Protocol for a Systematic Literature Review on Security-related Research in Ubiquitous Computing
(second and updated version)

Ema Kušen Mark Strembeck

Contact information:
Vienna University of Economics and Business,
Institute for Information Systems and New Media,
Welthandelsplatz 1, 1020 Vienna
{firstname.lastname}@wu.ac.at

Abstract

Context: This protocol is as a supplementary document to our review paper that investigates security-related challenges and solutions that have occurred during the past decade (from January 2003 to December 2014).

Objectives: The objective of this systematic review is to identify security-related challenges, security goals and defenses in ubiquitous computing by answering to three main research questions. First, demographic data and trends will be given by analyzing where, when and by whom the research has been carried out. Second, we will identify security goals that occur in ubiquitous computing, along with attacks, vulnerabilities and threats that have motivated the research. Finally, we will examine the differences in addressing security in ubiquitous computing with those in traditional distributed systems.

Method: In order to provide an overview of security-related challenges, goals and solutions proposed in the literature, we will use a systematic literature review (SLR). This protocol describes the steps which are to be taken in order to identify papers relevant to the objective of our review. The first phase of the method includes *planning*, in which we define the scope of our review by identifying the main research questions, search procedure, as well as inclusion and exclusion criteria. Data extracted from the relevant papers are to be used in the second phase of the method, *data synthesis*, to answer our research questions. The review will end by *reporting* on the results.

Results and conclusions: The expected results of the review should provide an overview of attacks, vulnerabilities and threats that occur in ubiquitous computing and that have motivated the research in the last decade. Moreover, the review will indicate which security goals are gaining on their significance in the era of ubiquitous computing and provide a categorization of the security-related countermeasures, mechanisms and techniques found in the literature.

Keywords: systematic review; ubiquitous computing; mobile computing; wearable computing; security

1 Note on the updates

This is a second and updated version of our research protocol. The following changes have been made:

1. We included the details on the automatic search conducted in January 2015 (pg. 30)
2. We included the mappings between papers and their corresponding categories (pg. 32-38)
3. We updated the list of selected papers (pg. 43-59)

Contents

2 Background

Ubiquitous computing, as envisioned by Mark Weiser [Wei99], assumes disappearance of technologies into the everyday environment, making them invisible to a user. With the proliferation of mobile and wearable devices enhanced with sensing capabilities, users are able to seamlessly collect and receive information from their surroundings [DMWS09] [PM03] [YHGY06] [ZMN06b]. Such an opposing image to virtual reality introduces a number of unprecedented characteristics to the era of ubiquitous computing. For one, devices participating in a ubiquitous environment are heterogeneous with respect to their hardware capabilities and operating systems. On the one hand, such a nature of devices introduces a number of advantages while designing ubiquitous infrastructures. For example, smartphones and tablets enriched with a number of embedded sensors, such as microphones, GPS, accelerometer and gyroscope [WCMA13], are able sense the changes of the environment and respond accordingly. Such a capability to react to the context has been recognized as an important factor in designing dynamic and complex infrastructures [LSP+14] which support the mobility of users. Furthermore, the notion of context-awareness has brought changes to the research and development in the human-computer interaction [HCS05] where the emphasis has been put on designing such interfaces, which do not interrupt or distract users from their surroundings.

Although such a vision offers many advantages to the way users interact with their environment and use available services, designing ubiquitous computing systems and environments that are privacy-sensitive and ensure security of user data still remains a challenge [Oh08][PAN05][RL07]. Over the last decade, a large and growing body of literature has tackled different security-related challenges, such as ensuring the availability of applications and services [ASA08], dealing with the lack of a fixed pre-deployed infrastructure [AHH+10] [AMD+08b], designing security mechanisms for the resource-constrained devices [HCC+12] [HHNL07] and managing trust among the large number of nodes participating in a mobile ad-hoc network (MANET) [WF07], to name a few.

To the best of our knowledge, there is no systematic review which provides a comprehensive overview of the research in the area of security in ubiquitous computing. It is, therefore, our aim to identify which attacks, vulnerabilities and threats have motivated the researchers in the last decade. Moreover, we are interested in security goals, as well as security countermeasures presented in the literature. Additionally, we will examine whether the necessary algorithms and technologies are publicly available and identify the validation mechanisms used to assess the appropriateness of the proposed solutions.

In order to provide an overview of the aforementioned security-related challenges and solutions, we will use a systematic literature review (SLR) method proposed by [KC07], which consists of 3 phases: planning, conducting and reporting. This document provides guidelines for our SLR developed in the first phase of the review (planning). To ensure rigor in the review process, the following procedures have been defined and presented in this document in detail:

1. Design of the research questions (see Section 3),
2. Search strategy (see Section 4),
3. Definition of the inclusion and exclusion criteria (see Section 5.1),
4. Quality assessment (see Section 5.4),
5. Data extraction (see Section 5.5),
6. Data synthesis (see Section 6).

Report on the pilot procedures will also be provided in this document, as well as any revisions to the first version of the protocol.

3 Research questions

The review is motivated by three research questions:

RQ1: Demographic data and trends.

RQ2: Which security-related goals have been addressed in ubiquitous computing in the last decade (from January 2003 - December 2014)?

RQ3: Is there a difference in addressing security in distributed systems in comparison with ubiquitous computing?

As suggested in [ATF09b] [KC07] [RHTi13], we used the *population*, *intervention*, *comparison*, *outcomes* and *context* (PICOC) criteria to clarify the general goal of the review (see Table 1). The details of each PICOC criterion will form the basis for the construction of our search terms (see section 4). In order to reach the goal of our review, we included additional terms that are related to ubiquitous computing. These are pervasive computing, mobile computing and wearable computing. The choice of the additional terms can be justified through the definition of ubiquitous computing found in the literature which identifies wireless networks, mobile and wearable devices as an essential part of a ubiquitous computing environment [DMWS09] [PM03] [YHGY06] [ZMN06b]. Moreover, we introduced *wireless body area network* (WBAN)[1] to the list of terms because we wanted to ensure that papers on the topic of security in wearable computing (that are considered relevant for the purpose of our research) are found and included in our review.

PICOC	Terms
Population	ubiquitous computing, pervasive computing, mobile computing, wearable devices, wearable computing, wireless body area network (WBAN).
Intervention	security mechanisms.
Comparison	distributed computing.
Outcomes	security of user data.
Context	empirical papers in industry and academic environment.

Table 1: PICOC criteria and research questions.

3.1 Details of the first research question

The main goal of the **first research question (RQ1)** is threefold:

RQ1.1: provide an overview of where the research on security in ubiquitous computing has been carried out (*expected outcome*: list of countries),

RQ1.2: examine when the research on security in ubiquitous computing has been carried out (*expected outcome*: number of articles per year),

RQ1.3: identify by whom the research on security in ubiquitous computing has been carried out (*expected outcome*: names of the researchers).

Moreover, we will also look for the information on the paper citations and venue where the paper was published.

RQ1.4: identify the most cited papers based on the Google Scholar citation count (*expected outcome*: number of citations).

[1] WBAN is the network of wearable computing devices and differs from traditional wired networks due to its specific characteristics, such as shared resources, node mobility and short transmission range [BR08].

We decided to use Google Scholar search engine to count the number of citations for each paper because it is able to search for scholarly literature across many disciplines and sources and, therefore, provide a more comprehensive citation count than individual databases.

RQ1.5: identify journals where the papers on security in ubiquitous computing have been published (*expected outcome*: list of journals),

RQ1.6: identify conferences where the papers on security in ubiquitous computing have been published (*expected outcome*: list of conference proceedings),

Data will be presented using the diagrams presented in Table 3.1. The list of countries (RQ1.1) will be presented using a bar diagram. Since we expect a lengthy list of countries, we will present only the first ten countries based on the number of times they have occurred in the papers. On the horizontal axis we will present the number of times (in percentages) a country occurred and on the horizontal axis the names of the countries. Since we expect to find at least one paper for each year in the interval [2003-2014], we will present the distribution of papers over years (RQ1.2) by a line diagram. The vertical axis will represent the number of papers published each year. On the horizontal axis we will plot the year interval. In case the distribution of numbers is not continuous, i.e. in case it happens that we could not identify any paper for one year within the interval, we will use a bar diagram. Author's names (RQ1.3) will be presented in a table format, which consists of two columns - author's name and number of papers identified. We will provide information for the first five authors based on the amount of papers identified in our SLR. Number of citations (RQ1.4) will be presented with a bar diagram, where the horizontal axis represents a paper and a vertical axis its corresponding number of citations. We will show the results for the first five papers based on the number of citations. The results of the questions RQ1.5 and RQ1.6 will be presented in a table, where the first column stands for a title of a journal/conference, and the second column for the number of papers identified, respectively. We will present the results for the first five journals/conference proceedings based on the number of papers found.

3.2 Details of the second research question

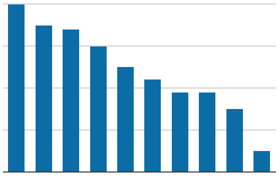
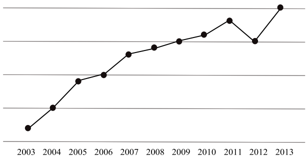
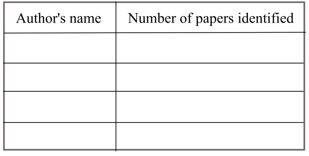
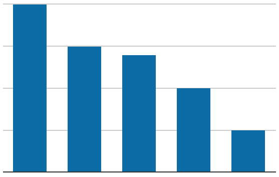
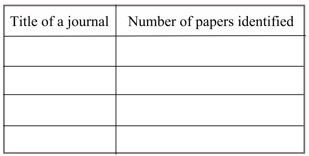
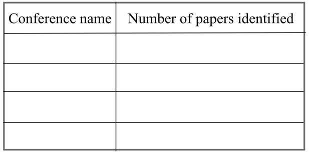
The **second research question (RQ2)** can be addressed in more depth. Therefore, six additional subquestions (see Table 2) are included to identify the security goals, motivation for the papers and proposed techniques, algorithms and methods used to solve security issues. We are also interested in the assessment of the proposed solutions, as well as limitations, recommendations and future work. Additionally, we will examine whether the algorithms and technologies used in the proposed solutions are publicly available, i.e. whether the results can be repeated and validated.

3.3 Details of the third research question

The aim of the **third research question (RQ3)** is to analyze the differences in addressing security in traditional distributed computing with those in ubiquitous computing based on the results obtained from the second research question. More specifically, we will compare security-related mechanisms and techniques that occur in both computing paradigms in order to find out whether the proposed solutions are inherited from distributed computing or newly introduced to ubiquitous computing.

4 Search strategy

In this section we will provide details of the following procedures: definition of the search terms, construction of the search strings, list of the resources to be searched and inclusion and exclusion criteria.

ID	**Expected outcome**	**Visualization**		**Restrict to**
		Type	Presentation	
RQ1.1	List of countries	bar diagram		10 countries
RQ1.2	Nr. of papers per year	line diagram		-
RQ1.3	Names of the researchers	table	Author's name Number of papers identified	5 researchers
RQ1.4	Number of citations	bar diagram		5 papers
RQ1.5	Number of journal papers	table	Title of a journal Number of papers identified	5 journals
RQ1.6	Number of conference papers	table	Conference name Number of papers identified	5 conferences

RQ	Motivation
RQ 2: Which security-related goals have been addressed in terms of ubiquitous computing?	Identify security goals addressed in the papers.
RQ 2.1: What is the motivation for the research?	Identify factors which motivated the papers, such as vulnerabilities, threats, and attacks.
RQ 2.2: Which solutions have been presented?	Identify suggested techniques, algorithms, and methods.
RQ 2.3: Are the algorithms and technologies publicly available?	Investigate whether the papers can be repeated in order to check the validity of results.
RQ 2.4: What kind of validation of the results has been performed?	Assess the appropriateness of the proposed solution.
RQ 2.5: Which future work has been proposed?	Investigate future trends in development and implementation of security mechanisms in ubiquitous computing.

Table 2: Refinement of the second research question.

4.1 Definition of the search terms

Based on the definition of the research scope and the PICOC details, we chose the first keyterms for a pilot search in order to determine whether the relevant papers will be identified. In addition to the PICOC terms (pervasive, ubiquitous, wearable, mobile computing and security), we included security goals to increase the probability of finding relevant papers. In order to identify the list of security goals that we will refer to in this review, we examined the proposed categorizations by [SRM13], [Wol08], [TS06] and [PS09]. Although the aforementioned categorizations include the same list of the basic security goals (data confidentiality, authentication, integrity and availability), the main difference lies in identifying the list of additional goals. For example, [PS09] identifies goals specific to the wireless sensor networks (WSN), such as data freshness, self-organization of a network, time synchronization and secure localization. Furthermore, categorization by [Wol08] includes only one goal (audit) additionally to the list of the basic goals. Therefore, we will use the list of security goals by [SRM13], which includes 4 basic goals (confidentiality, integrity, authentication and availability), 5 composite goals (access control, non-repudiation, authenticity of data, privacy and accountability) and audit. Throughout our SLR we will not exclude the possibility of identifying additional security goals, i.e. in addition to the predefined list of security goals we will use a general term "security" to increase our chances of finding as many relevant papers as possible.

We conducted a **pilot search** with a smaller subset of the search terms *pervasive*, *ubiquitous*, *wearable*, *mobile computing*, *security*, *authentication*, *confidentiality*, *privacy* and the alternative term *protection*. The results have shown that this combination of keyterms produces a large number of papers that are irrelevant for our review. For example, the keyword *protection* found papers on the topic of a homeland security, which was not in the scope of our review. Moreover, not many papers related to security in wearable computing were found. Thus, we included an additional search term "wireless body area network (WBAN)" to increase the chance of finding relevant papers on the topic. The list of keyterms was iteratively refined until we got a satisfactory list of initial papers. The final list of keyterms is presented below (Table 3), and includes the security goals proposed by [SRM13].

Keyterms		Alternative terms
T1	ubiquitous computing	pervasive computing, wearable computing, body area network, mobile computing
T2	security	confidentiality, authentication, access control, non-repudiation, audit, integrity, authenticity of data, availability, accountability, privacy

Table 3: Search terms.

4.2 Design of the search string

We constructed a search string using the identified keywords, their alternatives and related terms linked with Boolean *AND* and *OR* operators. Since our review will focus on identifying security goals in ubiquitous computing, the search string is built in the following way: $(T1_1 \lor T1_2 \lor \ldots \lor T1_\mathrm{n}) \land (T2_1 \lor T2_2 \lor \ldots \lor T2_\mathrm{n}) \quad where \quad T1_{1\,\ldots\,\mathrm{n}} \in T1 \land T2_{1\,\ldots\,\mathrm{n}} \in T2$.

Due to the large number of keywords and the specific limitations of search engines [FSGC13], the general search string is divided into three search strings, as presented in Table 4.

String	Form
S1	(ubiquitous *OR* "pervasive computing" *OR* "mobile computing" *OR* wearable *OR* "body area network") *AND* (security *OR* confidentiality *OR* "access control" *OR* authentication)
S2	(ubiquitous *OR* "pervasive computing" *OR* "mobile computing" *OR* wearable *OR* "body area network") *AND* (privacy *OR* integrity *OR* "authenticity of data" *OR* availability)
S3	(ubiquitous *OR* "pervasive computing" *OR* "mobile computing" *OR* wearable *OR* "body area network") *AND* ("non-repudiation" *OR* audit *OR* accountability)

Table 4: Search strings.

4.3 Resources to be searched

In order to find relevant papers for our review, we will perform the search procedure automatically by using scientific databases' search engines and manually by scanning through the selected conferences, as shown in Figure 1.

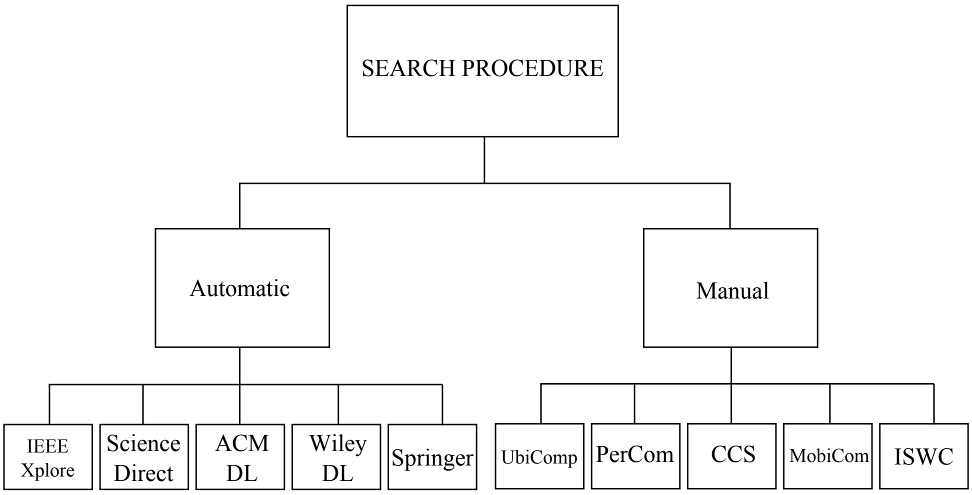


Figure 1: Manual and automatic search

The following 5 scientific databases have been chosen for our review because they publish a substantial amount of peer-reviewed papers on the subject of computer science, including security and privacy:

1. Science Direct,
2. IEEEXplore,
3. ACM DL,
4. Wiley DL,
5. Springer library.

In addition to the automatic database search, we identified 5 conferences that will be searched manually. The choice of the conferences has been made according to the topics the conferences focus on and encompass the search terms defined in 4.1, as shown in Figure 2.

1. ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp),
2. IEEE Pervasive Computing and Communication conference (PerCom),
3. ACM Conference on Computer and Communications Security (CCS),

4. Annual ACM International Conference on Mobile Computing and Networking (MobiCom),
5. International Symposium on Wearable Computers (ISWC).

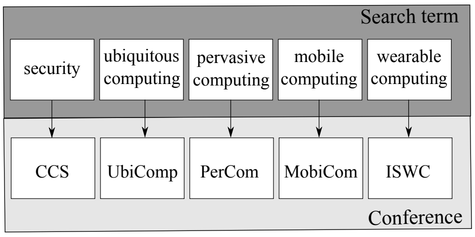


Figure 2: Conferences and search terms

4.4 Refinement of the general search string

Due to the specific requirements of each search engine, we adapted our search procedure to each scientific database, as seen in Table 5.

Scientific database	**Search type**	**Search in**	**Refinement**
Science Direct	Expert search	Title, abstract and keywords	Limit the search to journals and a time-frame [2003-2014]
Wiley DL	Advanced search	Abstract	Limit the search to a time-frame [2003-2014]
IEEEXplore	Command search	Abstract	Limit the search to a time-frame [2003-2014]
ACM DL	Advanced search	Abstract	Limit the search to a time-frame [2003-2014]
Springer	Advanced search	Title	Limit the search to a time-frame [2003-2014] and English

Table 5: Requirements of scientific databases.

Once the search procedure has been adapted for each database, we refined the general search string defined in 4.2 (see Table 6).

Scientific Database	**First set of search strings**
Science Direct	*TITLE-ABSTR-KEY(ubiquitous OR ”pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) and TITLE-ABSTR-KEY(security OR confidentiality OR ”access control” OR authentication)*
IEEEXplore	*(”Abstract”:ubiquitous OR ”Abstract”:”pervasive computing” OR ”Abstract”:”mobile computing” OR ”Abstract”:wearable OR ”Abstract”:”body area network”) AND (”Abstract”:security OR ”Abstract”:confidentiality OR ”Abstract”:”access control” OR ”Abstract”:authentication)*
ACM Digital Library	*(Abstract:ubiquitous OR Abstract:”pervasive computing” OR Abstract:”mobile computing” OR Abstract:wearable OR Abstract:”body area network”) AND (Abstract:security OR Abstract:confidentiality OR Abstract:”access control” OR Abstract:authentication)*
Wiley Digital Library	*(ubiquitous OR “pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) AND (security OR confidentiality OR ”access control” OR authentication)*
Springer	*(ubiquitous OR “pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) AND (security OR confidentiality OR ”access control” OR authentication)*
Scientific Database	**Second set of search strings**
Science Direct	*TITLE-ABSTR-KEY(ubiquitous OR ”pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) and TITLE-ABSTR-KEY(privacy OR integrity OR ”authenticity of data” OR availability)*

IEEEXplore	*(”Abstract”:ubiquitous OR ”Abstract”:”pervasive computing” OR ”Abstract”:”mobile computing” OR ”Abstract”:wearable OR ”Abstract”:”body area network”) AND (”Abstract”:privacy OR ”Abstract”:integrity OR ”Abstract”:”authenticity of data” OR ”Abstract”:availability)*
ACM Digital Library	*(Abstract:ubiquitous OR Abstract:”pervasive computing” OR Abstract:”mobile computing” OR Abstract:wearable OR Abstract:”body area network”) AND (Abstract:privacy OR Abstract:integrity OR Abstract:”authenticity of data” OR Abstract:availability)*
Wiley Digital Library	*(ubiquitous OR “pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) AND (privacy OR integrity OR ”authenticity of data” OR availability)*
Springer	*(ubiquitous OR “pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) AND (privacy OR integrity OR ”authenticity of data” OR availability)*
Scientific Database	**Third set of search strings**
Science Direct	*TITLE-ABSTR-KEY(ubiquitous OR ”pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) and TITLE-ABSTR-KEY(”non-repudiation” OR audit OR accountability)*
IEEEXplore	*(”Abstract”:ubiquitous OR ”Abstract”:”pervasive computing” OR ”Abstract”:”mobile computing” OR ”Abstract”:wearable OR ”Abstract”:”body area network”) AND (”Abstract”:”non-repudiation” OR ”Abstract”:audit OR ”Abstract”:accountability)*
ACM Digital Library	*(Abstract:ubiquitous OR Abstract:”pervasive computing” OR Abstract:”mobile computing” OR Abstract:wearable OR Abstract:”body area network”) AND (Abstract:”non-repudiation” OR Abstract:audit OR Abstract:accountability)*
Wiley Digital Library	*(ubiquitous OR “pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) AND (”non-repudiation” OR audit OR accountability)*
Springer	*(ubiquitous OR “pervasive computing” OR ”mobile computing” OR wearable OR ”body area network”) AND (”non-repudiation” OR audit OR accountability)*

Table 6: List of search strings.

The results for each database search and its corresponding search string are given in Appendix A.

4.5 Evaluation of the search process

Before undertaking the review, search strings will be evaluated by their ability to detect the papers presented in Table 7. The list of papers was identified by using the general keyterms “security” and “ubiquitous computing” over the scientific databases prior to the definition of the search strings.

DB	Author	Title	Venue	Year	Page Nr.	Reference
IEEE	Cahill et al.	Using trust for secure collaboration in uncertain environments	IEEE Pervasive Computing (2)3	2003	52-61	[CGS$^+$03]
	Ahmadian et al.	Recursive linear and differential cryptanalysis of ultralightweight authentication protocols	IEEE Transactions on Information Forensics and Security 8(7)	2013	1140-1151	[ASA13]
	Zhu et al.	Understanding and minimizing identity exposure in ubiquitous computing environments	International Conference on Mobile and Ubiquitous Systems: Networking Services, MobiQuitous'09	2009	1-10	[ZCK$^+$09]
	Hoque et al.	An Adaptive Initial Trust and Demand Aware Secure Resource Discovery (AID-SRD) model for pervasive environments	International Conference on Pervasive Computing and Communications, PerCom'09	2009	1-6	[HRA09]
Science Direct	Hengartner, Steenkiste	Exploiting information relationships for access control in pervasive computing	Pervasive and Mobile Computing 2(3)	2006	344-367	[HS06]
	Tan, Z.	A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments	Journal of Network and Computer Applications 35(6)	2012	1839-1846	[Tan12]
	Bahtiya, Caglayan	Extracting trust information from security system of a service	Journal of Network and Computer Applications 31(1)	480-490	2012	[BU12]
ACM	Shi et al.	BANA: body area network authentication exploiting channel characteristics	Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC'12	2012	27-38	[SLYY12]
	Shahzad et al.	Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you cannot do it	Proceedings of the 19th Annual International Conference on Mobile Computing & Networking, MobiCom'13	2013	39-50	[SLS13]
Wiley	Jang et al.	Hybrid security protocol for wireless body area networks	Wireless Communications and Mobile Computing 11(2)	2011	277-288	[JLHP11]
	Yau et al.	Support for situation awareness in trustworthy ubiquitous computing application software	Software: Practice and Experience 36(9)	2006	893-921	[YHGY06]
Springer	English et al.	Towards self-protecting ubiquitous systems: monitoring trust-based interactions	Personal and Ubiquitous Computing	2006	50-54	[ETN06]
	Li et al.	An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments	Nonlinear Dynamics 74(4)	2013	1133-1143	[LLW13]

Table 7: The known subset of papers.

5 Paper selection

5.1 Inclusion and exclusion criteria

In order to identify the papers that are in line with the objective of our review, we conducted a consensus meeting where the inclusion and exclusion criteria were defined. The initial list of criteria is presented below (Table 8 and Table 9 present exclusion and inclusion criteria, respectively).

Criterion ID	Criterion
E01	Summaries of workshops and tutorials, title pages, editorials and extended abstracts as they do not provide sufficient information to the objective of our review.
E02	Workshop articles as they report on a study in its early stage.
E03	Posters, as they do not provide enough information for the purpose of our review.
E04	Books and PhD theses, as they are beyond the scope of this review.
E05	Double entries. If an extended journal article is found, it will be chosen over the conference article. If a more recent paper is found, it will be chosen over its preceding paper.
E06	Papers whose focus was not put on security goals in ubiquitous, mobile and wearable computing, i.e. papers that mentioned security in their abstracts as one of the issues.
E07	Opinion papers, discussion papers and survey papers that do not propose a solution.
E08	Any paper whose full text is not accessible.
E09	Papers not written in English.
E10	Papers with a low quality assessment score (to be done after the quality assessment procedure, see Section 5.4).

Table 8: Exclusion criteria

Criterion ID	Criterion
I01	Full version of journal and conference articles that report on, discuss or investigate security issues in ubiquitous, mobile and wearable computing.
I02	Papers that propose a solution to the identified security issue.
I03	Papers written in English.
I04	Papers published since 2003.

Table 9: Inclusion criteria

We conducted a pilot selection procedure with the criteria defined above, which resulted in a large number of potentially relevant papers (n=4369). Both reviewers participated in the search procedure, one searched for the papers according to the defined set of criteria, while the other checked titles and abstracts against the inclusion criteria.

Due to the large number of papers identified in the initial search process, two additional criteria are introduced to keep the selection process manageable:

1. Papers published in the journals with a Scimago Journal Ranking (SJR) where h-index [2] ≥ 35 or SJR ≥ 0.8.

2. Papers published in the conference proceedings with a rank A+ or A based on the CORE ranking (Computer Science Conference Rankings) [3]

The latter criterion was formerly used in literature review papers [WW02] where it was indicated that researchers should examine conference proceedings with a reputation for quality.

[2] journal's number of papers that have received at least h citations over the whole period. For additional information refer to [sci]

[3] For additional information refer to [Cor].

5.2 Filtering of the papers

We will use the inclusion and exclusion criteria on the initial pool of papers in the following way (see Figure 3). While obtaining the papers for the initial pool, we will check whether they are written in English. This criterion can be incorporated within the automatic database search for some databases, such as Springer. For the results of the remaining databases, we will manually check the list of papers and exclude those written in any other language than English (exclusion criterion E09).

Once the initial papers have been identified, we will begin with the first filtering phase in which the double entries will be removed (**P1**) with the help of the Zotero reference manager (exclusion criterion E5). In order to ensure that there are only unique entries left, we will check the papers and manually remove any doubles remaining in the pool. Our second phase will be to look for the workshop articles, summaries of workshops and tutorials, title pages, editorials, posters and extended abstracts (**P2**). If such papers are found, we will exclude them from the pool (exclusion criteria E01-E04). Next we will look for the papers whose focus is not put on security in ubiquitous computing based on the information provided in the titles and abstracts (**P3**, exclusion criterion E06). Moreover, opinion and discussion papers will also be removed from the pool (exclusion criterion E07). The filtering procedure will continue by checking the journal and conference rankings (**P4**), as described in section 5.1. Once the papers have been removed based on the rankings, our next step (**P5**) will be to combine the remaining ones with those found manually while scanning through the selected conference proceedings. Since we expect double entries to occur as a result of the phase P5, we will remove them before continuing with the filtering procedure (**P6**). The next phase (**P7**) is to obtain the full version of each paper. If it is not available in a corresponding database, we will check the authors' personal websites and, if necessary, contact the authors. If we still cannot obtain the full version of a paper, we will exclude it from our review (exclusion criterion E08). The following two phases will be conducted in parallel - quality assessment and screening of the content of the papers (**P8a** and **P8b**).

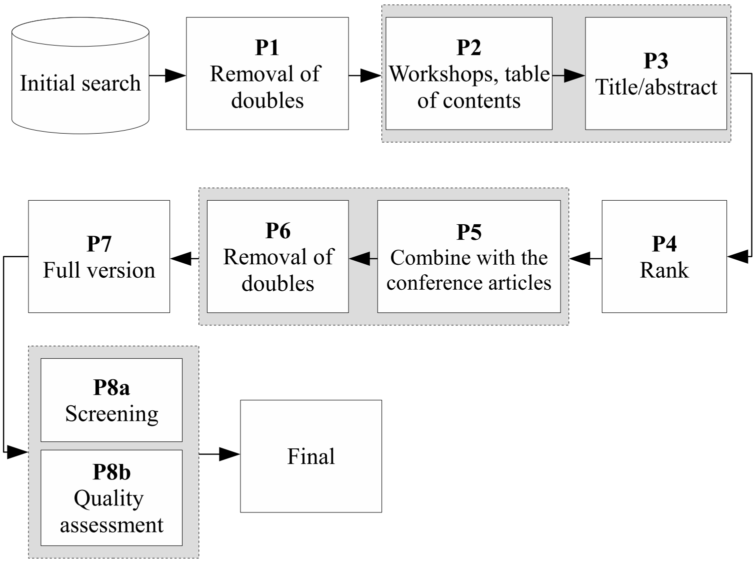


Figure 3: Filtering of papers.

If a paper is given a low quality assessment score, we will exclude it from our review, as described in Section 5.4 (exclusion criterion E10). We expect to identify the papers that are out of the scope of the review while screening through their full version and exclude them from our review, as well. After the filtering procedure has been completed, we expect to have a pool of relevant papers that will go through the data extraction procedure.

Report on the details of the selection procedure is given in Appendix B.

5.3 Tools to be used during the selection procedure

During the selection procedure, we will use a Zotero reference manager to automatically collect the general information about the papers, such as authors, publication venue, publication year and the corresponding source (titles of journals and conferences). In order to be able to track in which database each paper was found, we will organize the information into folders, as shown in Figure 4.

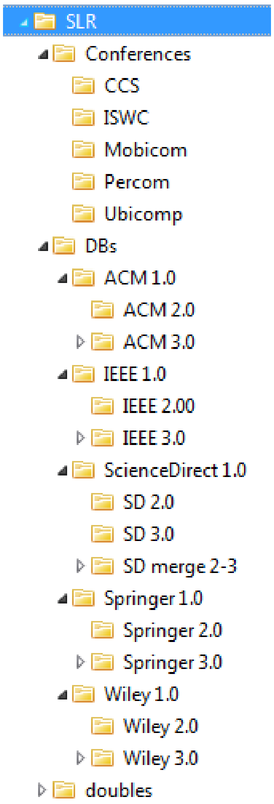
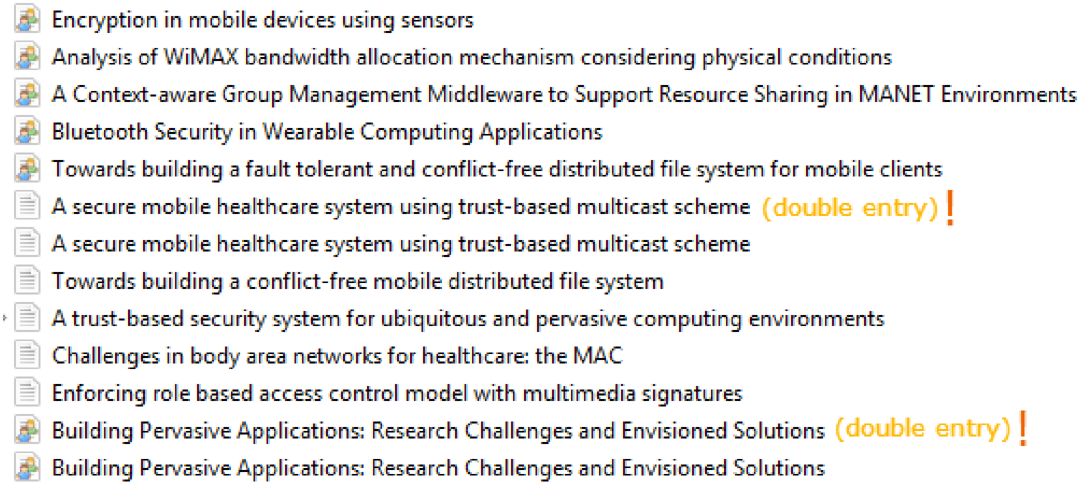


Figure 4: Zotero tree-like organization

Initially, the manager will consist of a root folder named "SLR" and two parent folders - one to store the information about the conference papers found manually (named "Conferences"), and the other to store the information about the papers found by an automatic search (named "DBs"). In each parent folder, the information will be further organized into subfolders that represent the specific source where the paper has been found. Therefore, the folder "Conferences" will include in total five subfolders (named "CCS", "ISWC", "Mobicom", "Percom" and "Ubicom"). Information collected in these subfolders will not be checked for the double entries, as they are mutually exclusive. However, the same is not valid for the information stored in the subfolders of the folder "DBs". This is the case for two reasons. First, some conference papers are indexed in both the ACM and the IEEEXplore database. Second, since our search procedure is based on three different search strings for each database, we expect to find a number of the same papers in each run. For this reason, after the automatic search has been completed, we will check for any double entries by using a separate folder called "doubles". This folder will initially hold all the entries found during the automatic search. We will go through the list of papers and gradually remove any double entries. The resulting list should hold only unique entries. This list will be used for the filtering procedure (as described in Section 5.2). A screenshot of the list of the papers prior to the removal of the double entries is presented in Figure 5.

It is important to note that both reviewers will participate in the selection process in order to minimize personal bias, as recommended in [GBBGG$^+$13] [KB13] [RHTi13].

In addition to Zotero, we will use a Google Spreadsheet (see Table 10) shared between the



Encryption in mobile devices using sensors
Analysis of WiMAX bandwidth allocation mechanism considering physical conditions
A Context-aware Group Management Middleware to Support Resource Sharing in MANET Environments
Bluetooth Security in Wearable Computing Applications
Towards building a fault tolerant and conflict-free distributed file system for mobile clients
A secure mobile healthcare system using trust-based multicast scheme (double entry) !
A secure mobile healthcare system using trust-based multicast scheme
Towards building a conflict-free mobile distributed file system
A trust-based security system for ubiquitous and pervasive computing environments
Challenges in body area networks for healthcare: the MAC
Enforcing role based access control model with multimedia signatures
Building Pervasive Applications: Research Challenges and Envisioned Solutions (double entry) !
Building Pervasive Applications: Research Challenges and Envisioned Solutions

Figure 5: Double entries

both reviewers to record search and selection details, such as a number of papers found for each search string, number of double entries identified for each database, number of workshops, number of papers left after the inclusion based the titles and abstracts, number of papers after checking the journal and conference rankings.

String Nr.	Database	Doubles	Workshops, table of contents, summaries	Title, abstract	Rank
	ACM				
S1					
S2					
S3					
	Springer				
S1					
S2					
S3					
	Science Direct				
S1					
S2					
S3					
	IEEE				
S1					
S2					
S3					
	Wiley				
S1					
S2					
S3					

Table 10: Search form

Once the initial pool of relevant papers has been made, we will obtain their full versions (in a PDF format) and put them in a shared Google Drive folder. These papers will be used in the collaborative quality assessment procedure.

5.4 Quality Assessment

After the relevant papers have been identified, we will prepare them for the quality assessment procedure by renaming each in the following way. Each paper will be given a prefix S[000]_ (*S* stands for *paper*) and a three-digit number starting from 000. For example, a paper with a title "A compensation scheme of fingerprint distortion using combined radial basis function model for ubiquitous services" is alphabetically first in our initial pool of relevant papers. After the renaming procedure, the PDF document will have the following title: "S001_A compensation scheme of fingerprint distortion using combined radial basis function model for ubiquitous services". The renaming will be done automatically by using a script written in Perl (see Listing 1).

Listing 1: Perl script

```
#!/usr/bin/perl -w
use File::Find;
use File::Basename;
use File::Spec;
use strict;

my $i='001';
find ({'wanted' => \&renamefile }, '(source)');

sub renamefile {
    my $file = $_;
     return unless (-f $file);
    my $dirname = dirname($file);
    my $file_name = basename($file);
    my $new_file_name = $file_name;
     $new_file_name = 'S'.$i.'_'.$file_name;
     rename($file, File::Spec->catfile($dirname, $new_file_name))
                or die $!;
          $i++;
}
```

Based on the suggestions by [ATF09b] [DD08] [GBBGG+13] [KB13] [SJV+12], we will use a quality assessment form that consists of 7 questions represented in a three-point scale with *Yes* (1), *No* (0) and *To some extent* (0.5) as the possible answers.

QA1: Is the paper based on research?

1.1 Yes, it is based on research (1).

1.2 To some extent (0.5).

1.3 No, it is a lessons learned based on expert opinion (0).

QA2: Is there a clear statement of the aim?

2.1 Yes, the aim is specific and mentioned explicitly (1).

2.2 To some extent (0.5).

2.3 No, there is no mention of the aim, or the aim is too general (0).

QA3: Is there an adequate description of the context in which the research was carried out?

3.1 Yes, the paper reports on the application domain for which the security mechanism is designed (1).

3.2 To some extent (0.5).

3.3 No, the application domain is unclear (0).

QA4: Did the paper make a review of previous research of the topic?

4.1 Yes, the paper provided a thorough review of the related work (1).

4.2 To some extent (0.5).

4.3 No, the paper did not provide a review of the related work (0).

QA5: Is the methodology described adequately?

5.1 Yes, the process of creating the research artifacts is clear and provides sufficient information on data collection and algorithms used (1).

5.2 The paper provides a description of the research process, but lacks in detail (0.5).

5.3 No, the paper does not report on the creation of research artifacts (0).

QA6: Is there a clear statement of the findings?

6.1 Yes, the paper provides an adequate description of the findings, as well as the corresponding evaluation (1).

6.2 The paper reports on the findings, but lacks in evaluation (0.5).

6.3 No, the paper does not clearly state its findings (0).

QA7: Did the paper discuss future work?

7.1 Yes, the paper discusses future work (1).

7.2 The paper briefly mentions future work (0.5).

7.3 No, the paper does not discuss future work (0).

The form is presented in Table 12.

ID	Question	Score
QA1	Is the paper based on research?	
QA2	Is there a clear statement of the aim?	
QA3	Is there an adequate description of the context in which the research was carried out?	
QA4	Did the paper make a review of previous research of the topic?	
QA5	Is the methodology described adequately?	
QA6	Is there a clear statement of the findings?	
QA7	Did the paper discuss future work?	

Table 11: Quality assessment scores.

The maximum value of the assessment for a paper is 7, indicating high quality, whereas 0 value means poor quality. The range is further divided into three categories:

1. High quality (*final score*≥6),
2. Medium quality (4≤*final score*≤5.5),
3. Poor quality (*final score*≤3.5).

For each paper we will calculate the final quality assessment scores. This information will be used to identify the number of papers placed in each quality assessment category (poor, medium and high quality). Additionally, we will find the final scores for each question to identify the overall weaknesses of the papers used in our review. For example, as reported in a systematic

Paper ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Final score per paper
S001								
S002								
S003								
...								
Final score per question								

Table 12: Quality assessment form

review paper [SLB14], future work scored low in the quality assessment procedure indicating that authors of the reviewed papers did not properly discuss future plans. The cumulative scores found for each quality assessment question will be presented in a form presented in Table 12.

Following the example of the other systematic reviews [MHGA13] [RHTi13], we will exclude the papers placed in the poor quality category and include those that have a substantial quality assessment score into the data extraction process.

In order to ensure that the selected papers will make a valuable contribution to the findings of the review, we considered the concepts of reporting, rigor, credibility and relevance (proposed in [DD08]) while designing our quality assessment questions.

- **Reporting:** questions QA1, QA2 and QA3 examine the quality of reporting on the rationale, aim and context of the research.
- **Rigor:** question QA5 is used to examine the rigor and validity of the research methodology.
- **Credibility:** question QA6 is designed to assess the validity and meaningfulness of a paper.
- **Relevance:** questions QA4 and QA7 are introduced to assess the relevance of a paper.

Both reviewers will be involved in the quality assessment procedure. The pool of the potentially relevant papers will be divided into two parts, each assessed by one author and checked by the other.

5.4.1 Report on the pilot quality assessment

Based on the suggestion by [KB13], we performed a pilot quality assessment with a random sample of 10 papers to ensure that all researchers understand how to apply the quality assessment checklist. Each author has individually assessed the papers. After comparing the quality scores, a Cohen's Kappa coefficient was calculated (23% fair). In order to reduce the differences in the individual understanding of the procedure, additional refinements to the quality assessment form were made. In particular, more explanation was given to the checklist of the *research methodology* and the *context of the research.*

5.5 Data extraction

In order to manage the data extraction procedure, we designed an online form using Google Forms, which will help us during the collaborative data extraction process and, later on, while aggregating and synthesizing the information for further analysis. The data extracted from the papers will be recorded in a Google Spreadsheet, which is automatically generated once an entry has been submitted to the form. As the data extraction procedure will be conducted in parallel with the quality assessment, reviewer A will check the data extracted by the reviewer B, and vice versa. We will discuss any potential disagreements and, if an agreement cannot be reached, we will ask for a third opinion.

5.5.1 Details of the extraction form

It is possible to choose one of the nine question types:

1. Text - includes a small one-line text box.

2. Paragraph text - includes a multi-line text box, which is well suited for writing a longer paragraph of text

3. Multiple choice - allows two types of answers: 1) predefined (as designed by the form owners), 2) custom answer (any additional answer a reviewer might come up with during the data extraction process). Though the name implies that this question is a multiple choice type of a question, we have found out that in practice a reviewer can choose only one option from the list. Therefore, this option stands for a single choice question type. While testing the questions types, we found out that it is not possible to allow a reviewer to enter an additional value to the ones already given in the list of options. The advanced settings additionally allow to shuffle option order. To avoid confusion, we decided not to use this option for any question in our data extraction form.

4. Checkbox - as in the multiple choice question type, it allows two types of answers: 1) predefined answer, 2) custom answer. In our case, we provided a list of security goals, which included confidentiality, integrity, authentication, availability, access control, non-repudiation, authenticity of data, privacy, accountability, and audit. The list of these security goals can be found in [SRM13]. In case an additional security goal is identified in the papers, a reviewer is given an option to enter it by using a custom answer textbox. In this way we wanted to ensure that the important information for our SLR get recorded without restricting the reviewers by the predefined options.

5. Choose from list - provides a drop-down list of options. For this type of a question it is impossible to have a custom answer textbox. We decided not to use this type of a question.

6. Scale - includes a scale of values on which a reviewer can place a response. We choose not to use this type of a question.

7. Grid - includes a grid of rows and columns where a reviewer has to click a single cell to place a response. This type is often used for Likert scale questions. We did not use this type of a question.

8. Date - includes a calendar on which a reviewer has to click to enter a date in the format *dd.mm.yyyy*, where *d* stands for day, *m* for month and *y* for year. In addition, it is also possible to enter time in the format *hh:mm*, where *h* stands for hours and *m* for minutes. Although this question type might have been useful to check the time and date an entry has been submitted to our data extraction form by each reviewer, we decided not to use it because the timestamps were automatically recorded for each form entry in the first column in a Google Spreadsheet.

9. Time

It is possible to define every question as a "required question", meaning that a reviewer will be forced to answer the corresponding question before being able to proceed to the next question. We used this option only for one textbox, namely *Paper ID.*

Once a reviewer is done with extracting the data from the papers, he/she is prompted to press the submit button. The data is then automatically transferred to the Google Spreadsheet in a sheet called "Form Responses", where the number of columns corresponds to the number of questions in a form and number of rows correspond to the number of entries a reviewer has submitted. In our case, the number of rows will respond to the number of papers that were identified as relevant for our SLR.

5.5.2 Description of the data extraction form

The form consists of four parts, as presented in Table 13.

Part	RQ	Data extracted	Question type
1[4]	**RQ1**	Name of the reviewer	Textbox
		Paper ID (***required**)	Textbox
		Title of the paper	Textbox
		Authors	Textbox
		Country/list of countries where the research has been carried out	Textbox
		Publication venue	Textbox
		Publication details for journal	Textbox
		Conference acronym	Textbox
		Page numbers	Textbox
		Date of publication	Textbox
		Cited by (number of citations based on the Google Scholar citation count)	Textbox
2	**RQ2**	Aim of the paper	Textbox
	RQ2	List of security goals addressed in the paper[5]	Checkbox with *confidentiality*, *integrity*, *authentication*, *availability*, *access control*, *non-repudiation*, *authenticity of data*, *privacy*, *accountability* and *audit* as possible choices.
	RQ2.1	Motivation for the research	Textbox
3	**RQ2.2**	Solutions	Textbox
	RQ2.3	Are the necessary algorithms publicly available?	Single choice with *yes* and *no* as possible answers.
	RQ2.4	Has the validation been performed?	Single choice with *yes* and *no* as possible answers.
	RQ2.4	If yes, which validation methods have been used?[6]	Checkbox with *experiment*, *case paper*, *data mining*, *opinion survey*, *lessons learned*, *example*, *formal verification* and *other* as possible answers.
4	**RQ2.5**	Did the authors identify limitations to their solution?	Single choice with *yes* and *no* as possible answers.
		List of limitations	Textbox
		Have any directions for future work been proposed?	Single choice with *yes* and *no* as possible answers.
		Which future work has been proposed?	Textbox

Table 13: Description of the data extraction form

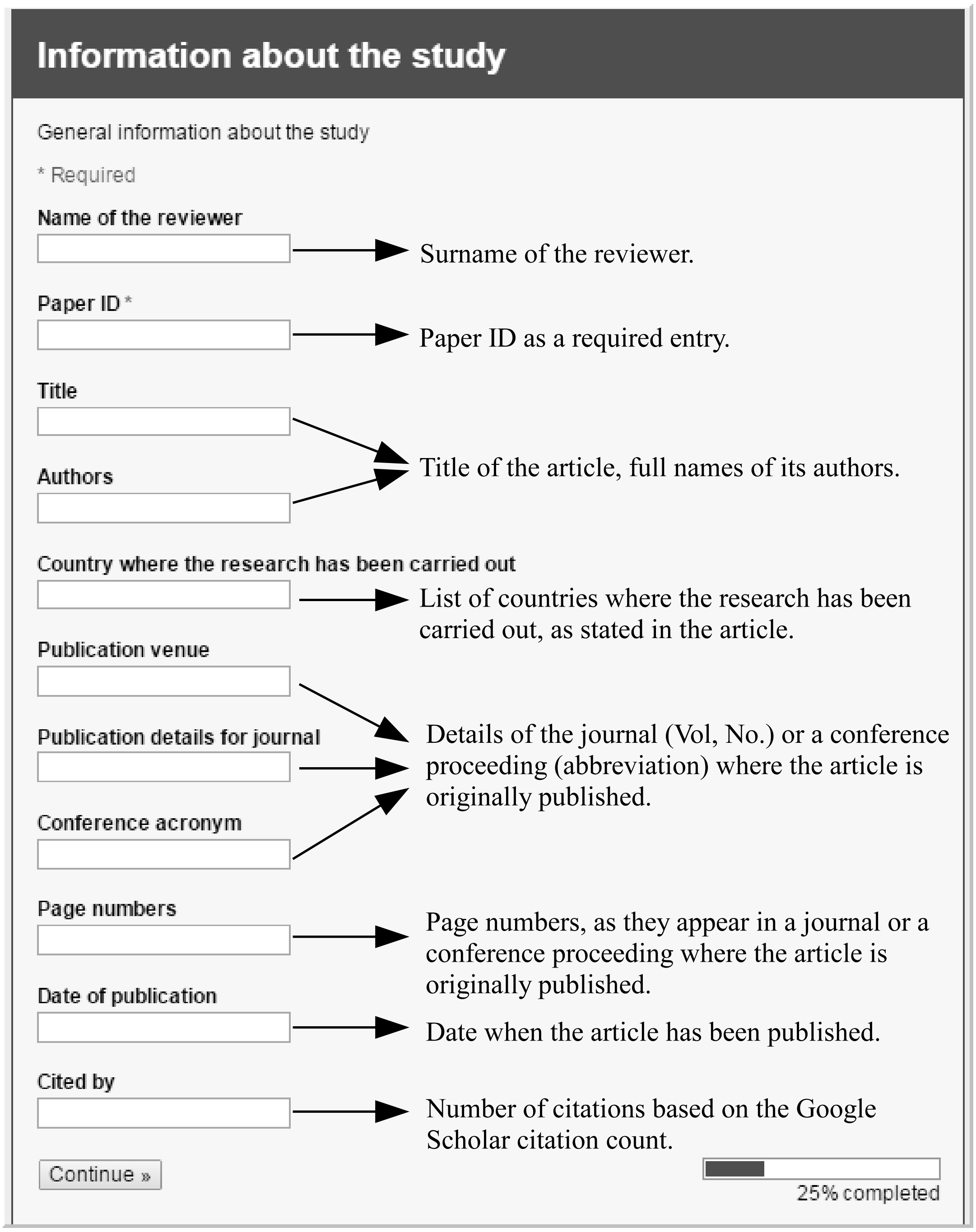
[4] We will not manually fill in the date when the information is extracted, as the timestamp is automatically assigned to each entry once the answers are submitted in the Google Forms.

[5] Due to the specific characteristics of the technologies, devices and networks that we will come across in our review, we expect to identify additional security goals and put them into the *Other* category.

[6] Validation methods are defined in Table 14

5.5.3 Description of the pages included in the form

The first page of the data extraction form (see Figure 6) consists of 11 data-entry fields, namely name of the reviewer, paper ID (required), title of the paper, author's name, country where the research has been carried out (country where the author worked at the moment when the paper written), publication venue, publication details for a journal (volume, number), conference acronym, page numbers (as they appear in the original publication venue), date of publication, number of cites (based on Google Scholar citation count).



Information about the study

General information about the study

* Required

Name of the reviewer

Surname of the reviewer.

Paper ID *

Paper ID as a required entry.

Title

Authors

Title of the article, full names of its authors.

Country where the research has been carried out

List of countries where the research has been carried out, as stated in the article.

Publication venue

Publication details for journal

Conference acronym

Details of the journal (Vol, No.) or a conference proceeding (abbreviation) where the article is originally published.

Page numbers

Page numbers, as they appear in a journal or a conference proceeding where the article is originally published.

Date of publication

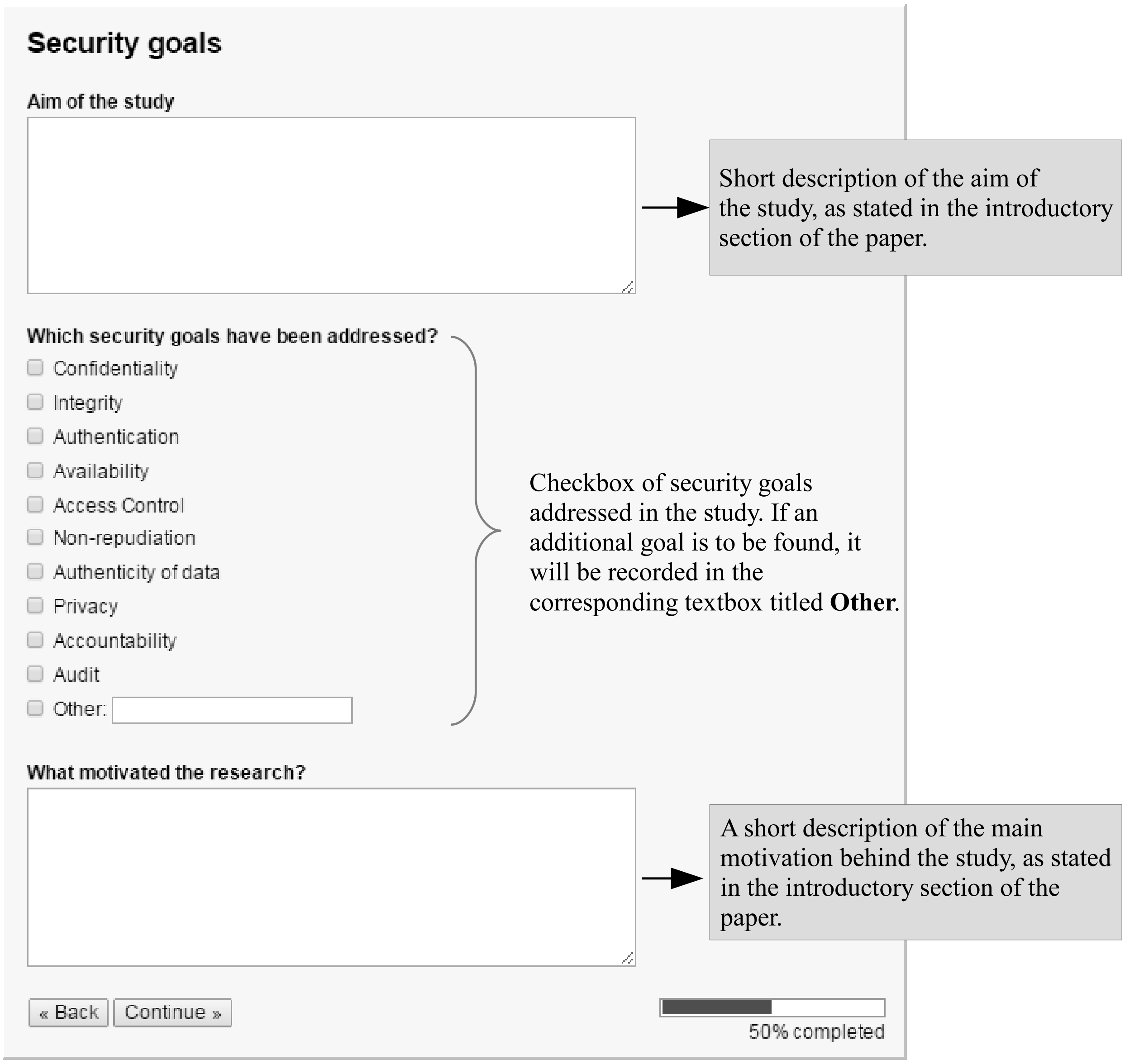
Date when the article has been published.

Cited by

Number of citations based on the Google Scholar citation count.

Figure 6: Extraction form, page 1.

The second page of the data extraction form (see Figure 7) consists of three questions, out of which two are multi-line textboxes (one for the aim of the study and the other one for the motivation behind the researcg) and one checkbox with the list of security goals, as proposed in [SRM13]. For the checkbox, the predefined possible answers are: confidentiality, integrity, authentication, availability, access control, non-repudiation, authenticity of data, privacy, accountability, and audit. The final check-box option is a blank single-line textbox in which a reviewer can write an additional security goal identified in the papers.



Security goals

Aim of the study

Which security goals have been addressed?

□ Confidentiality
□ Integrity
□ Authentication
□ Availability
□ Access Control
□ Non-repudiation
□ Authenticity of data
□ Privacy
□ Accountability
□ Audit
□ Other:

What motivated the research?

50% completed

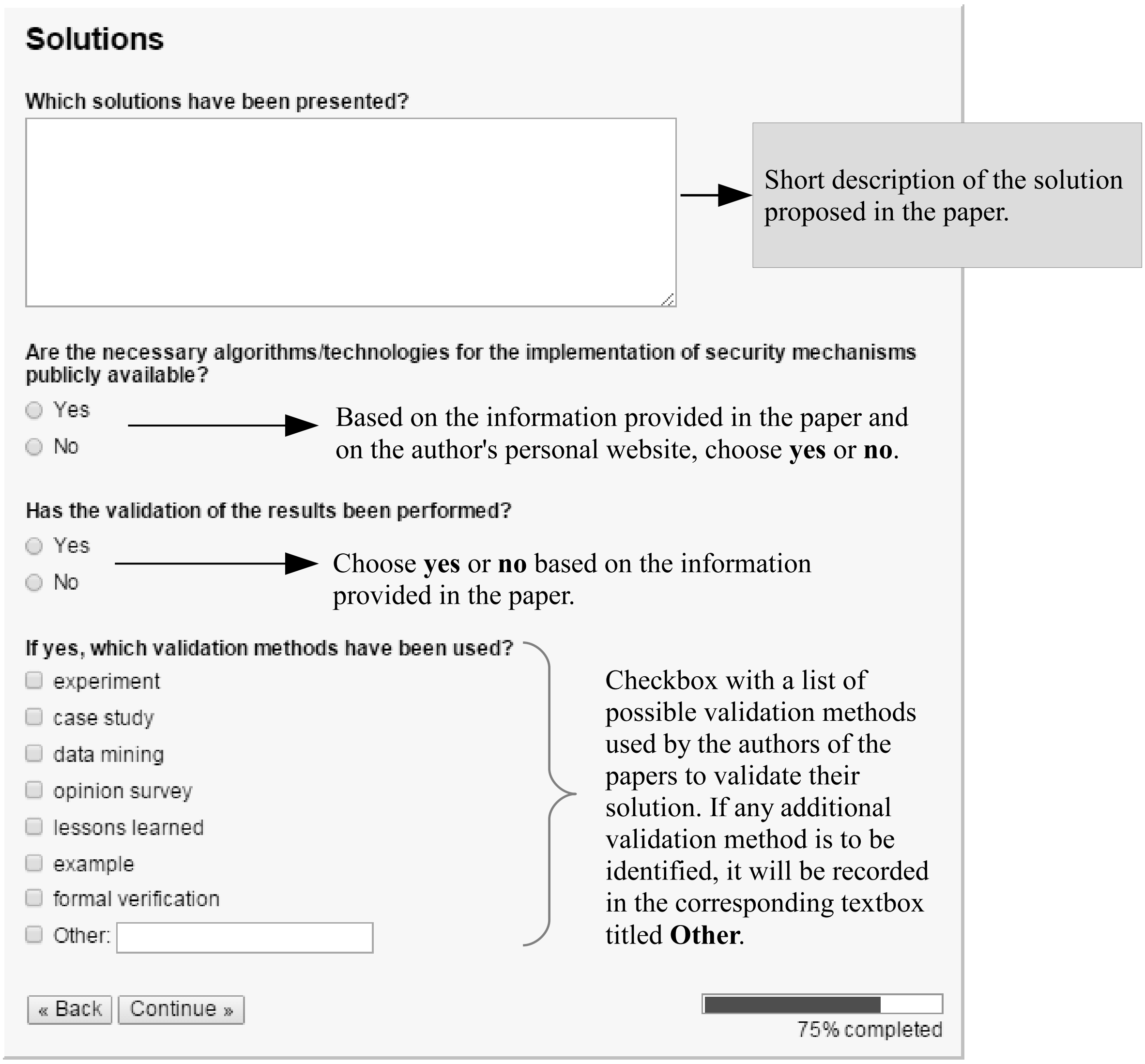
Short description of the aim of the study, as stated in the introductory section of the paper.

Checkbox of security goals addressed in the study. If an additional goal is to be found, it will be recorded in the corresponding textbox titled **Other**.

A short description of the main motivation behind the study, as stated in the introductory section of the paper.

Figure 7: Extraction form, page 2.

The third page of the data extraction form (see Figure 8) consists of four questions - one multi-line textbox, two single-choice questions, and one checkbox. The reviewer is expected to provide a short description of the solution proposed and described in the paper in the multi-line textbox. We will also check whether the algorithms and technologies needed for the implementation of security mechanisms are publicly available by checking the information provided in the paper, as well as authors' personal websites. If the algorithms and technologies are available, we will mark it as *Yes* in our form. The second single-choice question refers to the validation of results. We will examine the papers to identify whether the authors of the paper have validated their solution. If they reported on the validation, we will mark it as *Yes* in our form. The last question on the third page of the form should be answered only if the previous question was answered with *Yes*. Although Google Forms provides some navigation control (it is possible to define the page to be opened based on the respondent's answer), it did not react to a reviewer's response the way we wanted to. For example, by choosing an option *No* for the question "Has the validation of the results been performed?", we could not forbid a reviewer to choose validation methods presented in the checkbox on the bottom of the page. Therefore, we agreed to manually skip the checkbox question in case the previous question was answered with *No*.



Solutions

Which solutions have been presented?

Short description of the solution proposed in the paper.

Are the necessary algorithms/technologies for the implementation of security mechanisms publicly available?

○ Yes

○ No

Based on the information provided in the paper and on the author's personal website, choose **yes** or **no**.

Has the validation of the results been performed?

○ Yes

○ No

Choose **yes** or **no** based on the information provided in the paper.

If yes, which validation methods have been used?

□ experiment

□ case study

□ data mining

□ opinion survey

□ lessons learned

□ example

□ formal verification

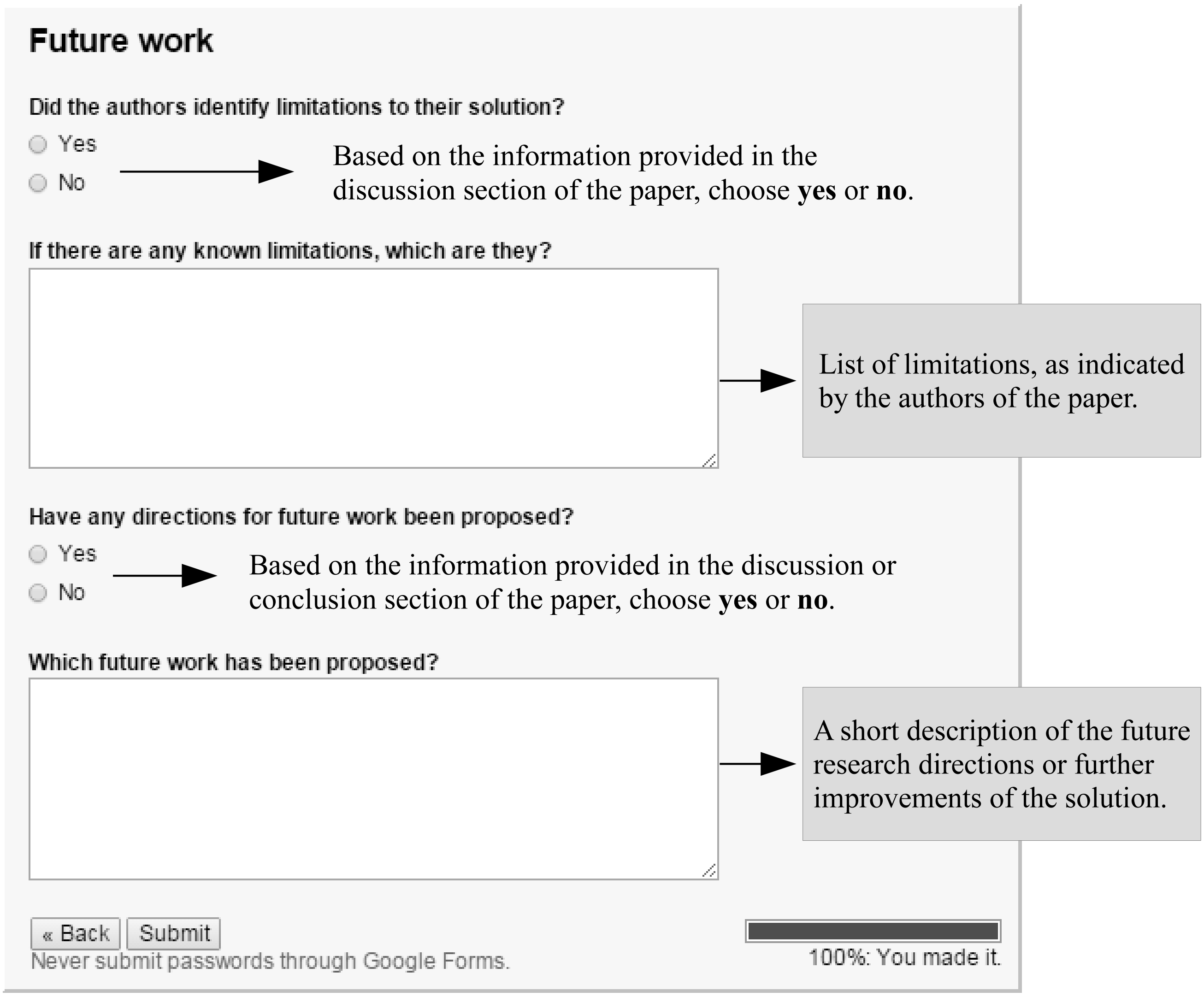
□ Other:

Checkbox with a list of possible validation methods used by the authors of the papers to validate their solution. If any additional validation method is to be identified, it will be recorded in the corresponding textbox titled **Other**.

Figure 8: Extraction form, page 3.

The final page of the data extraction form (see Figure 9) consists of four questions. The first one is a single-choice question, which refers to the limitations of the solution presented in the paper, with *Yes* and *No* as two possible answers. In order to provide an answer to this question, we will examine results, discussion, and conclusion sections of the papers. The second question is a multi-line textbox and refers to the description of the limitations, as stated by the authors of the paper. Again, we faced the same problem with restricting the reviewer to answer to the question once the previous question was answered with *No*. The third question is a single-choice question, which refers to the future work, with *Yes* and *No* as two possible answers. The final question in our data extraction form is a multi-line textbox, in which a short description of future work, as stated by the authors of the paper in the discussion and conclusion sections of the paper, is expected.

Once the data has been entered by a reviewer, the answers can be submitted by clicking on a button *Submit*, found at the very bottom of the form. As we linked the Google Forms with a Google Spreadsheet, the answers provided are automatically put into the corresponding cells in a Google Spreadsheet's sheet titled "Form Responses". An additional column, timestamp (date and time the answers have been submitted) is automatically created in the first column in the Spreadsheet.



Future work

Did the authors identify limitations to their solution?

○ Yes
○ No

Based on the information provided in the discussion section of the paper, choose **yes** or **no**.

If there are any known limitations, which are they?

List of limitations, as indicated by the authors of the paper.

Have any directions for future work been proposed?

○ Yes
○ No

Based on the information provided in the discussion or conclusion section of the paper, choose **yes** or **no**.

Which future work has been proposed?

A short description of the future research directions or further improvements of the solution.

Never submit passwords through Google Forms.

100%: You made it.

Figure 9: Extraction form, page 4.

The validation methods are defined as follows (see Table 14):

Method	**Description**	**Example**
Experiment	Manipulation of one or more independent variables. In our review, a simulation will be regarded as an experiment.	A simulation is conducted in [83] where the authors provide the objective of the simulation, a list of parameters, report on the simulation process and discuss the results.
Case paper	One case or a small number of cases are studied in detail with a holistic focus, i.e. it aims to understand the wholeness of the case.	In [36] the authors consider the case of a user moving through different localities and changes in the context condition while using a ubiquitous service.
Opinion survey	Inquiry designed to collect the opinion of a sample population.	A report on the opinion survey is given in [100]. The survey was conducted on a number of users to gain insight into whether a virtual password scheme is applicable in a certain scenario.
Lessons learned	After a solution had been implemented, authors report on the experience in working with the solution.	paper [82] reports on a home respiratory therapy system.
Example	Authors provide a description of a scenario, actors and procedures in order to illustrate a certain process or behavior.	Examples are provided in [164] in order to show how an algorithm assigns privileges to categories in an RBAC model.
Formal verification	Proving the validity of algorithms by using formal methods and mathematics. Formal proof and first-order logic were put into this category.	A protocol is formally verified using BAN logic in [221].
Other	Any other validation methods that could not be categorized into the above-mentioned categories, such as a theoretical comparison with existing solutions, usability test or data mining.	paper [107] provides a comparison of a a group device pairing protocol with existing schemes.

Table 14: Validation methods

6 Data synthesis

Before we start synthesizing and reporting on the findings, we will check if the data extraction procedure resulted in any missing information. If required, we will re-check the paper whose information might be missing. If the answer is not provided, we will mark the field in the data extraction form as “information unknown” or “general”, depending on whether the information is entirely missing or the authors of a particular paper provided general information. We expect to come across papers that provide, for example, a general list of attacks while reporting on the motivation. Therefore, we will write “general” in the respective textbox.

During the data synthesis procedure, we will use separate tables to group the information extracted in the Google Spreadsheet. This step will be taken to help summarize the information needed to answer to our research questions.

6.1 Synthesis of data for the RQ1

The first form used for the data synthesis will contain the information about the researchers who published papers on security in ubiquitous computing (see Table 15). We will provide a list of authors identified in our systematic literature review and count the number of papers published by each author. This information will identify the most active researchers in the area.

Paper ID	Author
S001	
S002	
...	

Table 15: Demographic data: active researchers

The second table (see Table 16) will present the demographic information. More precisely, we will look for the list of countries whose authors published the papers identified in our review. This information will give us an insight into where the research on security in ubiquitous computing is being carried out.

Paper ID	Country
S001	
S002	
...	

Table 16: Demographic data: country which contributed to the paper

In Table 17, we will present the number of papers published per year.

Year	Number
2003	
2004	
2005	
2006	
2007	
2008	
2009	
2010	
2011	
2012	
2013	

Table 17: Trends: Papers per year

The fourth table will present the most cited papers identified in our review (see Table 18).

Paper ID	Number of citations
S001	
S002	
...	

Table 18: Trends: citation count

Journals and conferences with the most published papers on security in ubiquitous computing will be identified by using the information given in Tables 19 and 20, respectively. Once identified, we will fill in the names of the journals in place of “JournalX” and conference abbreviations in place of “ConferenceX”.

Journal name	No. of papers
JournalX	
JournalX	
...	

Table 19: Number of papers found in each journal

Conference abbreviation	No. of papers
ConferenceX	
ConferenceX	
...	

Table 20: Number of papers found in each conference proceeding

6.2 Synthesis of data for the RQ2

The second research question "Which security goals have been addressed in terms of ubiquitous computing?" was examined in more depth by including six additional research questions, as reported in Section 3. We designed a data synthesis form for each additional research question.

6.2.1 Synthesis for the RQ 2.1: What is the motivation for the papers?

A list of threats, attacks and vulnerabilities that have motivated the papers will be recorded in Table 21. Instead of marking the cells with the uninformative "Yes" and "No", the table will contain a short description of each motivating factor found in a specific paper. For example, paper S004 (paper [151] in our list of references) reports on two vulnerabilities and one threat, as shown in Table 21. Since there were no attacks identified in the paper S004, the corresponding table cell is left blank.

	Motivation for the paper		
Paper ID	Vulnerability	Threat	Attack
S001			
S002			
S003			
S004	device's resource constraints (limited memory and processing power), insecure and untrustworthy nodes in a P2P network	presence of malicious and unreliable peers may deteriorate the accuracy and system performance	
...			

Table 21: Motivation for the paper

This information will be used to summarize and categorize the motivating factors found in the papers and to count the number of occurrences for each attack. The list of motivating factors with their corresponding source (paper) is given in the Appendix C.

6.2.2 Synthesis for the RQ 2.2: Which solutions have been presented?

Table 22 will hold the information on the solutions proposed in the papers. If additional information is needed during reporting, we will refer to the corresponding paper to find any further explanations or information missing from our data synthesis table. Additionally to the table, we are planning to provide a narrative description of the findings.

Paper ID	Short description of the solution
S001	
S002	
...	

Table 22: Solutions.

6.2.3 Synthesis for the RQ 2.3: Are the algorithms and technologies publicly available?

We are also interested in the availability of the algorithms and technologies used to present a solution (see Table 23). In particular, we will examine the way algorithms and technologies are presented (for the purpose of this review we will call it "presentation types"), such as diagrams and programming code excerpts, and categorize them during our reporting process.

Paper ID	**Availability of algorithms** (Y or N)	Presentation type
S001		
S002		
...		

Table 23: Algorithms.

6.2.4 Synthesis for the RQ 2.4: Which security goals have been addressed in the papers?

Using the information recorded in the spreadsheet, we will count the number of occurrences for each security goal (see Table 24) and present them in a bar chart. We will pay special attention to the list of goals placed in the *Other* category by examining whether there are any additional security goals with a high frequency of appearance. If such are found, we will add an additional row in the Table 24.

The information about the number of security goals identified in the papers will be used in the reporting phase of the review where we will explain and interpret the obtained results.

Security goals	Number
Confidentiality	
Integrity	
Authentication	
Availability	
Access control	
Non-repudiation	
Authenticity	
Privacy	
Accountability	
Audit	
Other	

Table 24: Security goals.

6.2.5 Synthesis for the RQ 2.5: What kind of validation of the results been performed?

To assess the appropriateness of the proposed solutions, we will synthesize the information about the validation mechanisms as reported in the papers. First we will identify the number of papers that did not report on any validation mechanisms used (see Table 25). For the remaining, we will count the number of occurrences of each validation mechanism and record it in the Table 26. This information will be used to identify the mechanisms that researchers tend and prefer to use.

Has the validation been performed?	**Number**
Yes	
No	

Table 25: Performance of the validation mechanisms.

Validation mechanism	**Number**
Experiment	
Case paper	
Opinion survey	
Lessons learned	
Example	
Formal verification	
Other	

Table 26: Validation mechanisms.

6.2.6 Synthesis for the RQ 2.6: Which future work has been proposed?

While summarizing the information about the future work, we will first use the data recorded in the Google spreadsheet to identify the number of papers that did not provide any plans for future work or research directions (see Table 27). The same data will be also available in our quality assessment form (0 points is given to the papers that do not report on the future work).

Future work reported?	**Number**
Yes	
No	

Table 27: Report on the future work.

Table 28 presents a data synthesis form in which we will summarize the short descriptions of future work extracted from the papers. Since we expect to encounter similarities in the reported future plans, we plan to categorize them and show frequencies for each category. For example, information about the performed validation of results given in the Table 25 may indicate that researchers who did not report on any validation mechanisms in they paper, might plan it as their future work. Therefore, "validate" can be regarded as a potential category of the planned future work.

Paper ID	**Short description of the future work**
S001	
S002	
...	

Table 28: Future work.

7 Potential conflict of interest

None known.

8 Review timetable

The SLR will be conducted within the following time-frame:

Task	**Date**	**Task description**
Completion of the protocol	30/12/2013	After the examples of the SLRs found in the literature[a] have been examined, identify and describe all the procedures and their details that are essential to conduct the SLR, such as definition of the research scope, search procedure, filtering of papers, quality assessment, data extraction and data synthesis.
Completion of the protocol review	20/01/2014	Conduct pilot procedures and report on their results. If necessary, refine the protocol.
Completion of search	10/02/2014	Use the defined search strings to automatically search for the papers in the scientific databases and manually in the conference proceedings, as defined in the protocol.
Completion of paper selection	23/03/2014	Perform the quality assessment procedure and filter the initial pool of papers according to the defined inclusion and exclusion criteria.
Completion of data extraction	20/05/2014	Extract the information by using a predefined form, as defined in the protocol.
Completion of data synthesis	30/06/2014	Synthesize the data extracted from the papers by using the predefined forms.
Completion of reporting	31/07/2014	Report on the results obtained from the review.

Table 29: Review timetable

[a] While defining review procedures we followed the examples from the following systematic reviews: [SLB14], [RHTi13], [DBCG14], [ATF09a], [BBH+08], [KB13], [KC07], [GBBGG+13] and [SJV+12].

We repeated our search in January 2015 to obtain results from papers published in 2014.

A Appendix: Results of the search and selection procedures

A.1 Results of the automatic search

We first obtained the papers for the time period 2003-2013.

Search string	**Database**	**Doubles**	**Workshops, table of contents, summaries**	**Title, abstract**	**Rank**
	ACM				
S1	384	638	537	302	24
S2	377				
S3	15				
	Springer				
S1	93	281	265	32	6
S2	246				
S3	31				
	Science Direct				
S1	247	506	498	95	66
S2	312				
S3	10				
	IEEE				
S1	1387	2018	1893	1144	97
S2	980				
S3	34				
	Wiley				
S1	116	213	209	52	6
S2	125				
S3	12				
Sum	4369	3656	3402	1625	199

Table 30: Details of the automatic search and selection.

We repeated the search with the same set of search strings in January 2015 to obtain the papers published in 2014.

Search string	Database	Doubles	Workshops, table of contents, summaries	Title, abstract	Rank
	ACM				
S1	49	74	49	22	13
S2	44				
S3	0				
	Springer				
S1	56	86	83	9	5
S2	34				
S3	1				
	Science Direct				
S1	47	95	95	23	15
S2	59				
S3	3				
	IEEE				
S1	140	200	169	59	16
S2	114				
S3	4				
	Wiley				
S1	30	59	59	14	3
S2	34				
S3	2				
Sum	617	514	455	127	52

Table 31: Details of the automatic search and selection, repeated search in 2015.

A.2 Results of the manual search

Conference name	Abbreviation	Results
ACM International Joint Conference on Pervasive and Ubiquitous Computing	Ubicomp	24
IEEE Pervasive Computing and Communication conference	PerCom	47
ACM Conference on Computer and Communications Security	CCS	34
Annual ACM International Conference on Mobile Computing and Networking	MobiCom	16
International Symposium on Wearable Computers	ISWC	2

Table 32: Details of the manual search.

B Report on the paper selection

Our initial pool (results for the time period 2003-2013) included n=4369 papers. We followed the filtering procedure and its corresponding phases in order to identify those papers that are of good quality and that would provide information relevant for the purposes of our review. In phase P4 we reached a more manageable number of papers (n=199) and combined them with those found during the manual search process (n=320). The double entries were removed, which further reduced the number of papers to n=291. After taking all the steps to obtain the full versions, we had to exclude in total 7 from our review. Therefore, the total number of papers that were considered for the quality assessment and data extraction phase was 284. The filtering procedure continued during the screening of the papers. We read the full versions of the articles while performing quality assessment and data extraction in parallel. Those papers that were not in scope of our research or had a poor quality assessment score were not considered for the data extraction process. As shown in Figure 10, out of 284 papers 70 (24%) were out of the research scope. For 8 (2%) papers a matching journal article or a more recent paper was found. Quality assessment was done for the remaining 206 (74%) papers.

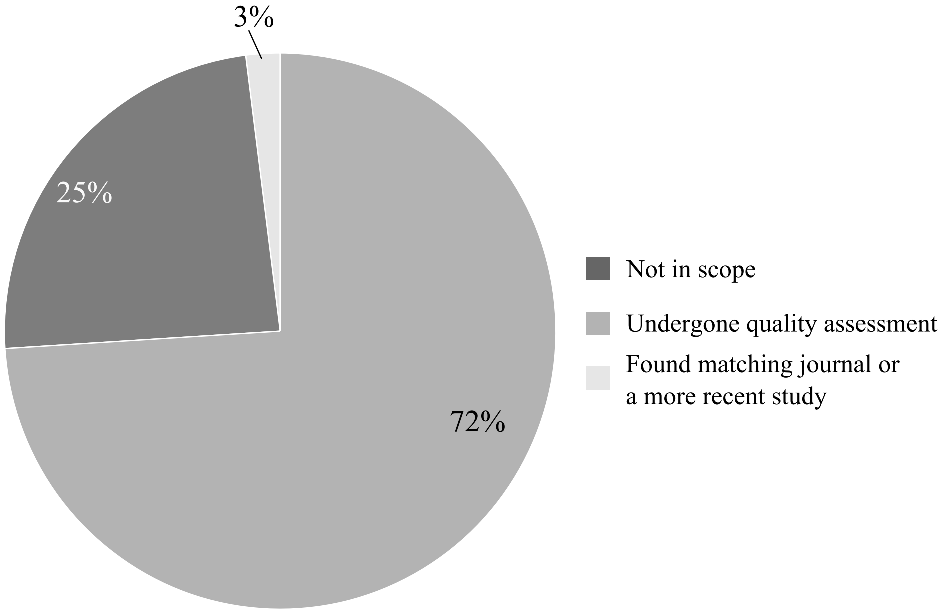


Figure 10: Filtering of papers.

C Motivation

List of vulnerabilities is presented in a Table 33.

Vulnerabilities	Papers	Nr.
1. Network dynamics	[1] [2] [4] [5] [6] [9] [11] [13] [14] [15] [20] [21] [22] [25] [32] [33] [35] [37] [38] [40] [43] [45] [49] [51] [52] [53] [60] [67] [70] [74] [75] [83] [88] [89] [96] [108] [112] [116] [122] [124] [127][132] [136] [139] [142] [143] [144] [148] [151] [156] [159] [161] [167] [165] [172] [176] [179] [182] [188] [191] [192] [193] [198] [195] [206] [210] [213] [214] [212] [215] [219]	**70**
2. Large scale networks	[5] [6] [8] [11] [13] [15] [20] [21] [27] [32] [33] [35] [54] [59] [60] [63] [74] [76] [81] [88] [89] [99] [103] [107] [112] [116] [117] [118] [122] [124] [123] [131] [139] [142] [143] [144] [147] [148] [151] [156] [159] [161] [167] [175] [177] [180] [184] [191] [192] [199] [213] [214] [216] [219] [222]	**55**
3. Resource constraints		**53**
3.1. RFID resource constraints	[24] [29] [64] [68] [82] [110] [111] [128] [158] [208]	10
3.2. WSN resource constraints	[23] [32] [34] [46] [72] [81] [89] [92] [118] [136] [107] [112] [113] [153] [154] [165] [192] [183] [191] [211] [212]	21
3.3. Mobile handheld devices' constraints	[2] [6] [5] [11] [39] [45] [67] [97] [108] [119] [121] [130] [147] [157] [151] [164] [177] [179] [181] [193] [198] [213]	22
4. Authentication-related challenges	[9] [17] [18] [19] [26] [31] [33] [35] [38] [39] [43] [44] [46] [48] [50] [94] [100] [102] [103] [109] [114] [119] [126] [137] [154] [155] [158] [160] [162] [163] [165] [170] [177] [184] [194] [196] [200] [209] [213] [221] [220]	**41**
5. Wireless link	[2] [24] [29] [30] [32] [55] [58] [59] [60] [71][79] [86] [90] [98] [116] [122] [124] [123] [135] [137] [139] [141] [156] [157] [161] [167] [171] [173] [177] [186] [212] [217] [218] [222]	**34**
6. Other		**19**
6.1. Malicious apps	[45] [69] [120] [134] [197] [201]	6
6.2. Service exploitation and misuse	[36] [115] [155] [189] [223]	5
6.3. Session vulnerabilities	[73] [113] [200]	3
6.4. Bluetooth vulnerabilities	[79] [140]	2
6.5. GPS receiver vulnerability	[138]	1
6.6. Mobile push notification vulnerability	[42]	1
6.7. RFID protocol vulnerability	[111]	1

Table 33: List of vulnerabilities.

List of threats is presented in a Table 34.

Table 34: Threats

Threat	**Papers**	**Nr.**
1. Privacy		**127**
1.1. Tracking a user	[3] [12] [16] [22] [24] [41] [29] [47] [51] [53] [54] [59] [62] [63] [64] [66] [68] [76] [84] [86] [89] [93] [117] [119] [120] [125] [128] [138] [143] [149] [155] [158] [168] [169] [171] [176] [178] [179] [181] [182] [190] [208] [200] [203] [204] [222] [221] [219]	52
1.2. Leaking private information	[6] [25] [33] [36] [50] [59] [63] [64] [70] [68] [77] [81] [89] [93] [102] [112] [113] [120] [133] [134] [143] [164] [171] [172] [176] [190] [192] [196] [200] [202] [213] [212] [217] [215] [221] [220] [223] [219]	38
1.3. Loss of a mobile device	[17] [31] [39] [88] [102] [119] [137] [154] [162] [160] [170] [145] [212]	13
1.4. Unlocked devices	[10] [17] [137] [154] [160] [162] [163] [177]	8
1.5. Identity exposure	[16] [17] [71] [93] [112] [117] [155] [222]	8
1.6. Recording	[58] [70] [182] [222]	4
1.7. Malicious apps	[69] [120] [134] [197]	4
2. Unauthorized access to data	[11] [14] [25] [38] [72] [71] [68] [81] [98] [107] [116] [140] [154][160] [176] [194] [197] [200] [201] [145] [211] [212] [213]	**23**
3. Communication interference	[13] [26] [29] [60] [75] [122] [135] [157] [165] [191]	**10**
4. Other[7]	[12] [16] [84] [142] [144] [154] [186] [191] [192] [197]	**10**
5. Installation of untrusted apps	[45] [69] [120] [134] [201]	**5**

Table 34: List of threats.

List of attacks is presented in a Table 35.

Table 35: Attacks

Attack	Refs.	Number
1. Denial of Service (DoS)		**99**
1.1. Network jamming		**25**
1.1.1. Network jamming	[24] [81] [84] [116] [135] [138] [142] [199] [153] [176] [190] [192] [211] [212]	14
1.1.2. Flashing cache with bogus references	[212] [213]	2
1.1.3. CPU processing time attack	[216]	1
1.1.4. Buffer overflow	[137] [150]	2
1.1.5. Rushing attack	[191]	1
1.1.7. On-off attack (dynamic behavior) attack	[40] [183] [192] [199]	4
1.2. Interrupting a communication channel		**42**
1.2.1. Packet interception	[64] [81] [88] [124] [180] [208]	6
1.2.2. Black hole (packet drop)	[142] [148]	2
1.2.3. Gray hole	[142] [148]	2
1.2.4. Jellyfish attack	[142]	1
1.2.5. Hello flood	[142] [144] [192]	3

[7] physically harm a patient, battery drain, stalking and harassment, disabling functionalities, destroying assets

Table 35: Attacks

Attack	Refs.	Number
1.2.7. Wormhole attack	[53] [116] [137] [144] [177] [191] [192]	7
1.2.12. SYN flooding attack	[191] [213]	2
1.2.13. Blocker attack	[190]	1
1.2.14. IMSI paging attack	[12]	1
1.2.15. Stolen verifier attack	[209] [196]	2
1.2.16. Fake base station attack	[12]	1
1.2.17. Injection and deletion of messages	[12] [79] [81] [88] [92] [107] [118] [122] [157] [177] [211] [212]	14
1.3. Disruption of the physical properties of a device		**12**
1.3.1. Power draining attack	[79] [121] [154] [191] [211] [212]	6
1.3.2. Physical corruption	[118] [142] [213]	3
1.3.3. Node compromise	[89] [175]	2
1.3.4. Deplete resources in general	[7]	1
1.4. False trust ratings	[5] [20] [37] [40] [60] [95] [116] [151] [199]	**9**
1.5. Other service degradation attacks		**9**
1.5.1. Storage space filling attack	[164]	1
1.5.2. Server timing attack	[119]	1
1.5.3. Denial of authentication (DoA)	[71]	1
1.5.4. Newcomer attack	[5] [199]	2
1.5.5. Denial of proof	[111]	1
1.5.6. Desynchronization attack	[88] [107] [205]	3
1.6. DDoS	[32] [46] [135] [213]	**4**
2. Impersonation or masquerading		**64**
2.1. Spoofing	[33] [38] [41] [84] [90] [102] [112] [122] [138] [142] [148] [165] [173] [176] [192] [205] [208] [209]	18
2.2. Consensual impersonation	[3]	1
2.3. Sybil attack	[8] [30] [37] [51] [60] [76] [97] [107] [133] [176] [192] [199]	12
2.4. Phishing	[31] [90] [100]	3
2.5. Man-in-the-middle	[3] [11] [24] [30] [37] [41] [46] [53] [62] [75] [76] [81] [90] [102] [110] [118] [119] [122] [128] [140] [142] [148] [165] [172] [174] [209] [212]	27
2.6. Relay attack (ghost and leech)	[3] [158]	2
2.7. Denning-Sacco attack	[209]	1
3. Eavesdropping		**53**
3.1. Passive		**14**
3.1.1. Shoulder surfing	[94] [100] [152] [160] [162] [163]	6
3.1.2. Snooping	[4] [12] [63] [119] [170] [171] [177] [211]	8
3.2. Active		**39**
3.2.1. Replay attack	[1] [2] [4] [12] [23] [24] [27] [46] [56] [68] [71] [76] [86] [88] [104] [111] [118] [119] [124] [123] [127] [128] [131] [138] [142] [144] [145] [147] [148] [155] [165] [177] [178] [192] [196] [200] [208] [209] [223]	39
4. Cryptanalytic attacks		**35**
4.1. Password cracking		20
4.1.1. Brute Force	[17] [25] [46] [66] [79] [175] [205]	7
4.1.2. Dictionary attack	[26] [31] [100] [209]	4

Table 35: Attacks

Attack	Refs.	Number
4.1.3. Password cracking	[71] [124] [126] [131] [138] [152] [162] [196] [213]	9
4.2. Side-channel attack		9
4.2.1. Electromagnetic attack	[120] [171]	2
4.2.2. Acoustic cryptanalysis	[120]	1
4.2.3. Side-channel attacks	[121] [154] [152] [177] [211] [212]	6
4.3. Key search attack	[150]	1
4.4. Birthday attack	[34] [128]	2
4.5. Preimage attack	[34]	1
4.6. RSA key generation attack	[16]	1
4.7. AKA protocol linkability attack	[12]	1
5. Other		**30**
5.1. Zero day	[79] [201]	2
5.2. Session hijacking	[142] [145]	2
5.3. Stealing a mobile device	[39] [88] [119] [163] [177]	5
5.4. Attack on a person by modifying sensor readings	[88] [192] [211]	3
5.5. RFID cloning attack	[16]	1
5.6. Smudge attack	[94] [160] [162] [163]	4
5.7. Reconnaissance attack	[186]	1
5.8. IMSI paging attack	[140]	1
5.9. Tampering attack	[37] [142] [144]	3
5.10. Pattern matching attack	[94]	1
5.11. Reverse attack	[74]	1
5.12. Conspiracy attack	[74]	1
5.13. Fabrication of false queries	[133]	1
5.14. Bluetooth-related attacks		3
5.14.1. BlueSnarfer	[140]	1
5.14.2. CarWhisperer	[140]	1
5.14.3. HIDattack	[140]	1
5.15. Physical node capture	[55]	1
6. Geo-location inference attacks		**19**
6.1. Tracking	[22] [41] [48] [64] [66] [86] [111] [120] [149] [158] [176] [178] [204] [205]	14
6.2. Location inference attack	[47] [168]	2
6.3. Distance intersection attack	[53] [57] [135]	3
7. Malware	[38] [48] [69] [79] [80] [81] [90] [102] [104] [121] [120] [126] [140] [145] [162] [181] [197] [212]	**18**
8. Cross-origin attack		**5**
8.1. Cross-site request forgery	[197]	1
8.2. Permission re-delegation	[201]	1
8.3. Permission misuse (confused deputy)	[134] [197] [201]	3

Table 35: List of attacks.

D Solutions

Table 36 summarizes solutions proposed in the papers analyzed.

Table 36: Solutions

Solution	**Papers**	**Nr.**
1. Authentication and access control mechanisms		**86/79**[8]
1A - Authentication mechanisms	[2] [3] [9] [17] [18] [24] [26] [28] [30] [31] [38] [39] [44] [46] [50] [71] [76] [78] [86] [89] [90] [94] [100] [100] [102] [105] [109] [116] [124] [123] [126] [128] [131] [137] [147] [145] [154] [155] [158] [160] [163] [165] [170] [177] [178] [179] [196] [208] [209] [214] [220]	51
1B - Access control mechanisms	[3] [9] [25] [33] [35] [36] [43] [52] [62] [61] [63] [74] [75] [85] [91] [98] [99] [103] [114] [121] [127] [129] [130] [139] [141] [145] [154] [155] [172] [179] [180] [184] [194] [202] [206]	36
Solutions based on identity		
1.1. Identity-based solutions	[2] [3] [9] [17] [18] [26] [28] [30] [31] [39] [38] [44] [46] [50] [71] [76] [78] [86] [89] [90] [94] [100] [105] [109] [121] [124] [123] [126] [128] [131] [137] [147] [145] [154] [155] [158] [160] [163] [170] [177] [179] [196] [209] [220]	43
1.2. Non-identity-based solutions	[24] [102] [124]	3
Properties		
1.1. Dynamics	[2] [9] [33] [35] [36] [62] [76] [89] [98] [116] [124] [126] [127] [130] [141] [154] [155] [165] [172] [179] [194] [145]	22
1.2. Unobtrusiveness	[3] [17] [28] [39] [50] [94] [124] [123] [137] [153] [170] [177] [221]	13
1.3. Speed	[2]	1
1.4. Lightweight	[179]	1
2. Privacy protection		**63/54**[9]
2.1. Masking	[13] [55] [59] [66] [69] [112] [113] [131] [142] [149] [155] [168] [169] [179] [196] [200] [204] [220]	19
2.2. Privacy protection layer	[22] [48] [80] [93] [143] [159] [182] [188] [197]	9
2.3. Proximity detection schemes	[3] [51] [53] [57] [106] [135] [182] [80] [119]	8
2.4. Game-based approach	[51] [95] [108] [168] [222] [218]	6
2.5. Consent and notification	[3] [58] [70] [77] [87] [185]	6
2.6. Negotiation approach	[47] [93] [145] [221] [223]	5
2.7. Blocker tag	[84] [190]	2
2.8. Other	[16] [125] [132] [203]	4
2.9. Obfuscation	[47] [188] [207]	3
3. Cryptographic protocols		**63**
3.1. Symmetric	[1] [7] [5] [41] [59] [68] [82] [86] [88] [92] [112] [115] [135] [166] [177] [176] [179] [192] [198]	19

[8] 79 stands for a number of unique papers.

[9] 54 stands for a number of unique papers.

3.2. Asymmetric	[19] [31] [34] [60] [63] [74] [71] [72] [76] [107] [111] [139] [153] [167] [173] [174] [189] [195]	18
3.3. Hybrid	[12] [20] [23] [46] [45] [54] [56] [81] [83] [89] [97] [103] [118] [130] [136] [145] [147] [155] [156] [157] [161] [171] [215]	23
3.4. Hashing	[122] [175] [205]	3
Lightweight protocols		
Lightweight	[1] [7] [12] [20] [41] [45] [46] [54] [56] [59] [63] [71] [76] [82] [83] [86][88] [92] [97] [112] [111] [113] [107] [115] [135] [139] [136] [155] [156] [157] [177] [176] [179] [189] [192] [205]	35
4. Trust	[1] [6] [4] [8] [11] [15] [21] [20] [27] [37] [40] [49] [65] [67] [76] [96] [107] [110] [119] [133] [134] [139] [144] [151] [164] [181] [182] [187] [188] [199] [210] [216]	**32**
5. Other		**16**
5.1. Security awareness model for BYOD	[10]	1
5.2. Framework for secure smart environment	[14]	1
5.3. Edge sampling algorithm for WSN	[32]	1
5.4. Model for secure mobile push services	[42]	1
5.5. Hash-chain for RFID systems	[64]	1
5.6. Key management for session mobility	[73]	1
5.7. Masking page references in databases	[117]	1
5.8. IdS	[140] [148] [213]	3
5.9. ILP security optimization	[150]	1
5.10. MAC for WBAN	[183]	1
5.11. Queue management	[186]	1
5.12. Framework for resource provisioning	[193]	1
5.13. Anomaly detection mechanism	[211]	1
5.14. Steganography	[217]	1
Papers that demonstrate novel attacks, but do not propose a solution		**9**
RFID attacks	[29]	1
Bluetooth viruses	[79]	1
Decoding keystrokes from nearby mobile phones	[120]	1
GPS software attacks	[138]	1
Input reconstruction from nearby mobile devices	[152]	1
Breaching mobile phones	[162]	1
DoS attacks on WSN	[191] [212]	2
Analysis of Android apps	[201]	1

Table 36: List of solutions.

D.1 Papers in common to two categories

- Authentication/access control mechanisms $\cap$ Cryptographic protocols = 16
- Authentication/access control mechanisms $\cap$ Privacy mechanisms = 6
- Authentication/access control mechanisms $\cap$ Trust-based solutions = 2
- Privacy $\cap$ Cryptographic protocols = 5
- Privacy $\cap$ Trust = 3
- Trust-based solutions $\cap$ Cryptographic protocols = 5

E List of journals

Journal name	Publisher	Coverage
ACM Transactions on Information and System Security	ACM	2003-2013
ACM Transactions on Sensor Networks	ACM	2006-2013
American Journal of Preventive Medicine	Elsevier	1985-2014
Computers & Security	Elsevier	1982-2014
Computer Communications	Elsevier	1978-2014
Computer Networks	Elsevier	1977-1984, 1989-1990, 1996-2014
Computer Standards and Interfaces	Elsevier	1985-2014
Data and Knowledge Engineering	Elsevier	1985, 1987-2014
Decision Support Systems	Elsevier	1985-2014
Future generation computer systems	Elsevier	1984-2014
IEEE/ACM Transactions on Networking	IEEE	1993-2013
IEEE Communications Magazine	IEEE	1979-2013
IEEE Journal on selected areas in communications	IEEE	1983-2014
IEEE Pervasive Computing	IEEE	2002-2013
IEEE Sensors Journal	IEEE	2001-2014
IEEE Transactions on Biomedical Circuits and Systems	IEEE	2007-2014
IEEE Transactions on Computers	IEEE Computer Society	1969-2014
IEEE Transactions on Consumer Electronics	IEEE	1975-2013
IEEE Transactions on Dependable and Secure Computing	IEEE	2004-2013
IEEE Transactions on Information Forensics and Security	IEEE	2006-2014
IEEE Transactions on Mobile Computing	IEEE	2002-2014
IEEE Transactions on Parallel and Distributed Systems	IEEE Computer Society	1990-2013
IEEE Transactions on Services Computing	IEEE	2008-2013
IEEE Vehicular Technology	IEEE	2006-2013
IEEE Wireless Communications	IEEE	2002-2013
Information Sciences	Elsevier	1968-2014
Journal of Network and Computer Applications	Academic Press Inc.	1996-2014
Lecture Notes in Computer Science	Springer Verlag	1981-1984, 1986, 1996-2013
Mathematical and Computer Modelling	Elsevier Limited	1988-2013
Mobile Networks and Applications	Springer Netherlands	1996-2014
Nonlinear Dynamics	Springer Netherlands	1990-2014
Journal of Computer Security	IOS Press	1994, 1996-2013
Journal of Computer and System Sciences	Academic Press Inc.	1967-2014
Journal of Intelligent Manufacturing	Springer Netherlands	1990-2014
Journal of Systems and Software	Elsevier	1979-2014
Personal and Ubiquitous Computing	Springer London	2005-2013
Pervasive and Mobile Computing	Elsevier	2005-2013
Science of Computer Programming	Elsevier	1981-2014
Sensors	MDPI	2001-2013
Software - Practice & Experience	John Wiley and Sons	1972-2014
Theoretical Computer Science	Elsevier	1975-2014
Wireless Communications and Mobile Computing	John Wiley and Sons	2001-2014
Wireless Networks	Springer Netherlands	1995-2014

Table 37: List of journals in alphabetical order.

F Journal ranking

Journal name	SJR Ranking	H-index	References	No. of articles
IEEE Wireless Communications	3.83	98	[187]	1
IEEE Journal on selected areas in communications	3.34	165	[20] [72] [75] [82] [165]	5
IEEE Communications Magazine	3.2	144	[59] [180]	2
IEEE Transactions on Wireless Communications	2.72	118	[178]	1
Information Sciences	2.61	91	[26] [98]	2
American Journal of Preventive Medicine	2.52	131	[87]	1
IEEE Transactions on Mobile Computing	2.26	80	[123] [137] [145] [191] [221]	5
IEEE/ACM Transactions on Networking	2.04	124	[116] [186]	2
IEEE Transactions on Biomedical Circuits and Systems	1.88	29	[211]	1
Decision Support Systems	1.81	76	[93]	1
Journal of Computer and System Sciences	1.61	56	[150]	1
ACM Transactions on Information and System Security	1.55	41	[24] [62]	2
IEEE Transactions on Information Forensics and Security	1.41	46	[7] [190]	2
Data and Knowledge Engineering	1.33	59	[117]	1
Nonlinear Dynamics	1.28	59	[105]	1
IEEE Transactions on Parallel and Distributed Systems	1.25	78	[111] [142] [204] [223]	4
Future generation computer systems	1.24	59	[194]	1
IEEE Transactions on Services Computing	1.18	27	[115]	1
Mathematical and Computer Modelling	1.16	59	[13]	1
Journal of Intelligent Manufacturing	1.09	44	[141]	1
Pervasive and Mobile Computing	1.03	28	[63] [127]	2
Journal of Computer Security	0.97	40	[184]	1
ACM Transactions on Sensor Networks	0.96	36	[107] [192]	2
Theoretical Computer Science	0.93	74	[35]	1
IEEE Pervasive Computing	0.92	69	[27] [58] [66] [106] [102]	5
IEEE Vehicular Technology	0.92	21	[155]	1
Journal of Network and Computer Applications	0.9	30	[15] [114] [133] [157] [166] [167] [179]	7
Personal and Ubiquitous Computing	0.9	31	[14] [28] [49] [76] [91] [172]	6
IEEE Transactions on Dependable and Secure Computing	0.87	36	[37] [79]	2
Computer Networks	0.88	78	[128]	1
Computers & Security	0.84	51	[3] [45]	2
Journal of Systems and Software	0.82	60	[4] [5] [73] [129] [188] [195]	6
IEEE Transactions on Computers	0.77	81	[147]	1
Mobile Networks and Applications	0.75	57	[31] [112] [189] [200] [210] [215]	6
Computer Standards and Interfaces	0.75	38	[74] [198]	2
IEEE Sensors Journal	0.73	56	[110]	1
IEEE Transactions on Consumer Electronics	0.73	69	[78] [89] [177]	3

Journal name	SJR Ranking	H-index	References	No. of articles
Science of Computer Programming	0.67	44	[161]	1
Sensors	0.66	63	[118]	1
Computer Communications	0.65	58	[21] [32] [40] [86] [97] [100] [104] [109] [131] [146] [151] [156] [169] [176] [196] [209] [216]	17
Software - Practice & Experience	0.63	49	[206]	1
Wireless Networks	0.53	65	[33] [99] [164] [213]	4
Wireless Communications and Mobile Computing	0.32	39	[81] [132]	2
Lecture Notes in Computer Science	0.31	118	[23] [101]	2
			Total	**113**

Table 38: List of journal rankings in descending order based on the SJR value.

G List of conferences

Conference abbr.	Conference Name	CORE ranking	References	No. of papers
ACSAC	Annual Computer Security Applications Conference	A	[140] [173]	2
CCS	ACM Conference on Computer and Communications Security	A*	[12] [16] [48] [51] [69] [84] [119] [120] [134] [138] [149] [152] [154] [162] [168] [197] [201]	17
CHI	International Conference on Human Factors in Computing Systems	A*	[77]	1
HICSS	Hawaii International Conference on System Sciences	A	[39]	1
ICDE	International Conference on Data Engineering	A*	[217]	1
ICWS	IEEE International Conference on Web Services	A	[202]	1
IEEE INFOCOM	IEEE International Conference on Computer Communications	A*	[199]	1
IJCNN	IEEE International Joint Conference on Neural Networks	A	[44]	1
IPDPS	IEEE International Parallel and Distributed Processing Symposium	A	[52]	1
LCN	IEEE Conference on Local Computer Networks	A	[2] [34] [43]	3
MobiCom	ACM International Conference on Mobile Computing and Networking	A*	[30] [122] [125] [163]	4
MobiQuitous	International Conference on Mobile and Ubiquitous Systems: Networks and Services	A	[6] [54] [83] [143] [218]	5
NCA	IEEE International Symposium on Network Computing and Applications	A	[36]	1
PerCom	International Conference on Mobile and Ubiquitous Systems: Networks and Services	A*	[9] [11] [19] [25] [22] [41] [55] [56] [60] [61] [64] [67] [68] [85] [88] [95] [96] [103] [108] [121] [130] [148] [158] [170] [175] [205] [222] [219] [220]	29
PERVASIVE	International Conference on Pervasive Computing	A*	[47]	1
S&P	IEEE Symposium on Security and Privacy	A*	[80]	1
SRDS	Symposium on Reliable Distributed Systems	A	[92]	1
TrustCom	IEEE/IFIP International Symposium on Trusted Computing and Communications	A	[17] [46] [50] [174] [181]	5
UbiComp	Ubiquitous Computing	A*	[57] [90] [124] [159] [171]	5
WOWMOM	IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks	A	[8] [29] [214]	3
			Total	**84**

Table 39: List of conferences in ascending alphabetical order based on abbreviations.

H Selected papers

[1] Raed Abd-Alhameed, Trust Mapoka, and Simon Shepherd. A new multiple service key management scheme for secure wireless mobile multicast. *IEEE Transactions on Mobile Computing*, PP(99):1–1, 2014.

[2] Nidal Aboudagga, Giacomo de Meulenaer, Mohamed Eltoweissy, and Jean-Jacques Quisquater. IMAPS: Imbricated authentication protocol suite for mobile users and groups. In *IEEE 34th Conference on Local Computer Networks*, LCN '09, pages 30–36, Oct 2009.

[3] Isaac Agudo, Ruben Rios, and Javier Lopez. A privacy-aware continuous authentication scheme for proximity-based access control. *Computers & Security*, 39:117–126, November 2013.

[4] Sheikh I. Ahamed, Munirul M. Haque, Md. Endadul Hoque, Farzana Rahman, and Nilothpal Talukder. Design, analysis, and deployment of omnipresent Formal Trust Model (FTM) with trust bootstrapping for pervasive environments. *Journal of Systems and Software*, 83(2):253–270, February 2010.

[5] Sheikh Iqbal Ahamed, Haifeng Li, Nilothpal Talukder, Mehrab Monjur, and Chowdhury Sharif Hasan. Design and implementation of S-MARKS: A secure middleware for pervasive computing applications. *Journal of Systems and Software*, 82(10):1657–1677, October 2009.

[6] S.I. Ahamed, N. Talukder, and M. Haque. Privacy challenges in context-sensitive access control for pervasive computing environment. In *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services*, MobiQuitous '07, pages 1–6, Aug 2007.

[7] Zahra Ahmadian, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Recursive Linear and Differential Cryptanalysis of Ultralightweight Authentication Protocols. *IEEE Transactions on Information Forensics and Security*, 8(7):1140–1151, July 2013.

[8] M.D. Aime and Antonio Lioy. Incremental trust: building trust from past experience. In *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, WoWMoM '05, pages 603–608, June 2005.

[9] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell, and M.Dennis Mickunas. Cerberus: a context-aware security scheme for smart spaces. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*, PerCom '03, pages 489–496, March 2003.

[10] Sean Allam, Stephen V. Flowerday, and Ethan Flowerday. Smartphone information security awareness: A victim of operational pressures. *Computers & Security*, 42:56–65, May 2014.

[11] Florina Almenarez, Andres Marin, Daniel Diaz, Alberto Cortes, Celeste Campo, and Carlos Garcia-Rubio. A trust-based middleware for providing security to ad-hoc peer-to-peer applications. In *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '08, pages 531–536, Washington, DC, USA, 2008. IEEE Computer Society.

[12] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. New privacy issues in mobile telephony: Fix and verification. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 205–216, New York, NY, USA, 2012. ACM.

[13] Joan Arnedo-Moreno, Noemí Pérez-Gilabert, and Marc Domingo-Prieto. Anonymously accessing JXTA community services through split message forwarding. *Mathematical and Computer Modelling*, 58(5–6):1313 – 1327, 2014. The Measurement of Undesirable Outputs: Models Development and Empirical Analyses and Advances in mobile, ubiquitous and cognitive computing.

[14] F. Bagci, H. Schick, J. Petzold, W. Trumler, and T. Ungerer. The reflective mobile agent paradigm implemented in a smart office environment. *Personal and Ubiquitous Computing*, 11(1):11–19, February 2006.

[15] Şerif Bahtiyar and Mehmet Ufuk Çağlayan. Extracting trust information from security system of a service. *Journal of Network and Computer Applications*, 35(1):480–490, January 2012.

[16] Daniel V. Bailey, Dan Boneh, Eu-Jin Goh, and Ari Juels. Covert channels in privacy-preserving identification systems. In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, pages 297–306, New York, NY, USA, 2007. ACM.

[17] Marc Barisch. Design and evaluation of an architecture for ubiquitous user authentication based on identity management systems. In *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, TrustCom '11, pages 863–872, Nov 2011.

[18] Silvio Barra, Andrea Casanova, Fabio Narducci, and Stefano Ricciardi. Ubiquitous iris recognition by means of mobile devices. *Pattern Recognition Letters*, October 2014.

[19] Allan Beaufour and Philippe Bonnet. Personal servers as digital keys. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications*, PerCom '04, pages 319–328, March 2004.

[20] A Boukerche and Yonglin Ren. A secure mobile healthcare system using trust-based multicast scheme. *IEEE Journal on Selected Areas in Communications*, 27(4):387–399, May 2009.

[21] Azzedine Boukerche and Yonglin Ren. A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications*, 31(18):4343–4351, December 2008.

[22] I Boutsis and V. Kalogeraki. Privacy preservation for participatory sensing data. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '13, pages 103–113, March 2013.

[23] An Braeken, Antonio De La Piedro, and Karel Wouters. Secure event logging in sensor networks. In Svetla Petkova-Nikova, Andreas Pashalidis, and Günther Pernul, editors, *Public Key Infrastructures, Services and Applications*, volume 7163 of *Lecture Notes in Computer Science*, pages 194–208. Springer Berlin Heidelberg, 2012.

[24] Mike Burmester, Tri Van Le, Breno De Medeiros, and Gene Tsudik. Universally composable rfid identification and authentication protocols. *ACM Transactions on Information and System Security*, 12(4):21:1–21:33, April 2009.

[25] Laurent Bussard and Rrefik Molva. One-time capabilities for authorizations without trust. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications*, PerCom '04, pages 351–355, March 2004.

[26] Jin Wook Byun, Dong Hoon Lee, and Jong In Lim. Ec2c-paka: An efficient client-to-client password-authenticated key agreement. *Information Sciences*, 177(19):3995–4013, October 2007.

[27] V. Cahill, E. Gray, J. M Seigneur, C.D. Jensen, Yong Chen, B. Shand, N. Dimmock, A Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. Di Marzo Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielson. Using trust for secure collaboration in uncertain environments. *IEEE Pervasive Computing*, 2(3):52–61, July 2003.

[28] Pierluigi Casale, Oriol Pujol, and Petia Radeva. Personalization and user verification in wearable systems using biometric walking patterns. *Personal and Ubiquitous Computing*, 16(5):563–580, July 2011.

[29] Qi Chai, Guang Gong, and Daniel W. Engels. How to develop clairaudience - active eavesdropping in passive rfid systems. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, WoWMoM '12, pages 1–6, June 2012.

[30] Chia-Hsin Owen Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M. McCune, Ahren Studer, Adrian Perrig, Bo-Yin Yang, and Tzong-Chen Wu. GAnGS: Gather, authenticate 'n group securely. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom '08, pages 92–103, New York, NY, USA, 2008. ACM.

[31] Chunhua Chen, ChrisJ. Mitchell, and Shaohua Tang. Ubiquitous one-time password service using the generic authentication architecture. *Mobile Networks and Applications*, 18(5):738–747, 2013.

[32] Bo-Chao Cheng, Huan Chen, Yi-Jean Li, and Ryh-Yuh Tseng. A packet marking with fair probability distribution function for minimizing the convergence time in wireless sensor networks. *Computer Communications*, 31(18):4352–4359, December 2008.

[33] Jay Chin, Ning Zhang, Aleksandra Nenadic, and Omaima Bamasak. A context-constrained authorisation (CoCoA) framework for pervasive grid computing. *Wireless Networks*, 16(6):1541–1556, September 2010.

[34] Panoat Chuchaisri and Richard E. Newman. Multi-resolution elliptic curve digital signature. In *Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks*, LCN '12, pages 93–101, Washington, DC, USA, 2012. IEEE Computer Society.

[35] Adriana Compagnoni, Elsa L. Gunter, and Philippe Bidinger. Role-based access control for boxed ambients. *Theoretical Computer Science*, 398(1-3):203–216, May 2008.

[36] Antoino Corradi, Rebecca Montanari, and Daniela Tibaldi. Context-based access control management in ubiquitous environments. In *Proceedings of the Third IEEE International Symposium on Network Computing and Applications*, NCA '04, pages 253–260, Aug 2004.

[37] A Das and M.M. Islam. Securedtrust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*, 9(2):261–274, March 2012.

[38] Maria De Marsico, Chiara Galdi, Michele Nappi, and Daniel Riccio. FIRME: Face and Iris Recognition for Mobile Engagement. *Image and Vision Computing*, 32(12):1161–1172, December 2014.

[39] C. Decker, S. Nguissi, J. Haller, and R. Kilian-Kehr. Proximity as a security property in a mobile enterprise application context. In *Proceedings of the 37th Annual Hawaii International Conference on Dystem Sciences*, HICSS '04, pages 10 pp.–, Jan 2004.

[40] Mieso K. Denko, Tao Sun, and Isaac Woungang. Trust management in ubiquitous computing: A Bayesian approach. *Computer Communications*, 34(3):398–406, March 2011.

[41] Tassos Dimitriou. A secure and efficient RFID protocol that could make big brother (partially) obsolete. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '06, pages 6 pp.–275, March 2006.

[42] Junhua Ding, Wei Song, and Dongmei Zhang. An Approach for Modeling and Analyzing Mobile Push Notification Services. In *2014 IEEE International Conference on Services Computing*, pages 725–732. IEEE, June 2014.

[43] AL.M. dos Santos, V. Scarlata, AC. Lima, IC. Alves, and D.D.C. Sampaio. SACM: Stateful access control model. In *IEEE 36th Conference on Local Computer Networks*, LCN '11, pages 159–162, Oct 2011.

[44] H. Dozono, M. Nakakuni, H. Sanada, and Y. Noguchi. The Analysis of Pen Inputs of Handwritten Symbols using Self Organizing Maps and its Application to User Authentication. *The 2006 IEEE International Joint Conference on Neural Network Proceedings*, 3:2577–2582, 2006.

[45] N. Dragoni, F. Massacci, T. Walter, and C. Schaefer. What the Heck is this Application doing? - A Security-by-Contract Architecture for Pervasive Services. *Computers and Security*, (7):566–577, 2009.

[46] W. Drira, E. Renault, and D. Zeghlache. A hybrid authentication and key establishment scheme for wban. In *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, TrustCom '12, pages 78–83, June 2012.

[47] Matt Duckham and Lars Kulik. A formal model of obfuscation and negotiation for location privacy. In *Proceedings of the Third International Conference on Pervasive Computing*, Pervasive '05, pages 152–170, Berlin, Heidelberg, 2005. Springer-Verlag.

[48] William Enck, Machigar Ongtang, and Patrick McDaniel. On lightweight mobile phone application certification. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 235–245, New York, NY, USA, 2009. ACM.

[49] Colin English, Sotirios Terzis, and Paddy Nixon. Towards self-protecting ubiquitous systems: monitoring trust-based interactions. *Personal and Ubiquitous Computing*, 10(1):50–54, August 2006.

[50] Md. Sadek Ferdous and Ron Poet. Portable personal identity provider in mobile phones. In *Proceedings of the 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, TrustCom '13, pages 736–745, Washington, DC, USA, 2013. IEEE Computer Society.

[51] Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux, and David C. Parkes. On non-cooperative location privacy: A game-theoretic analysis. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 324–337, New York, NY, USA, 2009. ACM.

[52] Song Fu and Cheng-Zhong Xu. A coordinated spatio-temporal access control model for mobile computing in coalition environments. In *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium*, IPDPS '05, pages 8 pp.–, April 2005.

[53] Sebastien Gambs, Marc-Olivier Killijian, Matthieu Roy, and Moussa Traore. PROPS: A PRivacy-Preserving Location Proof System. In *2014 IEEE 33rd International Symposium on Reliable Distributed Systems*, pages 1–10. IEEE, October 2014.

[54] O. Garcia-Morchon, T. Falck, T. Heer, and K. Wehrle. Security for pervasive medical sensor networks. In *6th Annual International Conference on Mobile and Ubiquitous Systems: Networking Services*, MobiQuitous '09, pages 1–10, July 2009.

[55] M.M. Groat, B. Edwards, J. Horey, Wenbo He, and S. Forrest. Enhancing privacy in participatory sensing applications with multidimensional data. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '12, pages 144–152, March 2012.

[56] V. Gupta, M. Millard, S. Fung, Yu Zhu, N. Gura, H. Eberle, and S.C. Shantz. SIZZLE: a standards-based end-to-end security architecture for the embedded internet. In *Third IEEE International Conference on Pervasive Computing and Communications*, PerCom '05, pages 247–256, March 2005.

[57] Tanzima Hashem, Mohammed Eunus Ali, Lars Kulik, Egemen Tanin, and Anthony Quattrone. Protecting privacy for group nearest neighbor queries with crowdsourced data and computing. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '13, pages 559–562, New York, NY, USA, 2013. ACM.

[58] Gillian R. Hayes, Erika Shehan Poole, Giovanni Iachello, Shwetak N. Patel, Andrea Grimes, Gregory D. Abowd, and Khai N. Truong. Physical, Social, and Experiential Knowledge in Pervasive Computing Environments. *IEEE Pervasive Computing*, 6(4):56–63, October 2007.

[59] Qi He, Dapeng Wu, and Pradeep Khosla. The quest for personal control over mobile location privacy. *IEEE Communications Magazine*, 42(5):130–136, May 2004.

[60] Wenbo He, Ying Huang, K. Nahrstedt, and W.C. Lee. SMOCK: A self-contained public key management scheme for mission-critical wireless ad hoc networks. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '07, pages 201–210, March 2007.

[61] U. Hengartner and P. Steenkiste. Avoiding privacy violations caused by context-sensitive services. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '06, pages 10 pp.–233, March 2006.

[62] Urs Hengartner and Peter Steenkiste. Access control to people location information. *ACM Transactions on Information and System Security*, 8(4):424–456, November 2005.

[63] Urs Hengartner and Peter Steenkiste. Exploiting information relationships for access control in pervasive computing. *Pervasive and Mobile Computing*, 2(3):344–367, September 2006.

[64] Dirk Henrici and Paul M. Providing Security and Privacy in RFID Systems Using Triggered Hash Chains. *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 50–59, March 2008.

[65] Holger Hoffmann and Matthias Söllner. Incorporating Behavioral Trust Theory into System Development for Ubiquitous Applications. *Personal Ubiquitous Comput.*, 18(1):117–128, January 2014.

[66] Henry Holtzman, Sanghoon Lee, and Daniel Shen. OpenTag: privacy protection for RFID. *IEEE Pervasive Computing*, 8(2):71–77, 2009.

[67] M.E. Hoque, F. Rahman, and S.I Ahamed. An adaptive initial trust and demand aware secure resource discovery (AID-SRD) model for pervasive environments. In *IEEE International Conference on Pervasive Computing and Communications.*, PerCom '09, pages 1–6, March 2009.

[68] M.E. Hoque, F. Rahman, and S.I Ahamed. AnonPri: An efficient anonymous private authentication protocol. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '11, pages 102–110, March 2011.

[69] Peter Hornyack, Seungyeop Han, Jaeyeon Jung, Stuart Schechter, and David Wetherall. These aren't the droids you're looking for: Retrofitting Android to protect data from imperious applications. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 639–652, New York, NY, USA, 2011. ACM.

[70] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. Privacy Behaviors of Lifeloggers Using Wearable Cameras. UbiComp '14, pages 571–582. ACM, January 2014.

[71] Wen-Bin Hsieh and Jenq-Shiou Leu. Anonymous authentication protocol based on elliptic curve Diffie-Hellman for wireless access networks. *Wireless Communications and Mobile Computing*, 14(10):995–1006, July 2014.

[72] Chunqiang Hu, Nan Zhang, Hongjuan Li, Xiuzhen Cheng, and Xiaofeng Liao. Body area network security: A fuzzy attribute-based signcryption scheme. *IEEE Journal on Selected Areas in Communications*, 31(9):37–46, September 2013.

[73] Chung-Ming Huang, Jian-Wei Li, and I-Ting Tseng. Multimedia Internet Rekeying for secure session mobility in ubiquitous mobile networks. *Journal of Systems and Software*, 82(9):1526–1539, September 2009.

[74] Kuo-Hsuan Huang, Yu-Fang Chung, Chia-Hui Liu, Feipei Lai, and Tzer-Shyong Chen. Efficient migration for mobile computing in distributed networks. *Computer Standards & Interfaces*, 31(1):40–47, January 2009.

[75] Y. Huang, M. Hsieh, H. Chao, S. Hung, and J. Park. Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. *IEEE Journal on Selected Areas in Communications*, 27(4):400–411, May 2009.

[76] Anas El Husseini, Abdallah M'hamed, Bachar El-Hassan, and Mounir Mokhtari. Trust-based authentication scheme with user rating for low-resource devices in smart environments. *Personal and Ubiquitous Computing*, 17(5):1013–1023, 2013.

[77] Giovanni Iachello, Khai N. Truong, Gregory D. Abowd, Gillian R. Hayes, and Molly Stevens. Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 1009–1018, New York, NY, USA, 2006. ACM.

[78] H. Jabbar. Viewer Identification and Authentication in IPTV using RFID Technique. *IEEE Transactions on Consumer Electronics*, 54(1):105–109, February 2008.

[79] Jennifer T. Jackson and Sadie Creese. Virus propagation in heterogeneous Bluetooth networks with human behaviors. *IEEE Transactions on Dependable and Secure Computing*, 9(6):930–943, Nov 2012.

[80] S. Jana, A Narayanan, and V. Shmatikov. A Scanner Darkly: Protecting user privacy from perceptual applications. In *IEEE Symposium on Security and Privacy*, S&P '13, pages 349–363, May 2013.

[81] Chol Soon Jang, Deok Gyu Lee, Jong-wook Han, and Jong Hyuk Park. Hybrid security protocol for wireless body area networks. *Wireless Communications and Mobile Computing*, 11(2):277–288, 2011.

[82] Antonio J. Jara, Miguel A Zamora-Izquierdo, and Antonio F. Skarmeta. Interconnection framework for m-health and remote monitoring based on the Internet of Things. *IEEE Journal on Selected Areas in Communications*, 31(9):47–65, September 2013.

[83] Assed Jehangir and Sonia M.H. de Groot. A security architecture for personal networks. In *Third Annual International Conference on Mobile and Ubiquitous Systems: Networking Services*, Mobiquitous '06, pages 1–8, July 2006.

[84] Ari Juels, Ronald L. Rivest, and Michael Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *Proceedings of the 10th ACM Conference on Computer and Communications Security*, CCS '03, pages 103–111, New York, NY, USA, 2003. ACM.

[85] D.N. Kalofonos, Z. Antoniou, F.D. Reynolds, M. Van-Kleek, J. Strauss, and P. Wisner. MyNet: A platform for secure P2P personal and social networking services. In *Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '08, pages 135–146, March 2008.

[86] Soo-Young Kang, Deok-Gyu Lee, and Im-Yeong Lee. A study on secure RFID mutual authentication scheme in pervasive computing environment. *Computer Communications*, 31(18):4248–4254, December 2008.

[87] Paul Kelly, Simon J Marshall, Hannah Badland, Jacqueline Kerr, Melody Oliver, Aiden R Doherty, and Charlie Foster. An ethical framework for automated, wearable cameras in health behavior research. *American journal of preventive medicine*, 44(3):314–9, March 2013.

[88] Sye Loong Keoh, E. Lupu, and M. Sloman. Securing body sensor networks: Sensor association and key management. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '09, pages 1–6, March 2009.

[89] Jangseong Kim, Joonsang Baek, and Taeshik Shon. An efficient and scalable re-authentication protocol over wireless sensor network. *IEEE Transactions on Consumer Electronics*, 57(2):516–522, May 2011.

[90] Tim Kindberg, Chris Bevan, Eamonn O'Neill, James Mitchell, Jim Grimmett, and Dawn Woodgate. Authenticating ubiquitous services: A study of wireless hotspot access. In *Proceedings of the 11th International Conference on Ubiquitous Computing*, Ubicomp '09, pages 115–124, New York, NY, USA, 2009. ACM.

[91] V. Koufi, F. Malamateniou, and G. Vassilacopoulos. A system for the provision of medical diagnostic and treatment advice in home care environment. *Personal and Ubiquitous Computing*, 14(6):551–561, March 2010.

[92] V. Kumar and S. Madria. PIP: Privacy and integrity preserving data aggregation in wireless sensor networks. In *IEEE 32nd International Symposium on Reliable Distributed Systems*, SRDS '13, pages 10–19, Sept 2013.

[93] Ohbyung Kwon. A pervasive P3P-based negotiation mechanism for privacy-aware pervasive e-commerce. *Decision Support Systems*, 50(1):213–221, December 2010.

[94] Taekyoung Kwon and Sarang Na. TinyLock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Computers & Security*, 42:137–150, May 2014.

[95] Brent Lagesse and Mohan Kumar. A Novel Utility and Game-Theoretic Based Security Mechanism for Mobile P2P Systems. *2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 486–491, March 2008.

[96] Brent Lagesse, Mohan Kumar, Justin M. Paluska, and Matthew Wright. Dtt: A distributed trust toolkit for pervasive systems. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '09, pages 1–8, March 2009.

[97] Kwok-Yan Lam, Siu-Leung Chung, Ming Gu, and Jia-Guang Sun. Lightweight security for mobile commerce transactions. *Computer Communications*, 26(18):2052–2060, December 2003.

[98] Xuan Hung Le, Sungyoung Lee, Young-Koo Lee, Heejo Lee, Murad Khalid, and Ravi Sankar. Activity-oriented access control to ubiquitous hospital information and services. *Information Sciences*, 180(16):2979–2990, August 2010.

[99] Ki-Dong Lee and Athanasios V. Vasilakos. Access stratum resource management for reliable u-healthcare service in LTE networks. *Wireless Networks*, 17(7):1667–1678, July 2011.

[100] Ming Lei, Yang Xiao, Susan V. Vrbsky, and Chung-Chih Li. Virtual password using random linear functions for on-line services, ATM machines, and pervasive computing. *Computer Communications*, 31(18):4367–4375, December 2008.

[101] Adrian Leung and ChrisJ. Mitchell. Ninja: Non identity based, privacy preserving authentication for ubiquitous environments. In John Krumm, GregoryD. Abowd, Aruna Seneviratne, and Thomas Strang, editors, *UbiComp 2007: Ubiquitous Computing*, volume 4717 of *Lecture Notes in Computer Science*, pages 73–90. Springer Berlin Heidelberg, 2007.

[102] Maylor K.H. Leung, a.C.M. Fong, and Siu Cheung Hui. Palmprint Verification for Controlling Access to Shared Computing Resources. *IEEE Pervasive Computing*, 6(4):40–47, October 2007.

[103] Chen Li, Ye Zhang, and Lijuan Duan. Establishing a trusted architecture on pervasive terminals for securing context processing. In *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '08, pages 639–644, Washington, DC, USA, 2008. IEEE Computer Society.

[104] Chun-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu. Further improvement on a novel privacy preserving authentication and access control scheme for pervasive computing environments. *Computer Communications*, 31(18):4255–4258, December 2008.

[105] Chun-Ta Li, Cheng-Chi Lee, and Chi-Yao Weng. An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. *Nonlinear Dynamics*, 74(4):1133–1143, August 2013.

[106] Hong Ping Li, Haibo Hu, and Jianliang Xu. Nearby friend alert: Location anonymity in mobile geosocial networks. *IEEE Pervasive Computing*, 12(4):62–70, Oct 2013.

[107] Ming Li, Shucheng Yu, Joshua D. Guttman, Wenjing Lou, and Kui Ren. Secure ad hoc trust initialization and key management in wireless body area networks. *ACM Transactions on Sensor Networks*, 9(2):18:1–18:35, April 2013.

[108] Qinghua Li and Guohong Cao. Providing privacy-aware incentives for mobile sensing. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '13, pages 76–84, March 2013.

[109] Xuefeng Liang, Naixue Xiong, Laurence T. Yang, Hui Zhang, and Jong Hyuk Park. A compensation scheme of fingerprint distortion using combined radial basis function model for ubiquitous services. *Computer Communications*, 31(18):4360 – 4366, 2008. Secure Multi-Mode Systems and their Applications for Pervasive Computing.

[110] Hong Liu and Huansheng Ning. Zero-knowledge authentication protocol based on alternative mode in RFID systems. *IEEE Sensors Journal*, 11(12):3235–3245, Dec 2011.

[111] Hong Liu, Huansheng Ning, Yan Zhang, Daojing He, Qingxu Xiong, and L.T. Yang. Grouping-proofs-based authentication protocol for distributed RFID systems. *IEEE Transactions on Parallel and Distributed Systems*, 24(7):1321–1330, July 2013.

[112] Jing Liu and Yang Xiao. Temporal Accountability and Anonymity in Medical Sensor Networks. *Mobile Networks and Applications*, 16(6):695–712, July 2010.

[113] Jingwei Liu, Zonghua Zhang, Xiaofeng Chen, and Kyung Sup Kwak. Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):332–342, February 2014.

[114] Gabriel López, Oscar Cánovas, Antonio F. Gómez, Jesús D. Jiménez, and Rafael Marín. A network access control approach based on the AAA architecture and authorization attributes. *Journal of Network and Computer Applications*, 30(3):900–919, August 2007.

[115] Hanping Lufei, Weisong Shi, and Vipin Chaudhary. Adaptive Secure Access to Remote Services in Mobile Environments. *IEEE Transactions on Services Computing*, 1(1):49–61, January 2008.

[116] Haiyun Luo, Jiejun Kong, P. Zerfos, Songwu Lu, and Lixia Zhang. Ursa: ubiquitous and robust access control for mobile ad hoc networks. *IEEE/ACM Transactions on Networking*, 12(6):1049–1063, Dec 2004.

[117] Xi Ma, HweeHwa Pang, and Kian-Lee Tan. Masking page reference patterns in encryption databases on untrusted storage. *Data & Knowledge Engineering*, 58(3):466–483, September 2006.

[118] Kriangsiri Malasri and Lan Wang. Design and implementation of a secure wireless mote-based medical sensor network. *Sensors*, 9(8):6273–97, January 2009.

[119] Justin Manweiler, Ryan Scudellari, and Landon P. Cox. SMILE: Encounter-based trust for mobile social services. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 246–255, New York, NY, USA, 2009. ACM.

[120] Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. (sp)iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 551–562, New York, NY, USA, 2011. ACM.

[121] Thomas Martin, Michael Hsiao, Dong Ha, and Jayan Krishnaswami. Denial-of-service attacks on battery-powered mobile computers. In *Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications*, PerCom '04, pages 309–, Washington, DC, USA, 2004. IEEE Computer Society.

[122] Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye, and Alex Reznik. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom '08, pages 128–139, New York, NY, USA, 2008. ACM.

[123] Rene Mayrhofer, Jürgen Fuss, and Iulia Ion. Uacap: A unified auxiliary channel authentication protocol. *IEEE Transactions on Mobile Computing*, 12(4):710–721, April 2013.

[124] Rene Mayrhofer, Hans Gellersen, and Mike Hazas. Security by spatial reference: Using relative positioning to authenticate devices for spontaneous interaction. volume 4717 of *UbiComp '07*, pages 199–216. Springer Berlin Heidelberg, 2007.

[125] Joseph Meyerowitz and Romit Roy Choudhury. Hiding stars with fireworks: Location privacy through camouflage. In *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking*, MobiCom '09, pages 345–356, New York, NY, USA, 2009. ACM.

[126] Markus Miettinen. Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices Categories and Subject Descriptors. pages 880–891, 2014.

[127] Kazuhiro Minami and David Kotz. Secure context-sensitive authorization. *Pervasive and Mobile Computing*, 1(1):123–156, March 2005.

[128] M. Moessner and Gul N. Khan. Secure authentication scheme for passive C1G2 RFID tags. *Computer Networks*, 56(1):273–286, January 2012.

[129] Mubarak Mohammad and Vangalur Alagar. A formal approach for the specification and verification of trustworthy component-based systems. *Journal of Systems and Software*, 84(1):77–104, January 2011.

[130] M.M. Molla, P. Madiraju, S. Malladi, and S.I Ahamed. An xml based access control architecture for pervasive computing. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '09, pages 1–6, March 2009.

[131] Jong Sik Moon and Im-Yeong Lee. An AAA scheme using ID-based ticket with anonymity in future mobile communication. *Computer Communications*, 34(3):295–304, March 2011.

[132] Thomas H. Morris and V. S. S. Nair. Private computing on public platforms: portable application security. *Wireless Communications and Mobile Computing*, 10(7):942–958, 2010.

[133] Eduardo Moschetta, Rodolfo S. Antunes, and Marinho P. Barcellos. Flexible and secure service discovery in ubiquitous computing. *Journal of Network and Computer Applications*, 33(2):128–140, March 2010.

[134] Adwait Nadkarni and William Enck. Preventing accidental data disclosure in modern operating systems. In *Proceedings of the 2013 ACM SIGSAC conference on Computer &; communications security*, CCS '13, pages 1029–1042, New York, NY, USA, 2013. ACM.

[135] Abhinav Narain, Nick Feamster, and Alex C Snoeren. Deniable Liaisons. CCS '14, pages 525–536. ACM, January 2014.

[136] Vincent Ngo, Isaac Woungang, and Alagan Anpalagan. A schedule-based medium access control protocol for mobile wireless sensor networks. *Wireless Communications and Mobile Computing*, 14(6):629–643, April 2014.

[137] Anthony J. Nicholson, Mark D. Corner, and Brian D. Noble. Mobile device security using transient authentication. *IEEE Transactions on Mobile Computing*, 5(11):1489–1502, November 2006.

[138] Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley. Gps software attacks. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 450–461, New York, NY, USA, 2012. ACM.

[139] Huansheng Ning, Hong Liu, and Laurence Yang. Aggregated-proof Based Hierarchical Authentication Scheme for the Internet of Things. *IEEE Transactions on Parallel and Distributed Systems*, PP(99):1–1, 2014.

[140] T. OConnor and D. Reeves. Bluetooth network-based misuse detection. In *Annual Computer Security Applications Conference*, ACSAC '08, pages 377–391, Dec 2008.

[141] Sejong Oh. New role-based access control in ubiquitous e-business environment. *Journal of Intelligent Manufacturing*, 21(5):607–612, November 2008.

[142] Stephan Olariu, Mohamed Eltoweissy, and Mohamed Younis. ANSWER: AutoNomouS netWorked sEnsoR system. *Journal of Parallel and Distributed Computing*, 67(1):111–124, January 2007.

[143] G. Pallapa, M. Kumar, and S.K. Das. Privacy infusion in ubiquitous computing. In *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services*, MobiQuitous '07, pages 1–8, Aug 2007.

[144] Christoforos Panos, Christos Xenakis, Platon Kotzias, and Ioannis Stavrakakis. A specification-based intrusion detection engine for infrastructure-less networks. *Computer Communications*, 54:67–83, December 2014.

[145] Hyun-A Park and Justin Zhan. Combined Authentication-Based Multilevel Access Control in Mobile Application for DailyLifeService. *IEEE Transactions on Mobile Computing*, 9(6):824–837, June 2010.

[146] Hyung-Soo Park, Hyung-Woo Lee, Dong Hoon Lee, and Hong-Ki Ko. Multi-protocol authentication for SIP/SS7 mobile network. *Computer Communications*, 31(11):2755–2763, July 2008.

[147] Ki-Woong Park, Sang Seok Lim, and Kyu-Ho Park. Computationally efficient PKI-based single sign-on protocol, PKASSO for mobile devices. *IEEE Transactions on Computers*, 57(6):821–834, June 2008.

[148] A Patwardhan, J. Parker, A Joshi, M. Iorga, and T. Karygiannis. Secure routing and intrusion detection in ad hoc networks. In *Third IEEE International Conference on Pervasive Computing and Communications*, PerCom '05, pages 191–199, March 2005.

[149] Raluca Ada Popa, Andrew J. Blumberg, Hari Balakrishnan, and Frank H. Li. Privacy and accountability for location-based aggregate statistics. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 653–666, New York, NY, USA, 2011. ACM.

[150] Meikang Qiu, Lei Zhang, Zhong Ming, Zhi Chen, Xiao Qin, and Laurence T. Yang. Security-aware optimization for ubiquitous computing systems with SEAT graph approach. *Journal of Computer and System Sciences*, 79(5):518–529, August 2013.

[151] Basit Qureshi, Geyong Min, and Demetres Kouvatsos. A distributed reputation and trust management scheme for mobile peer-to-peer networks. *Computer Communications*, 35(5):608–618, March 2012.

[152] Rahul Raguram, Andrew M. White, Dibyendusekhar Goswami, Fabian Monrose, and Jan-Michael Frahm. iSpy: Automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 527–536, New York, NY, USA, 2011. ACM.

[153] Mahmudur Rahman, Bogdan Carbunar, and Umut Topkara. SensCrypt: A Secure Protocol for Managing Low Power Fitness Trackers. In *2014 IEEE 22nd International Conference on Network Protocols*, pages 191–196. IEEE, October 2014.

[154] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S. Heydt-Benjamin, and Srdjan Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS'09, pages 410–419, New York, NY, USA, 2009. ACM.

[155] Kui Ren, Wenjing Lou, Kwangjo Kim, and R. Deng. A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Transactions on Vehicular Technology*, 55(4):1373–1384, July 2006.

[156] Rabia Riaz, Ayesha Naureen, Attiya Akram, Ali Hammad Akbar, Ki-Hyung Kim, and H. Farooq Ahmed. A unified security framework with three key management schemes for wireless sensor networks. *Computer Communications*, 31(18):4269–4280, December 2008.

[157] Bruno P.S. Rocha, Daniel N.O. Costa, Rande a. Moreira, Cristiano G. Rezende, Antonio a.F. Loureiro, and Azzedine Boukerche. Adaptive security protocol selection for mobile computing. *Journal of Network and Computer Applications*, 33(5):569–587, September 2010.

[158] Nitesh Saxena, Md. Borhan Uddin, Jonathan Voris, and N. Asokan. Vibrate-to-Unlock: Mobile phone assisted user authentication to multiple personal RFID tags. In *Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications*, PerCom '11, pages 181–188, Washington, DC, USA, 2011. IEEE Computer Society.

[159] Florian Schaub, Bastian Könings, Stefan Dietzel, Michael Weber, and Frank Kargl. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, UbiComp '12, pages 752–757, New York, NY, USA, 2012. ACM.

[160] Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. SmudgeSafe: Geometric Image Transformations for Smudge-resistant User Authentication. UbiComp '14, pages 775–786. ACM, January 2014.

[161] Jean-Marc Seigneur and Christian Damsgaard Jensen. The Claim Tool Kit for ad hoc recognition of peer entities. *Science of Computer Programming*, 54(1):49–71, January 2005.

[162] Abdul Serwadda and Vir V. Phoha. When kids' toys breach mobile phone security. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer &; Communications Security*, CCS '13, pages 599–610, New York, NY, USA, 2013. ACM.

[163] Muhammad Shahzad, Alex X. Liu, and Arjmand Samuel. Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, MobiCom '13, pages 39–50, New York, NY, USA, 2013. ACM.

[164] Brian Shand, Nathan Dimmock, and Jean Bacon. Trust for Ubiquitous, Transparent Collaboration. *Wireless Networks*, 10(6):711–721, November 2004.

[165] Lu Shi, Ming Li, Shucheng Yu, and Jiawei Yuan. Bana: Body area network authentication exploiting channel characteristics. *IEEE Journal on Selected Areas in Communications*, 31(9):1803–1816, September 2013.

[166] Q. Shi, N. Zhang, and D. Llewellyn-Jones. Efficient autonomous signature exchange on ubiquitous networks. *Journal of Network and Computer Applications*, 35(6):1793–1806, November 2012.

[167] Q. Shi, N. Zhang, M. Merabti, and R. Askwith. Achieving autonomous fair exchange in ubiquitous network settings. *Journal of Network and Computer Applications*, 34(2):653–667, March 2011.

[168] Reza Shokri, George Theodorakopoulos, Carmela Troncoso, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Protecting location privacy: Optimal strategy against localization attacks. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 617–627, New York, NY, USA, 2012. ACM.

[169] Agusti Solanas and Antoni Martínez-Ballesté. A TTP-free protocol for location privacy in location-based services. *Computer Communications*, 31(6):1181–1191, April 2008.

[170] E. Soriano, F.J. Ballesteros, and G. Guardiola. SHAD: A human-centered security architecture for the plan b operating system. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '07, pages 272–282, March 2007.

[171] Vijay Srinivasan, John Stankovic, and Kamin Whitehouse. Protecting your daily in-home activity information from a wireless snooping attack. In *Proceedings of the 10th International Conference on Ubiquitous Computing*, UbiComp '08, pages 202–211, New York, NY, USA, 2008. ACM.

[172] Robert Steele and Will Tao. MobiPass: a passport for mobile business. *Personal and Ubiquitous Computing*, 11(3):157–169, November 2006.

[173] Ahren Studer, Timothy Passaro, and Lujo Bauer. Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement. In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC '11, pages 333–342, New York, NY, USA, 2011. ACM.

[174] Chunhua Su, Guilin Wang, and K. Sakurai. Analysis and improvement of privacy-preserving frequent item protocol for accountable computation framework. In *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, TrustCom '12, pages 1012–1017, June 2012.

[175] N. Subramanian, Chanjun Yang, and Wensheng Zhang. Securing distributed data storage and retrieval in sensor networks. In *Fifth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '07, pages 191–200, March 2007.

[176] Bo Sun, Yang Xiao, Chung Chih Li, Hsiao-Hwa Chen, and T. Andrew Yang. Security co-existence of wireless sensor networks and RFID for pervasive computing. *Computer Communications*, 31(18):4294–4303, December 2008.

[177] Da-Zhi Sun, Jin-Peng Huai, Ji-Zhou Sun, Jia-Wan Zhang, and Zhi-Yong Feng. A new design of wearable token system for mobile device security. *IEEE Transactions on Consumer Electronics*, 54(4):1784–1789, November 2008.

[178] C.C. Tan, Bo Sheng, and Qun Li. Serverless search and authentication protocols for RFID. *IEEE Transactions on Wireless Communications*, 7(4):1400–1407, April 2008.

[179] Zuowen Tan. A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments. *Journal of Network and Computer Applications*, 35(6):1839–1846, November 2012.

[180] S. Tarkoma, C. Prehofer, S. Sovio, and P. Laitinen. Composable mediation for security-aware mobile services. *IEEE Communications Magazine*, 45(7):58–65, July 2007.

[181] W.B. Tesfay, T. Booth, and K. Andersson. Reputation based security model for Android applications. In *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, TrustCom '12, pages 896–901, June 2012.

[182] Keerthi Thomas, Arosha K Bandara, Blaine a Price, and Bashar Nuseibeh. Distilling Privacy Requirements for Mobile Applications Conference Item Distilling Privacy Requirements for Mobile Applications. *Icse'14*, pages 871–882, 2014.

[183] Kasun M. S. Thotahewa, Jamil Y. Khan, and Mehmet R. Yuce. Power Efficient Ultra Wide Band Based Wireless Body Area Networks with Narrowband Feedback Path. *IEEE Transactions on Mobile Computing*, 13(8):1829–1842, August 2014.

[184] Manachai Toahchoodee and Indrakshi Ray. On the formalization and analysis of a spatio-temporal role-based access control model. *Journal of Computer Security*, 19(3):399–452, August 2011.

[185] Eran Toch. Crowdsourcing Privacy Preferences in Context-aware Applications. *Personal Ubiquitous Comput.*, 18(1):129–141, January 2014.

[186] P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Mitigating attacks on open functionality in SMS-capable cellular networks. *IEEE/ACM Transactions on Networking*, 17(1):40–53, Feb 2006.

[187] Denis Trcek and Andrej Brodnik. Hard and soft security provisioning for computationally weak pervasive computing systems in e-health. *IEEE Wireless Communications*, 20(4):22–29, August 2013.

[188] Markus Tschersich, Christian Kahl, Stephan Heim, Stephen Crane, Katja Böttcher, Ioannis Krontiris, and Kai Rannenberg. Towards privacy-enhanced mobile communities—Architecture, concepts and user trials. *Journal of Systems and Software*, 84(11):1947–1960, November 2011.

[189] Jeffrey Undercoffer, Filip Perich, Andrej Cedilnik, Lalana Kagal, and Anupam Joshi. A secure infrastructure for service discovery and access in pervasive computing. *Mobile Networks and Applications*, 8(2):113–125, April 2003.

[190] E. Vahedi, V. Shah-Mansouri, V.W.S. Wong, IF. Blake, and R.K. Ward. Probabilistic analysis of blocking attack in RFID systems. *IEEE Transactions on Information Forensics and Security*, 6(3):803–817, Sept 2011.

[191] E. Y. Vasserman and N. Hopper. Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. *IEEE Transactions on Mobile Computing*, 12(2):318–332, February 2013.

[192] Krishna K. Venkatasubramanian and Sandeep K. S. Gupta. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Transactions on Sensor Networks*, 6(4):1–36, July 2010.

[193] Hariharasudhan Viswanathan, Eun Kyung Lee, Ivan Rodero, and Dario Pompili. Uncertainty-aware Autonomic Resource Provisioning for Mobile Cloud Computing. *IEEE Transactions on Parallel and Distributed Systems*, PP(99):1–1, 2014.

[194] Hua Wang, Yanchun Zhang, and Jinli Cao. Access control management for ubiquitous computing. *Future Generation Computer Systems*, 24(8):870–878, October 2008.

[195] Nen-Chung Wang and Shian-Zhang Fang. A hierarchical key management scheme for secure group communications in mobile ad hoc networks. *Journal of Systems and Software*, 80(10):1667–1677, October 2007.

[196] Ren-Chiun Wang, Wen-Shenq Juang, and Chin-Laung Lei. Robust authentication and key agreement scheme preserving the privacy of secret key. *Computer Communications*, 34(3):274–280, March 2011.

[197] Rui Wang, Luyi Xing, XiaoFeng Wang, and Shuo Chen. Unauthorized origin crossing on mobile platforms: Threats and mitigation. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer &; Communications Security*, CCS '13, pages 635–646, New York, NY, USA, 2013. ACM.

[198] Shu-Ching Wang and Kuo-Qin Yan. Byzantine Agreement under dual failure mobile network. *Computer Standards & Interfaces*, 28(4):475–492, April 2006.

[199] Xinlei Wang, Wei Cheng, P. Mohapatra, and T. Abdelzaher. ArtSense: Anonymous reputation and trust in participatory sensing. In *Proceedings of the IEEE International Conference on Computer Communications*, IEEE InfoCom '13, pages 2517–2525, April 2013.

[200] Edgar Weippl and Wolfgang Essmayr. Personal trusted devices for web services: Revisiting multilevel security. *Mobile Networks and Applications*, 8(2):151–157, 2003.

[201] Lei Wu, Michael Grace, Yajin Zhou, Chiachih Wu, and Xuxian Jiang. The impact of vendor customizations on Android security. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 623–634, New York, NY, USA, 2013. ACM.

[202] Ning Xi, Jianfeng Ma, Cong Sun, and Tao Zhang. Decentralized information flow verification framework for the service chain composition in mobile computing environments. In *IEEE 20th International Conference on Web Services*, ICWS '13, pages 563–570, June 2013.

[203] Jierui Xie and Bart Piet Knijnenburg. Location Sharing Preference: Analysis and Personalized Recommendation. *Proceedings of the International Conference on Intelligent User Interfaces*, pages 189–198, 2014.

[204] Jianliang Xu, Xueyan Tang, Haibo Hu, and Jing Du. Privacy-conscious location-based queries in mobile environments. *IEEE Transactions on Parallel and Distributed Systems*, 21(3):313–326, 2010.

[205] Qingsong Yao, Yong Qi, Jinsong Han, Jizhong Zhao, XiangYang Li, and Yunhao Liu. Randomizing RFID private authentication. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '09, pages 1–10, March 2009.

[206] Stephen S. Yau, Dazhi Huang, Haishan Gong, and Yisheng Yao. Support for situation awareness in trustworthy ubiquitous computing application software. *Software: Practice and Experience*, 36(9):893–921, 2006.

[207] Tengqi Ye, Brian Moynagh, Rami Albatal, and Cathal Gurrin. Negative FaceBlurring: A Privacy-by-Design Approach to Visual Lifelogging with Google Glass. CIKM '14, pages 2036–2038. ACM, January 2014.

[208] Tzu Chang Yeh, Zhi Xiang Wang, and Chia Sheng Wu. Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Systems with Applications*, 37(1):7678–7683, 2010.

[209] Eun-Jun Yoon, Kee-Young Yoo, Cheonshik Kim, You-Sik Hong, Minho Jo, and Hsiao-Hwa Chen. A secure and efficient SIP authentication scheme for converged VoIP networks. *Computer Communications*, 33(14):1674–1681, September 2010.

[210] John Zachary and Richard Brooks. Bidirectional mobile code trust management using tamper resistant hardware. *Mobile Networks and Applications*, 8(2):137–143, April 2003.

[211] Meng Zhang, Anand Raghunathan, and Niraj K Jha. MedMon: securing medical devices through wireless monitoring and anomaly detection. *IEEE Transactions on Biomedical Circuits and Systems*, 7(6):871–81, December 2013.

[212] Meng Zhang, Anand Raghunathan, and Niraj K. Jha. Trustworthiness of Medical Devices and Body Area Networks. *Proceedings of the IEEE*, 102(8):1174–1188, August 2014.

[213] Yongguang Zhang, Wenke Lee, and Yi-An Huang. Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, 9(5):545–556, September 2003.

[214] Zhenxia Zhang, R.W. Pazzi, and A Boukerche. Design and evaluation of a fast authentication scheme for WiFi-based wireless networks. In *IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*, WoWMoM '10, pages 1–6, June 2010.

[215] Sheng Zhong and Yang Richard Yang. Verifiable Distributed Oblivious Transfer and Mobile Agent Security. *Mobile Networks and Applications*, 11(2):201–210, March 2006.

[216] Bo Zhou, Qi Shi, and Madjid Merabti. Balancing intrusion detection resources in ubiquitous computing networks. *Computer Communications*, 31(15):3643–3653, September 2008.

[217] X. Zhou, HweeHwa Pang, and K.-L. Tan. Hiding data accesses in steganographic file system. In *Proceedings of the 20th International Conference on Data Engineering*, ICDE '04, pages 572–583, March 2004.

[218] Feng Zhu, S. Carpenter, A Kulkarni, C. Chidambaram, and S. Pathak. Understanding and minimizing identity exposure in ubiquitous computing environments. In *6th Annual International Conference on Mobile and Ubiquitous Systems: Networking Services*, MobiQuitous '09, pages 1–10, July 2009.

[219] Feng Zhu, M. Mutka, and L. Ni. Splendor: A secure, private, and location-aware service discovery protocol supporting mobile services. In *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*, PerCom '03, pages 235–242, March 2003.

[220] Feng Zhu, Matt W. Mutka, and L.M. Ni. The Master Key: a private authentication approach for pervasive computing environments. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '06, pages 10 pp.–221, March 2006.

[221] Feng Zhu, Matt W. Mutka, and L.M. Ni. A private, secure, and user-centric information exposure model for service discovery protocols. *IEEE Transactions on Mobile Computing*, 5(4):418–429, April 2006.

[222] Feng Zhu and Wei Zhu. Rational exposure: A game theoretic approach to optimize identity exposure in pervasive computing environments. In *IEEE International Conference on Pervasive Computing and Communications*, PerCom '09, pages 1–8, March 2009.

[223] Feng Zhu, Wei Zhu, M.W. Mutka, and L.M. Ni. Private and secure service discovery via progressive and probabilistic exposure. *IEEE Transactions on Parallel and Distributed Systems*, 18(11):1565–1577, Nov 2007.

9 References

[AHH+10] Sheikh I. Ahamed, Munirul M. Haque, Md. Endadul Hoque, Farzana Rahman, and Nilothpal Talukder. Design, analysis, and deployment of omnipresent Formal Trust Model (FTM) with trust bootstrapping for pervasive environments. *Journal of Systems and Software*, 83(2):253–270, February 2010.

[AMD+08b] Florina Almenarez, Andres Marin, Daniel Diaz, Alberto Cortes, Celeste Campo, and Carlos Garcia-Rubio. A trust-based middleware for providing security to ad-hoc peer-to-peer applications. In *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PERCOM '08, pages 531–536, Washington, DC, USA, 2008. IEEE Computer Society.

[ASA08] Sheikh I. Ahamed, Moushumi Sharmin, and Shameem Ahmed. A risk-aware trust based secure resource discovery (rtsrd) model for pervasive computing. In *Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications*, PERCOM '08, pages 590–595, Washington, DC, USA, 2008. IEEE Computer Society.

[ASA13] Zahra Ahmadian, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Recursive Linear and Differential Cryptanalysis of Ultralightweight Authentication Protocols. *IEEE Transactions on Information Forensics and Security*, 8(7):1140–1151, July 2013.

[ATF09a] Wasif Afzal, Richard Torkar, and Robert Feldt. A systematic review of search-based testing for non-functional system properties. *Information and Software Technology*, 51(6):957–976, June 2009.

[ATF09b] Wasif Afzal, Richard Torkar, and Robert Feldt. A systematic review of search-based testing for non-functional system properties. *Information and Software Technology*, 51(6):957–976, 2009.

[BBH+08] Sarah Beecham, Nathan Baddoo, Tracy Hall, Hugh Robinson, and Helen Sharp. Motivation in Software Engineering: A systematic literature review. *Information and Software Technology*, 50(9-10):860–878, August 2008.

[BR08] Azzedine Boukerche and Yonglin Ren. A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications*, 31(18):4343–4351, 2008.

[BU12] Şerif Bahtiyar and Mehmet Ufuk Çağlayan. Extracting trust information from security system of a service. *Journal of Network and Computer Applications*, 35(1):480–490, January 2012.

[CGS+03] V. Cahill, E. Gray, J. M Seigneur, C.D. Jensen, Yong Chen, B. Shand, N. Dimmock, A Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. Di Marzo Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielson. Using trust for secure collaboration in uncertain environments. *Pervasive Computing, IEEE*, 2(3):52–61, July 2003.

[Cor] Core conference ranking. `http://103.1.187.206/core/`. [Online; Accessed 20-December-2013].

[DBCG14] Serdar Doğan, Aysu Betin-Can, and Vahid Garousi. Web application testing: A systematic literature review. *Journal of Systems and Software*, 91:174–201, May 2014.

[DD08] Tore Dybå and Torgeir Dingsøyr. Strength of evidence in systematic reviews in software engineering. In *Proceedings of the Second ACM-IEEE international symposium on Empirical software engineering and measurement*, ESEM '08, pages 178–187, New York, NY, USA, 2008. ACM.

[DMWS09] Nicola Dragoni, Fabio Massacci, Thomas Walter, and Christian Schaefer. What the heck is this application doing? - a security-by-contract architecture for pervasive services. *Computers and Security*, 28(7):566–577, 2009.

[ETN06] Colin English, Sotirios Terzis, and Paddy Nixon. Towards self-protecting ubiquitous systems: monitoring trust-based interactions. *Personal and Ubiquitous Computing*, 10(1):50–54, August 2006.

[FSGC13] Ana M. Fernández-Sáez, Marcela Genero, and Michel R. V. Chaudron. Empirical studies concerning the maintenance of uml diagrams and their use in the maintenance of code: A systematic mapping study. *Information and Software Technology*, 55(7):1119–1142, 2013.

[GBBGG+13] L. García-Borgoñóna, M.A. Barcelona, J.A. García-García, M. Albab, and M.J. Escalonab. Software process modeling languages: A systematic literature review. *Information and Software Technology*, 56(2):103–116, February 2013.

[HCC+12] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V Vasilakos. ReTrust: attack-resistant and lightweight trust management for medical sensor networks. *IEEE transactions on information technology in biomedicine : a publication of the IEEE Engineering in Medicine and Biology Society*, 16(4):623–32, July 2012.

[HCS05] Dan Hong, Dickson K. W. Chiu, and Vincent Y. Shen. Requirements elicitation for the design of context-aware applications in a ubiquitous environment. In *Proceedings of the 7th International Conference on Electronic Commerce*, ICEC '05, pages 590–596, New York, NY, USA, 2005. ACM.

[HHNL07] Wenbo He, Ying Huang, K. Nahrstedt, and W.C. Lee. Smock: A self-contained public key management scheme for mission-critical wireless ad hoc networks. In *Pervasive Computing and Communications, 2007. PerCom '07. Fifth Annual IEEE International Conference on*, pages 201–210, March 2007.

[HRA09] M.E. Hoque, F. Rahman, and S.I Ahamed. An adaptive initial trust and demand aware secure resource discovery (aid-srd) model for pervasive environments. In *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, pages 1–6, March 2009.

[HS06] Urs Hengartner and Peter Steenkiste. Exploiting information relationships for access control in pervasive computing. *Pervasive and Mobile Computing*, 2(3):344 – 367, 2006.

[JLHP11] Chol Soon Jang, Deok Gyu Lee, Jong-wook Han, and Jong Hyuk Park. Hybrid security protocol for wireless body area networks. *Wireless Communications and Mobile Computing*, 11(2):277–288, 2011.

[KB13] Barbara Kitchenham and Pearl Brereton. A systematic review of systematic review process research in software engineering. *Information and Software Technology*, 55(12):2049–2075, December 2013.

[KC07] Barbara Kitchenham and Stuart Charters. Guidelines for performing systematic literature reviews in software engineering. *EBSE Technical Report*, 2.3, July 2007.

[LLW13] Chun-Ta Li, Cheng-Chi Lee, and Chi-Yao Weng. An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. *Nonlinear Dynamics*, 74(4):1133–1143, August 2013.

[LSP$^+$14] João Lopes, Rodrigo Souza, Ana Pernas, Adenauer Yamin, and Cláudio Geyer. A distributed architecture for supporting context-aware applications in ubicomp. In *Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications*, AINA '14, pages 584–590, Washington, DC, USA, 2014. IEEE Computer Society.

[MHGA13] Sara Mahdavi-Hezavehi, Matthias Galster, and Paris Avgeriou. Variability in quality attributes of service-based software systems: A systematic literature review. *Information and Software Technology*, 55(2):320–343, 2013.

[Oh08] Sejong Oh. New role-based access control in ubiquitous e-business environment. *Journal of Intelligent Manufacturing*, 21(5):607–612, November 2008.

[PAN05] Blaine A. Price, Karim Adam, and Bashar Nuseibeh. Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *Int. J. Hum.-Comput. Stud.*, 63(1-2):228–253, July 2005.

[PM03] Roberto Di Pietro and Luigi V. Mancini. Security and privacy issues of handheld and wearable wireless devices. *ACM Communications*, 46(9):74–79, 2003.

[PS09] G. Padmavathi and D. Shanmugapriya. A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security*, 4, 2009.

[RHTi13] Danijel Radjenović, Marjan Heričko, Richard Torkar, and Aleš Živković. Software fault prediction metrics: A systematic literature review. *Information and Software Technology*, 55(8):1397–1418, 2013.

[RL07] Kui Ren and Wenjing Lou. Privacy-enhanced, attack-resilient access control in pervasive computing environments with optional context authentication capability. *Mob. Netw. Appl.*, 12(1):79–92, January 2007.

[sci] Scimago journal ranking. `http://www.scimagojr.com/`. [Online; accessed 20-December-2013].

[SJV$^+$12] Iván Santiago, Álvaro Jiménez, Juan Manuel Vara, Valeria de Castro, Verónica Andrea Bollati, and Esperanza Marcos. Model-driven engineering as a new landscape for traceability management: A systematic literature review. *Information and Software Technology*, 54(12):1340–1356, 2012.

[SLB14] Mojtaba Shahin, Peng Liang, and Muhammad Ali Babar. A systematic review of software architecture visualization techniques. *Journal of Systems and Software*, 94(0):161 – 185, 2014.

[SLS13] Muhammad Shahzad, Alex X. Liu, and Arjmand Samuel. Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, MobiCom '13, pages 39–50, New York, NY, USA, 2013. ACM.

[SLYY12] Lu Shi, Ming Li, Shucheng Yu, and Jiawei Yuan. Bana: Body area network authentication exploiting channel characteristics. In *Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WISEC '12, pages 27–38, New York, NY, USA, 2012. ACM.

[SRM13] Mark Strembeck and Stefanie Rinderle-Ma. Security and Privacy in Business Processes: A Posteriori Analysis Techniques. *it - Information Technology*, 5(6):247–253, December 2013.

[Tan12] Zuowen Tan. A lightweight conditional privacy-preserving authentication and access control scheme for pervasive computing environments. *Journal of Network and Computer Applications*, 35(6):1839–1846, November 2012.

[TS06] Andrew S. Tanenbaum and Maarten van Steen. *Distributed Systems: Principles and Paradigms (2Nd Edition)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2006.

[WCMA13] Xinlei Oscar Wang, Wei Cheng, Prasant Mohapatra, and Tarek F. Abdelzaher. Artsense: Anonymous reputation and trust in participatory sensing. In *INFOCOM*, pages 2517–2525. IEEE, 2013.

[Wei99] Mark Weiser. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.*, 3(3):3–11, July 1999.

[WF07] Nen-Chung Wang and Shian-Zhang Fang. A hierarchical key management scheme for secure group communications in mobile ad hoc networks. *Journal of Systems and Software*, 80(10):1667–1677, October 2007.

[Wol08] Christoph Meinel Christian Wolter. Modelling security goals in business processes. March 2008.

[WW02] J. Webster and R.T. Watson. Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2):13–23, 2002.

[YHGY06] Stephen S. Yau, Dazhi Huang, Haishan Gong, and Yisheng Yao. Support for situation awareness in trustworthy ubiquitous computing application software: Papers from compsac 2004. *Softw. Pract. Exper.*, 36(9):893–921, July 2006.

[ZCK$^+$09] Feng Zhu, S. Carpenter, A Kulkarni, C. Chidambaram, and S. Pathak. Understanding and minimizing identity exposure in ubiquitous computing environments. In *Mobile and Ubiquitous Systems: Networking Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International*, pages 1–10, July 2009.

[ZMN06b] Feng W. Zhu, Matt W. Mutka, and Lionel M. Ni. A private, secure, and user-centric information exposure model for service discovery protocols. *IEEE Transactions on Mobile Computing*, 5(4):418–429, 2006.