, J. Slankas, J. King, and L. Williams, "Using Templates To Elicit Implied Security Requirements From Functional Requirements - A Controlled Experiment," in *ACM The 8th International Symposium on Empirical Software Engineering and Measurement, ESEM 2014*, 2014, p. 22.

[22] P. Salini and S. Kanmani, "Elicitation of Security Requirements for E-Health System by Applying Model Oriented Security Requirements Engineering (MOSRE) Framework," in *ACM The Second International Conference on Computational Science, Engineering and Information Technology, CCSEIT 2012*, 2012, pp. 126–131.

[23] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, "A Comparison Of Security Requirements Engineering Methods," *Springer Requir. Eng.*, vol. 15, no. 1, pp. 7–40, Mar. 2010.

[24] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh, "Security Requirements Engineering: A Framework for Representation and Analysis," *IEEE Trans. Softw. Eng.*, vol. 34, no. 1, pp. 133–153, Jan. 2008.

[25] F. A. Braz, E. B. Fernandez, and M. VanHilst, "Eliciting Security Requirements Through Misuse Activities," in *19th International Conference on Database and Expert Systems Application, DEXA 2008*, 2008, pp. 328–333.

[26] D. Mellado, E. Fernández-Medina, and M. Piattini, "A Common Criteria Based Security Requirements Engineering Process For The Development Of Secure Information Systems," *Comput. Stand. Interfaces*, vol. 29, no. 2, pp. 244–253, 2007.

[27] H. Mouratidis and P. Giorgini, "Secure Tropos: A Security-Oriented Extension Of The Tropos Methodology," *Int. J. Softw. Eng. Knowl. Eng.*, vol. 17, no. 02, pp. 285–309, Apr. 2007.

[28] D. Wu, "Security Functional Requirements Analysis For Developing Secure Software," 2007.

[29] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh, "A Framework For Security Requirements Engineering," in *Proceedings of the 2006 international workshop on Software engineering for secure systems - SESS '06*, 2006, p. 35.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[30] N. R. Mead and T. Stehney, "Security Quality Requirements Engineering (SQUARE) Methodology," in *Workshop on Software Engineering for Secure Systems—Building Trustworthy Applications*, 2005, vol. 30, no. 4, pp. 1–7.

[31] G. Sindre and A. L. Opdahl, "Eliciting Security Requirements With Misuse Cases," *Requir. Eng.*, vol. 10, no. 1, pp. 34–44, Jan. 2005.

[32] D. G. Firesmith, "Engineering Security Requirements," *J. Object Technol.*, vol. 2, no. 1, pp. 53–68, 2003.

[33] G. Sindre, D. G. Firesmith, and A. L. Opdahl, "A Reuse-Based Approach To Determining Security Requirements," in *9th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ 2003)*, 2003, vol. 8, pp. 127–136.

[34] L.-C. Lin, B. Nuseibeh, D. Ince, M. Jackson, and J. Moffett, "Introducing Abuse Frames For Analysing Security Requirements," in *The 11th IEEE International Requirements Engineering Conference*, 2003, pp. 371–372.

[35] J. Jurjens, "UMLsec: Extending UML For Secure Systems Development," in *International Conference on The Unified Modeling Language 2002*, 2002, pp. 412–425.

[36] J. Viega, "Building Security Requirements With CLASP," in *Workshop on Software Engineering for Secure Systems—Building Trustworthy Applications*, 2005, pp. 1–7.

[37] G. Sindre and A. L. Opdahl, "Capturing Security Requirements Through Misuse Cases," in *Norsk Informatikkonferanse, NIK 2001*, 2001.

[38] L. Chung, "Dealing with Security Requirements During the Development of Information Systems," in *5th International Conference on Advanced Information Systems Engineering (CAISE 1993)*, 1993, pp. 234–251.

[39] C. Banerjee, A. Banerjee, and S. . Sharma, "Use Case And Misuse Case In Eliciting Security Requirements : MCOQR Metrics Framework Perspective," *Int. J. Mod. Electron. Commun. Eng.*, vol. 5, no. 3, pp. 35–39, 2017.

[40] M. Riaz, J. King, J. Slankas, L. Williams, F. Massacci, C. Quesada-lópez, and M. Jenkins, "Identifying the Implied: Findings from Three Differentiated Replications On The Use Of Security Requirements Templates," *Empir. Softw. Eng.*, vol. 22, no. 4, pp. 2127–2178, 2016.

[41] N. Yusop, M. Kamalrudin, S. Sidek, and J. Grundy, "Automated Support to Capture and Validate Security Requirements for Mobile Apps," in *Communications in Computer and Information Science*, vol. 671, no. November, 2016, pp. 97–112.

[42] R. Goel, M. C. Govil, and G. Singh, "Security Requirements Elicitation And Assessment Mechanism (SecREAM)," in *International Conference on Advances in Computing, Communications and Informatics, (ICACCI 2015)*, 2015, pp. 1862–1866.

[43] N. Ikram, S. Siddiqui, and N. F. Khan, "Security Requirement Elicitation Techniques: The Comparison Of Misuse Cases And Issue Based Information Systems," *2014 IEEE 4th Int. Work. Empir. Requir. Eng. Emp. 2014 - Proc.*, pp. 36–43, 2014.

[44] T. Abe, S. Hayashi, and M. Saeki, "Modeling Security Threat Patterns To Derive Negative Scenarios," in *20th Asia-Pacific Software Engineering Conference (APSEC 2013)*, 2013, pp. 58–66.

[45] B. Guttman and E. A. Roback, *An Introduction to Computer Security The NIST Handbook*, no. 800. 1995.

[46] Margaret Rouse, "What is confidentiality, integrity, and availability (CIA triad)?," 2014. [Online]. Available: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA. [Accessed: 16-Jan-2018].

[47] M. Barbacci, M. H. Klein, T. A. Longstaff, and C. B. Weinstock, "Quality Attributes," 1995.

[48] ISO/IEC, "International Standard ISO/IEC 27000 (Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary)," 2016.