Research Protocol of

Classification and Mapping of Adaptive Security for Mobile Computing

Maryam Sajjad
Postgrad Student
School of Electrical Engineering and Computer Science (SEECS)
National University of Science and Technology (NUST), Pakistan
maryam.sajjad@seecs.edu.pk

Aakash Ahmad
Assistant Professor
College of Computer Science and Engineering (CCSE)
University of Ha'il (UoH), Kingdom of Saudi Arabia
a.abbasi@uoh.edu.sa

Asad Waqar Malik
Assistant Professor
School of Electrical Engineering and Computer Science (SEECS)
National University of Science and Technology (NUST), Pakistan
asad.waqar@seecs.edu.pk

Ahmed B. Altamimi
Assistant Professor
College of Computer Science and Engineering (CCSE)
University of Ha'il (UoH), Kingdom of Saudi Arabia
altamimi.a@uoh.edu.sa

Ibrahim Alseadoon
Assistant Professor
College of Computer Science and Engineering (CCSE)
University of Ha'il (UoH), Kingdom of Saudi Arabia
i.alsedon@uoh.edu.sa]@uoh.edu.sa

University of Ha'il Technical Report - 2016
College of Computer Science and Engineering (CCSE)

Contents

Research Protocol of

Classification and Mapping of Adaptive Security for Mobile Computing

Maryam Sajjad[1], Aakash Ahmad[2], Asad Waqar Malik[1], Ahmed B. Altamimi[2], Ibrahim Alseadoon[2]

[1]School of Electrical Engineering and Computer Science (SEECS)
National University of Science and Technology (NUST), Islamabad, Pakistan

[2]College of Computer Science and Engineering (CCSE),
University of Ha'il, Ha'il, Kingdom of Saudi Arabia

[1][maryam.sajjad | asad.waqar]@seecs.edu.pk, [2][a.abbasi | altamimi.a |
i.alsedon@uoh.edu.sa]@uoh.edu.sa

Overview

Context: In recent years, mobile computing has emerged as a disruptive technology that has empowered its users with portable and context-aware computation. Mobile computing represents a paradigm shift from traditional computing platforms to anytime and anywhere connected computation. However, issues such as resource poverty; energy efficiency and specifically data security and privacy represent critical challenges that mobile computing must overcome.

Objective: We aim to systematically identify and taxonomically classify the state of existing research on adaptive security (a.k.a self-protection) for mobile computing. The taxonomy highlights the impacts of existing research, its strengths and limitations and outlines dimensions of futuristic research.

Methodology of Research: We followed evidence based software engineering method to conduct a systematic mapping study of 36 qualitatively selected studies focused on adaptive security for mobile computing. The mapping study has (i) taxonomically classified existing and emerging research themes, and (ii) systematically mapped the security threats, proposed solutions, tools and frameworks that support adaptive security.

Conclusions: Classification and mapping of the existing research highlights three prominent themes that support adaptive security for (i) *Mobile Device Data and Resources*, (ii) *Mobile to Mobile Communication*, and (iii) *Mobile to Server Communication*. The analysis of these themes suggests that privacy and confidentiality of mobile device data and resources is an emerging research trend. Tools and frameworks (as research prototypes) are being developed that enhance adaptive security as a mechanism of self-protection for mobile devices against unforeseen security threats. The mapping study highlights that futuristic research is focused on context aware adaptive security that allows dynamically evolving security mechanism(s) to protect a devices' assets against frequently evolving security threats. The results of this mapping study facilitate knowledge transfer that can benefit researchers and practitioners who are engaged with the research and development of solutions that enable adaptive security for mobile computing.

1 Defining the Research Protocol

To conduct the mapping study, we have used evidence based software engineering method that guides systematic mapping studies and systematic literature reviews [4, 19]. A systematic method for review and mapping reduces bias during the identification, selection, and synthesis of data along with reporting results. The methodology and its underlying steps to conduct our mapping study are illustrated in Figure 1 that includes (i) Study Planning, (ii) Data Collection, and (iii) Results Classification.

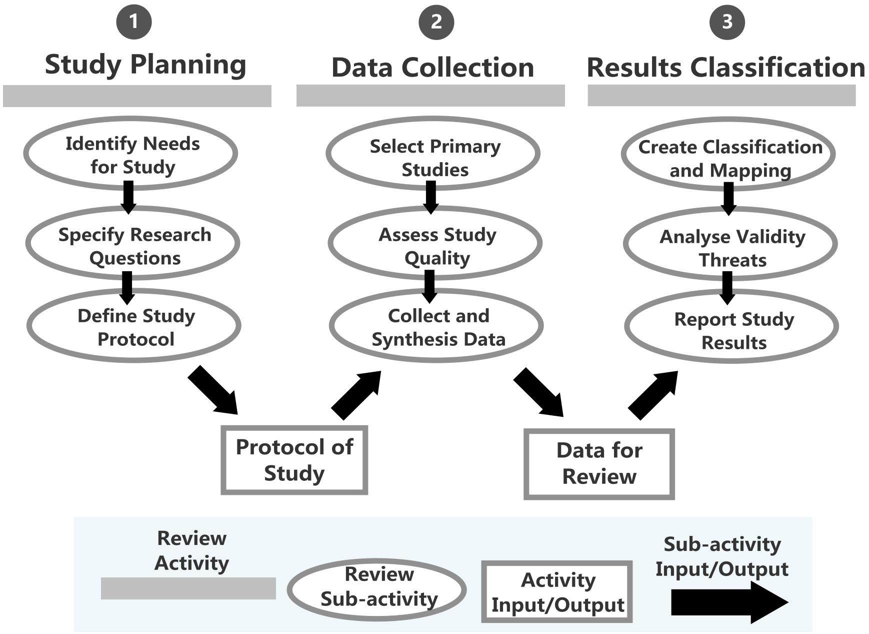


Figure 1 Research Methodology for Conducting the Mapping Study

1.1 Defining the Protocol for Systematic Mapping Study

The first and foremost step to conduct a valuable systematic mapping study is to plan and structure the study protocol i.e., the identification of the needs and justification of the study. The plan for the mapping study provides a blue-print to conduct the study as well as it identifies and justifies the needs and defines the scope of the study with specific research questions. The plan helps with defining the protocol of the mapping study and creating the search strategies for data collection as illustrated in Figure 1.

1.1.1 Identify the Needs for Mapping Study

Despite the growing interest and progression of research, there has been no effort to systematically identify, analyse, and report the peer-reviewed research on adaptive security for mobile computing. Mapping and analysing the state-of-research can highlight its progress, maturation, emerging trends and futuristic dimensions that is currently lacking. To ensure that, no such work exists similar to our mapping study, we searched *IEEE*, *ACM*, *Springer*, *Science Direct* and *Scopus* digital libraries (on 29/07/2016).

The search string used for locating any relevant secondary studies on adaptive security for mobile computing is detailed in Listing 1. Based on the search string in Listing 1, none of the publications that we retrieved (cf. Section 2) were related to the outlined research questions below that motivated the needs for our mapping study.

```
(“Systematic Literature Review” OR “Systematic Mapping” OR “Study” OR “Survey”)
AND
(“Adaptive” OR “Dynamic” OR “Runtime”)
AND
(“Security” OR “Confidentiality” OR “Protection” OR “Security”)
AND
(“Mobile” OR “Ubiquitous”)
```

Listing 1 Search String to Identify Relevant Secondary Studies

1.1.2 Specifying the Research Questions

In order to conduct the mapping study and to report the results, we have outlined a number of research questions (RQs) as listed below. The answers to these questions help us define the scope of study and support a subjective investigation and interpretation of the results. The RQs aim to investigate:

A. **Research Themes, Security Challenges and Solutions**

RQ 1. *What is the frequency of publications over the years in the area of adaptive security for mobile computing?*

Objective(s): To highlight the growth of research in terms of the publications and progression of research over the years that focus on adaptive security for mobile computing.

RQ 2. *What are the existing research themes and how are they classified?*

Objective(s): The identification of research themes is fundamental to a systematic analysis and a collective impact of the existing research on the topics to be investigated.

RQ 3. *What are the prominent challenges for adaptive security in the context of mobile computing, and what solutions are provided to address the challenges?*

Objective(s): An investigation of the challenges highlights the problems pertaining to security related issues for mobile computing that needs to be addressed. Moreover, the discussion of the solution presents the proposed methods and techniques to address the identified challenges.

RQ 4. *What data or entities are affected as a consequence of adaptive security problems?*

Objective(s): To identify the various types of data or entities (user location, mobile app, personal information) that are affected as a consequence of the security breach.

B. **Tool Support for Solutions**

RQ 5. *What tool or frameworks are provided to enhance or enable adaptive security for mobile computing?*

Objective(s): Identification of the existing tools and frameworks that are available to enable or enhance adaptive security for mobile computing.

C. **Past Research and Emerging Trends**

RQ 6. *What were the past trends of research on adaptive security for mobile computing?*

Objective(s): To identify the past trends and how these trends have evolved overtime.

RQ 7. *What are the emerging trends of research on adaptive security for mobile computing?*

Objective(s): To identify the dimensions of future research based on emerging trends.

1.1.3 Searching the Relevant Literature – Primary Studies

After the RQs have been specified, the search string is composed and executed on various databases (digital libraries) to identify the relevant literature, as illustrated in Figure 2. Specifically, the RQs and their objectives help us to compose the search string that is executed on *IEEE*, *ACM*, *Springer Link*, *Science Direct* and *Scopus* digital libraries. In Figure 3, the literature search was limited to peer-reviewed, published research from years 2003 to 2016 with 8094 hits (*search string executed in Dec 2016*). The year 2003 was chosen because with an initial search, we could not find any study published before 2003 that was related to any of the research questions in general and adaptive security for mobile computing in particular. After screening and selecting the most relevant studies, 24 studies from IEEE, 3 studies from ACM, 06 studies from Springer Link, 1 study from Science Direct and 2 studies from Scopus were selected to be included in the mapping study.

Please note that the first search string (cf. Listing 1) helped us to identify the relevant secondary studies - systematic reviews and surveys in Table 1 - on adaptive security for mobile computing. In contrast, the search string in Figure 2 aims to identify the primary studies for review in the mapping study. We have selected a total of 29 studies to be included in the mapping study. The details of the studies included in the review are provided in Appendix A. Extended details of the research methodology are provided in [24].

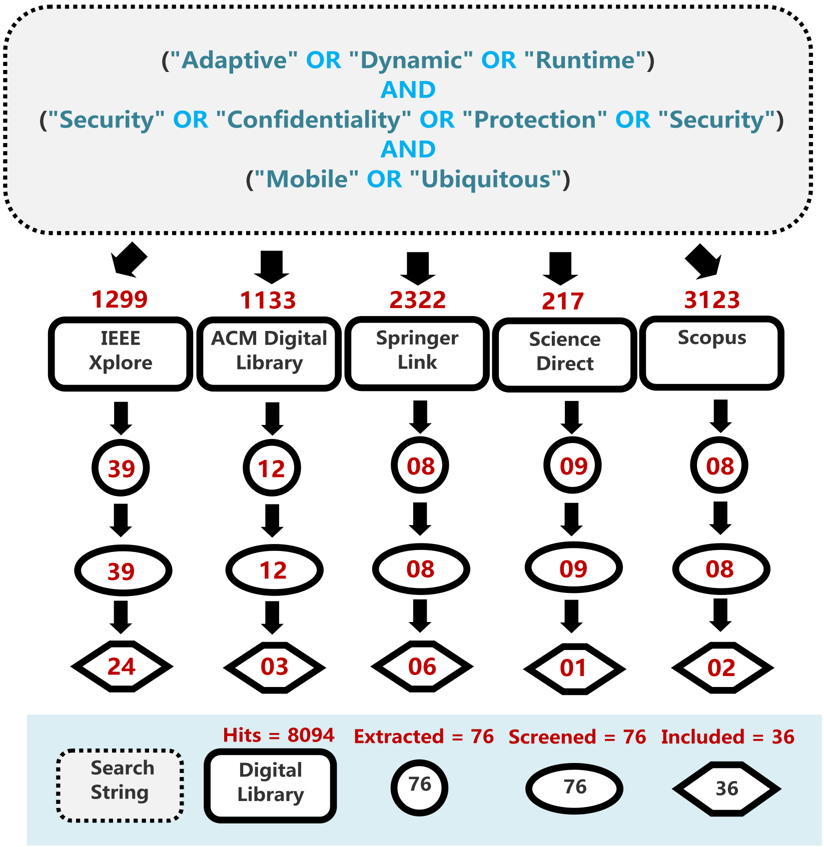


Figure 2 Summary of the Literature Search Process with Search String

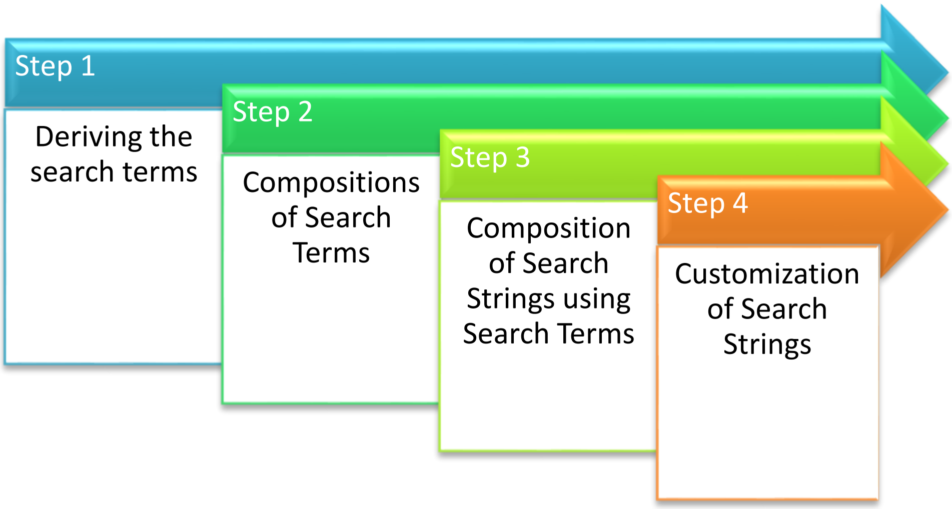
Please note that the first search string (cf. Listing 1) helped us to identify the relevant secondary studies - systematic reviews and surveys in Table 1 - on adaptive security for mobile computing. In contrast, the search string in Figure 2 aims to identify the primary studies listed in Appendix A and included for review in the mapping study. We have selected a total of 36 studies to be included in the mapping study. The publication years of selected studies are between year 2003 to year 2016.

2 Identification, Qualitative Assessment and Data Extraction of Primary Studies

2.1 Selection of Primary Studies

2.1.1 Primary Search

In order to identify the relevant literature, the procedure of conducting the primary search is decomposed into 4 steps.


Step 1
Deriving the search terms
Step 2
Compositions of Search Terms
Step 3
Composition of Search Strings using Search Terms
Step 4
Customization of Search Strings

1) **Deriving the search terms**: We have derived the search terms from the research questions listed in the section 1.1.2 of the current document

2) **Composition of Search Terms**: In order to derive the Search Terms, we have considered the alternative keywords along with the standard keywords. For instance, adaptive as [*dynamic, runtime*]

3) **Composition of Search Strings using Search Terms**: In third step of selecting primary studies, we have combined various search terms by using “AND” and “OR” operators in order to create the search strings. Boolean AND is used when there is a need to link the search terms whereas Boolean OR is used to integrate the synonyms and other alternative words as discussed in the step 2.

4) **Customization of Search Strings**: Forth step is the division and customization of the created search strings. The customised search strings are then used to conduct the search for primary studies through various databases /digital libraries.

2.1.2 Customized Search Strings

The customised search strings created in the above section are used for conducting the search in the digital libraries such as ACM, IEEE, Springer, Science Direct and Scopus. We have utilized the services of Google Scholar search engine as an auxiliary search engine in order to ensure that no related and relevant research study may be missed.

The customised search strings that have been used to search various database engines are listed below.

IEEE Explore (www.ieeexplore.ieee.org)

("Document Title": Adaptive OR “Document Title": Dynamic OR “Document Title": Runtime OR "Abstract": Adaptive OR "Abstract": Dynamic OR "Abstract": Runtime)
AND
("Document Title": Security OR “Document Title": Confidentiality OR “Document Title": protection OR "Abstract": Security OR "Abstract": Confidentiality OR "Abstract": Protection)
AND
("Document Title": Mobile OR "Document Title": Ubiquitous OR "Abstract": Mobile OR "Abstract": Ubiquitous)

Search String 1 for IEEE explore

ACM Library (www. dl.acm.org)

```
((Owner: ACM) AND (Title "Adaptive" OR Title "Dynamic" OR Title "Runtime") AND
(Title "Security" OR Title "Confidentiality" OR Title "Protection")
AND
(Title "Mobile" OR Title "Ubiquitous"))
```

Search String 2 for ACM Digital Library

Springer Link Database (www. link.springer.com)

```
(Adaptive OR Dynamic OR Runtime) AND (Security OR Confidentiality OR Protection) AND
(Mobile OR Ubiquitous)
```

Search String 3 for Springer Link

Science Direct Search Engine (www.sciencedirect.com)

```
TITLE-ABSTR-KEY ((Adaptive OR Dynamic OR Runtime) AND (Security

OR Confidentiality OR Protection) AND (Mobile OR Ubiquitous))
```

Search String 4 for Science Direct

Scopus Database (www.scopus.com)

```
TITLE-ABS ((Adaptive OR Dynamic OR Runtime)

AND (Security OR Confidentiality OR Protection) AND (Mobile OR Ubiquitous))
```

Search String 5 for Scopus Database

The customised search strings; listed above; have helped us a lot in refining our research by eliminating a significant number of studies that are not relevant. On the contrary, there are chances that we may have skipped some of the relevant studies however we believe the other way around i.e. the customization of search string according to different databases has helped us minimizing the irrelevant literature. Hence, saving the time and efforts of all the researchers involved in the composition of the mapping study.

2.2 Screening and Qualitative Assessment of Studies

This section throws the light on two very important areas i.e. screening and qualitative assessment of the selected primary studies. The result of these assessments is presented in Table I and Table II given below.

2.2.1 Screening of the Studies

Screening of a study comprises of two main steps i.e. Generic Screening and Specific Screening. The first step i.e. Generic Screening provides the answers of five important questions (ref. Table I) such as whether the study is a duplicate study? Is English the medium of communications? etc. The second step i.e. Specific Screening helps us in eliminating the studies that are irrelevant hence by limiting the total number of selected studies for data extraction purpose. In this step, we analyse the relevance of the studies with respect to the abovementioned research questions.

Table I Study Selection Process

Step 1- Generic Screening			
1	Is the study a duplicate?	yes	no
2	Is English language used for writing the study?	yes	no
3	Is study a scientific peer-reviewed published research (which excludes white papers and technical reports)?	yes	no
4	Is study a primary study (not a secondary study)?	yes	no
5	Is the study not a part of any book?	yes	no
Step 2 - Specific Screening			
1	RQ1, RQ2 Does the study has any contribution in the area of adaptive security and mobile computing. If the answer is “YES” then go to the Table 2 for qualitative assessment. If the answer is “No” then exclude the study from the list of selected studies.		

Based on the result of the screening of studies, the total number of shortlisted studies is reduced to 76.

2.2.2 Qualitative Assessment of the Studies

We have performed quality assessment of 76 studies by emphasizing on the technical contents that have been presented in the studies by the researchers. The assessment is divided into two parts i.e. general assessment (G) and specific assessment (S) as shown in the Table 2.

Table II Quality Assessment Criteria

General Items for Quality Assessment (G)				
Score for G		**Yes = 1**	**Partial = 0.5**	**No = 0**
1	Are problem definition & motivation to conduct the study is manifestly presented?			
2	Is the research environment (in which study has been carried out) clearly mentioned?			
3	Is there the clarity of research methodology and organization of the study?			
4	Are the contributions are in-line with presented results?			
5	Does study explain the insights clearly?			
Specific Items for Quality Assessment (S)				
Score for S		**Yes = 1**	**Partial = 0.5**	**No = 0**
1	Is the research focused on the adaptive security for mobile computing?			

2	Are the details concerning related research clearly focus on the adaptive security related issues?			
3	Is the research evaluation clearly explains the existing tools and techniques used to ensure adaptive security in mobile computing?			
4	Is there any validation of the study in the real environment i.e. in real evaluation context?			
5	Are future research and existing limitations clearly documented?			

Quality assessment represents 5 factors criteria, providing a maximum score of 1. In the assessment formula below, S and G each represent a total of five factors as Specific and Generic Items with S having a maximum score of 3 and G with a maximum score 1. S contributes three times more than G (75% weight) as specific contributions of a study are more important than general factors for assessment. Based on the consensus among the researchers the maximum score was decided as G + S = 4, where a 3 – 4 score represented quality papers, a score less than 3 and greater than or equal to 1.5 was acceptable and a score less than 1.5 resulted in study exclusion.

$$\textbf{Quality Score} \quad = \frac{\sum_{G=1}^{5}}{5} + \left(\frac{\sum_{S=1}^{5}}{5} \times 3\right)$$

Based on the quality assessment of the selected 76 studies, we came to the conclusion that among the 76 studies only 29 studies are shortlisted as the potential candidate for the primary studies to be reviewed.

2.3 Data Extraction for Synthesis

The selected 36 primary studies are reviewed in order to extract the data and record it in a particular format as shown in Table 3. This table represents two types of data (i) generic and study demographic items and (ii) classification and mapping specific items.

Table III Data Extraction Strategy

	Data Item	Objective(s)
A - *Generic and Study Demographic Data Items (G)*		
G1	Study ID	The ID of the Study ____________________
G2	Study Title	The title of the Study ___________________
G3	Bibliography	1) Authors _______________________ 2) Publication Year ________________
G4	Citation Count	Count of Citations _____________________
G5	Quality Score	Quality Score of the Study_______________
G6	Additional Information	Any study oriented information ___________
B - *Classification and Mapping Specific Data Items (S)*		
S1	Research Problem	Research Problem/Challenge _________________________
S2	Research Solution	Proposed Solution/Method ____________________________

S3	Research Context	Application Domain of Solution__________________________
S4	Existing support (tools & techniques & frameworks)	Tools/Frameworks____________________________________ - Source Type_________________ - Automation Support___________ - Evaluation____________________ - Usage_______________________
S5	Validation Method	Methods/Techniques to Validate Solution_________________
S6	Evaluation Strategy	Strategy to Evaluate the Solution_________________________
S7	Research Trends	Existing Research Trends______________________________
S8	Future Research	Emerging and Futuristic Trends _________________________

3 Evaluating the Protocol for SMS

Once the protocol is defined, the next step for conducting mapping study is the internal and external evaluation of the protocol before its real time execution. We have tried to minimize the biasness by conducting the internal and external evaluation of the protocol defined above. Our main focus has been on the evaluation of the critical steps i.e. (i) primary studies identification and qualitative assessment, (ii) consistency of data extraction and reporting and (iii) data synthesis and result generation.

3.1 Internal Evaluation

As a team of researchers, we have focused on the representation of the information i.e. Table 2 (qualitative assessment of the shortlisted studies) and Table 3 (data extraction template). In first step, we, researchers, have executed the customised search strings on the selected databases/ digital libraries individually and later on we have compared the search results with each other. We have screened the shortlisted studies and then performed the qualitative analysis on the shortlisted studies. Based on the results, we have discussed and shortlisted 29 studies for reviewing and extracting data. One of the researchers among us has also cross-checked the results of literature review from different digital libraries (more specifically from 2 out of 5 selected digital libraries) and has also assessed the studies against the qualitative assessment criteria as mentioned in Table 2.

3.2 External Evaluation

External evaluation is basically a two-step procedure which is performed by an external researcher. In first step, we have shared the primary studies along with research questions RQs and data extraction template form with the external researcher. After analysing all the input that our team has provided, the external researcher has enlightened us with the valuable reviews and suggestions. Based on the feedback obtained, we have brought the required refinements in the RQs and alterations in the data extraction template form.

As per the second step, we have shared the refined RQs and data extraction form with the external researcher. After a detailed discussion on the obtained results, some possible validity threats to our research are also discussed.

4 Validity Threats

As an empirical research, the objective of this mapping study is to review and analyse the peer-reviewed literature in terms of challenges and reported solutions. In order to systematically conduct the mapping study, we have followed the procedure and guidelines provided in [4, 19], however; based on the context and scope of the study we also have deviations from the guidelines. These deviations from standards procedure represent some threats to the validity of this research. In the following, we highlight some possible threats to the validity of the mapping study.

4.1 Threats to Identification of Primary Studies

One the most fundamental steps in conducting the mapping study is the identification of the relevant literature for the review. In the methodological process highlighted in Section 3 and detailed in, the aim of systematically defined search string is to retrieve all the possible research studies and accommodate all the relevant published evidences in order to avoid literature selection biasness. We faced the challenges regarding the scope of the study, for instance the term security in mobile computing may have different interpretations among different researchers. To avoid such a bias, we devised an explicit inclusion and exclusion criteria to qualitatively assess each study to be included or excluded for the review. The adopted procedure for identification and selection of the relevant studies has increased the time and efforts, however; to the best of our knowledge all relevant studies have been included in the review.

4.2 Threats to the Quality of the Selected Studies and Data Extraction

The quality of the results of the mapping study depends on the quality of the studies included in the review. Specifically, if the quality of the primary studies is not good then the result deducted in this mapping study would also be questionable that leads to weak and unreliable evidence. In order to minimise this threat, each study has been evaluated objectively based on (i) the quality of the selected primary studies and (ii) the way the data is extracted and represented from the selected studies. Further, we have tried to ensure a structured template in order to capture and extract the data using the research questions.

4.3 Threats to Data synthesis and Results Reporting

Finally, there are also the threats to systematically synthesising the data due to the lack of a structured approach. We tried to minimise this threat by defining the data point and capture information from each study corresponding to a specific data point. For example, the mapping of the challenges and solutions was only possible after we have explicitly captured data points corresponding to *Security Challenge(s)* and *Solution(s)*. Furthermore, to derive the taxonomy of research, we have tried to classify the studies by following the ACM classification criteria for computing research. We have also mapped the results corresponding to the available evidence for better understanding, organisation and disjoint findings.

References

1. H. Qi and A. Gani, "Research on mobile cloud computing: Review, trend and perspectives," *Digital Information and Communication Technology and it's Applications (DICTAP), 2012 Second International Conference on*, Bangkok, 2012, pp. 195-202.

2. Y. Brun, G. Di Marzo Serugendo, C. Gacek, H. Giese, H. Kienle, M. Litoiu, H. Müller, M. Pezzè and M. Shaw, "Engineering Self-Adaptive Systems through Feedback Loops", *Software Engineering for Self-Adaptive Systems*, 2009, pp. 48-70.

3. N. Fernando, S. Loke and W. Rahayu, "Mobile cloud computing: A survey", *Future Generation Computer Systems*, 2013, vol. 29, no. 1, pp. 84-106.

4. K. Petersen, R. Feldt, S. Mujtaba, M. Mattsson, “Systematic Mapping Studies in Software Engineering”, *In 12th International Conference on Evaluation and Assessment in Software Engineering (EASE 2008)*, ACM, 2008, pp: 68 – 77.

5. "Xposed - General info, versions & changelog", XDA Developers, 2016. [Online]. Available: http://forum.xda-developers.com/xposed/xposed-installer-versions-changelog-t2714053. [Accessed: 26- Jun- 2016].

6. "A framework for analyzing and transforming Java and Android Applications", Sable.github.io, 2016. [Online]. Available: https://sable.github.io/soot/.

7. "Android Testing Tutorial", www.tutorialspoint.com, 2016. [Online]. Available: http://www.tutorialspoint.com/android/android_testing.htm. [Accessed: 26- Jun- 2016].

8. "An Introduction to the Resource Description Framework", Dlib.org, 2016. [Online]. Available: http://www.dlib.org/dlib/may98/miller/05miller.html. [Accessed: 30- Jun- 2016].

9. G. Chen and D. Kotz, “A Survey of Context-Aware Mobile Computing Research”, Technical Report, Dartmouth College, Hanover, NH, USA, 2000.

10.

11. H. Suo, Z. Liu, J. Wan and K. Zhou, "Security and privacy in mobile cloud computing," *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Sardinia, 2013, pp. 655-659.

12. A. Elkhodary and J. Whittle, “A Survey of Approaches to Adaptive Application Security”, *In Proceedings of the 2007 International Workshop on Software Engineering for Adaptive and Self-Managing Systems (SEAMS '07),* IEEE Computer Society, Washington, DC, USA, 2007, 16.

13. M. Satyanarayanan, “Mobile Computing: the Next Decade”, *ACM SIGMOBILE Mobile Computing and Communications Review*, 2011, vol 15, no 2, pp: 2-10.

14. A. Mtibaa, K. Harras, K. Habak, M. Ammar, and E. Zegura, “Towards mobile opportunistic computing”, *In Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on*, June 2015, pp. 1111–1114.

15. Ardagna, C.A.; Conti, M.; Leone, M.; Stefa, J., "An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments," *Services Computing, IEEE Transactions on*, 2014, vol.7, no.3, pp. 373-386.

16. J. O. Kephart and D. M. Chess, “The Vision of Autonomic Computing” *In IEEE Computer,* 2003, vol. 36, no. 1, pp. 41–50.

Appendix A – List of Studies for Mapping Study

Study ID	Author(s), Title, and Channel of Publication	Publication Year	Publication Type	Citation Count
[S1]	K. Zhao, D. Zou, H. Jin, Z. Tian, W. Qiang, W. Dai. **Privacy Protection for Perceptual Applications on Smartphones.** *In IEEE International Conference on Mobile Services.*	2015	Conference	00
[S2]	M. Garcia, D. Llewellyn-Jones, F. Ortin, M. Merabti. **Applying Dynamic Separation of Aspects to Distributed Systems Security: A Case Study.** *In IET Software, vol. 6, no. 3, pp: 231 – 248*	2012	Journal	07
[S3]	S. P. Alampalayam, A. Kumar. **An Adaptive Security Model for Mobile Agents in Wireless Networks.** *In IEEE Global Telecommunications Conference.*	2003	Conference	07
[S4]	M. Protsenko, S. Kreuter, T. Muller. **Dynamic Self-Protection and Tamper proofing for Android Apps Using Native Code**. *In 10th International Conference on Availability, Reliability and Security*.	2015	Conference	00
[S5]	G. An, G. Bae, K. Kim, D. Seo. **Context-Aware Dynamic Security Configuration for Mobile Communication Device.** *In 3rd International Conference on New Technologies, Mobility and Security.*	2009	Conference	01
[S6]	C. Wanpeng, B. Wei. **Adaptive and Dynamic Mobile Phone Data Encryption Method.** *In China Communications, vol. 11, no. 1, pp: 103 – 109.*	2014	Journal	02
[S7]	K. Kim, H. Hwang, H. Ko, H. Lee, U. Kim. **Multi-Policy Access control considering Privacy in Ubiquitous Environment.** *In International Conference on Hybrid Information Technology*	2006	Conference	03
[S8]	B. Lagesse, M. Kumar, M. Wright. **AREX: An Adaptive System for Secure Resource Access in Mobile.** *In International Conference on Peer-to-Peer Computing.*	2008	Conference	04
[S9]	G. Pallapa, N. Roy, S. K. Das. **A scheme for Quantizing Privacy in Context-aware Ubiquitous Computing.** *In 4th International Conference on Intelligent Environments.*	2008	Conference	09
[S10]	P. C. Castro, J. W. Ligman, M. Pistoia, J. Ponzo, G. S. Thomas, U. Topkara. **Runtime Adaptive Multi-Factor Authentication for Mobile Devices.** *In IBM Journal of Research and Development, vol 57, no 6, pp: 1 – 17*	2013	Journal	00
[S11]	F. Martinelli, P. Mori, T. Quillinan, C. Schaefer. **A Runtime Monitoring Environment for Mobile Java.** *In IEEE International Conference on Software Testing Verification and Validation Workshop.*	2008	Conference	01
[S12]	I. Bae, H. Lee, K. Lee. **Design and Evaluation of a Dynamic Anomaly Detection Scheme Using the Age of User Profiles.** *In 4th International Conference on Fuzzy Systems and Knowledge Discovery.*	2007	Conference	01
[S13]	F. Li, Y. Rahulamathavan, M. Rajarajan. **LSD-ABAC: Lightweight Static and Dynamic Attributes Based Access Control Scheme for Secure Data Access in Mobile Environment.** *In IEEE 39th Conference on Local Computer Networks.*	2014	Conference	04
[S14]	M. Salehie, L. Pasquale, I. Omoronyia, R. Ali, B. Nuseibeh. **Requirements-driven Adaptive Security: Protecting Variable Assets at Runtime.** *In 20th IEEE International Requirements Engineering Conference.*	2012	Conference	08
[S15]	S. Tarkoma, C. Prehofer, S. Sovio, P. Laitinen. **Composable Mediation for Security-Aware Mobile Services.** *In IEEE Communications Magazine, vol. 45, no. 7, pp: 58 – 65.*	2007	Journal	01
[S16]	Z. Yang, S. Lu, P. Yang. **Runtime Security Verification for Itinerary-Driven Mobile Agents.** *In 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*	2006	Symposium	02
[S17]	X. Zhang, G. Kim, H. Bae. **An Adaptive Spatial Cloaking Method for Privacy Protection in Location-based Service.** *In International Conference on Information and Communication Technology Convergence.*	2014	Conference	01
[S18]	F. Schaub, B. Konings, M. Weber. ***Context-Adaptive Privacy: Leveraging Context Awareness to Support Privacy Decision Making*.** *In IEEE Pervasive Computing, vol 14, no. 1, pp: 34 – 43.*	2015	Journal	02
[S19]	S. C. Joo, C. W. Jeong, S. J. Park. **Context Based Dynamic Security Service for Healthcare Adaptive Application in Home Environments.** *In Software Technologies for Future Dependable Distributed Systems*.	2009	Conference	16
[S20]	P. E. Khoury, F. Massacci, A. Saidane. **A Dynamic Security Framework for Ambient Intelligent Systems: A Smart-Home Based eHealth Application.** *In Transactions on Computational Science/Special Issue on Security in Computing, Part I, pp: 1 – 24, Springer Berlin Heidelberg*	2010	Book Chapter	01

[S21]	S. Hacini, Z. Boufaïda, H. Cheribi. **Mobile Agent Protection in E-Business Application: A Dynamic Adaptability Based Approach**. *In the Proceedings of OTM Confederated International Conference on the Move to Meaningful Internet Systems.*	2007	Conference	00
[S22]	H. Aloulou, M. Loulou, S. Kallel, A. H. Kacem. **RDyMASS: Reliable and Dynamic Enforcement of Security Policies for Mobile Agent Systems.** *In 4th International Workshop on SETOP Data Privacy Management and Autonomous Spontaneous Security.*	2010	Workshop	02
[S23]	B. P. S. Rocha, D. N. O. Costa, R. A. Moreira, C. G. Rezende, A. A. F. Loureiro, A. Boukerche. **Adaptive Security Protocol Selection for Mobile Computing.** *In Journal of Network and Computer Applications, vol 33, no. 5, pp: 569–587.*	2010	Journal	13
[S24]	T. El-Maliki, J. Seigneur. **Security Adaptation based on Autonomic and Trust Systems for Ubiquitous Mobile Network and Green IT.** *In 7th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies.*	2013	Conference	00
[S25]	S. Arzt1, K. Falzon, A. Follner, S. Rasthofer, E. Bodden1, V. Stolz. **How useful are existing monitoring languages for securing Android apps?** In Arbeitstagung Programmiersprachen (ATPS)	2013	Symposium	04
[S26]	J. Xiong, K. Jamieson. **SecureArray: Improving Wifi Security with Fine-grained Physical-layer Information.** *In Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*	2013	Conference	24
[S27]	G. Thamilarasu, Z. Ma. **Autonomous mobile agent based intrusion detection framework in wireless body area networks.** In IEEE *16th International Symposium on a World of Wireless, Mobile and Multimedia Networks*.	2015	Symposium	00
[S28]	P. Ortiz, O. Lázaro, M. Uriarte, M. Carnerero. **Enhanced Multi-domain Access Control for Secure Mobile Collaboration through Linked Data Cloud in Manufacturing.** *In IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks*.	2013	Symposium	06
[S29]	Y. Zhao, J. Ye, T. Henderson. **Privacy-aware Location Privacy Preference Recommendations.** *In Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services.*	2014	Conference	05
[S30]	Ş. Bahtiyar, O. Ermiş, M. U. Çağlayan**. Adaptive Trust Scenarios for Mobile Security.** *In 13th International Conference on Mobile Web and Intelligent Information Systems*	2016	Conference	0
[S31]	D. Moon, I. Kim, J. W. Joo, H. J. Im, J. H. Park, Y-Sik Jeong. **Intelligent Security Model of Smart Phone Based on Human Behavior in Mobile Cloud Computing.** *Wireless Personal Communications,* vol. *91, no 4, pp: 1697 – 1710*	2016	Journal	02
[S32]	K. Gai, M. Qiu, H. Zhao. **Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing**. *In IEEE 3rd International Conference on Cyber Security and Cloud Computing*	2016	Conference	07
[S33]	K. Gai, M. Qiu, H. Zhao, W. Dai. **Privacy-Preserving Adaptive Multi-channel Communications Under Timing Constraints**. *In IEEE International Conference on Smart Cloud*	2016	Conference	0
[S34]	Z-Yuan Li, L. Liu R-Long Chen, J-Lei Bi. **An Adaptive Secure Communication Framework for Mobile Peer-to-Peer Environments Using Bayesian Games**. *In Peer-to-Peer Networking and Applications, vol. 9, no 6, pp: 1005–1019*	2016	Journal	02
[S35]	A. M. Rashwan, A-E M. Taha, H. S. Hassanein. ***Toward Designing an Adaptive Communication Security for the Next-generation Mobile Computing***. *In IEEE International Conference on Communications*	2016	Conference	0
[S36]	D. M. SHILA, W. Shen, Y. Cheng, X. Tian, X. Shen. **AMCLOUD: Toward a Secure Autonomic Mobile Ad Hoc Cloud Computing System.** *In IEEE Wireless Communications, no. 99, pp: 2 – 9.*	2016	Journal	03