Jurnal
Teknologi

Full Paper

SECURITY REQUIREMENTS VALIDATION FOR MOBILE APPS: A SYSTEMATIC LITERATURE REVIEW

Noorrezam Yusop, Massila Kamalrudin*, Safiah Sidek

Centre for Advanced Computing Technology(C-ACT)
Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka

Article history
Received
15 July 2015
Received in revised form
1 October 2015
Accepted
25 October 2015

*Corresponding author
massila@utem.edu.my

Graphical abstract

Criteria	Paper Study
Before Quality Assessment	157
Duplicate	4
Exclusion	23
After Quality Assessment	130
Accepted	68
Rejected	62

Abstract

Security requirements are important to increase the confidence of mobile users to perform many online transactions, such as banking, booking and payment via mobile devices. Objective: This study aims to identify the attributes of security requirements for mobile applications (mobile apps) and the existing tools, techniques and approaches used in security requirements. The gaps and limitations for each approach are also discussed. Method: We conducted a systematic literature review to identify and analyse related literatures on validation of security requirements for mobile apps. We identified 68 studies that provide relevant information on security requirements for mobile apps. Result: There were two main findings: (1) the attributes of security requirements that are relevant for mobile apps are authentication, confidentiality, authorization, access control and integrity; (2) Mobile security testing methods for validating security requirements of mobile apps were also identified. Finally, the gaps and limitation of each approach requirements in relation to mobile apps were also discussed. Conclusions: The main challenge of security requirements is to identify the most appropriate security attributes and security testing technique to validate security requirements for mobile apps. As such, requirements engineers should consider the challenges posed by security requirements such as testing when validating and developing security requirements for mobile apps testing technique. Further, correct security requirements for security attributes of security requirements need to be considered at the early stage of development of the mobile apps development.

Keywords: Security requirements, security attribute, mobile application and validation

Abstrak

Keperluan keselamatan adalah penting untuk menambahkan keyakinan kepada pengguna telefon bimbit bagi melaksanakan banyak transaksi atas talian seperti perbankan, penempahan dan pembayaran melalui perkakasan telefon bimbit. Objektif: Tujuan kajian ini adalah untuk mengenalpasti atribut pada keperluan keselamatan untuk aplikasi telefon bimbit dan peralatan, teknik dan kaedah yang tersedia yang digunakan dalam keperluan keselamatan. Jurang dan penghadan bagi setiap kaedah juga turut dibincangkan. Kaedah: Kami juga mengendalikan Kajian Literatur Sistematik untuk mengenalpasti dan menganalisis Kajian Literatur Sistematik yang berkaitan pengesahan pada keperluan keselamatan bagi aplikasi telefon bimbit. Kami telah mengenalpasti 68 kajian membekalkan informasi yang setaraf dengan keperluan keselamatan untuk aplikasi telefon bimbit. Keputusan: Terdapat 2 pengenalpastian utama: (1) atribut pada keperluan keselamatan yang setaraf kepada aplikasi telefon bimbit iaitu pengesahan, keyakinan, kebenaran, kawalan akses, dan integriti. (2) Kaedah pengujian keselamatan telefon bimbit untuk mengesahkan keperluan keselamatan pada aplikasi telefon bimbit dikenalpasti juga. Akhir sekali, jurang dan penghadan bagi setiap kaedah keperluan dalam hubungan pada aplikasi telefon bimbit dibincangkan juga. Kesimpulan: Cabaran utama pada keperluan keselamatan adalah untuk mengenalpasti atribut keselamatan dan teknik pengujian keselamatan yang sesuai bagi pengesahan keperluan keselamatan pada telefon bimbit. Seperti, Jurutera Keperluan sepatutnya mengenalpasti cabaran yang terdedah pada keperluan keselamatan seperti pengujian apabila pengesahan dan pembangunan keperluan keselamatan bagi teknik pengujian applikasi telefon bimbit. Seterusnya, pembetulan keperluan keselamatan bagi atribut keselamatan pada keperluan keselamatan diperlukan bagi mengenalpasti pada peringkat awal pembangunan applikasi telefon bimbit.

Kata kunci: Keperluan keselamatan, atribut keselamatan, aplikasi telefon bimbit, pengesahan.

1.0 INTRODUCTION

In this era of interconnectivity, the use of mobile apps has been rapidly growing. These applications have provided easy access to bank accounts and credit card data when users do online transactions, such as flight booking and hotel booking. Thus, security is identified to be crucial requirements for any type of mobile apps and it needs need to be considered and validated from the very beginning of the application development. This is because accurate definition of security requirements helps to safeguard the accuracy and completeness of data and processing methods as well as to prevent unauthorized entities to access and to modify data especially when the transaction is made on a mobile device.

Today, mobile apps development is found to be widespread, with application development tools free of charged and a plethora of free and low-cost training resources due to low cost entry into mobile app development. However, many developers do not have any formal training in software engineering, security or quality assurance [1]. Thus, apps must adopt functionality that is more typical of larger scale, enterprise-level software to remotely access the database backend. Features such as remote data access automatically bring additional security considerations to the application that the developer may not be aware of or fully understand [2].

Drawn from the above mentioned scenario, we believe that more and more applications produced today have some of the functionality and security characteristics of enterprise-scale software. However, they do not have sufficient testing to show that app is secure [3]. In this respect, we argue that security requirements for mobile apps need to be validated as early as possible since a validation that specifies and implements security measures often reveal critical security holes and threats.

This study presents a report on a Systematic Literature Review (SLR) that identifies two findings for security requirements related to mobile apps. The first finding reveals the attributes or characteristics of security requirements for mobile apps. The second findings focuses on the identification of the gaps and limitations of the techniques, tools and approach used for validating security requirements of mobile apps. In this case, approaches and methods to validate security requirements for mobile apps will be analysed based on the selected attributes.

This paper is organized as follows: Section II describes the SLR process that addresses our research questions. The selected approaches of security requirements as well as the review of the results are described in section III. Section IV presents the discussion of the overall findings. Finally, section V presents the conclusion and future works.

2.0 REVIEW METHOD

We have conducted the SLR based on the original guidelines as proposed by Kitchenham [4]. The SLR consists of three phases, which are (1) Planning the SLR, (2) Conducting review and (3) Reporting the review. Figure 1 summarizes the activities carried out within the three steps. The following are the description of the tasks performed in each phase.

Planning
Conducting
Reporting

Figure 1 The three phases in systematic literature review

2.1 Planning the SLR

2.1.1 Research Questions

To keep the review focused, research questions (RQ) were specified. Kitchenhams et. al[4] used the Population, Intervention, Comparison, Outcomes and Context criteria (PICOC) to structure the research questions. Table I shows the use of PICOC for the structuring of the research questions.

Table 1 Summary of PICOC

Population	Security requirements, validation requirements, mobile application
Intervention	Security requirements problem, models, methods, techniques
Comparison	Existing model, methods, techniques
Outcomes	Prediction accuracy of security attributes, validating and testing method, successful security attributes, validating and testing method of security requirements prediction methods
Context	Empirical studies in academia and industry.

During the planning of our SLR, the following questions were designed for data extractions as shown in Table 2. The SLR was conducted to address two main objectives: The first objective is to identify the most relevant security attribute for mobile apps. The second objective is to identify the gaps and limitations of existing techniques and approaches used for validating security requirements of mobile apps.

Table 2 Research questions

ID	Research Question		Motivation
RQ 1	1.1	What are the important security attributes for mobile apps?	Identify the important security attributes for mobile apps
RQ 2	2.	How to validate security requirements for mobile apps?	Explain the ways to validate security requirements for mobile apps
	2.1	HoWhat are the available approaches or model and tools to validate security requirements for mobile apps?	Identify the approaches or tools available to validate security requirements for mobile apps

2.1.2 Formulation and validation of the Review Protocol

The aim of this review was to thoroughly examine the empirical literature on validating security requirements of mobile apps in a mobile application development. Next, our review protocol specifies the source of selection procedures, search process, quality assessment criteria and data extraction strategies.

2.1.2.1 Source Selection

After finalising the research questions, the search process was conducted. The source of the search was digital libraries and databases using search string, and refining search string. The list of the digital databases is based on the most popular and familiar databases to ease and broaden the set of related search papers. The list of the digital databases used to search the papers in our study is shown in Table 3.

Table 3 Digital database library

Source	Links
IEEE Xplore	ieeexplore.iee.org
ScienceDirect	sciencedirect.com
Springer	Springerlink.com
Scopus	scopus.com
Google Scholar	scholar.google.com
Elsevier	Elsevier.com
ACM Digital Library	dl.acm.org

The search strings are based on the research questions and the keywords of the research field such as software requirement engineering and defect management. The searches for relevant papers were also based on the title and the author's name. Language for the search was limited to English only.

From each research question, we identified three major terms to be used in the searching process with search terms and their synonyms as shown below.
(Problems OR issues OR attributes OR characteristics) OR (technique OR methods OR approaches)) AND (test)) OR (error OR defect OR mistake OR problem) AND (Software OR application OR program OR tool).

2.1.2.2 Study Selection Procedure

The selection procedure was conducted systematically based on the following steps.

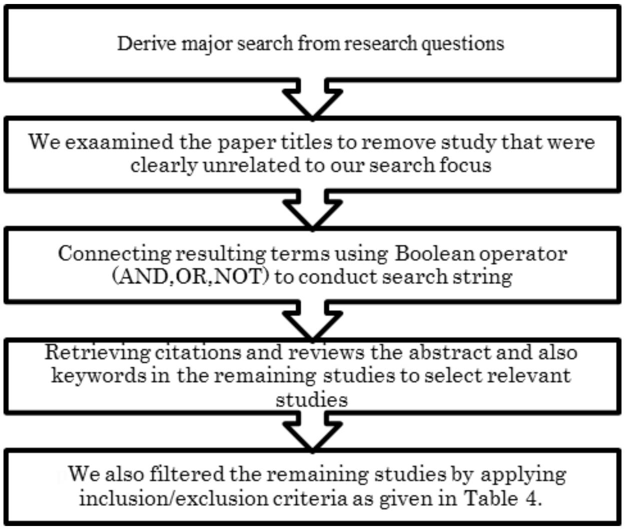
Derive major search from research questions
We exaamined the paper titles to remove study that were clearly unrelated to our search focus
Connecting resulting terms using Boolean operator (AND,OR,NOT) to conduct search string
Retrieving citations and reviews the abstract and also keywords in the remaining studies to select relevant studies
We also filtered the remaining studies by applying inclusion/exclusion criteria as given in Table 4.

Figure 2 Selection process

Table 4 Inclusion and Exclusion criteria

Inclusion criteria	Exclusion criteria
Papers focusing on security requirements	Papers present not subject to peer review
Papers describes Mobile security testing	Papers presenting results without supporting evidence
Systematic literature review	Studies not related to the research questions
Paper describes security requirements validation	Studies unclear
Paper describes validation method	
Papers describes testing method used	
Papers describes Functional and Non Functional Requirements	

2.1.2.3 . Quality Assessment Checklist

We also evaluated the quality of the selected primary studies using the selected items from the quality checklists provided by Kitchenham and Charters [5]. Table 5 and Table 6 show the quality checklists that we used for the quantitative and qualitative studies respectively. When creating quality questions, the evaluation involved four main stages of a quantitative study: design, conduct, analysis and conclusions.

Table 5 Quality assessments

QA1.	Are the review's inclusion and exclusion criteria described and appropriate?
QA2.	Is the literature search liable to have covered 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?

The questions were scored based on three potential answers to the questions: yes=1, partly=0.5 and no=0. If any of the criteria was not applicable on any studies, it was excluded from evaluating for only that particular study. Studies that scored less than 50% in quality assessment were excluded as they do not provide the basic information about their research methodology, as shown in Table 6:

Table 6 Question scores

QA1.	Y (yes), the inclusion criteria are explicitly defined in the study	P (Partly), the inclusion criteria are implicit.	N (No), the inclusion criteria are not defined and cannot be readily inferred.
QA2.	Y(yes), 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	P (Partly), the authors have search ¾ digital libraries with no extra search strategies or search a defined but restricted set of journals and conference proceedings	N (No), The authors have search up to 2 digital libraries or an extremely restricted set of journals
QA3.	Y(yes), the authors have explicitly defined quality criteria and extracted them from each primary study	P (Partly), the research question involves quality issues that are addressed by the study	N (No), no explicit quality assessment of individual primary studies has been attempted.
QA4.	Y, information is presented about each study	P (Partly), only summary information about primary studies is presented	N, the results of the individual primary studies are not specified

2.1.2.4 Data extraction strategy

The relevant information for answering the research questions required to be extracted from selected primary studies are shown in Table 7. We used data extraction form to make sure that this 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 mobile apps
	Examples	Examples of mobile validation 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

We first examined the title of the papers to remove any studies that are not clearly related to the research focus. Then we used the abstract, key words and the conclusion to eliminate additional unrelated studies. After applying these two steps, 157 studies remained. We examined these 157 studies and applied the inclusion/exclusion criteria in Table 4 to select 130 papers as primary studies for this SLR. Further, we applied the same selection steps to the reference lists of the selected 68 primary studies to find additional primary studies that are related to the research focus.

2.2.2 Data Extraction And Quality Assessments

We used the data extraction form in Table 7 to extract data from the primary studies. Many primary studies did not answer all of the questions in the data extraction form. We extracted the important information provided by the primary studies using the data extraction form. Then, depending on the type of the study, we applied the quality assessment questions in Table 5 or Table 6 to each primary study. We provided 'yes' and 'no' answers to our quality assessment questions. We used a binary scale since we were not interested in providing a quality score for the studies [6].

2.3 Reporting the Review

The data extracted from the 68 primary papers were used to formulate answers to the two research questions given in Section 2.1.1. We closely followed the guidelines provided by Kitchenham [7] when preparing the SLR report.

3.0 THE REVIEW RESULT

In this section, we present the synthesis of evidence of our SLR, beginning with the analysis from the literature. We used the selected primary papers to provide answers to the research questions as well. Table VIII describes the number of studies for quality assessment through level layer of SLR. The exclusion on this paper, 23 studies were investigated and four were investigated as redundancy during this study. After quality assessment of 130 studies, 68 studies were identified for synthesis of evidences.

Table 8 No. of Paper Study for Quality Assessment

Criteria	Paper Study
Before Quality Assessment	157
Duplicate	4
Exclusion	23
After Quality Assessment	130
Accepted	68
Rejected	62

3.1 Quality Assurances

Table 9 show the details based on the quality assessments conducted during searching process. The calculation results of this quality assessment identified above than 50% were considered accepted, while below or than 50% were rejected. Thus, we have the final result that was 68 primary studies accepted and 62 primary studies rejected.

Table 9 Quality Assurances

REF	Paper Study	QA 1	QA 2	QA 3	QA 4	Result	Status
1	PS1	0	0	0	0	0	REJECTED
2	PS2	1	0.5	1	1	0.875	ACCEPTED
3	PS3	0.5	0	0	0	0.125	REJECTED
4	PS4	0.5	0	0.5	0.5	0.375	REJECTED
5	PS6	1	0	0.5	1	0.625	ACCEPTED
6	PS7	1	0	0.5	0.5	0.5	REJECTED
7	PS9	0.5	1	0.5	0.5	0.625	ACCEPTED
8	PS11	1	0	0.5	1	0.625	ACCEPTED
9	PS12	0.5	0	0.5	0.5	0.375	REJECTED
10	PS13	1	0	0.5	1	0.625	ACCEPTED
11	PS15	0.5	0.5	0.5	0.5	0.5	REJECTED
12	PS16	1	0.5	1	1	0.875	ACCEPTED
13	PS18	0.5	0	0	0.5	0.25	REJECTED
14	PS23	1	0	0.5	0.5	0.5	REJECTED
15	PS24	0.5	0	0.5	0	0.25	REJECTED
16	PS27	0.5	0	1	1	0.625	ACCEPTED
17	PS30	0.5	0	0.5	0	0.25	REJECTED
18	PS31	0.5	0	0.5	0.5	0.375	REJECTED
19	PS32	0.5	0.5	0	0	0.25	REJECTED
20	PS33	0.5	0	0.5	0.5	0.375	REJECTED
21	PS34	1	0	0.5	0.5	0.5	REJECTED
22	PS35	0.5	0	0.5	0	0.25	REJECTED
23	PS36	0.5	0	0.5	0.5	0.375	REJECTED
24	PS37	0.5	0	0.5	0.5	0.375	REJECTED
25	PS39	0.5	0	0.5	1	0.5	REJECTED
26	PS40	1	0	0.5	1	0.625	ACCEPTED
27	PS41	1	0	0.5	1	0.625	ACCEPTED
28	PS42	1	0	0.5	1	0.625	ACCEPTED
29	PS43	0.5	0.5	1	1	0.75	ACCEPTED
30	PS44	0.5	0	0.5	0.5	0.375	REJECTED
31	PS45	0.5	0	0.5	0.5	0.375	REJECTED
32	PS46	1	0.5	1	0.5	0.75	ACCEPTED
33	PS49	0.5	0.5	0	0.5	0.375	REJECTED
34	PS50	0.5	0	0	0.5	0.25	REJECTED
35	PS52	1	0	0.5	1	0.625	ACCEPTED
36	PS53	0.5	0	0	0	0.125	REJECTED
37	PS54	0.5	0	0.5	0.5	0.375	REJECTED
38	PS55	1	0	0.5	0.5	0.5	REJECTED
39	PS56	0.5	0	0.5	0.5	0.375	REJECTED
40	PS57	1	0	0.5	1	0.625	ACCEPTED
41	PS58	1	0.5	1	1	0.875	ACCEPTED
42	PS59	0.5	0	0.5	0.5	0.375	REJECTED
43	PS60	1	0	0.5	0.5	0.5	REJECTED
44	PS61	0.5	0	0.5	0.5	0.375	REJECTED
45	PS62	0.5	0	0.5	0	0.25	REJECTED
46	PS63	0.5	0.5	0.5	0.5	0.5	REJECTED
47	PS64	0.5	0	0	0	0.125	REJECTED
48	PS65	0.5	0	0.5	0.5	0.375	REJECTED
49	PS66	0.5	0	0.5	0	0.25	REJECTED
50	PS68	0.5	0	0.5	1	0.5	REJECTED

51	PS69	0.5	0	0.5	0.5	0.375	REJECTED
52	PS70	0.5	0	0.5	0.5	0.375	REJECTED
53	PS71	0.5	0	0.5	0.5	0.375	REJECTED
54	PS72	0.5	0	0.5	0.5	0.375	REJECTED
55	PS73	0.5	0	0.5	0.5	0.375	REJECTED
56	PS74	0.5	0	0.5	0.5	0.375	REJECTED
57	PS75	1	0	0.5	1	0.625	ACCEPTED
58	PS76	1	0.5	1	1	0.875	ACCEPTED
59	PS77	1	0	1	1	0.75	ACCEPTED
60	PS78	1	0.5	1	1	0.875	ACCEPTED
61	PS80	1	0	0.5	1	0.625	ACCEPTED
62	PS82	0.5	0.5	0.5	0.5	0.5	REJECTED
63	PS83	1	0	0.5	1	0.625	ACCEPTED
64	PS84	0.5	0	1	1	0.625	ACCEPTED
65	PS85	1	0	0.5	1	0.625	ACCEPTED
66	PS86	0.5	0	0.5	0.5	0.375	REJECTED
67	PS87	0.5	0	0.5	0.5	0.375	REJECTED
68	PS88	0.5	1	0.5	1	0.75	ACCEPTED
69	PS89	0.5	0	0.5	0.5	0.375	REJECTED
70	PS90	1	0.5	0.5	1	0.75	ACCEPTED
71	PS91	1	0.5	1	1	0.875	ACCEPTED
72	PS92	1	0.5	0.5	0.5	0.625	ACCEPTED
73	PS93	1	0	0.5	1	0.625	ACCEPTED
74	PS94	1	0.5	0.5	0.5	0.625	ACCEPTED
75	PS95	1	0	0.5	1	0.625	ACCEPTED
76	PS96	1	0	0.5	1	0.625	ACCEPTED
77	PS97	1	0.5	1	1	0.875	ACCEPTED
78	PS98	1	0	0.5	1	0.625	ACCEPTED
79	PS99	1	0.5	0.5	0.5	0.625	ACCEPTED
80	PS100	1	0.5	0.5	1	0.75	ACCEPTED
81	PS101	0.5	0	0.5	0.5	0.375	REJECTED
82	PS102	0.5	0	1	0.5	0.5	REJECTED
83	PS103	0.5	0.5	0.5	0.5	0.5	REJECTED
84	PS104	1	0	0.5	1	0.625	ACCEPTED
85	PS105	0.5	0	0.5	0.5	0.375	REJECTED
86	PS106	1	0	0.5	1	0.625	ACCEPTED
87	PS107	0.5	0	0.5	0.5	0.375	REJECTED
88	PS108	0.5	0.5	1	0.5	0.625	ACCEPTED
89	PS109	1	0	1	0.5	0.625	ACCEPTED
90	PS110	1	1	1	1	1	ACCEPTED
91	PS111	1	1	1	1	1	ACCEPTED
92	PS112	1	0	1	0.5	0.625	ACCEPTED
93	PS113	1	1	1	1	1	ACCEPTED
94	PS114	1	0	0.5	0.5	0.5	REJECTED
95	PS115	0.5	1	0.5	0.5	0.625	ACCEPTED
96	PS116	0.5	0.5	0.5	0.5	0.5	REJECTED
97	PS118	0.5	0	0.5	1	0.5	REJECTED
98	PS120	1	0	0.5	1	0.625	ACCEPTED
99	PS121	1	0.5	0.5	0.5	0.625	ACCEPTED
100	PS122	0.5	0	0.5	0.5	0.375	REJECTED
101	PS123	1	0.5	0.5	1	0.75	ACCEPTED
102	PS124	0.5	1	0.5	0.5	0.625	ACCEPTED
103	PS125	1	1	1	1	1	ACCEPTED
104	PS126	0.5	1	0.5	0.5	0.625	ACCEPTED
105	PS127	1	0	0.5	1	0.625	ACCEPTED
106	PS128	0.5	1	0.5	1	0.75	ACCEPTED
107	PS129	1	0.5	0.5	1	0.75	ACCEPTED
108	PS130	1	0.5	1	1	0.875	ACCEPTED
109	PS135	0.5	1	0.5	0.5	0.625	ACCEPTED
110	PS136	0.5	0	0	0	0.125	REJECTED
111	PS137	0.5	0.5	0.5	0.5	0.5	REJECTED
112	PS139	0.5	0.5	0	0	0.25	REJECTED
113	PS140	0.5	0	0.5	0.5	0.375	REJECTED
114	PS141	0.5	1	0.5	0.5	0.625	ACCEPTED
115	PS142	0.5	1	0.5	1	0.75	ACCEPTED
116	PS143	0.5	1	0.5	1	0.75	ACCEPTED
117	PS144	1	0	0.5	1	0.625	ACCEPTED
118	PS145	0.5	0.5	0.5	0.5	0.5	REJECTED
119	PS146	0.5	1	0.5	0.5	0.625	ACCEPTED
120	PS147	0.5	0	0.5	0.5	0.375	REJECTED
121	PS148	1	1	1	1	1	ACCEPTED
122	PS149	0.5	1	0.5	0.5	0.625	ACCEPTED
123	PS150	0.5	0.5	0.5	0.5	0.5	REJECTED
124	PS151	1	0	0.5	1	0.625	ACCEPTED
125	PS152	1	0	0.5	1	0.625	ACCEPTED
126	PS153	0.5	0	0.5	0.5	0.375	REJECTED
127	PS154	1	0	0.5	1	0.625	ACCEPTED
128	PS155	1	0	1	0.5	0.625	ACCEPTED
129	PS156	1	0	0.5	1	0.625	ACCEPTED
130	PS157	1	0	1	1	0.75	ACCEPTED

3.2 Quality Extractions

Based on Table 10, we sorted the accepted 68 papers studies to related research question. We identified that several studies were appointed to single and multiple research questions. Based on our studies illustrated in Table 11, we found that IEEE Xplore provided 33 studies relevant to our study, followed by Google scholar with 27 studies and both Dblp and ACM with eight and six studies. Table 12 shows the types of papers that were investigated based on their effectiveness for our study. Journals and Papers were found to be the highest with 28 and 18 studies. Further, this study also included whitepapers and thesis with seven and four articles, as well as with the inclusion of one book.

Table 10 Quality extractions

Paper Study	Title	RQ1	RQ2	RQ2(1)
PS2	On lightweight Mobile Phone Application	/		
PS6	Mobile Testing : A Comprehensive approach	/	/	
PS9	Towards an Elastic Application Model for Augmenting the Computing Capabilities of Mobile Devices with Cloud Computing	/	/	
PS11	Testing Mobile Web Applications for W3C Best Practice Compliance			/
PS13	Security of mobile TAN on smartphones			/
PS16	Vision: Automated Security Validation of Mobile		/	/
PS27	Security in the Development Process of Mobile Grid Systems	/		
PS40	Test Automation Tools for Mobile Applications: A brief survey		/	
PS41	Device Anywhere Enterprise Automation™ and HTML			/
PS42	Selecting the Right Mobile Test Automation Strategy: Challenges and Principles			/
PS43	A Cloud based Software Testing Paradigm for Mobile		/	
PS46	Agile Development Methods for Mobile Applications		/	
PS52	Why effective Test Automation drives successful and quality driven mobile payments			/
PS57	Testing Requirements for Mobile Applications		/	
PS58	Automating GUI Testing for Android Applications		/	/
PS75	Testing Java ME Applications			/
PS76	Literature Review of Mobile Applications Testing on Cloud from Information Security Perspective	/	/	
PS77	Mobile Test Automation Framework for Automotive HM		/	/
PS78	Security Testing of the Communication among Android Applications		/	
PS80	Mobile Application Testing		/	
PS83	Cloud Enabled Test Evaluation on Mobile Web Application			/
PS84	Why Automate Test Design		/	/
PS85	MobileTest: A Tool Supporting Automatic Black Box Test for Software on Smart Mobile Devices		/	/
PS88	Concord: A Secure Mobile Data Authorization Framework for Regulatory Compliance	/		/
PS90	Mobile Application Testing – Challenges and Solution		/	/
PS91	ADAutomation: An Activity Diagram Based Automated		/	/
PS92	Cloud Based Mobile Application Testing		/	/
PS93	Secure solution for mobile access to patient's health care record	/		
PS94	Adaptive Random Testing of Mobile Application		/	
PS95	Research on Software Security and Compatibility Test for Mobile Application	/	/	/
PS96	Testing Requirements for Mobile Applications		/	
PS97	A Novel Approach of Automation Testing on Mobile		/	/
PS98	Research on Automatic Testing Technology Oriented Intelligent Mobile Terminal Software		/	/
PS99	empirical research on user acceptance of mobile searches	/		
PS100	Applying Security Assurance Techniques to a Mobile Phone Application: An Initial Approach	/	/	
PS104	Information Security of Remote File Transfers with Mobile Devices	/		
PS106	A standard for developing secure mobile applications	/		
PS108	Android forensics: Automated data collection and reporting from a mobile device	/		/
PS109	Internet of Things and Smart Objects for M-Health	/	/	/
PS110	A Service Oriented Tele-health Promotion Information System with Mobile Application			/
PS111	Mobile Testing-As-A-Service (MTaaS)– Infrastructures, Issues, Solutions and Needs		/	
PS112	A Study on the Security Technology of Enterprise Mobile Information System	/		/
PS113	Pervasive authentication and authorization infrastructures for mobile users	/	/	/
PS115	A platform for the development of location-based mobile applications with privacy protection	/		
PS120	Security Requirement of Mobile Application Based Mobile Payment System	/		
PS121	Business Process Assignment and Execution in Mobile Environments		/	/
PS123	A Systems Engineering Approach to Improving the Accuracy of Mobile Station Location Estimation	/	/	
PS124	Mobile Systems from a Validation Perspective: a Case Study		/	
PS125	Superdistribution: Testability, Security and Management of Digital Applications		/	
PS126	DataMonitor - A Formal Approach for Passively Test		/	
PS127	Development of a Smartphone Application for Bedside Assessment of Neuro-cognitive Functions		/	/
PS128	Building an Open Toolkit of Digital Certificate Validation for Mobile Web Services		/	
PS129	Blind User Requirements Engineering for Mobile Services		/	
PS130	Flexible R&D Integration Platform of Process Informatics for Automated Medical Applications and Mobile Data Acquisition	/		/
PS135	Securing Enterprise Data on Smartphones using Run Time Information Flow Control	/		

PS141	Big Mobile Data Mining: Good or Evil?		/	
PS142	Mobile Big Data Analytics:Research, Practice and Opportunities		/	
PS143	Engineering Privacy for Big Data Apps with the Unified Modeling Language		/	
PS144	Design of Applicative Quality Testing System for Data Services in Mobile Networks			/
PS146	Real-time QoS monitoring for Cloud-based Big Data Analytics Applications in Mobile Environments			/
PS148	A Script-Based Testbed for Mobile Software Frameworks		/	
PS149	Robustness Testing of Mobile Telecommunication Systems A Case Study on Industrial Practice and Challenges		/	
PS151	Authentication and Authorization for Mobile Devices	/		
PS152	Mobile Security Reference Architecture	/		
PS154	Mobile Software Testing – Automated Test Case Design Strategies		/	
PS156	The Intractable Problem Insecure Software			/
PS157	Specification, Validation and Verification of mobile application behavior	/		/

Table 11 Digital library of paper study

Database library	No. Paper Study	Detail
IEEE Xplore	33	PS57, PS78, PS85, PS90, PS91, PS90, PS91, PS92, PS93, PS94, PS95, PS95, PS96, PS97, PS98, PS99, PS100, PS104, PS111, PS115, PS121, PS123, PS124, PS125, PS126, PS127, PS128, PS129, PS130, PS135, PS142, PS143, PS144, PS146, PS148, PS149
IEEE Transaction	0	
IEEE Society	1	PS124
ScienceDirect	4	PS106 1PS108 PS109 PS110
Springer	2	PS9 PS121
Scopus	0	
Google Scholar	14	PS90, PS90, PS97, PS99, PS100, PS115, PS123, PS124, PS125, PS126, PS146, PS148, PS149
Dblp Computer Science Bibliography	16	PS91, PS111, PS115, PS125, PS126, PS128, PS129, PS130, PS135, PS142, PS143, PS148, PS149
ACM Digital Library	18	PS78, PS111, PS128, PS135, PS142, PS143, PS144, PS146, PS148, PS149
CiteSeerx	5	PS2 PS9 PS46 PS76 PS120

Table 12 Type of paper study

Type Study	Paper Study	Detail
Whitepaper	7	PS9 PS16 PS43 PS76 PS77 PS83 PS91 PS92 PS93 PS94 PS95 PS97 PS99 PS100 PS106 PS108
Thesis	5	PS11 PS13 PS46 PS151 PS157
Article	5	PS58 PS88 PS141 PS143PS144
Journal	29	PS9PS16 PS43 PS76 PS77 PS83 PS91 PS92 PS93 PS94 PS95 PS97PS99 PS100 PS106 PS108 PS109 PS110 PS115 PS121 PS123 PS124 PS126 PS146 PS148 PS149 PS154 PS155 PS156
Paper	19	PS57 PS75 PS78 PS85 PS90 PS96 PS98 PS104 PS111 PS112 PS113 PS120 PS127 PS128 PS129 PS130 PS135 PS142 PS152
Book	1	PS27

A conclusion to this quality extraction, we found 65 primary studies were identified in the analysis of evidence. In the following section, we present the results for the SLR's for the main and sub-research questions.

3.3 RQ1: What Are The Important Security Attributes For Mobile Apps?

Altogether, 59 security attributes were identified from a total of 68 studies related to the security attributes involved in security requirements on mobile apps. Based on the list of the security attributes in Table XIII, we found that Authentication is be the most commonly investigated attribute, which accounts for ten studies. This is followed by, Authorization with eight studies, Confidentiality with three studies while Integrity, Audit and Access Control with two studies each. The rest of this section provides a brief description of these findings. These studies play an important role in the authentication for security attribute on mobile apps. For the purpose of this paper, we focus the most top structured test approach security requirements studies for mobile security testing based on the most common attributes:

1. Authentication

One of the important security attributes found in this study is authentication. It involves a two-way communication. The user is authenticated by something he/she knows (pin NUMBER) and something he/she has (the mobile application that created the second communication channel and receives a unique OTP [8]. Other study proposes a novel transaction based authentication scheme (TBAS) for mobile communication using cognitive agents. The proposed approach provides a range of authentication based on mobile transaction sensitivity and users behaviours [9].

2. Authorization

Several studies found that authorization is the process of determining whether an already identified and authenticated user is allowed to access information resources in a specific way [10]. In addition, all users are neither required to have the same access and functional capabilities in a mobile environment, nor access to the same, specific digital assets. For this study, authorization will give a consideration in the following areas of the mobile device architecture to restrict user access and functional capabilities.

i. What the user can do on the device?

ii. What the user has access to with respect to data assets and the application that access them? and

iii. What the user has access to within the mobile device management infrastructure? [11].

3. Confidentiality

Most of the studies focus on confidentiality. Several studies identify that confidentiality enables protection of private data during client-server communication through utilization of the secure encrypted channel. Some of the vulnerabilities of HTTPS are identified as using weak communication protocol, inappropriate cipher suite and short encryption [9]. Confidentiality of system is breached if user changes the configuration system without knowing exactly the reason he is doing the task. User may select weak password or worst case which totally disables the authentication [12] and other techniques need to be applied to ensure the privacy of the transmitted and stored data, by not allowing unauthorized parties to read the data [13].

4. Access control

Several studies choose Access Control that verifies user identity in each and every step of the request similar to the point-to-point access control scheme. The access control is managed under a single representative or organization for user identities. Thus, trust is established between organizations where access to resources is granted on behalf of the users' associated organization [14]. Further, this study found that access control solutions based on semantic web standard could help to realizing some advanced mechanism such as access control based on learning of users behaviour, rating-based fair provisioning of mobile web services, pro-active authorization based on monitoring of peers in years proximity and other [15].

5. Integrity

The seven attribute identified in this study is integrity. For this, authors proposed Integrity as an attribute functions to protect the transferred messages through communication. For example, to protect patient medical record against unwanted disclosure, private data must be protected against unwanted modification and deletion during transfer and storage [9]. In another study, Integrity means the detection of any intentional or unintentional transmitted or stored changes [13].

6. Audit

One study claimed that it is necessary that audit events occurred in application. The mobile software application should allow an unauthorized user can delete or modify the function in audit records. The administrators need to regularly generate audit records to query, statistics, analysis and generate audit reports for analysis and checking abnormal events in mobile applications [16].

7. Availability

Several studies found that availability is one of the factors that contribute to security evaluation. In this study, a Denial of Service (DoS) attack may drive Apache or the whole server computer into a state where it is not available for the mobile device [12]. Further, it applies common attacking method server-based services to avoid attacker from harming the mobile solution in any way [17].

As a conclusion, although authentication is the most concerned attributes identified in this review, the weightage of applying the security attributes is different. It shows that all the seven attributes: Access Control, Audit, Authentication, Authorization, Confidentiality and Integrity gained more attention in mobile apps that the common system/software..

Table 13 Security attributes

Types Selection	**Paper Study**	**Detail**
Access Control	3	PS89 PS95 PS 150
Anti-Malware	1	PS120
Application Classification	1	PS135
Audit	2	PS120 PS152
Audit, Logging, alert	1	PS106
Authentication	10	PS6 PS27 PS88 PS93 PS95 PS100 PS109 PS113 PS115 PS151 PS152
Authorization	6	PS6 PS27 PS88 PS113 PS151 PS152
Availability	2	PS55 PS104
Classification	1	PS9
Classified data handling	1	PS106
Communication	1	PS93
Communication(FCO)	1	PS120
Confidentiality	3	PS6 PS27 PS104
Credential Management	1	PS27
Cryptographic support(FCS)	1	PS120
Data Classification	1	PS135
Data Loss Prevention	1	PS152
Dual-persona devices	1	PS106
Effort Expectancy	1	PS99
Encryption	1	PS152
Identity Management	1	PS27
Integrity	2	PS6 PS104
Network communications	1	PS106
Network security	1	PS95
Non-repudiation	1	PS6
Performance expectancy	1	PS99
Procurement and Provisioning Considerations	1	PS152
Protection of the TSF(FPT)	1	PS120
Rule	1	PS2
Sandbox	1	PS152
Security audit	1	PS120
Security management (FMT)	1	PS120
Simple Parameter	1	PS130

Social influence	1	PS99
Trust Management	1	PS27
Use experience	1	PS99
Use intention	1	PS99
User data protection (FDP)	1	PS120
Validation	1	PS123
Verification	1	PS76

3.4 RQ2: How To Validate Security Requirements For Mobile Apps?

As shown in Table 14(a), security testing and software testing are the most commonly used approaches for validating security requirements of mobile apps, followed by black box, cloud and system testing. This finding indicates that automation is needed in validating security requirements for mobile apps. The primary studies that conducted testing at different level of abstractions were also identified.

Table 14(a) Testing method

Types Selection	No. Paper Study	Paper Study
Acceptance Testing	1	PS154
Adaptive Random Testing	1	PS94
Automating Test Design-Method	1	PS84
Automating Unit Testing	1	PS75
Black Box Testing	2	PS40 PS85
Cloud based Software Testing	1	PS43
Cloud Testing	2	PS76 PS92
Compability Test	1	PS95
Computerized cognitive testing	1	PS127
Formal approach	1	PS126
Generic Script Based Tools	1	PS40
GUI Testing	1	PS91
Integration Testing	1	PS154
Intelligent Mobile Terminal Software Automatic Test	1	PS98
Keyword Driven Testing	1	PS84
Manual Testing Process	1	PS84
mobile APP testing	1	PS111
Mobile Security Testing	1	PS6
mobile TaaS	1	PS111
mobile testing	1	PS111
mobile web testing	1	PS111
Model Based Testing	1	PS84
Object Repository	1	PS97
Passive conformance testing	1	PS126
Platform Specific Tools	1	PS40
Query Processing-Method	1	PS142
Record and Playback	1	PS84
Regression Testing	1	PS154
Robustness testing	1	PS104
Scripted Testing	1	PS84
Security Requirements	1	PS57
Security testing	3	PS78PS95PS104
Software Quality	1	PS96
software testing	3	PS90 PS92 PS96
System Testing	2	PS149 PS154
TaaS	1	PS111
Test Automation	1	PS40
Test Executor	1	PS97
Test Platform	1	PS124
Test Report Exporter	1	PS97
Test Report Generator	1	PS97
Testing Requirements	1	PS96
Unit Testing	1	PS154
User Interface Testing	1	PS154
Vulnerability scanning	1	PS104
White Box Testing	1	PS40

Table 14 (b) indicate 11 studies related to the required validating method for security requirements of mobile application. We found that 2 studies claimed that X509 Certificates have been the most common tools used for validating security requirements.

Table 14(b) Validating method

TypesSelection	No. Paper Study	Paper Study
Information-flow and action tracking runtime	1	PS16
Input Generation	1	PS16
Agile Development	1	PS46
Test Case Generation	1	PS58
Test Execution	1	PS77
Security Assurance	1	PS100
Security Protocols	1	PS109
Pervasive public key infrastructure	1	PS113
X509 Certificate	2	PS125 PS128
Testbed Components	1	PS148

In summary, all testing and validation methods used for testing and validating mobile apps are based on the functional and behaviour of the tool itself. Yet, these testing and validation methods were found to be difficult and tedious for Requirements engineers and Clients-Stakeholders to handle since there is lack of appropriate mechanism to test and validate the security requirements at the requirements phase. Specifically, there is no validation at the early stage of gathering requirement before the implementation phase.

3.4.1 RQ2: What Are The Approaches Or Models And Tools Available To Validate Security Requirements For Mobile Apps?

1. Approaches/Model

25 different approaches were identified in the 34 of the 65 studies. Out of the 25 approaches, automation is identified as the most common approach as it is reported in 12 studies. The other 23 approaches were reported in a single study respectively. The list of approaches or model used on mobile apps is in Table 15(a).

2. Tools

Table 15(b) shows the five tools to validate security requirements for mobile applications that are reported in the studies. The security attributes for each tool are identified. It is found that the tool is also commonly used in software housing and customer software testing tools.

Table 15(a) Approach/model

Types Selection	No. Paper Study	Paper Study
Automation	12	PS11 PS16 PS42 PS41 PS52 PS58 PS77 PS83 PS84 PS85 PS90 PS91
Cloud Computing	1	PS92
Concord Framework	1	PS88
Cross-Layer	1	PS146
Multi-Cloud Application Monitoring		
DroidWatch	1	PS108
Dynamic Trust Model	1	PS113
IoT Service Arch.	1	PS109
JUnit Framework	1	PS75
Mobile Environment Model	1	PS121
Mobile Test Automation	1	PS97
Model Mobile	1	PS13
Modeling Intelligent Mobile Terminal	1	PS98
MVC pattern structures	1	PS110
neurocognitive assessment tools	1	PS127
Quality model	1	PS95
Robust Test Tool	1	PS95
Sensitive-event based testing approach	1	PS85
Service Quality Testing System	1	PS144
Software model	1	PS95
System Model Driven MBT Process	1	PS84
TaaS	1	PS92
Threat Model	1	PS88
UML	1	PS91
Veracode	1	PS156

Table 15(b) Tools

Tool names	Security Attributes				
	Audit	Authentication	Authorization	Confidentiality	Integrity
AppsInpector[18]	/	/	/	/	/
A2T2[19]	X	X	X	X	X
AppTwack[20]	/	/	/	/	/
Veracode[21]	/	/	/	/	/
Perfecto[22]	X	/	/	/	/

to the board using wireless USB adapter. This is only needed when manipulation of code is required. The power is supplied to the board by connecting a micro USB to USB cable to a wall socket USB adapter or power bank.

4.0 CONCLUSION

4.1 Findings

The findings have addressed the following two research questions and one sub-research questions of this study:

1. What are the most relevant attributes of security requirements for mobile apps?
2. How to validate security requirements on mobile apps?

2.1 What are the techniques, approaches and tool for validating security requirements of mobile apps?

The following are the summary of the main findings from the SLR. These findings are considered as the challenges in the security requirements for mobile apps. We discovered the important security attributes for mobile apps, namely: Access Control, Audit, Authentication, Confidentiality, Authorization, Availability and Integrity were applied to mobile apps. In addition, the study identified that the use of specific authorization attributes for certain mobile apps security requirements is important in order to determine user's credential and access control. Authentication is commonly applied for mobile apps rather than system. Therefore, the focus on the seven attributes can help requirements engineer to improve the security requirements relevant for mobile apps. We also observed that many of the applied testing and method not controlled or not specific/focus for a particular method and testing. Therefore, requirements engineer and clients were unclear evidence whether Security Requirements should improve their requirements as well as improve their testing and validating method.

4.2 Validation And Testing Method Useful For Mobile Security Requirements

We describe how validation and testing method can cater the issues of mobile security requirements. Validation of security requirements at the early process of requirements phase is crucially required. A few studies claimed a Certificate method as the most commonly used method for validation. Moreover, software, system and security testing is also required in this study as the primary testing on software development. It also includes that automation is in need to automate the validation. However, the need of Test Driven Development (TDD) on testing the mobile security requirements that involves the software developer, requirements engineer and also stake-holders still excluded. By having them, it could help software house or software tester to reduce time effort and cost of testing.

4.2.1 Approaches Or Techniques Useful For Mobile Security Requirements

We also discovered how certain techniques can be used to overcome the problems of the security requirements for mobile apps. Techniques such as automated web application test can be used to define and access the requirement for developers and designers as well as to design test case [23].Only few studies applied new techniques developed to overcome some of the common validation challenges. We found no empirical study that evaluates the effectiveness of these techniques using automated testing during validating security requirement. However, there is no end to end security requirements attributes validation for automated technique used.

4.3 Strengths And Weakness Of SLR

The strength and weakness of the conduct of SLR were identified based on keyword search, inclusion and exclusion process. The strength of SLR is the use of a systematic approach that includes the inclusion and exclusion. This SLR examined a reference list of selected primary studies to identify any additional studies. This SLR also extracts relevant information consistency while reducing biasness and validity by authors. The weakness of this SLR is that it cannot 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 mobile security testing approach and tools in section 3.4 and 3.4.1 due to the failure to capture some of the validating, testing and approach proposed.

4.4 Implications For Research And Society

From our knowledge, this study is thus far, the first SLR conducted to investigate on the validation of security requirements for mobile apps. It is also the first SLR to identify the security requirements attributes related to mobile apps development. Our research work contributes to research efforts for mobile validation or testing environment especially on security requirements for mobile apps. The security requirements attributes discussed in this paper could help the requirements engineers and client-stakeholders to validate and identify the appropriate security requirement attributes for any mobile apps and improve the quality of security requirements. In addition, there are advantages for mobile software engineering researcher to find solution, be aware of the process or method, identify and approach for related security requirements to solve the challenges identified.

5.0 CONCLUSION

This paper described a SLR targeted at empirical studies of validating security requirements for mobile apps and total of 68 primary studies were selected. We found that access control, audit, authentication, confidentiality, authorization, availability and integrity are important attributes for mobile apps. However, the most important security requirements attribute was the authentication security attributes, which are related to the use of mobile apps development such as the Internet banking, Flight booking and etc. Seven categories have been used to measure the different attributes of security requirements between the mobile and software system. The findings also showed that mobile security requirements attributes are the major concern in the studies. There were various methods employed to validate security requirements for mobile apps to measure the effectiveness of security requirements for mobile apps. Few studies reported the use of security and software testing for testing method and several studies reported that X509 Certificate is the most commonly used method for validation. The studies also found that there is a need to use automation in validation.

This study concludes that validation of security requirements for mobile apps are rarely employed in the development of mobile apps although it is crucial needed from the early stage as it is highly exposed to vulnerabilities and privacy issue.

Acknowledgement

We would like to thank Universiti Teknikal Malaysia Melaka for its support and Sciencefund grant: 01-01-14-SF0106 and also Ministry of Education (MOE), MyBrain15.

References

[1] SQE Training. Software Quality. 2014. http://www.sqetraining.com/consulting-services/software-quality.

[2] Oracle. 2013. Fushion Middleware Access Management. *Oracle Mobile and Social Access Management*.

[3] Reuter. M and E.Field. 2012. *Tableue for the Enterprise: An overview for IT*.

[4] Kitchenham, B. A., E. Mendes, G. H. Travassos. 2007. A Systematic Review of Cross- vs. Within-Company Cost Estimation Studies. *IEEE Trans on SE.* 33(5): 316-329

[5] Kitchenham, B. A., and S. Charters. 2007. Procedures for Performing Systematic Literature Review in Software Engineering. *EBSE Technical Report version 2.3.* EBSE-2007.

[6] Dyba. T, T.Dingsoyr, G.Hanssen. 2007. Applying Systematic Reviews To Diverse Study Types: An Experience Report. *First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007).*

[7] Kitchenham, B. A. 2004. Procedure For Performing Systematic Reviews. *Technical Report*, Keele University and NICTA.

[8] Mirkovic. J, H. Bryhni, C. M. Ruland. 2011. Secure Solution for Mobile Access to Patient's Health Care Record, e-

Health Networking Applications and Services (Healthcom). *13th IEEE International Conference on 13-15 June 2011*, Columbia. MO. 296 – 303.

[9] Sathish Babu. B and P. Venkataram. 2008. A Dynamic Authentication Scheme for Mobile Transactions. *International Journal Network Security*.

[10] Ranjbar N., M. Abdinejadi. 2012. *Authentication and Authorization for Mobile Devices*. https://gupea.ub.gu.se/handle/2077/30043.

[11] Product of the Federal CIO Council. 2013. Mobile Security Reference Architecture v1.0. *Mobile Security Reference Architecture.*

[12] Noponen. S and K. Karppinen. 2008. Information Security of Remote File Transfers with Mobile Devices. *Annual IEEE International Computer Software and Applications Conference*.

[13] Souppaya M. and K. Scarfone. 2013. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. National Institute of Standards and Technology, NIST SP 800-124 Revision 1, NIST.

[14] Gupta. K. K. and R. Gupta. 2013. Analysis of End-to-End SOA Security Protocols with Mobile Devices. *IEEE 14th International Conference on Mobile Data Managemen.* 116-170.

[15] Naumenko A., S. Srirama, V. Terziyan and M. Jarke. 2006. Semantic Authorization of Mobile Web Services Semantic Authorization of Mobile Web Services. *JTAER / Journal of Theoretical and Applied Electronic Commerce Research.* 1(3): 1-15.

[16] Liu. Z, Y. Hu and L. Chi. 2014. *Research on Software Security and Compability Test for Mobile Application.* 1(3): 140-145.

[17] Capgemini. 2014. *Taking Mobile Security to the Next* Level. https://www.capgemini.com/resource-file access/resource/pdf/mobile_security_pov_final.pdf.

[18] Gilbert. P and B. Cun. 2011. *Vision: Automated Security Validation of Mobile Apps at App Market*. Proceedings of the second international workshop on Mobile cloud computing and services. ACM. 21-26.

[19] Amalfitano. D, A. R. Fasolino, P. Tramontana, and N. Federico. 2011. *A GUI Crawling-Based Technique For Android Mobile Application Testing*. Proceedings of the 2011 IEEE Fourth International Conference on Software Testing, Verification and Validation Workshops, ICSTW "11, IEEE Computer Society (2011). 252–261.

[20] Apptwack. 2014. https://appthwack.com/overview.

[21] Veracode. 2011. State Of Software Security Report. *The Intractable Problem Insecure Software*. 4.

[22] Perfecto Mobile. 2013. http://perfectomobile.com.

[23] Mee. S. 2012. *Testing Mobile Web Applications for W3C Best Practice Compliance*. Master Dissertation. Dublin Institute of Technology.

Appendix

Empirical studies:

[PS2] Enck ,W., M.Ongtang, and P. McDaniel.2009. On lightweight Mobile Phone Application, *CCS '09 Proceedings of the 16th ACM conference on Computer and communications security*. ACM New York, NY, USA.. 235-245.

[PS6] Oracle, Fushion Middleware Access Management, Oracle Mobile and Social Access Management. 2013.

[PS9] Reuter.M and E.Field. 2012. Tableue for the Enterprise: An overview for IT.

[PS11] Xinwen.Z and K.Anug.2011. *Towards an Elastic Application Model for Augmenting the Computing Capabilities of Mobile Devices with Cloud Computing.* Vol.16, Issue:3.270-284.

[PS13] Koot.L.2012. *Security of mobile TAN on smartphones*.

[PS16] Gilbert.P, L.Cox.2011. Vision: Automated Security Validation of Mobile, *MCS'11, June 28, 2011, Bethesda, Maryland*, USA..

[PS27]David.G., Rosado1,E.Fernandez.2011.*Security in the Development Process of Mobile Grid Systems*.

[PS40] HSC PROPRIETARY.2013 *Test Automation Tools for Mobile Applications: A brief survey*..

[PS41] Keynote.2013 *DeviceAnywhere Enterprise Automation and HTML*.

[PS42] Cognizant.2012. *Selecting the Right Mobile Test Automation Strategy: Challenges and Principles*.

[PS43] Baride,S.,, Kamlesh Dutta.2011. A Cloud based Software Testing Paradigm for Mobile, *ACM SIGSOFT Software Engineering Notes archive*, Volume 36 Issue 3, May 2011. 1-4.

[PS44] Syntel, *Secure Automated Solutions for Mobile Application*.

[PS46] Spataru,,A.C., *Agile Development Methods for Mobile Applications.*

[PS52] "Why effective Test Automation drives successful and quality driven mobile payments".

[PS55] Capgemini.2014. *Taking Mobile Security to the Next* Level.

[PS57] Dantas ,L.V., .Marinho, G.Fabiana.2009.Testing Requirements for Mobile Applications. *Computer and Information Sciences, 2009. ISCIS 2009. 24th International Symposium on 14-16 Sept. 2009.*:555 – 560.

[PS58] 2011.Automating GUI Testing for Android Applications, *AST'11, May 23-24, 2011, Waikiki, Honolulu, HI*, US.

[P75] Paul.2008. *Testing Java ME Applications*.

[PS76] Shilpa, Chaturvedi. 2013. Literature Review of Mobile Applications Testing on Cloud from Information Security Perspective. International Journal of Computer Applications (0975 – 8887), Volume 79 – No 14, October 2013.

[PS77] Rajkumar, K.Vivekanandan, Subramaniam.2014. Mobile Test Automation Framework for Automotive HM, *International Journal of Advanced Research in Computer and Communication Engineering.* Vol. 3. Issue 1.

[PS78] Andria, Mariano. 2013. Security Testing of the Communication among Android Applications. *Automation of Software Test (AST), 2013 8th International Workshop*, San Francisco, CA. 57 - 63.

[PS80] Mobile Application Testing

[PS83] Rajkumar, K.Vivekanandan, Subramaniam.2014. Cloud Enabled Test Evaluation on Mobile Web Application, *International Journal of Advanced Research in Computer and Communication Engineering*. Vol. 3. Issue 6. June 2014.

[PS84] White paper, "Why Automate Test Design".

[PS85] Bao.J, L.Xiang, G. Xiapeng. 2007 MobileTest: A Tool Supporting Automatic Black Box Test for Software on Smart Mobile Devices. *Automation of Software Test, AST '07. Second International Workshop*. 20-26 May.

[PS88] Singaraju.G, B.H.Kang. 2008. Concord: A Secure Mobile Data Authorization Framework for Regulatory Compliance, *22nd Large Installation System Administration Conference (LISA '08)*.

[PS89] Naumenko.A, S. Srirama, V. Terziyan and M. Jarke. 2006. Semantic Authorization of Mobile Web Services Semantic Authorization of Mobile Web Services, *JTAER / Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 1, n. 3, 1-15.

[PS90] B. Kirubakaran. 2013. Mobile Application Testing – Challenges and Solution. *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on 21-22 Feb. 2013*.

[PS90] Li.A, Z.Qin, M.Chen and J.Liu. 2014. ADAutomation: An Activity Diagram Based Automated. *Software Security and Reliability (SERE), 2014 Eighth International Conference on June 30 2014-July 2 2014, San Francisco*, CA.

[PS91] B. Kirubakaran. 2013. Mobile Application Testing – Challenges and Solution. *Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on 21-22 Feb. 2013*.

[PS92] Murugesan, Logeshwaran. 2014. *Cloud Based Mobile Application Testing*.

[PS93] Mirkovic, J. Bryhni, H.Ruland, Cornelia. 2011. Secure solution for mobile access to patient's health care record. *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on 13-15 June 2011*, Columbi.

[PS94] Liu, Zhifang. 2010. Adaptive Random Testing of Mobile Application. *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on (Volume:2), 16-18 April 2010*, Chengdu.

[PS95] Liu.Z, Y.Hu, L.Cai. 2014. Research on Software Security and Compatibility Test for Mobile Application. Innovative Computing Technology (INTECH), *2014 Fourth International Conference on 13-15 Aug. 2014*.

[PS96] Lelli.V, L.Dantas, F.G. Marinho. 2009. Testing Requirements for Mobile Applications. *Computer and Information Sciences, 2009. ISCIS 2009*.

[PS97] Nagowah.L and G.Sowamber. 2012. A Novel Approach of Automation Testing on Mobile, Computer & Information Science (ICCIS), *2012 International Conference on (Volume:2)*,Kuala Lumpur.

[PS98]Yin1.Y , B.Liu1, C.Wang1, Hongyin. 2010. Research on Automatic Testing Technology Oriented Intelligent Mobile Terminal Software. *Communications and Mobile Computing (CMC), 2010 International Conference on (Volume:1)*,Shenzhen.

[PS99] 2010. Empirical research on user acceptance of mobile searches, *Tsinghua Science and Technology, volume 15, Number 2*, April 2010.

[PS100] Krishnan.P 2011. Applying Security Assurance Techniques to a Mobile Phone Application: An Initial Approach. *Software Testing, Verification and Validation Workshops (ICSTW), 2011 IEEE Fourth International Conference on 21-25 March 2011*, Berlin.545 – 552.

[PS104] Noponen, S. and K. Karppinen. 2008 Information Security of Remote File Transfers with Mobile Devices. *Computer Software and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International July 28 2008*.

[PS106] Stephen. M. A.Dye, K.Scarfone. 2014. A standard for developing secure mobile applications, *Computer Standards & Interfaces 36 (2014)*. 524–530.

[PS108] Grover.J, 2014. *Android forensics: Automated data collection and reporting from a mobile device*, Contents lists available at SciVerse ScienceDirect.

[PS109] Santosa.A, J. Macedoa and A.Co, 2014. Internet of Things and Smart Objects for M-Health, *CENTERIS 2014 - Conference on ENTERprise Information Systems / ProjMAN*.

[PS110] Sua.X.Y., F.Lina , L.Chena , Kuo. 2014. A Service Oriented Tele-health Promotion Information System with Mobile Application, *The 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2014*..

[PS111] Tsai2.J. G.W., R.Paul3 , Xiaoying. 2014. *Mobile Testing-As-A-Service (MTaaS)– Infrastructures, Issues, Solutions and Need*..

[PS112] Yun.D and C.Xiao-hui. 2009. A Study on the Security Technology of Enterprise Mobile Information System. *2009 International Conference on Computational Intelligence and Security* ,Beijing December..

[PS113] Forne.J, F.Hinarejos, Andre´s. 2010. *Pervasive authentication and authorization infrastructures for mobile users, Computers & Security*, Volume 29, Issue 4, June 2010. 501–514.

[PS115] Jorns.O, O.Jung, G.Quirchmayr. 2008. *A* platform for the development of location-based mobile applications with privacy protection, *Communication Systems Software and Middleware and Workshops*.

[PS120] Lee.H and D.Won, 2013. Security Requirement of Mobile Application Based Mobile Payment System. *Proceedings, The 2nd International Conference on Information Science for Industry, ISI 2013*, ASTL Vol. 25, 312 – 316.

[PS121] Peng1.T, C.Chi4, A.Chiasera. 2014. *Business Process Assignment and Execution in Mobile Environments*.

[PS123] 2013. A Systems Engineering Approach to Improving the Accuracy of Mobile Station Location Estimation, *Systems Journal, IEEE* (Volume:8 , Issue: 1).14 - 22

[PS124] Waeselynck.H., Z.Micskei, M.D.Nguy. 2007. *Mobile Systems from a Validation Perspective: a Case Study.*

[PS125] Anand.V., J.Saniie. 2012. Superdistribution: Testability, Security and Management of Digital Applications, Electro/Information Technology (EIT). *2012 IEEE International Conference on 6-8 May 2012,* Indianapolis, 1- 5.

[PS126] Lalanne.F, S.Maag, T.SudParis. 2013. *DataMonitor - A Formal Approach for Passively Test.*

[PS127] Ghosh.S, M.Das, A.Ghosh, Aritra. 2014. Development of a Smartphone Application for Bedside Assessment of Neuro-cognitive Functions. *Applications and Innovations in Mobile Computing (AIMoC), 2014 , Feb. 27 2014-March 1 2014,* Kolkata. 54 - 59.

[PS128] Almenarez.F, A.Mandrin, D.Diaz, A.Cortes, C.Campo, C.G.Rubio. *2008.* Building an Open Toolkit of Digital Certificate Validation for Mobile Web Services, Pervasive Computing and Communications, 2008. PerCom 2008. *Sixth Annual IEEE International Conference on 17-21 March 2008*, Hong Kong.560 – 565.

[PS129] Hebler.S.,T.Tuunanen, K.Peffers. 2007. Blind User Requirements Engineering for Mobile Services, Requirements Engineering Conference, 2007. *RE '07. 15th IEEE International 15-19 Oct. 2007*, Delhi. 205 – 208.

[PS130] Holzmuller-Laur.S, K.Rimane, S.Neubert, S.Kreuzfeld. 2008. Flexible R&D Integration Platform of Process Informatics for Automated Medical Applications and Mobile Data Acquisition, *Automation Science and Engineering, 2008. CASE 2008. IEEE International Conference on 23-26 Aug. 2008.*

[PS135] Kodeswaran.P, V.Nandakumar, Shalini. 2012. Securing Enterprise Data on Smartphones using Run Time Information Flow Control, *Mobile Data Management (MDM), 2012 IEEE 13th International Conference on 23-26 July 2012*, Bengaluru, Karnataka, 300 - 305.

[PS141] Musolesi.M. 2014. Big Mobile Data Mining: Good or Evil?, Journal, IEEE Internet Computing archive, Volume 18 Issue 1, January 2014.78-81.

[PS142] Zeinalipour-Yazti.D, S.Krishnaswamy.2014. Mobile Big Data Analytics: Research, Practice and Opportunities..

[PS143] Dawn N. Jutla1, P.Bodorik2, S. Ali1. 2013. Engineering Privacy for Big Data Apps with the Unified Modeling Language, Big Data (BigData Congress). *2013 IEEE International Congress on, June 27 2013-July 2 2013,* Santa Clara, CA. 38 - 45.

[PS144] Janevski .DT., A.Tudzarov, P.Latkoski, M.Porjazoski , I.Efnushev, G.Madzarov, D.Gjorgjiev. 2009. Design of Applicative Quality Testing System for Data Services in Mobile Networks, *Global Mobile Congress 2009, 12-14 Oct. 2009*, Shanghai. 1 – 6.

[PS146] Alhamazani.K, R.Ranjan, P.Prakash. 2014. Real-time QoS monitoring for Cloud-based Big Data Analytics Applications in Mobile Environments Mobile Data Management (MDM). *2014 IEEE 15th International Conference on (Volume:1), 14-18 July 2014,* Brisbane, QLD. 1 – 2.

[PS148] Hargassner.W.,T.Hofer,C.Klammer,J.Pichler, G.Reisinger. 2008. A Script-Based Testbed for Mobile Software Frameworks, *Proceeding ICST '08 Proceedings of the 2008 International Conference on Software Testing, Verification, and Validation*. 448-457.

[PS149] Eldh.S, D.Sundmark. 2012. Robustness Testing of Mobile Telecommunication Systems A Case Study on Industrial Practice and Challenges, *Software Testing, Verification and Validation (ICST), 2012 IEEE Fifth International Conference on 17-21 April 2012*, Montreal, QC. 895-900.

[PS150] Guptal.K. K., R. Gupta. 2013. Analysis of End-to-End SOA Security Protocols with Mobile Devices. *2013 IEEE 14th International Conference on Mobile Data Management*. 116-170.

[PS151] Authentication and Authorization for Mobile Devices.

[PS152] *Mobile Security Reference Architecture*, [Online]. From: https://cio.gov/wp-content/.../Mobile-Security-Reference-Architecture.pd.

[PS154] Selvam R. 2011. Mobile Software Testing – Automated Test Case Design Strategies, *International Journal on Computer Science and Engineering (IJCSE)*, Vol. 3 No. 4 Apr 2011.

[PS155] *A GUI Crawling-based technique for Android Mobile Application Testing*.

[PS156] *The Intractable Problem Insecure Software*..

[PS157] Christopher.B., Bonine. *Specification, Validation and Verification of Mobile Application Behavior*.