IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 1, 2018, accepted December 19, 2018, date of publication January 18, 2019, date of current version February 8, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893493

Aspects of Quality in Internet of Things (IoT) Solutions: A Systematic Mapping Study

BESTOUN S. AHMED[1,2], MIROSLAV BURES[1], KAREL FRAJTAK[1], AND TOMAS CERNY[3]

[1]Department of Computer Science, Faculty of Electrical Engineering, Czech Technical University in Prague, 166 36 Prague, Czech Republic
[2]Department of Mathematics and Computer Science, Karlstad University, 651 88 Karlstad, Sweden
[3]Department of Computer Science, ECS, Baylor University, Waco, TX 76798, USA

Corresponding author: Bestoun S. Ahmed (albeybes@fel.cvut.cz)

This work was supported by the project TACR "Quality Assurance for Internet of Things Technology" under Grant TH02010296.

ABSTRACT Internet of Things (IoT) is an emerging technology that has the promising power to change our future. Due to the market pressure, IoT systems may be released without sufficient testing. However, it is no longer acceptable to release IoT systems to the market without assuring the quality. As in the case of new technologies, the quality assurance process is a challenging task. This paper shows the results of the first comprehensive and systematic mapping study to structure and categories the research evidence in the literature starting in 2009 when the early publication of IoT papers for IoT quality assurance appeared. The conducted research is based on the most recent guidelines on how to perform systematic mapping studies. A set of research questions is defined carefully regarding the quality aspects of the IoT. Based on these questions, a large number of evidence and research papers is considered in the study (478 papers). We have extracted and analyzed different levels of information from those considered papers. Also, we have classified the topics addressed in those papers into categories based on the quality aspects. The study results carry out different areas that require more work and investigation in the context of IoT quality assurance. The results of the study can help in a further understanding of the research gaps. Moreover, the results show a roadmap for future research directions.

INDEX TERMS Internet of Things, IoT, quality assurance of IoT, quality aspects, smart environments.

I. INTRODUCTION

Internet of things (IoT) is an evolving technological topic that gained importance recently due to its potential impact on our daily life and future societies. It is expected that in the near future our cars, consumer products, industries, and other everyday objects become collaborative via an Internet connection and robust data analysis. This combination of connective objects with data analysis capabilities could be an authoritative source for the intelligent decisions that could transform the way people live in the future. In 1999, the British technology pioneer Kevin Ashton introduced the term "Internet of Things" (IoT) to describe the ability of connected sensors on the Internet to bring new services [1]. Although the term was new, the concept has been around for decades when computer and networks combined to control and monitor devices.

The applications using the concepts of IoT are emerging tremendously day by day. These applications span a broad range of eHealth, security, entertainment, smart cities, defense and in many other necessary directions. Also, more objects are going to gain the ability of direct Internet connection in the coming years. As this range of connectivity and application expands, the IoT is going to affect our personal lives and public safety directly. With its expansion, the chance of system and network failure in IoT becomes higher than before. To this end, it is not acceptable to develop poor quality IoT systems that might cause loss of fortune, data or even life. For this reason, Quality Assurance (QA) is an essential and valuable issue for the IoT systems before the consolidation of these sensors, devices, applications, and systems go to the market. For example, to ensure accurate delivery timing, a shipment tracking system may use many sensors that communicate with many back-end software and many sophisticated algorithms. This system needs a robust QA process to validate the algorithms and workflow carefully.

In conventional software engineering process, the QA spans each step of the software development process, which aims to deliver software with minimum defects, meeting

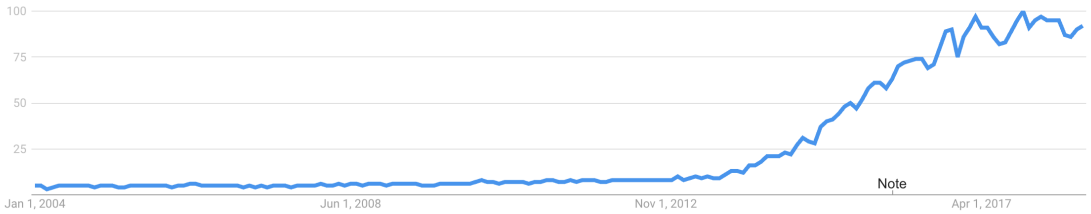

FIGURE 1. Google search trends since 2004 for terms internet of things and IoT. The relative value 0 to 100 represents search interest.

specific levels of functionality according to reliability and performance [3]. As with the case of an evolving technology, the QA aspect of IoT must be defined clearly and should be optimized. These QA aspects must also be improved periodically to meet the market and user expectations of many core principles, such as security, privacy, compatibility, reliability, and many others aspects. Moreover, it is the systematic pattern of all actions for providing and proving the ability of a software process to build high–quality products [4]. It also attempts to improve the development process from the requirement step till the end [5]. Thus, it improves software functionality, including safety and reliability. In fact, the QA for IoT does not deviate from this context. Ensuring the quality of IoT system is a more challenging process than ensuring the quality of software thanks to the interaction of different objects, usage of various platforms, configurations, and input domains. Ensuring the quality of this type of system requires a framework to evaluate each component individually and verify the expected output.

This paper provides the first comprehensive and systematic mapping study to organize and categorize the research evidence in the literature starting in 2009 when the early publication of the QA aspect of IoT systems papers started. The goal of the study is to identify the quantity, the results available, type of research and disclose available research opportunities for the future. The study also tries to answer important research questions in the context of QA for IoT. The most up–to–date methodologies and guidelines are used in the study to collect and analyze the related studies published. In doing so, methods and aspects of quality assurance are addressed in the study as there is no comprehensive and dedicated study in this direction. The study selects the evidence and papers published in the past starting from 2009. The paper aims to serve as a guide for future researchers by providing an unbiased mapping study of the published research and addressing several significant research questions (RQ).

The rest of this paper is organized as follows: Section II presents the motivation and the overview of related work for this study. Section III describes the methodology of the mapping study. Section IV presents the results and outcomes of the study followed by a discussion in Section V. Threats to the validity of the study are given in Section VI. Finally, Section VII concludes the work.

II. MOTIVATION AND RELATED WORKS

Since its existence, IoT gained more popularity, especially in the last decade. For example, Figure 1 shows the web search measured by Google search trends for "IoT" and "Internet of Things" words since the first search event until September 2018. The figure shows us the increasing interest in IoT owing to its influence and impact. This influence and impact on our life are expected to increase in the coming years. For example, Garter's Information Technology Hype Cycle [2] identified IoT as one of the emerging technologies in the coming decade as of August 2018. Figure 2 shows the expected time periods for the emerging technologies that have been identified by the Hype Cycle. Garter's Information Technology expects that IoT platforms will take around 5-10 years for entirely market adoption (See the red arrow in Figure 2).

Today's impact of IoT and its expectation for the future is beyond the term. A number of expectations about the potential impact of IoT on the economy for coming years are also available. For example, Cisco expects more than 24 billion connected objects to the Internet by 2019 [6], Morgan Stanley expects more than 75 billion by 2020 [6], and Huawei expects 100 billion by 2025 [7]. Of course, the financial impact of these connected objects on the future global economy is enormous. For example, McKinsey Global Institute expected this impact as much as 3.9 to 11.1 trillion US dollars by 2025 [8]. While these numbers are expectations, however, they can tell us the potential impact of IoT on the future.

As a reflection of this importance and expectations, many research groups are working on projects related directly or indirectly to IoT. As a result, many papers coming out from these research activities. To summarize these activities, collect these efforts, and identify research directions, few survey and mapping study papers tried to address IoT. However, due to the broad area of IoT's research, it is impossible to address those research activities and evidence in one study. To this end, researchers tried to do several survey and mapping studies for specific areas in IoT. However, these studies do not directly focus on quality aspects of the contemporary IoT systems and primarily does not discuss quality assurance and testing techniques in this context.

For instance, Stojkoska and Trivodaliev [9] performed a systematic study for the state–of–the–art applications for smart homes to identify the challenges and solutions for

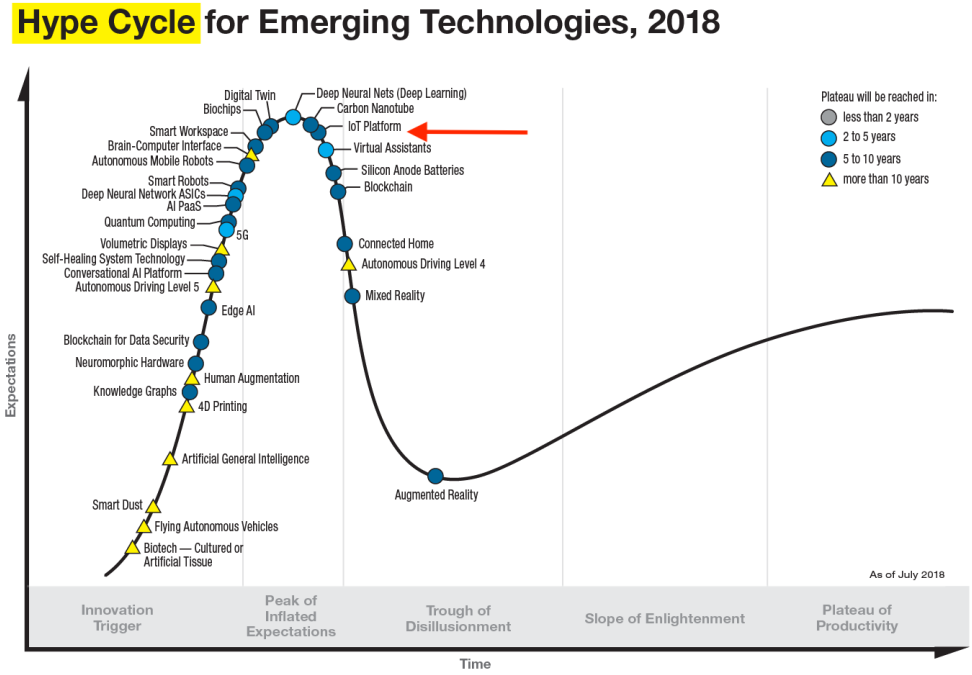

FIGURE 2. Gartner 2018 hype cycle of emerging technologies. Source gartner inc. [2].

integration into IoT environments. In these challenges, two QA–related aspects are discussed, namely interoperability and security and privacy. However, a discussion of quality aspects is not the primary goal of this study and these two issues are not analyzed to a broader extent. Also, another QA–related issues as challenged testing of the IoT system caused by a number of possible configurations, backward–compatibility testing issues or reliability of the system are not targeted in the study.

Ray [10] performed a systematic review study to survey the existing architectures of IoT applications that are solving real–life problems. Unfortunately, implications of the particular architectures for the quality of the solution is not analyzed systematically in this study. Ray discusses the reliability of the system on several occasions in the paper. Moreover, this discussion is not conducted in a focused and systematic manner, as it was not the main goal of the paper.

Atzori *et al.* [11] performed a systematic literature study on IoT from the communication and network perspective to show different implemented network paradigms, communication protocols, wired and wireless sensors used in the literature. This paper summarized the IoT–related state–of–the–art in the year 2010 and also mentions security and privacy concerns. Nevertheless, the paper does not discuss all other QA–related issues of IoT systems, partially because of its publication date and because it was not the primary focus of the study.

Perera *et al.* [12] performed a survey study to address the context–awareness issues in the literature from an IoT perspective. The paper discussed Quality of Context (QoC), having an impact on the quality of data processed by the IoT system. Further, security and privacy aspects of the IoT systems are discussed as the significant concern in context–aware systems. Possibilities of quality checking are also analyzed during categorization of context reasoning decision modeling techniques discussed in the paper. All these quality–related discussions are, however, driven by the primary analysis of the context–awareness IoT concepts and the discussion does not extend to other relevant quality–related areas.

Whitmore *et al.* [13] performed a study to report the state–of–the–art on IoT to identify the future research directions. The study looks into the general research direction rather than a particular area of research in IoT to identify the open research questions. Despite its broad focus, the study does not analyze QA–related issues and challenges of the IoT systems; in the challenges discussed in the study, security, and privacy are mentioned briefly. The study classifies the papers to three–level of categories. However, quality, testing, and verification of IoT systems have not been dedicated to any category in this study. Considering the fact that the paper is published in 2015, this is an implication of the design of the study and composition of search strings, as the significant number of IoT quality–related papers have been published from 2012, as we show in Figure 5 later on.

Gubbi *et al.* [14] performed a literature study to clarify the elements and architectures used for IoT in the literature. In the open challenges and future directions related to IoT systems quality aspects, Gubbi *et al.* mention energy efficiency, security, protocols, and Quality of Service (QoS). From these

aspects, only QoS and security are given broader floor in the analysis of the state–of–the–art.

QoS in IoT has been addressed by a separate systematic mapping study by White *et al.* [15]. Several quality models are surveyed and discussed and software product quality model ISO/IEC 25010 is discussed in this context. This systematic study focuses only on rather a narrow scope of QA when compared to the scope of this paper. The study by White *et al.* primarily analyzes papers dedicated to QoS, quality models, monitoring and Service Level Agreement, as the authors clearly state in the description of search methodology.

In all the studies mentioned above, in addition to the state–of–the–art research addressing, the research challenges have also been discussed along with the future directions for research.

Several systematic literature reviews were also conducted in the areas, which closely relate to IoT technology and in the verification and testing techniques. These can be related to the IoT systems. Bakar and Selamat [16] conducted a systematic literature review and mapping study of the verification techniques used in the agent systems area. The study covers various types of verification techniques used during the design, development and runtime phases of the project. Methods analyzed in this study are applicable to IoT systems in general; however, the study is, by its design, limited to the agent systems.

Model-based Testing (MBT) represents a significant stream in system verification techniques. MBT is subject of another recent systematic literature review by Khan *et al.* [17]. This study focuses on the empirical verification of MBT techniques and concludes that the overall quality of reporting details can be improved in the significant part of the analyzed studies. Despite the fact, that the discussed MBT techniques are applicable in the IoT domain, this study is not specifically IoT-focused and the majority of the analyzed papers are dedicated to standard software systems, or describe general MBT techniques.

Another related area is the early verification of SUT models created from the business requirements in a design phase of the project. A systematic literature review by Amjad *et al.* [18] discusses these verification methods in event-driven process chain, which can be used in the design of IoT systems. Despite this applicability, the study is not directly focused on the IoT domain, so it does not discuss IoT–related specifics of the verification methods.

As security and privacy are two of the most critical aspects discussed in the current IoT systems [19]–[22], authentication schemes and methods are assessed as part of the QA process. A recent systematic literature review by Velásquez *et al.* [23] analyzes and categorizes the current authentication methods applicable to IoT systems. The topic is closely relevant to the IoT security and privacy issues. However, the study is focused on the general analysis of authentication schemes and these schemes are not discussed in the IoT context. Also, testing and quality aspects are not included in the scope of the study.

Regarding the privacy aspect, anonymous communication systems are raising the user's interest in the recent period. A systematic literature review by Nia and Martínez [24] gives an overall picture of the state–of–the–art in this area and discusses its future research directions. In these directions, the quality of service is discussed; however, the work does not directly focus on other quality aspects. Moreover, the study is designed to analyze the general anonymous communication systems, which can be considered as a domain having an intersect with IoT systems.

In contrast to those mentioned systematic mapping or survey studies, this systematic mapping study looks directly into the QA aspect of IoT. As discussed previously, White *et al.* [15] addressed the quality of IoT from the service perspective that the application provides. The study considered the quality models that the ISO/IEC 25010 provides. The study tried to address three limited and straightforward research questions. In contrast to this approach, we are looking at the quality approach of the IoT from the system perspective. Here, we recognized those quality aspects considered when testing and evaluating IoT systems not necessarily from the service perspective. In line with this approach and with other research, the study tries to identify the different QA aspects addressed in the literature. In addition to the aims mentioned above, the study also seeks to answer many research questions regarding the QA aspects of IoT that have not been addressed so far.

III. METHOD

This section explains the method used in this mapping study. The applied method based on guidelines provided by Petersen *et al.* [25], [26]. The study first starts by identifying the scope. This research is only considering published papers that are related to the quality aspects of IoT. As can be seen in Figure 3, the study is composed of three main phases, each one of them has different stages. These phases are as follows:

1) **Searching Phase**: The research questions that determine the focus of the study are defined in this phase. Based on these research questions, the search string is designed. The search string has undergone different refinement process to identify and return the right papers.
2) **Filtering Phase**: Here, the relevant papers are selected, and their quality is assessed. The papers are excluded from the primarily selected papers based on the title, abstract, full–text reading and quality assessments.
3) **Mapping Phase**: The relevant data answering the research questions are extracted from the primarily selected papers in this phase. The extracted data from the selected papers are classified to visualize the outcome. Here, tables and illustrations are used. Threats to validity are also analyzed and presented in this phase with the aim to demonstrate the possible limitations of the study.

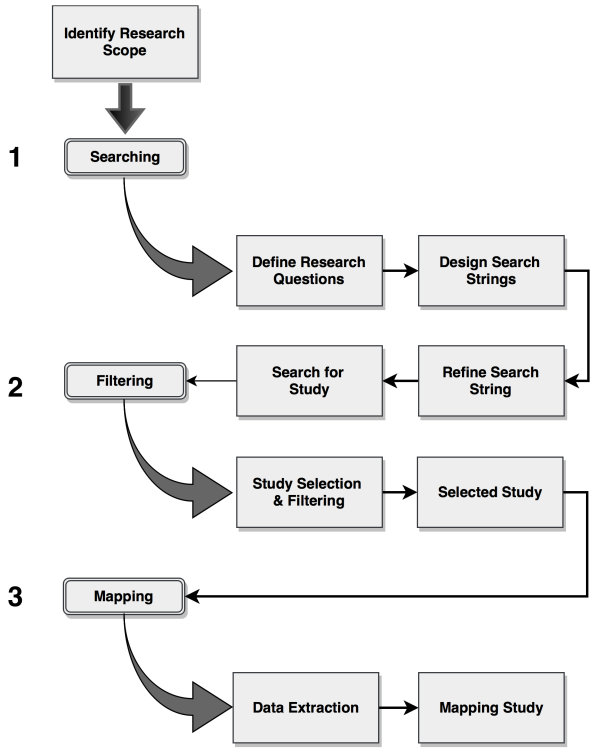

FIGURE 3. The systematic mapping detail steps.

The following subsections illustrate each of the phases mentioned above in further detail. From Figure 3, we can clearly identify the input and output of each stage in the methodology. Some of the stages are included together in one subsection for the explanation. For instance, before identifying the research questions, it is necessary to know the research scope first. Hence, we have included both steps in one subsection.

Within the answer of the RQs, (especially RQ3,4 and 6), we have also addressed the key research papers that illustrate the answers. In fact, the purpose of the paper is not to review each published paper in this direction; we are rather aiming to identify the future directions and the main aspects of research in addition to mapping them. This is considered a primary and essential study scope here.

A. RESEARCH QUESTIONS

For this study, multiple research questions have been raised, and different evidence examined. The study attempted to answer different questions that lead to a better understanding of the research notions and the future directions. Particularly, the study tries to answer the following questions:

- **RQ 1:** What was the evolution in the number of published studies over the last decade for QA of IoT?
- **RQ 2:** Which individuals and countries are active in conducting QA research for IoT?
- **RQ 3:** Which aspects of the IoT quality have been dealt with in previous research?
- **RQ 4:** Which principal testing techniques or concepts have been previously researched in the context of IoT?
- **RQ 5:** Which specific application domains of IoT systems have been investigated from a quality viewpoint?
- **RQ 6:** What are the current limitations and challenges in QA for IoT?

B. SEARCH STRATEGY

As previously mentioned, the scope of this study is the research papers related to the quality aspects of IoT. To define the right keywords for this scope this work considers the formal approach that establishes the Population, Intervention, Comparison, and Outcomes (PICO) criteria [27]. The Population represents the field discipline. The Inventions points to the methodologies and approaches to address the given issue. The Comparison considers available methods used for comparison. Finally, the Outcomes are the results for the readers and practitioners and help them with reaching the information.

Keywords can be categorized into three groups based on the research questions and the PICO. The primary group scopes the search for the QA in the IoT, such as ''quality assurance in the Internet of Things.'' Broadening the search the secondary group consists of terms and strings related to the testing domain. The last group is the application of the QA in the IoT, such as ''overload avoidance''. All these strings are combined to form strings with variations while combining search terms with logical AND and OR operators.

To form the final search string multiple preliminary attempts are made. The point of these attempts is to separate out QA from other domains not related to IoT. The intention is to narrow up the scope of the results. We have evaluated the search strings based on the quality of the returned results, which was assessed by the number of papers related to the scope of the study. For this quality assessment process of the search string, we have randomly selected 50 papers to search on IEEExplore and ScienceDirect and evaluated the search strings. The final test string was selected based on the results matching the expected scope. Also, we have assessed the quality of the search string based on the missing papers in the pilot set. Table 1 shows the result of each try of the search string including the results returned the number of missing papers for five attempts using different search strings.

As can be seen from Table 1, the first four sets of strings were excluded since they produce many irrelevant results. The reason is the use of general terms. Moreover, some terms such as ''quality assurance'' is employed in different ways based on the context. Finally, different terms were used, (quality assurance OR quality measure OR quality evaluation), which lead to revealing more papers. Next observation is that these terms were used with different conditions than quality assurance. As a result, alternative terms were used as well. Ensuring the coverage of RQs and the search breadth, additional aggregation of terms was performed, such as ''strategy, technique, method, approach, and tool''. Besides, we noticed that some of our pilot set of papers were missing in the first four sets of strings as can be seen in the table.

TABLE 1. Search string tries on the indexing data bases.

Keyword	Search Strings	# Results	# Missing Studies
Set #1	(”Internet of Things” OR ”IoT”) AND (”Testing” OR ”Quality”)	1,513	22
Set #2	(”Internet of Things” OR ”IoT”) AND (”Testing” OR ”Quality” OR ”Security”)	3,132	18
Set #3	(”Internet of Things” OR ”IoT”) AND (”Testing” OR ”Quality” OR ”QA” OR ”Quality Assurance” OR ”Reliability” OR ”Verification” OR ”Validation” OR ”Testware” OR ”Testing Data” OR ”Testbed” OR ”Performance” OR ”Security”)	3,1746	13
Set #4	(”Internet of Things” OR ”IoT”) AND (”Test” OR ”Tests” OR ”Testing” OR ”Quality” OR ”QA” OR ”Quality Assurance” OR ”Reliability” OR ”Verification” OR ”Validation” OR ”Testware” OR ”Testing Data” OR ”Testbed” OR ”Performance” OR ”Security” OR ”Privacy”)	3,560	7
Set #5	(”Internet of Things” OR ”IoT”) AND (”Testing” OR ”Quality” OR ”QA” OR ”Quality Assurance” OR ”Reliability” OR ”Verification” OR ”Validation” OR ”Testware” OR ”Testing Data” OR ”Testbed” OR ”Performance” OR ”Security” OR ”Privacy” OR ”Benchmark”)	4,698	0

For these reasons, the fifth set of the search string is used for this research.

The database selection was based on the guidelines and suggestions provided by [25], [26], and [28]. This led us to the IEEE Xplore, ACM Digital Library, SpringerLink, and ScienceDirect databases. During the searching, indexing, and sorting of a vast number of references, multiple duplicate references came to place due to the tight variations in the reference indexing in different databases. To avoid duplication, references manager software EndNote X7 was used. To further improve accuracy, Mendele v1.16 reference manager software is used to refine the results.

The study maps research for the past years starting from 2009 to 2017. Since then there has been increasing research trend. It should be mentioned that this study started in 2018. Thus, papers published in 2018 are excluded. Table 2 summarizes the number of research papers published in the mentioned period for each considered database.

TABLE 2. Numbers of published research.

Database	Search results
IEEE Xplore	9,175
ScienceDirect	6,030
ACM DL	1,288
SpringerLink	13,471
Total	29,964

C. PAPER SELECTION CRITERIA AND QUALITY ASSURANCE

The papers found by search strings were selected or excluded based on the title, abstract and full–text reading. During this selection, the quality of the papers was also taken into account. To increase the reliability of this process and to reduce possible threats of subjective selection, this process was conducted by the first and second authors and reviewed by the other authors of this study. Some papers could have been selected or excluded based on the title and abstract. Nevertheless, full–text reading was required for some papers to determine if the paper is relevant for the selection. In this mapping study, the papers fulfilling the following criteria were selected:

1) Papers discussing quality assurance aspects of IoT solutions in general terms.
2) Papers focusing on a particular aspect of IoT quality.
3) Industrial case studies, where quality aspects are discussed.
4) Methodologies for IoT quality assurance.
5) Papers with full text available in the selected databases.
6) Papers published with full text online from 2009 to 2017.

By quality aspects and quality assurance aspects we consider any aspect related to IoT solution reliability, correctness, and durability, together with security and privacy aspects. Following the guidelines provided by Petersen *et al.* [25], [26], papers meeting the following criteria were excluded:

1) Papers not exactly related to the scope of this paper, i.e., papers describing aspects of IoT other than quality.
2) Papers not presented in the English language.
3) Papers without full text available in the selected databases.
4) Books and gray literature.
5) Papers from non–peer reviewed sources.

Following the criteria mentioned above for selection and exclusion, we have considered many useful papers for our study. In fact, some of those papers were duplicated in the selected databases. For example, papers that appeared in ScienceDirect were also listed in ACM. Figure 4 shows the stages we followed to get the final set of the studied papers.

Following the robust methodologies of other mapping studies [29], [30], the selection process of the final papers underwent different filtering stages. The selection process started by searching for the papers in the IEEE Xplore, ScienceDirect, ACM Digital Library, and SpringerLink databases with the chosen search string in Section III-B. The outcome of this stage was 29,964 papers. The broad range of articles considering IoT in different parts of the text resulted

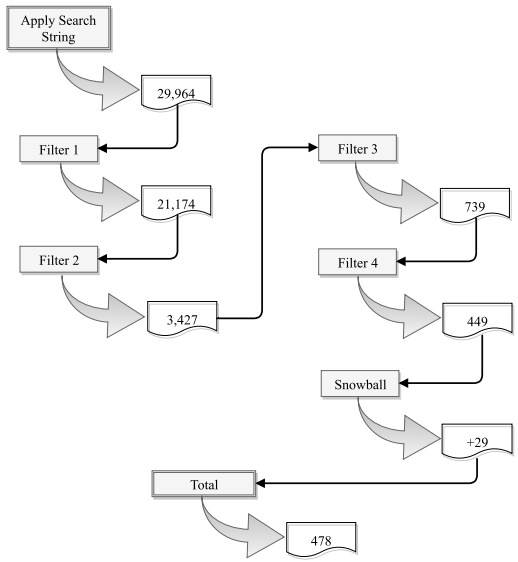

FIGURE 4. Filtering stages of the selected papers and the number of papers in each stage.

in this enormous number of papers. For example, we found many papers mentioning the usefulness of specific solutions for IoT applications in the conclusion section. However, none of these papers were related to the quality aspects of IoT. After retrieving the full list of papers, during the "Filter 1" stage, we removed the duplicates — the papers shared among the databases.

During "Filter 2" stage, we followed the inclusion and exclusion criteria described earlier. Here, the decision depended on the paper's title, reading abstract and if necessary reading the introduction section.

In "Filter 3" stage, we excluded other papers based on the full–text reading. Here, we excluded those papers without a particular method and experiments. We noticed that a huge number of papers was published only for illustrating possibilities of using IoT concepts in different applications. There is also a huge number of papers describing frameworks for IoT applications without performing any verification and validation experiment. For example, we noticed many papers describing security and privacy frameworks for IoT solutions. Also, we have also excluded pure review papers.

The final filtering stage "Filter 4" was related to the quality of the published papers. We noticed many papers with low–quality contents that have been coming from unreliable and non–reputable conferences. Another set of low–quality papers were coming from non–peer reviewed journals. For better reliability of the results, each author conducted a snowballing search for other possible missing relevant papers. Here, we have added 29 more papers. We end up with 478 papers that need to study for answering our established research questions. The online mapping resources and the full list of papers with all the details can be found in an online Spreadsheet.[1]

[1] http://bit.ly/2NDgpZk

D. DATA EXTRACTION AND ANALYSIS

In this stage of the study, we extracted the data from the selected set of papers. This stage aimed to map and classify the papers to enable us handling the RQs addressed in Section III-A. For better organization and systematic flow of the work, we have created a spreadsheet template (See Table 3) with all the relevant information about each paper. The sheet is an extended sheet with more details that have been originally presented by [25], [26], and [31]. For each paper, we filled the sheet with paper ID, publication title, publication year, authors' names and countries, venue, and the area of research. To extract and analyze the information from the sheet, we took two directions, manual and dynamic extraction. The first and fourth authors did the manual extraction and reviewed by the other authors. For double check and reliability, we have used mining and automatic text analyzers also for verification.

TABLE 3. Data extraction template.

Data item	Value
Study ID	Integer
Paper Title	Name of the paper
Author Name	Name of author(s)
Year of Publication	Calendar year
Venue	Name of publication venue
Country	Name of the country for each participated author
Area of research	Knowledge area of research
Research topic	Main topic or theme addressed by the study
Research problem	Research problem addressed by the study
Proposal	Proposed solution to the problem
Contribution	Main contribution of the paper
Evaluation process	Which benchmark adopted for evaluation?
Case study	Which case study used?

IV. RESULTS

By extracting the information from the selected papers, we can answer the RQs raised earlier. We have addressed the answer for the RQs individually. The following subsections illustrate the results of the study and the answer for each RQ. For abstraction, we used a short title for the sections that have been extracted from the main RQs.

A. FREQUENCY OF PUBLICATION (RQ1)

By analyzing the selected papers from 2009 to 2017, we can answer the RQ about the frequency of publication and also the evolution in the publication number. Figure 5 illustrates this evolution by showing the number of published papers per year. As we considered 478 papers for this study, we can observe that the average publication number per year is almost 53 papers starting from 2009 in which the first set of papers published.

Although the name IoT and the research related to it started in 1999, we can see that researchers have begun to publish papers about its quality aspects since 2009 actively. Figure 6 shows publication ration per year. In both Figures 5 and 6, we can see the number of published papers such that in 2016 there were 131 papers published which is almost

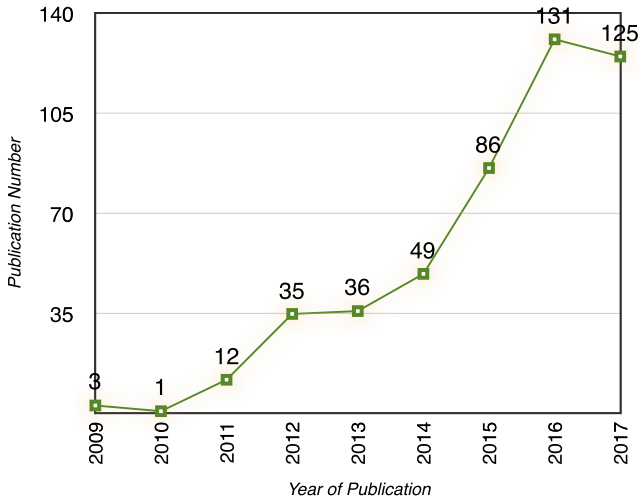

FIGURE 5. Publication per year.

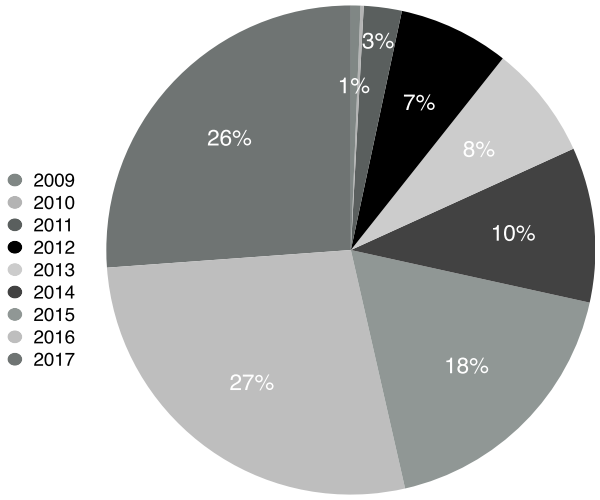

FIGURE 6. Publication ratio per year.

27% of the total published papers and in 2017; there were 125 papers published, which is almost 26% of total published paper volume. From the figures, it is clear that the interest of IoT quality aspects publication is increased in the research community after 2010. An important potential reason behind this increase is the emerge of many new IoT solutions for daily life applications and the influence of these applications in our daily lives.

It is also important to analyze the type of publication venues and also the ration of publication for each venue. This information can be extracted clearly from Figure 7. We can see that the majority of the papers (approximately 56%) published in conferences, while approximately 32% and 12% published in journals and workshops. Figure 7 also gives the analysis of publication type based on the venue per year. We note that the majority of the conference, journal, workshop papers was published in 2015, 2016 and 2017.

Another important observation from this analysis is the favorite and frequent peer–reviewed journals, conference, and workshops in which the papers have frequently been published. Figure 8, shows those favorite journals with the number of published papers for each journal. We have used Thomson Reuters Science Citation Index[2] for the journal abbreviation. The full name of journals can be found in Appendix A. Additionally, Figure 9 shows those active and popular conferences in which the related papers published. Note, we used conference abbreviation for the name and the full names could be found in Appendix B. It should be mention here that we considered a journal or conference to be popular when more than two related paper published in it.

We can observe from Figures 8 and 9 the targeted journals and conference by the author to publish papers related to the quality aspect of IoT. We can see that "Future Generation Computer Systems journal" with 17 published papers is the most popular journal in this field. Also, "Journal of Network and Computer Applications", "Wireless Personal Communications", and 'IEEE Internet of Things Journal" with 11, 6, and 6 published papers are the second and third popular journals in the field. The other set of the most active journal set is "Computer Networks", "Ad Hoc Networks", and "Computer and Electrical Engineering" with five published papers for each one of them. The journals with more than two papers published in this field form more than 48% (75/154) of the published journal papers and more than 15% (75/478) of the whole published papers.

Looking at the conference venues, we can see that "International Conference on Communications (ICC)", "IEEE World Forum on Internet of Things (WF–IoT)", and "International Conference on the Internet of Things (IoT)" are the most three active and targeted conferences by authors with 7, 7, and 6 published papers. These three conferences form more than 7.4% (20/269) of the conferences publication. Also, we noticed that those conferences with more than two published papers form more than 13.8% (66/478) of the publication. However, there are many papers related to the quality aspect of IoT published in individual conferences.

B. ACTIVE INDIVIDUALS, ORGANIZATIONS AND COUNTRIES (RQ2)

Within the answer of this RQ, we try to know those active researchers who published research papers related to any aspect of quality for IoT. By analyzing the frequent author names for the chosen population of papers, we found those active researchers. Here, we can define active researchers as those researchers (author/co–author) which are participating in more than one published paper. Figure 10 shows the ranking of those active researchers showing their full names.

As can be seen from Figure 10, "Habtamu Abie" from Norwegian Computing Center and "Ralf Tönjes" from "University of Applied Sciences Osnabrück, Germany" are the most active researcher by publishing seven and five papers. Also, as we can see from the figure, six researchers have published and participated in four papers. Based on our analysis,

[2]https://apps.webofknowledge.com

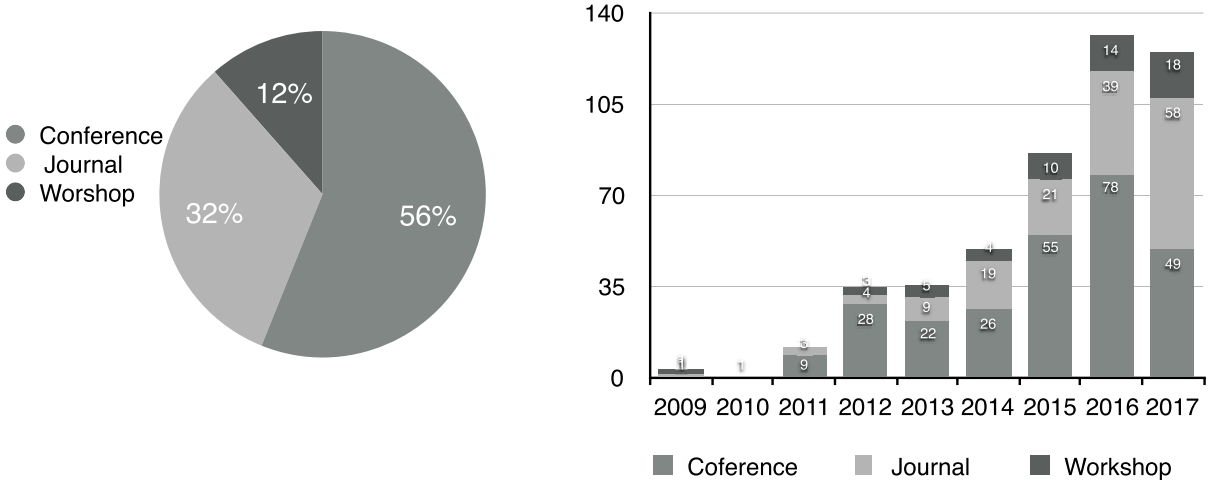

FIGURE 7. Publication number and ratio categorized by publication type.

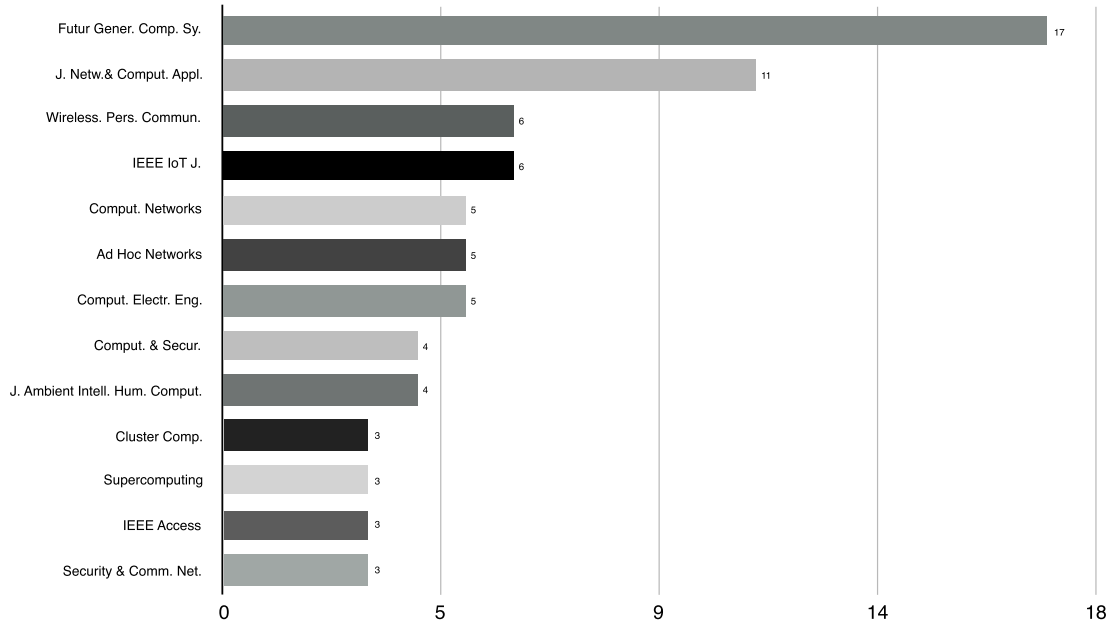

FIGURE 8. Amount of published articles vs. journal name.

we should mention here also that, 27 individual authors are participating in more than two published papers, 111 individual authors are participating in more than one paper, and 1416 individual authors are participating in one or more published papers related to different quality aspects of IoT.

Another valuable information can be obtained from the analysis of the extracted information from the papers is the list of participating countries. Figure 11 shows the result of this analysis. We took the participation of the countries based on the author's organization affiliation on each published paper. Each country is counted one time per paper. For example, if three authors from the USA participated in a paper, we count the USA for one time. Based on the results shown in Figure 11, we noticed that USA, China, and South Korea are the most active three countries in research publication related to different quality aspects of IoT by publishing 86, 73, and 38 papers respectively. These three countries together form more than 41% (197/478) of the whole publication. However, we also noticed other active countries that can be competitive in term of research numbers since they are so close to each other. These countries are India (37 papers), Italy (37 papers), United Kingdom (36 Papers), Germany (34 papers) and France (31 papers).

The output of this research question can reveal important pieces of information. The number of participated researchers in publication regarding different quality aspects of IoT

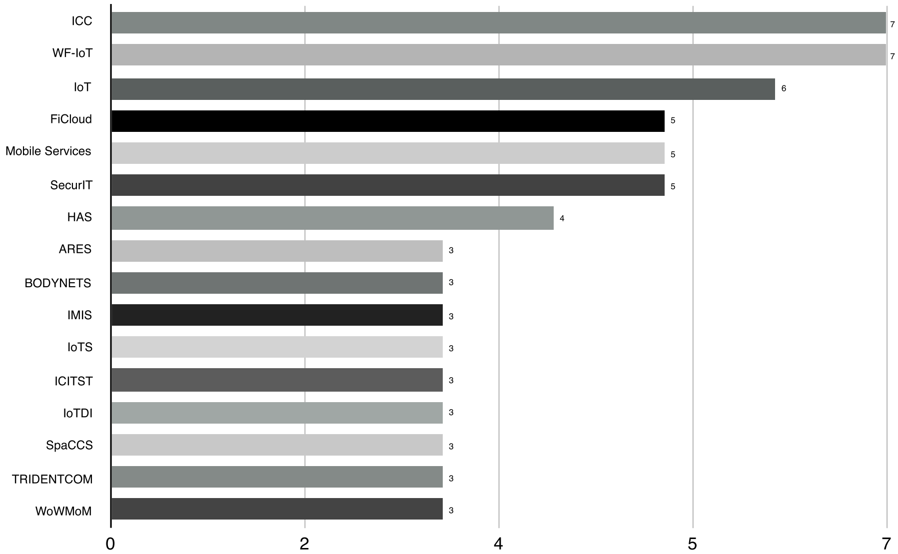

FIGURE 9. Amount of published articles vs. conference venues.

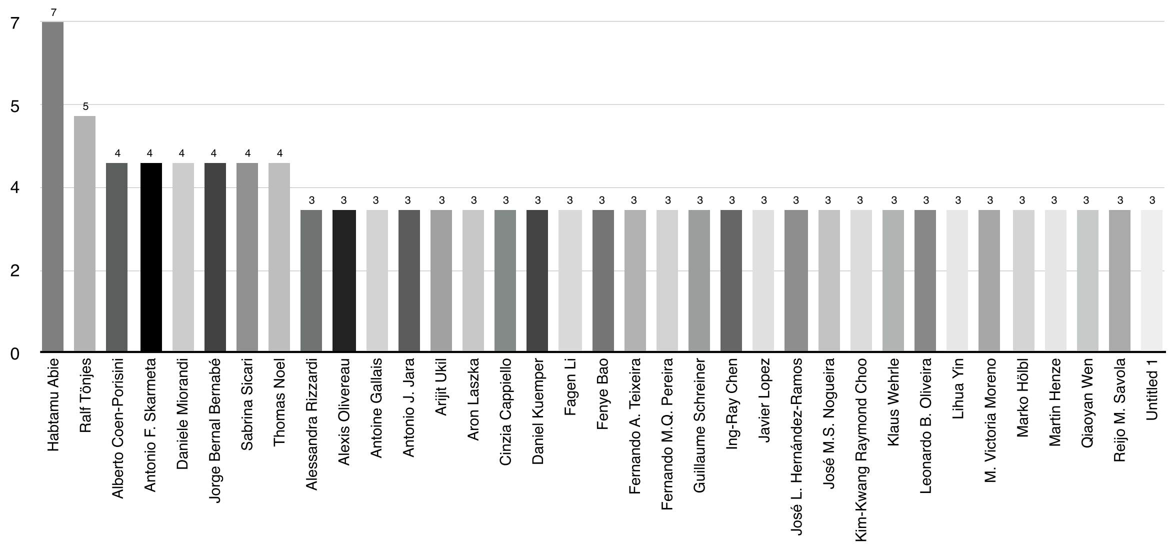

FIGURE 10. Active researchers.

shows a promising and important research direction. However, we noticed that there is no such active organization or research group that focusing on IoT quality.

C. ASPECTS OF IOT AND TOPICS ADDRESSED (RQ3)

It is impossible and unrealistic to cover all the detail issues, aspects, and topics related to the quality of IoT in one paper. However, we analyzed those selected papers and came out with a high–level classification that provides an essential overview of key aspects of quality for IoT. It should be mentioned here that these aspects are the aspects that were the focus of published research papers; however, many other aspects gain less attention in the published paper. Figure 12 shows a top view classification tree for the topics dealt with in the analyzed papers including the number of published papers for each topic.

1) QA STUDIES

QA studies are going side by side with testing studies. Generally, QA studies work on defining frameworks to assure the quality of selected aspects of IoT systems or discuss quality–related issues in general.

In this context, several studies that focusing on quality of *Cloud and big data* concepts can be identified (11 papers). This is a logical situation, as the cloud computing and big data concept closely related to a number of contemporary large IoT systems. On the network level, *Quality of Service (QoS)* is discussed by seven papers. The majority of papers

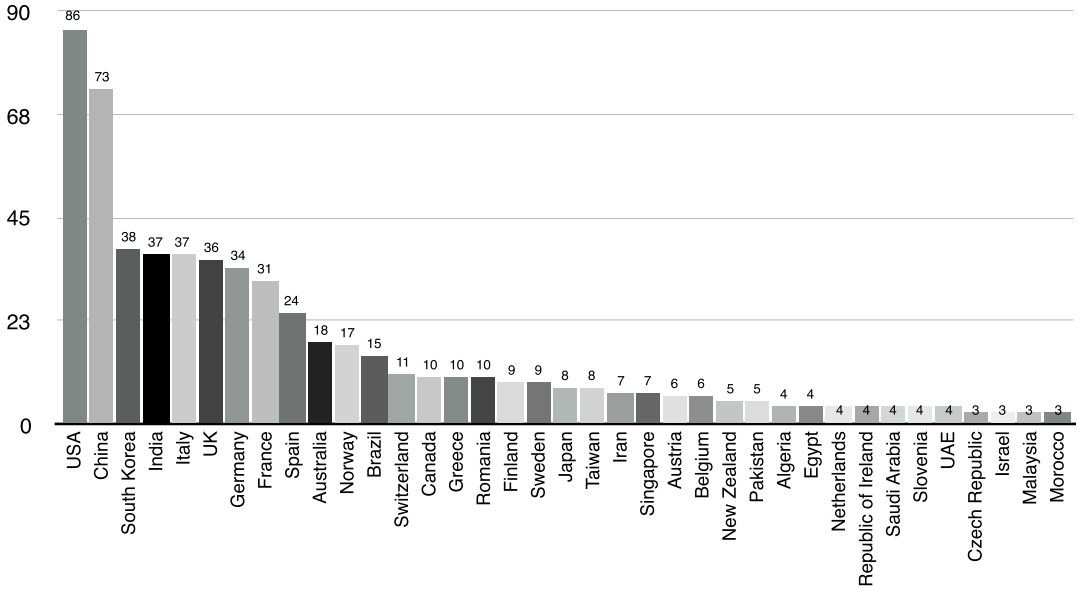

FIGURE 11. Active countries.

related to the QA studies category discusses various *Quality and Security challenges*, namely 68 papers in total. In this category, several subcategories can be clearly identified. The most concerns are raised regarding the security of the IoT systems (category *Quality and Security challenges*, 23 papers) and the topic is discussed from various aspects, including also user and data privacy (particular security and privacy studies are analyzed in subsections IV-C4 and IV-C3 of this chapter). Besides the security concerns, general *Quality management challenges* is the next frequently discussed area, covered by 19 papers. This area includes test management, metrics as well as organizational and line management aspects of IoT quality. Preparation of effective and accurate test cases with adequate coverage is important for the overall efficiency of the testing process and challenges in this area are also discussed (category *Challenges in test design*, 18 papers). Among the main challenges in the design of test cases, an excessive number of possible combinations to test and challenges in integration testing are reported. Besides the functional, integration and combinatorial testing, *Challenges in non-functional aspects* of the IoT systems were discussed by five papers. Finally, *Data quality challenges* were also subject of three analyzed studies.

As there are many applications in the IoT, it is impossible to determine general QA aspects. Here, methods of verification and validation are get involved in the research papers for specific purposes. The problem of underlying heterogeneous nature, platform variants, and type of IoT are some of those difficulties may arise when someone tries to define such a QA process. Though, few research studies attempted to follow this direction by introducing new methods for how to assure the quality of particular IoT service and platform.

Reetz *et al.* [32] described an approach to test IoT services based on the code insertion methodology to address the interaction with the physical world. To test the applicability and efficiency of classical approaches, the study emulated the IoT resources from an implementation perspective. Assuring the physical world and the real implementation of the IoT services and ''Things'' like sensors is not an easy task since it is difficult all the factors that affect the actual implementation in the emulator. To overcome this variation between real implementation and the emulator, Gimenez *et al.* [33] designed and developed a simulation environment for IoT services to implement multiple types of sensors. Here, to test the quality from an implementation perspective, the study uses a standard sensor database called Sensor Observation Service (SOS).

Assuring the quality of service for cloud platforms when interacting with a large number of things is an important approach. This quality assurance process will be an essential differentiation metric to choose among the many cloud providers available nowadays. For this reason, Zheng *et al.* [34] propose a quality model named CLOUDQUAL for cloud providers to assure the quality of service for IoT. The model can be used to measure, represent or compare the quality of different providers. The model takes six well-known quality dimensions which are reliability, availability, usability, security, elasticity, and responsiveness. While this study takes these six dimensions of quality, Ahmad [35] has just concentrated on the reliability models in more detail. The study focuses on the prediction and estimation of hardware and software reliability by deriving a probabilistic estimation of overall system reliability. Karkouch *et al.* [36] going further with this approach to develop a Model-Driven Architecture-based approach for quality. Here, the data consumer will be given an opportunity to choose and illustrate his data quality requirement through models and a user-friendly graphical model editor.

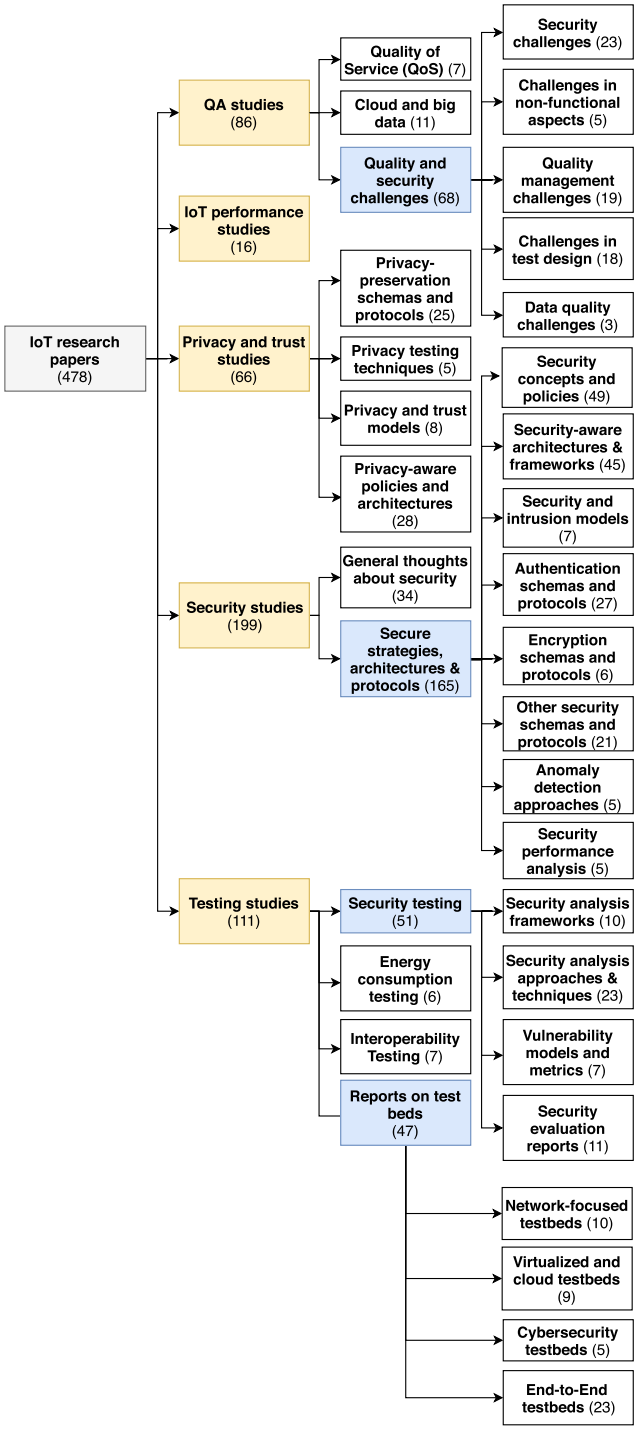

FIGURE 12. Top view classification for the IoT quality–related topics.

In the same way, Silva *et al.* [37] created a tool to evaluate the dependability of IoT applications, which is defined in the study as reliability and availability.

Apart from the definition of these quality models, there are few studies towards the assurance of different IoT services. For example, [38] worked on how to maximize the quality of information for IoT from a real-time scheduling perspective. Shi *et al.* [39] proposed an approach to design behavior patterns for the intelligent sensors in the IoT applications. The approach will help in the program implementation for these intelligent sensors which leads to improving the quality of service.

2) IOT PERFORMANCE STUDIES

For those analyzed papers in this study (18 papers in total), we noticed that performance studies are mainly focused on the performance evaluation of different IoT streams. Those streams are distributed on performance evaluation of specific IoT platform, security protocols, network infrastructure, or particular medical or industrial application. In fact, we can see that there is no universal and unique method for IoT performance evaluation as there are many forms of it. This shows the difficulty of IoT performance evaluation since there is a possibility to develop an entirely different performance evaluation strategy for each IoT stream.

In addition to the quality assessment of a particular application of IoT, performance evaluation is important for many other reasons. For example, it is essential to know which protocol can provide the appropriate level of security for an IoT system. This cannot be done without evaluating and comparing different protocols. To this end, few studies have been conducted to provide the appropriate performance evaluation and comparison process for this reason. For example, Rubertis *et al.* [40] proposed a performance evaluation process to compare two well–known security protocols which are IPSec and Datagram Transport Layer Security (DTLS). The process can be applied to different protocols to provide the design the most appropriate and secure protocol for end–to–end IP communications for IoT.

Performance evaluation is also used to assess the quality of IoT platforms (sometimes called framework). The IoT platform is a computational cloud middleware engine that manages the large number of data streams that coming from different sensors. Vandikas and Tsiatsis [41] assessed these frameworks based on the throughput of the system as well as stability concerning robustness (i.e., dropped connections) and memory consumption.

Performance evaluation processes have been designed specifically for individual IoT applications. For example, Yamada *et al.* [42] designed a performance assessment method for IoT-based e-Learning test bed. The evaluation is focused mainly on the Optimized Link State Routing (OLSR) protocol. For the evaluation, the throughput, PDR, hop count, delay and jitter metrics are considered.

3) PRIVACY AND TRUST STUDIES

In general, nowadays, Internet users need to use applications or devices that are connected to the Internet with a high level of privacy. This will enable the users to do daily activities with reliability and trust. In fact, IoT security is not far from this context, and it goes side by side with privacy. Users need to trust the IoT applications they use and to trust that the information generated by the IoT device is secure. In IoT applications, the number of connected devices could

be large, and hence there is a need for a robust design for this issue at the system level and also for each device.

In the analyzed studies, we have identified several main streams of research. Papers in the *Privacy–preservation schemas and protocols* category (25 papers) discusses various particular techniques, algorithms, schemas, and protocols to ensure data and user privacy in various IoT systems, covering IoT system users' personal data, as well as general business-domain data processed by the IoT system. Also, several particular testing techniques to assess the privacy level of IoT systems have been proposed (category *Privacy testing techniques*, 5 papers). Besides that, several attempts to model the privacy and trust problem in an IoT system by a formal technique were published (category *Privacy-aware policies and architectures*, 28 papers). These models can be further employed in the future development of privacy–aware architectures and various schemas an protocols. Finally, a considerable number of published studies discusses general processes, architectures, framework or policies to ensure privacy in an IoT system (category *Privacy-aware policies and architectures*, 28 papers). In contrast to *Privacy–preservation schemas and protocols* category, the privacy issue is described in the more broad context of particular policy or system architecture, including various case studies. These studies also include general discussions of the privacy concepts in IoT systems.

Generally, privacy and trust studies in IoT are swirling around defining privacy policy and trust management of different applications. This includes defining various models and protection frameworks for privacy to increase the trust perceptions in the IoT. In this context, Sun *et al.* [43] propose a privacy protection policy to protect the security of personal information on IoT systems. The policy is mainly based on the homomorphism encryption algorithm. Samani *et al.* [44] proposed another policy for privacy but this time by modeling the IoT system first as a Cooperative Distributed Systems (CDS). Here, the CDS model has been analyzed then the privacy protection is recognized as a form of "sensitive information" at the interactive level. In line with this modeling approach to privacy, Cao *et al.* [45] proposed another model for privacy but this time for data sharing in smart cities. The model covers the data abstraction and semantic, system architecture for data sharing, and strategies to enhance the transparency of data sharing without affecting the privacy. In fact, few research papers can be found in this direction, for example, [46]–[49].

Another set of research papers defined the location-based privacy for IoT systems. In this context, Liu *et al.* [50] proposed a strategy for how to protect the user's location when there is a personalized service inside the IoT application. The strategy also contains a pseudonym policy and a model for location-based privacy by protecting the user's location information acquisition.

Not far from these important areas for privacy, there are plenty of research papers that define privacy for specific applications of IoT. For example, Ukil *et al.* [51] defines the privacy issues within smart energy systems. Here, the study describes the uniqueness of privacy within smart energy systems from the smart meter (component of the smart energy management system) point of view. The meter could be a possible breaching activity for privacy when detecting in-house activities for example. Hence, the preservation of smart meter data would be essential. The study proposes a new scheme to minimize the privacy breaching risk in smart energy systems, called 'Dynamic Privacy Analyzer' scheme. In another study [52], the medical healthcare system is proposed for IoT to protect the privacy of patients' information in smart healthcare systems. Here, a private lightweight homomorphism algorithm is proposed that has been combined with an encryption algorithm.

4) SECURITY STUDIES

Security brings many concerns to IoT solutions e.g., [19]–[21]. In total, we identified 199 studies in the whole body of the analyzed papers corresponds to the importance of this topic. Besides the general discussions about various security aspects and consequences in the IoT systems (category *General thoughts about security*, 34 papers), 165 papers are discussing particular security strategies, architectures and protocols to ensure the desired level of security in the IoT systems. These studies span from reports on low–level security protocols to a description of general security–aware frameworks and security policies. Starting from the high–level conceptual descriptions, various *Security concepts, and policies* are discussed by 49 papers, which are covering a variety of particular IoT domains, for instance, Wireless Sensor Networks, Smart Homes, Healthcare or Wearables and personal devices. More detailed security–aware solutions, architectures, and particular frameworks are described by the second largest subcategory of the papers in this area (category *Security–aware architectures and frameworks*, 45 papers). Also here, these proposals are spanning among a number of various business domains and types of IoT systems, covering domains of Wireless Sensor Networks, Energy and Smart Grids, Healthcare, Smart Buildings, and Smart Homes as well as Smart Cars. Similarly, as in the Privacy area, models are also used to capture security issues and possible intrusion scenarios, seven analyzed papers were dedicated explicitly to the topic of *Security and intrusion models*. A considerable number of papers is dedicated to various security–related schemas and protocols. These studies cover *Authentication schemas and protocols* (27 papers), detailed presentation of *Encryption schemas and protocols* (6 papers) and *Other aspects of security schemas and protocols*, describing the problem from the broader perspective than only authentication or encryption mechanism (21 papers). Also, several *Anomaly detection approaches* are discussed (5 papers). We used this subcategory to distinguish papers which present a runtime anomaly detection approaches and algorithms, not formulated as specific security testing techniques, which are further analyzed in Section IV-C5. Besides, five papers were dedicated to *Security performance analysis* area, also

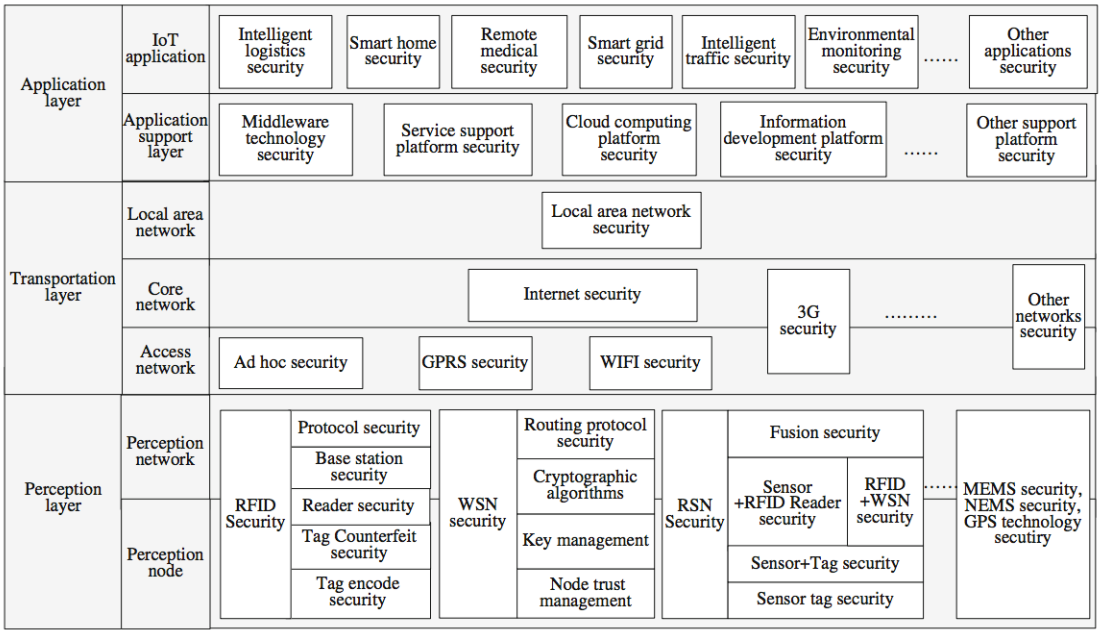

FIGURE 13. Security issue overview suggested by [54].

apart from specific security testing techniques discussed in Section IV-C5.

In IoT security, unfortunately, the variety of devices and vendors of "Things" make it hard to agree on how to implement security in devices. One cannot expect that existing security solutions that went through long evolution fitting to servers would also suit to IoT. IoT's have diametrical differences from centralized solutions involving client-server interaction. In this case, IoT is more similar to peer-to-peer (p2p) networks when it comes to security. A lot of research in p2p [53] addresses security and defense mechanisms in the distributed environment. However, p2p networks do expect peers to possess reliable hardware, which is not the case for IoT. In p2p networks we usually think of a distributed overlay network of computers, however, in IoT, we interconnect "small" things with limited processing power, which inhibits encryption and robust security measures. Vendors are pushing to reduce devices prices and rather focusing on sensors and data collection, which naturally leads to fewer efforts placed on security concerns. In IoT, there is no silver bullet to reduce security threats.

From our analysis of the published papers in this direction, we recognized many findings and multiple challenges left to address for IoT and security crosscuts most of them. Looking into various published studies in the literature, we noticed that they concern security issues in three layers. Jing *et al.* [54] summarized these layers as the perception layer, network layer, and application layer. Figure 13 depicts the detail of this three-layered roadmap.

The perception layer considers internal device security, such as particular sensor's concerns. The network layer looks at transmission, communication, and information security. Finally, the application layer involves the application–level perspective, such as service data security or security of support services. Some studies suggest to rather consider four layers in IoT, further dividing the application layer to an application and support layers, however, we consider both of these as a single layer.

There are various security perspectives we can consider delimited by the architectural layer, while a particular IoT design and features influence others. In the next subsections, we elaborate each layer in more detail.

a: PERCEPTION LAYER

On the lowest perception layer, the security concerns address information collection and transmission. Since the "things" possess low computation power, they have limitations on complex security protections. At this layer, we recognized that most of the studies are dealing with things equipped with Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN).

For the RFIDs, we can summarize the following findings:

1) RFIDs must prevent exposition of private information. Thus tags cannot be read by everyone, hiding meta information such as labeling, chips, antenna details, etc.
2) RFID signals need to be encrypted still preserving high-speed data transmission, not impacting energy.
3) Authentication and encryption allow both communicating peers to confirm the identity and preserve data confidentiality.
4) Cryptography can help with privacy and confidentiality of the system.
5) Side channel attack prevention should involve hiding or masking, to, e.g., prevent an attacker from

exploring energy consumption and thus identifying internal details.

Regarding sensors, we must be aware that data are in the public space. An attacker can bring laptop and harvest all the data. Many studies found that we usually need to:

1) Deal with key management, in particular, key distribution and consequent management to keep them valid.
2) Involve secret key algorithms to encrypt and decrypt messages.
3) Secure routing for clustering, data fusion, multi-routing, etc.
4) Integrate intrusion detection, monitoring the network and indicating odds.
5) Provide Authentication and Authorization control to provide node trust

Various sorts of attacks have been found at this layer in the studies:

1) A particular node can be captured and controlled by an attacker, leaking information or group communication, which threatens the entire subnet.
2) A fake node can appear publishing false data; the receiver may get confused ignoring real data.
3) This can lead to large processing on nodes draining battery charge leading into the fast discharge and network failure.
4) DoS attack can target a particular processing node eventually bringing down entire infrastructure.
5) Timing attacks are analyzing the node processing of encryption to steal device key.
6) Routing attacks are sending, tampering or re-sending routing information, possibly making loops impacting delay or even flooding the infrastructure.
7) Replay attacks push fake messages, accepted in the past, to a processing node, expecting to gain to trust impacting certification and authentication. Side channel attack can be issued towards encryption devices.
8) The side channel information can be exposed to the process of the device operation, such as time consumption, power consumption, etc..
9) Most of IoT solutions expect a uniform distribution of authentication. however, a mass node authentication can occur.

b: NETWORK LAYER (TRANSPORT)

General networking security solutions address the middle layer. However still many possible attacks exist that we live with on nowadays Internet. Security problems can appear on communication network threatening data confidentiality and integrity. The common threats are illegal access, eavesdropping information, privacy damage, integrity damage, DoS attack, man–in–the-middle attack, virus invasion, and exploit attacks.

This layer must also deal with the variety of sources and compatibility; existing security approaches emphasize human–computer interaction, while in IoT the attention it to machine–to–machine interaction. Support for various, heterogeneous endpoints only brings a high potential for errors and security vulnerability. Each device needs to be identified in the network, and the mass authentication can lead to congestion, with attacker potentially targeting the authentication server. Here, devices are often designed to harvest data and expose them; hackers can focus on retrieval and collect private information.

Several studies suggested that this layer provides an environment for access, transmission, and store for the perception layer. It can be further divided into three sub-layers with specific functions, such as access, core, and local area networks. The access network deals with wireless connections (WiFi, Adhoc, GPRS, etc.). The core network is responsible for the data transmission. The local area network prevents data from leakage as well as applies server protection, e.g., involving network access control, denial of malicious code execution and removal of unused services. In fact, many studies found that DDoS is the most common sort of attacks in IoT. However, the threats found so far can be summarized as:

1) Unauthorized access
2) Information theft or manipulation
3) DDoS attacks
4) Virus /Malware attack
5) Scalability of authentication

c: APPLICATION LAYER

The particular domain strongly influences the top layer. For instance, in information systems, security authorizations are usually associated with roles, these can be context–sensitive based on particular data, location, time or combination of these. A particular service may require a given role to perform a given service. Specific users or applications granted a role based on their status or setting. In IoT generally, no standard exists and will differ for domains, such as smart homes/medical sensing systems, community, cities, etc. In general, this layer needs to recognize valid and spam data and filter them.

This layer may have an internal subdivision to application support layer that is usually more general, including middleware, machine–to–machine can be organized in different ways according to different services. Usually, it includes middleware, platforms, such as cloud computing and service support, etc. Since we expect big data, middleware addresses scalability and elasticity of services. The application layer most likely involves integration of business logic or the high–level system. It deals with privacy protection with fingerprinting, watermarking, etc.

Several studies found that at this layer we must deal with the following:

1) Authentication to identify users
2) Access permission to verify their right to perform an action
3) Capability to deal with big data, as failed to scale leads into data loss, and possible failure.
4) Heterogeneous system security concerns, for instance, buffer overflow.

5) TESTING STUDIES

Area of studies focused directly on testing techniques and testing infrastructure is dominated by various reports on *Security testing* approaches, techniques and frameworks (51 papers) and various *Reports on test beds* created during previous IoT projects (47 papers). In the set of analyzed papers, we also identified another two related areas: *Energy consumption testing* techniques and reports, discussed by six papers and *Interoperability testing* techniques, being subject of seven relevant studies. We consider coverage of these two aspects relatively low due to their importance. Energy consumption aspect of the IoT devices has the direct impact on the reliability of the service, as well as on security aspects of the solution. Energy supply constraints might lead to the implementation of insufficient lightweight security algorithms and also to the impossibility to update IoT devices online, practically resulting in heterogeneity of variants of the devices deployed in production, causing combinatorial testing challenges later on during updates and maintenance of the system. Also, interoperability of the devices is one of the important aspects in the IoT systems, from the point of system reliability, as well as a possibility to integrate the particular solution with other IoT systems.

In the *Security testing* area, several types of studies can be identified. The most of papers, 23, discuss particular *Security analysis approaches and techniques*, spanning from various ethical–hacking techniques with the goal to detect a security flaw in an IoT system to approaches to detect security flaw based on analyses of collected system behavior data. Generally, these techniques can be based on *Vulnerability models and metrics*, which are presented explicitly by seven analyzed studies. On top of these reports, technical implementation of particular *Security analysis frameworks* has been described in 10 papers. Differently to cybersecurity testbeds classified as a separate category, these studies focus on technical frameworks to conduct the security testing process, rather than on particular configuration of the testbed to execute these tests. Finally, 11 studies presents various *Security evaluation reports*, for instance in the Healthcare [55] or Sensor Networks [56] areas.

The most of the *Reports on test beds* describe a general–purpose testbed for an IoT system, allowing End–to–End testing of this system (*End–to–End testbeds*, 23 papers). However, also specialized testbeds for the network–level testing have been described in ten studies (category *Network-focused testbeds*). Specifics of security testing leads to the construction of special *Cybersecurity testbeds* for this purpose, and these projects have been described in five papers in the analyzed sample. Finally, a virtualization and cloud deployment trends can be clearly identified also in the sample of testbed reports (category *Virtualized and cloud testbeds* represented by nine papers).

The IoT domain is considered as a source of testing challenges [19]–[21] which we found in contradiction to the fact that ratio of the papers dedicated directly to the description of a particular testing technique specifically designed or adapted to IoT context is relatively small. Here, the research streams discussed above are the exceptions.

Two possible scenarios can explain this situation. First, the IoT domain is not specific enough to justify the domain-specific testing technique. Second, the area of testing techniques that specifically designed for IoT solutions is significantly not covered in the current literature, and the definition of these techniques is pending as a future research task.

Due to the analysis of the papers for this study and our previous experience and knowledge of the IoT domain, our subjective conclusion is that the former scenario is much more probable. Concerning current literature coverage of IoT-specific testing techniques, the following issues have been classified as significant from QA point of view:

1) Security issues
2) Privacy issues
3) Performance issues
4) Interoperability, missing or insufficient standards, proprietary standards vs. Internet standards
5) Legislation issues
6) Behavior of the system under a limited network connection
7) Integration issues
8) Number of various configurations and types of the end nodes, making the solution hard to test using all these combinations
9) Focusing on test efforts efficiently to important aspects and critical parts of the infrastructure regarding the security and privacy.

These topics are widely discussed in the related literature, as our mapping study show. Nevertheless, for the other aspects rated as important, we found rather little direct literature support (except the areas mentioned in this subsection).

Already existing testing techniques can cover some of the areas, and hypothetically, it is possible, that particular technique is not explicitly needed. As an example, we can discuss issue 8 in the above mentioned QA points. One can imagine current Constrained Interaction Testing (CIT) discipline [57], covering the problem. But would it be efficient not reflecting specifics of the IoT domain at all in the construction and application of a testing technique? For this issue, more efficient Feature Models as a test-basis for CIT, explicitly describing the IoT infrastructure can be created, including the modeling constructs added specifically to cover unique situations in IoT solutions. Also, as the variety of platforms and versions of IoT firmware makes the CIT problems extensive and here, new constraint solving techniques have to be invented, as the current techniques do not perform efficiently.

Another example can be the issue 6 in the above mentioned QA points. Trivially, these situations can be covered by existing testing techniques for workflow testing (Process Cycle Test for instance [58]). However, such a process would be

very probably sub-optimal. Extending an underlying model by a reliability meta-data allowing a simulation of node outage and redefinition of the technique to address this problem directly can be a typical example of the coverage we have in mind and which remains an inspiration for further research directions.

D. PRINCIPAL TESTING TECHNIQUES HAVE BEEN PREVIOUSLY STUDIED (RQ4)

Several areas can be tracked in the analyzed papers. Model-based testing as a primary principal research stream in software development quality assurance is also represented in the case of testing techniques discussed in IoT context. However, underlying models and process of test case generation differ. As a modeling layer, we can find examples of semantic description of IoT services [59] or UML class and object diagrams combined with Object Constraint Language (OCL) [60].

The semantic description of IoT services and subsequent derivation of the test cases from this description proposed by Kuemper *et al.* [59] looks like a promising concept; however, issues may arise with keeping these semantic descriptions detailed enough and up to date with the SUT. More extensive automation of gathering these semantic descriptions from the actual state of the SUT would enhance the method further and might represent prospective future direction. The concept of MBT as a service for IoT platforms by Ahmad *et al.* [60] is relying on an established MBT approach based on OCL. The concept is valid, however, to achieve better efficiency, the MBT technique can be further extended to focus on the interoperability problem more systematically. One possible option is adding SUT configuration variants as an input into the MBT process pipeline presented in the study.

The Model checking is another principal testing technique, whose adoptions and applications are present in the analyzed sample. As underlying models, we can find formal specification languages [61] or Computation Tree Logic (CTL) [62]. A study by Choe *et al.* [61] proposes a modeling of a dynamic IoT system by a specialized formal specification language based on δ- Calculus and subsequent verification of dependencies among the movements in the IoT system using the Geo-Temporal Space (GTS) Logic. This proposal is primarily focused on modeling and verifying the dynamic properties of the systems, whose devices are mobile in a geographical environment. Despite the concept is promising, its verification on real examples is not presented in the study. Jia *et al.* proposed model–checking approach for publish–subscribe systems, which is directly applicable also to IoT systems, as this domain overlaps with IoT. The system is modeled by CTL and the model can be generated from actual SUT code. However, information about the experimental verification of this concept is not satisfactorily provided in the paper.

Runtime verification as a related area had also its representative in the sample [63], [64]. However, it seems that this area is rather emerging in the IoT context. A study by Torjusen *et al.* [63] explores the possibility of runtime verification of adaptive security in IoT systems, however, the paper focuses specifically at eHealth applications and does not explicitly discuss possible extensions to other types of IoT systems and other application domains. González *et al.* [64] propose runtime verification of behavior–aware mashups (web applications combining content from multiple sources and providing access to these sources via a unified user graphical interface), which can be considered as broader application scope in the IoT context. Unfortunately, broader experimental results reporting on the application of this proposal in an industry project are not presented in this study.

Model checking and Run-time verification, Reliability models, shall also be mentioned. Regarding this area, the first work related to IoT is focusing primarily on the combination of hardware and software [35], [65].

Ahmad proposed a method to derive probabilistic estimates for the reliability of software and hardware in an IoT system [35]. In his approach, he combines Numerical Finite Element Models (FEM), statistical techniques and Monte Carlo simulation. Unfortunately, the evaluation of this proposal is limited only to two relatively simple use cases from a telecommunication IoT system. Yong-Fei and Li-Quin proposed comprehensive evaluation model of the reliability of IoT systems. Proposed evaluation is based on the Analytic Hierarchy Process (AHP) method and might be promising for further applications, however, provided an experimental example presented in this study is rather limited. Analysis of behavioral patterns of the system on software level with the goal to improve the reliability of the system has been also explored by Shi *et al.* [39]. As the paper is limited to the mote (a wireless transceiver also works as a sensor device) IoT applications, exploration of this approach in other IoT domains might represent a prospective future research area.

Also, Usability testing of IoT solutions can be identified as already covered by the first works, including the specific usability testing framework [66]. In the related area, discussion on users' perception of IoT quality of service has been conducted [67].

The usability testing framework by Wittstock *et al.* [66] aims at expressing underlying security in an IoT system to support user tests. In this support, virtual reality is used, which makes this concept innovative. The study focuses on smart home and smart office domains. Unfortunately, applicability on other domains of IoT systems (e.g. manufacturing or smart city) is not explicitly discussed in the paper. Shin examined Quality of Experience (QoE) of the users with the IoT system, namely the relation between system and data quality and subjective perception of IoT system by its users, satisfaction, and utilization of the system. Despite the study represents a valid approach to evaluate the user experience with the IoT system, its limit might be too general formulation of the questions answered by the users to evaluate the QoE.

Another research and development stream, which is significantly represented in the analyzed sample is related to the

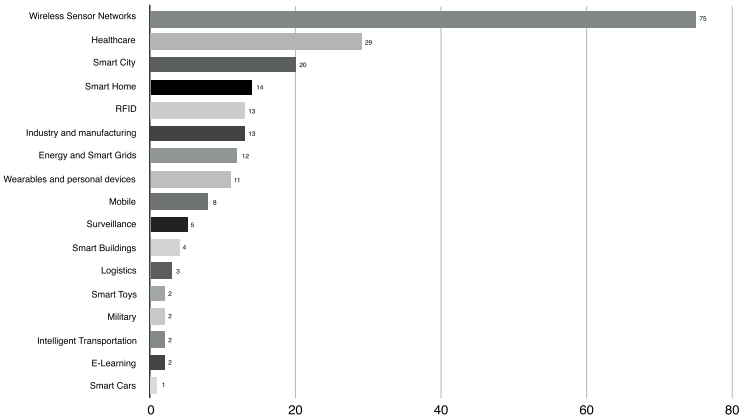

FIGURE 14. IoT application domains discussed in the analyzed papers.

construction of efficient test environments (or test beds) for IoT solutions. Simulation of the devices is a logical option in this area for instance [33]. In the analyzed samples, we can find examples of stand-alone tested setups [68], distributed architectures [69], or crowd-sourcing based test beds [70]. Also, the first testbed characterization works can be found, for instance, [71].

A study by Papadopoulos *et al.* [71] discussed contemporary testbed construction approaches in the area of RFID systems. The study analyzes and classifies the literature related to the RFID testbeds. However, a more detailed analysis of the literature is not presented. Instead, the authors focus on detailed analysis of particular FIT IoT-LAB testbed.

Regarding the focus on specific IoT solutions, examples of specifically-designed testing techniques can be found. For instance, the data-driven testing methodology for RFID systems presented by Lu *et al.* [72]. The proposed method is verified by mutation testing technique; however, a case study from a real industrial project would give more insight into the practical applicability of the method.

A particular area is protocol testing, which represents a significant part of the analyzed sample. The methods are varying here. For instance, statistical verification [73], formal verification [74], conformance testing [75], or randomness testing [76].

Bae *et al.* proposed a statistical verification of process conformance in an IoT system based on log equality test [73]. The concept seems promising and is experimentally verified by an application on data from a system supporting steel manufacturing processes. To draw more conclusions about the efficiency of the method, more results from other application domains shall be provided. Silva *et al.* [74] proposed formal verification methods for cross–layer protocols used in IoT systems. However, the method is primarily designed for WSN systems, and the study does not discuss possible applicability to other IoT domains. Also, another protocol testing approach proposed by Xie *et al.* [75], based on conformance testing is focused primarily on WSN IOT systems. A study by Gohring and Schmitz proposes randomness testing approach for physical layer key agreement and show preliminarily promising results; however, verification of the method on larger test data sets shall be made.

E. SPECIFIC DOMAINS OF IOT SYSTEMS HAVE BEEN INVESTIGATED FROM A QUALITY VIEWPOINT (RQ5)

To answer this research question, we investigated particular domains of IoT applications, which were discussed by the analyzed papers. Out of 478 studies, 216 papers were directly dedicated to particular IoT application domain. Figure 14 presents an overview of these domains with respective numbers of papers.

Among the analyzed papers, *Wireless Sensor Networks* is the IoT domain most frequently discussed from the quality viewpoint. From the analyzed sample, 75 papers are related to this area. Majority of these papers are discussing security issues (56 papers in total).

Regarding the number of studies, the Wireless Sensor Networks domain is followed by *Healthcare* systems discussed by 29 papers and *Smart City* domain discussed by 20 papers. Also, Smart Home systems (14 papers), various RFID tracking systems (13 papers) and IoT–aided manufacturing systems (13 papers) have been discussed from the quality viewpoint quite frequently.

Some areas are covered to marginally; this can be because the application area might be marginal from a research viewpoint, as *Smart Toys* or *E-learning*, or, research and development in the area is traditionally hindered from publication for security or competition reasons (*Military* or *Smart Cars*).

In the categorization presented in Figure 14, we made *RFID* and *Logistics* as two separate categories, as RFID systems can also be applied in other domains than logistics only. In the analysis of published studies, we also distinguished between Smart homes and Smart buildings. We understand *Smart homes* as personal houses and apartments employing IoT devices to enhance the quality of living and security of

these personal homes. In contrast, we use Smart buildings category for public or office buildings, benefiting from various IOT infrastructure to increase the quality of the workplace, secure conditions or to optimize the usage of these buildings.

We also distinguished *Smart City* category from *Intelligent Transportation* IoT–based systems. Intelligent Transportation focuses on optimization of general transport processes based on real–time data and this discipline spans beyond the IoT technology. The concept of Smart City is broader and employs the IoT technology to improve the quality of urban life and make the current cities more sustainable. IoT solutions, in which *Mobile* devices and smartphones interacting with the system plays a central role are also given a special category in this analysis.

F. CURRENT LIMITATIONS AND CHALLENGES IN QA FOR IOT (RQ6)

In fact, we can find many limitations and challenges from addressing the RQ4. However, here, we can add more content to that discussion. Currently, IoT system designer usually deals with a dilemma whether to equip the solution with a lot of low-cost nodes (e.g., sensors), which deteriorate security or rather high-performance nodes capable of encryption or advanced features impacting the overall costs. One must be aware of lightweight mechanisms due to the limited performance of nodes/sensors, which gives preference to light encryption and authentication mechanisms that are easier to break. When designing one part of the system, we must consider that the underlying network is asymmetric. For instance, a network terminal is performant, while gateway nodes lack the performance. At the same time activities must be well coordinated no matter the endpoint, which also requires efficient endpoint management, usually involving assigning them keys. Since the IoT system applies to a variety of domains, one must remember that the particular context and domain strongly impacts the potential security concerns, further affecting any of the IoT layers.

In addition, there are two aspects of the IoT solutions, which can make research and development of proper quality assurance methods more challenging. The first is heterogeneity of IoT in general. Here, various types of solutions are produced (for instance sensor networks, smart home, intelligent transport, personal devices and much more), which could require specific testing methods. The second is the necessity to focus on various levels of the solution, including the physical layer, protocols, firmware and software of a particular device and end-to-end functionality from user's viewpoint. In this aspect, IoT differs from classical software testing, where we usually consider physical and protocol level as standardized and thoroughly tested already.

V. DISCUSSION

As can be readily observed from data, security and privacy aspects of IoT solutions are amply discussed and many alternative approaches proposed. These two aspects remain the primary challenge of IoT solutions, especially for devices, where ensuring of security aspects is the principal problem (for instance solar-powered devices with implied lightweight security algorithms or devices located in hardly accessible areas, where physical intrusion detection can be tricky). Also, limited software and firmware updates can contribute to this problem.

Besides security and privacy aspects, the relatively low number of papers is dedicated to specialized testing methods customized for IoT specifics. We can observe classical established testing research and development streams as model-based testing or model checking is applied to IoT domain, but, in contrast to the volume of the business potentially enabled by IoT, the number of relevant papers is surprisingly low.

Also, interoperability of the devices, protocols and a large number of their possible combinations to test shall, according to our opinion, be supported by more extensive research.

Development of quality assurance methods for IoT seems a bit reactive, following the technology development, which is enabling widespread and evolution of various IoT solutions. We consider this as a natural process, since a certain extent similar to the development of software quality assurance methods.

According to the state of the art, there are several areas, which are prospective for further research and development in IoT quality assurance methods. First, security and privacy issues shall be dealt with. Analyzed data show that a relatively high number of studies covers these topics. Nevertheless, the problem of security and privacy is still considered as not solved satisfactorily.

The next area is the interoperability of IoT devices. Here, we consider two streams as perspective: (1) IoT specific methods for integration testing and (2) methods how to combine efficient sets of device and infrastructure parts variants and versions, regarding heterogeneity of IoT solutions and sometimes even impossibility to upgrade or update to a newer version of device firmware or software. Adoption of Current combinatorial interaction techniques [57] with the examination of their efficiency [77] seems like a prospective way to solve problems arising from an enormous number of combinations of particular device variants.

The next area relates to a general testing strategy. For software projects, many guidelines on how to determine the intensity of testing for particular parts of the system under test and how to choose the best testing techniques to exist. The same shall be developed for IoT projects, respecting all specifics of IoT infrastructures.

Another area worth exploring is the development of specific test design techniques for testing of IoT solutions under limited network connection and related technical constraints. As users' dependency on Internet and IoT services grows continuously, this area is also becoming more relevant.

Finally, in the area of modeling of the system under test, suitable models for the semi-automated or automated generation of test cases shall be developed and verified in the practical model-based testing process. Differently, to

TABLE 4. List of active journals with abbreviations.

Acronym	Journal Full Name
Futur Gener. Comp. Sy.	Future Generation Computer Systems
J. Netw.& Comput. Appl.	Journal of Network and Computer Applications
Wireless. Pers. Commun.	Wireless Personal Communications
IEEE IoT J.	IEEE Internet of Things Journal
Comput. Networks	Computer Networks
Ad Hoc Networks	Ad Hoc Networks
Comput. Electr. Eng.	Computers and Electrical Engineering
Comput. & Secur.	Computers & Security
J. Ambient Intell. Hum. Comput.	Journal of Ambient Intelligence and Humanized Computing
Cluster Comp.	Cluster Computing
Secur.& Commun. Netw.	Security and Communication Networks

TABLE 5. List of active conferences with abbreviations.

Acronym	Conference Full Name
ICC	IEEE International Conference on Communications
ICC	IEEE International Conference on Communications
WF–IoT	IEEE World Forum on Internet of Things
IoT	International Conference on the Internet of Things
FiCloud	IEEE International Conference on Future Internet of Things and Cloud
Mobile Services	IEEE International Conference on Mobile Services
SecurIT	International Conference on Security of Internet of Things
HAS	International Conference on Human Aspects of Information Security, Privacy and Trust
ARES	International Conference on Availability, Reliability and Security
BODYNETS	International Conference on Body Area Networks
IMIS	International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing
IoTS	International Internet of Things Summit
ICITST	International Conference for Internet Technology and Secured Transactions
IoTDI	IEEE/ACM International Conference on Internet–of–Things Design and Implementation
SpaCCS	International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage
TRIDENTCOM	EAI International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities
WoWMoM	IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks

classical software systems, these model shall also include physical and protocol layers, as these are much more heterogenic in the case of IoT solutions.

VI. THREATS TO VALIDITY

Mapping study usually suffers from threats to validity. During our study, we have counted several threats that need to address. In fact, we have tried to eliminate the effect of these threats on the quality of the results and the outcome of the study. For these elimination activities, we decided to follow well–known methods to design our experiments. Some of those significant threats can be addressed here with our elimination mechanism.

First, the selection of 100 percent related paper cannot be guaranteed although we have selected most of the papers that are within the scope of this study. We have tried to eliminate the effect of this threat by selecting and examining several search strings and conducting a pilot and snowball searches for several papers.

The second potential threat to validity is the bias of the data extraction. The possible source of this bias could be one author extraction process when just one person extracts the information from the papers. We have also tried to eliminate the effect of this threat by distributing the data extraction among the authors and then each author double check other authors. Part of this elimination process is the use of automatic mining tools by spreadsheets for result verification by the data extraction process.

The third potential threat is the inclusion and exclusion of papers due to the scope of the paper. We have followed well-known methods for the selection criteria (see section III-C). Owing to the broad range of papers that are dealing with the term IoT and the wide variety of published application using the concepts of IoT, we have spent much time in the scanning and reading the selected papers to assure that the papers are within the scope of the study. Hence, we have excluded those papers which are not related to the quality aspect of IoT. Those papers were covered by several studies related to other aspects of IoT such as [11], [14], and [80].

The analyzed sample also does not include preprints of the papers submitted to or accepted in journals and conferences published by sites as *arXiv.org*, *researchgate.net* or on individual personal pages of the researchers active in the IoT domain. These preprints might contain novel ideas and quality assurance methods relevant to the scope of analyzed papers, however, to ensure objectivity and reliability of the information sources, we decided that the papers had to undergo the peer review process and had to be published by the journal or conference.

Another excluded set of paper is the set of those papers without specific output. We called those papers as "opinion

papers" which are just giving suggestions or opinions regarding IoT quality aspects but without experiments or robust proposed methods. The final set of excluded papers is the set of those papers which are not published in the considered academic databases. For the reliability of the results, we did not consider those papers which are published on unreliable sources on the Internet.

VII. CONCLUSIONS

We have presented in this paper the results of mapping 478 published research papers related to different quality aspects of IoT. The mapping study takes the period between 2009 and 2017. We have gone through the detailed analysis of this population of papers from a different perspective based on a set of established significant RQs that have not been addressed before. In attempting to answering those RQs, we have gotten a set of significant results.

The results of the analysis showed us the dramatic increase in published research papers related to quality aspects of IoT. It appears from the results that majority of the papers published in conference and workshops while the rest were published in journals. We have highlighted those active researchers through their appearance as author/co–author of the published papers. We have further highlighted the active groups and countries. We have then arranged the contributions of the papers based on the quality aspects dealt with in the papers. We have given the detail of each study direction for those quality aspects. For each quality aspect, we have also discussed the methods and the principle techniques studied so far. We end this study with a discussion of limitations, challenges and areas for future research to improve the quality of IoT applications.

APPENDIX A

See Table 4.

APPENDIX B

See Table 5.

REFERENCES

[1] K. Ashton, "That 'Internet of Things' thing," *RFiD J.*, vol. 22, no. 7, pp. 97–114, 2009.
[2] Gartner Inc. (Aug. 2018). *Gartner's Hype Cycle Special Report for 2018*. [Online]. Available: https://www.gartner.com/smarterwithgartne
[3] B. R. Maxim and M. Kessentini, "An introduction to modern software quality assurance," in *Software Quality Assurance*, I. Mistrik, R. Soley, N. Ali, J. Grundy, and B. Tekinerdogan, Eds. Boston, MA, USA: Morgan Kaufmann, 2016, ch. 2, pp. 19–46.
[4] L. H. Rosenberg, "What is software quality assurance?" *J. Defense Softw. Eng.*, vol. 7, pp. 22–25, May 2002.
[5] D. Shoemaker, C. Woody, and N. R. Mead, "Advances in software engineering and software assurance," in *Advances in Computers*, vol. 102, A. R. Hurson and M. Goudarzi, Eds. Amsterdam, The Netherlands: Elsevier, 2016, pp. 1–46.
[6] K. Rose, S. Eldridge, and L. Chapin, "The Internet of Things: An overview," Internet Soc., Geneve, Switzerland, Tech. Rep. 2, Oct. 2015.
[7] Huawei Technologies co., Ltd. (Sep. 2015). *Global Connectivity Index*. [Online]. Available: http://www.huawei.com/minisite/gci/en/index.html
[8] J. Manyika *et al.*, "The Internet of Things: Mapping the value beyond the hype," McKinsey Global Inst., New York, NY, USA, Tech. Rep., Jun. 2015.
[9] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *J. Cleaner Prod.*, vol. 140, no. 3, pp. 1454–1464, 2017.
[10] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, Jul. 2018.
[11] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[12] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2014.
[13] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.
[14] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.
[15] G. White, V. Nallur, and S. Clarke, "Quality of service approaches in IoT: A systematic mapping," *J. Syst. Softw.*, vol. 132, pp. 186–203, Oct. 2017.
[16] N. A. Bakar and A. Selamat, "Agent systems verification: Systematic literature review and mapping Selamat," *Appl. Intell.*, vol. 48, no. 5, pp. 1251–1274, 2018.
[17] M. U. Khan, S. Iftikhar, M. Z. Iqbal, and S. Sherin, "Empirical studies omit reporting necessary details: A systematic literature review of reporting quality in model based testing," *Comput. Standards Interfaces*, vol. 55, pp. 156–170, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548916302112
[18] A. Amjad, F. Azam, M. W. Anwar, W. H. Butt, and M. Rashid, "Event-driven process chain for modeling and verification of business requirements—A systematic literature review," *IEEE Access*, vol. 6, pp. 9027–9048, 2018.
[19] E. J. Marinissen *et al.*, "IoT: Source of test challenges," in *Proc. 21th IEEE Eur. Test Symp. (ETS)*, May 2016, pp. 1–10.
[20] H. Foidl and M. Felderer, "Data science challenges to improve quality assurance of Internet of Things applications," in *Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications*. Cham, Switzerland: Springer, 2016, pp. 707–726, doi: 10.1007/978-3-319-47169-3_54.
[21] J. Kiruthika and S. Khaddaj, "Software quality issues and challenges of Internet of Things," in *Proc. 14th Int. Symp. Distrib. Comput. Appl. Bus. Eng. Sci. (DCABES)*, Aug. 2015, pp. 176–179.
[22] M. Trnka, T. Cerny, and N. Stickney, "Survey of authentication and authorization for the Internet of Things," *Secur. Commun. Netw.*, vol. 2018, Jun. 2018, Art. no. 4351603.
[23] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," *Inf. Softw. Technol.*, vol. 94, pp. 30–37, Feb. 2017.
[24] M. A. Nia and A. Ruiz-Martínez, "Systematic literature review on the state of the art and future research work in anonymous communications systems," *Comput. Elect. Eng.*, vol. 69, pp. 497–520, Jul. 2018.
[25] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.
[26] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. 12th Int. Conf. Eval. Assessment Softw. Eng. (EASE)*, Swindon, U.K.: BCS Learning & Development Ltd., 2008, pp. 68–77. [Online]. Available: http://dl.acm.org/citation.cfm?id=2227115.2227123
[27] B. Kitchenham *et al.*, "Systematic literature reviews in software engineering—A tertiary study," *Inf. Softw. Technol.*, vol. 52, no. 8, pp. 792–805, Aug. 2010.
[28] T. Dyba, T. Dingsoyr, and G. K. Hanssen, "Applying systematic reviews to diverse study types: An experience report," in *Proc. 1st Int. Symp. Empirical Softw. Eng. Meas. (ESEM)*, Washington, DC, USA: IEEE Computer Society, 2007, pp. 225–234, doi: 10.1109/ESEM.2007.21.
[29] P. A. da Mota Silveira Neto, I. do Carmo Machado, J. D. McGregor, E. S. de Almeida, and S. R. de Lemos Meira, "A systematic mapping study of software product lines testing," *Inf. Softw. Technol.*, vol. 53, no. 5, pp. 407–423, May 2011, doi: 10.1016/j.infsof.2010.12.003.

[30] N. S. R. Alves, T. S. Mendes, M. G. de Mendonça, R. O. Spínola, F. Shull, and C. Seaman, "Identification and management of technical debt: A systematic mapping study," *Inf. Softw. Technol.*, vol. 70, pp. 100–121, Feb. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950584915001743

[31] C. V. C. de Magalhães, F. Q. B. da Silva, R. E. S. Santos, and M. Suassuna, "Investigations about replication of empirical studies in software engineering: A systematic mapping study," *Inf. Softw. Technol.*, vol. 64, pp. 76–101, Aug. 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950584915000300

[32] E. S. Reetz, D. Kuemper, K. Moessner, and R. Toenjes, "How to test IoT-based services before deploying them into real world," in *Proc. 19th Eur. Wireless Conf. Eur. Wireless*, Apr. 2013, pp. 1–6.

[33] P. Giménez, B. Molína, C. E. Palau, and M. Esteve, "SWE simulation and testing for the IoT," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2013, pp. 356–361.

[34] X. Zheng, P. Martin, K. Brohman, and L. D. Xu, "CLOUDQUAL: A quality model for cloud services," *IEEE Trans Ind. Informat.*, vol. 10, no. 2, pp. 1527–1536, May 2014.

[35] M. Ahmad, "Reliability Models for the Internet of Things: A paradigm shift," in *Proc. IEEE Int. Symp. Softw. Rel. Eng. Workshops*, Nov. 2014, pp. 52–59.

[36] A. Karkouch, H. Mousannif, H. Al Moatassime, and T. Noel, "A model-driven architecture-based data quality management framework for the Internet of Things," in *Proc. 2nd Int. Conf. Cloud Comput. Technol. Appl. (CloudTech)*, May 2016, pp. 252–259.

[37] I. Silva, R. Leandro, D. Macedo, and L. A. Guedes, "A dependability evaluation tool for the Internet of Things," *Comput. Elect. Eng.*, vol. 39, no. 7, pp. 2005–2018, Oct. 2013, doi: 10.1016/j.compeleceng.2013.04.021.

[38] J.-E. Kim, T. Abdelzaher, L. Sha, A. Bar-Noy, R. Hobbs, and W. Dron, "On maximizing quality of information for the internet of things: A real-time scheduling perspective (invited paper)," in *Proc. IEEE 22nd Int. Conf. Embedded Real-Time Comput. Syst. Appl. (RTCSA)*, Aug. 2016, pp. 202–211.

[39] T. Shi, R. Wang, D. Zhang, W. Jiao, and B. Xie, "Quality driven design of program frameworks for intelligent sensor applications," in *Proc. 20th Asia–Pacific Softw. Eng. Conf. (APSEC)*, vol. 1, Dec. 2013, pp. 442–449.

[40] A. De Rubertis *et al.*, "Performance evaluation of end-to-end security protocols in an Internet of Things," in *Proc. 21st Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2013, pp. 1–6.

[41] K. Vandikas and V. Tsiatsis, "Performance evaluation of an IoT platform," in *Proc. 8th Int. Conf. Next Gener. Mobile Apps, Services Technol.*, Sep. 2014, pp. 141–146.

[42] M. Yamada, T. Oda, Y. Liu, K. Matsuo, M. Ikeda, and L. Barolli, "Performance evaluation of an IoT-based e-learning testbed considering OLSR protocol in a NLoS environment," in *Proc. 19th Int. Conf. Netw.-Based Inf. Syst. (NBiS)*, Sep. 2016, pp. 451–457.

[43] G. Sun, S. Huang, W. Bao, Y. Yang, and Z. Wang, "A privacy protection policy combined with privacy homomorphism in the Internet of Things," in *Proc. 23rd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2014, pp. 1–6.

[44] A. Samani, H. H. Ghenniwa, and A. Wahaishi, "Privacy in Internet of Things: A model and protection framework," *Procedia Comput. Sci.*, vol. 52, pp. 606–613, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050915008467

[45] Q. H. Cao, I. Khan, R. Farahbakhsh, G. Madhusudan, G. M. Lee, and N. Crespi, "A trust model for data sharing in smart cities," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–7.

[46] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2012, pp. 18–23.

[47] Y. Ben Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, pp. 351–365, Nov. 2013, doi: 10.1016/j.cose.2013.09.001.

[48] J.-H. Hoepman, "In things we trust? Towards trustability in the Internet of Things," in *Constructing Ambient Intelligence*. Berlin, Germany: Springer, 2012, pp. 287–295, doi: 10.1007/978-3-642-31479-7_49.

[49] T. Schulz and I. Tjøstheim, "Increasing trust perceptions in the Internet of Things," in *Human Aspects of Information Security, Privacy, and Trust*. Berlin, Germany: Springer, 2013, pp. 167–175, doi: 10.1007/978-3-642-39345-7-18.

[50] J. Liu, X. Hu, Z. Wei, D. Jia, and C. Song, "Location privacy protect model based on positioning middleware among the Internet of Things," in *Proc. Int. Conf. Comput. Sci. Electron. Eng.*, vol. 1, Mar. 2012, pp. 288–291.

[51] A. Ukil, S. Bandyopadhyay, and A. Pal, "Privacy for IoT: Involuntary privacy enablement for smart energy systems," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 536–541.

[52] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *Proc. 7th Int. Symp. Parallel Archit., Algorithms Program. (PAAP)*, Dec. 2015, pp. 217–222.

[53] L. Catuogno and S. Turchi, "The dark side of the interconnection: Security and privacy in the Web of things," in *Proc. 9th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.*, Jul. 2015, pp. 205–212.

[54] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014, doi: 10.1007/s11276-014-0761-7.

[55] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Jul. 2017, pp. 176–178.

[56] S. Asri and B. Pranggono, "Impact of distributed denial-of-service attack on advanced metering infrastructure," *Wireless Pers. Commun.*, vol. 83, no. 3, pp. 2211–2223, 2015.

[57] B. S. Ahmed, K. Z. Zamli, W. Afzal, and M. Bures, "Constrained interaction testing: A systematic literature study," *IEEE Access*, vol. 5, pp. 25706–25730, 2017.

[58] M. Bures, T. Cerny, and M. Klima, "Prioritized process test: More efficiency in testing of business processes and workflows," in *Proc. Int. Conf. Inf. Sci. Appl.* Singapore: Springer, 2017, pp. 585–593.

[59] D. Kuemper, E. Reetz, and R. Tönjes, "Test derivation for semantically described IoT services," in *Proc. IEEE Future Netw. Mobile Summit (FutureNetworkSummit)*, Jul. 2013, pp. 1–10.

[60] A. Ahmad, F. Bouquet, E. Fourneret, F. Le Gall, and B. Legeard, "Model-based testing as a service for IoT platforms," in *Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications*. Cham, Switzerland: Springer, 2016, pp. 727–742, doi: 10.1007/978-3-319-47169-3_55.

[61] Y. Choe, S. Lee, and M. Lee, "SAVE: An environment for visual specification and verification of IoT," in *Proc. IEEE 20th Int. Enterprise Distrib. Object Comput. Workshop (EDOCW)*, Sep. 2016, pp. 1–8.

[62] Y. Jia, E. Bodanese, and J. Bigham, "Model checking of the reliability of publish/subscribe structure based system," in *Proc. 1st IEEE Int. Conf. Commun. China (ICCC)*, Aug. 2012, pp. 155–160.

[63] A. B. Torjusen, H. Abie, E. Paintsil, D. Trcek, and A. Skomedal, "Towards run-time verification of adaptive security for IoT in eHealth," in *Proc. ACM Eur. Conf. Softw. Archit. Workshops (ECSAW)*, New York, NY, USA, 2014, pp. 4-1–4-8, doi: 10.1145/2642803.2642807.

[64] L. González, J. Cubo, A. Brogi, E. Pimentel, and R. Ruggia, "Run-time verification of behaviour-aware mashups in the Internet of Things," in *Advances in Service-Oriented and Cloud Computing*, C. Canal and M. Villari, Eds. Berlin, Germany: Springer, 2013, pp. 318–330.

[65] L. Yong-Fei and T. Li-Qin, "Comprehensive evaluation method of reliability of Internet of Things," in *Proc. 9th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, Nov. 2014, pp. 262–266.

[66] V. Wittstock, M. Lorenz, E. Wittstock, and F. Pürzel, "A framework for user tests in a virtual environment," in *Advances in Visual Computing*. Berlin, Germany: Springer, 2012, pp. 358–367, doi: 10.1007/978-3-642-33191-6_35.

[67] D.-H. Shin, "Conceptualizing and measuring quality of experience of the Internet of Things: Exploring how quality is perceived by users," *Inf. Manage.*, vol. 54, no. 8, pp. 998–1011, 2017.

[68] H. Kawazoe, D. Ajitomi, and K. Minami, "A test framework for large-scale message broker system for consumer devices," in *Proc. IEEE 5th Int. Conf. Consum. Electron. Berlin (ICCE-Berlin)*, Sep. 2015, pp. 24–28.

[69] P. Rosenkranz, M. Wählisch, E. Baccelli, and L. Ortmann, "A distributed test system architecture for open-source IoT software," in *Proc. ACM Workshop IoT Challenges Mobile Ind. Syst. (IoT-Sys)*, New York, NY, USA, 2015, pp. 43–48, doi: 10.1145/2753476.2753481.

[70] J. Fernandes *et al.*, "IoT lab: Towards co-design and IoT solution testing using the crowd," in *Proc. Int. Conf. Recent Adv. Internet Things (RIoT)*, Apr. 2015, pp. 1–6.

[71] G. Z. Papadopoulos, A. Gallais, G. Schreiner, E. Jou, and T. Noel, "Thorough IoT testbed characterization: From proof-of-concept to repeatable experimentations," *Comput. Netw.*, vol. 119, pp. 86–101, Jun. 2017.

[72] A. Lu, W. Fang, C. Xu, S.-C. Cheung, and Y. Liu, "Data-driven testing methodology for RFID systems," *Frontiers Comput. Sci. China*, vol. 4, no. 3, pp. 354–364, Sep. 2010, doi: 10.1007/s11704-010-0387-6.
[73] H. Bae, S.-H. Sim, Y. Choi, and L. Liu, "Statistical verification of process conformance based on log equality test," in *Proc. IEEE 2nd Int. Conf. Collaboration Internet Comput. (CIC)*, Nov. 2016, pp. 229–235.
[74] D. S. Silva, D. Resner, R. L. de Souza, and J. E. Martina, "Formal verification of a cross-layer, trustful space-time protocol for wireless sensor networks," in *Information Systems Security*. Cham, Switzerland: Springer, 2016, pp. 426–443, doi: 10.1007/978-3-319-49806-5_23.
[75] H. Xie, L. Wei, J. Zhou, and X. Hua, "Research of conformance testing of low-rate wireless sensor networks based on remote test method," in *Proc. Int. Conf. Comput. Inf. Sci.*, Jun. 2013, pp. 1396–1400.
[76] M. Göhring and R. Schmitz, "On randomness testing in physical layer key agreement," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 733–738.
[77] M. Bures and B. S. Ahmed, "On the effectiveness of combinatorial interaction testing: A case study," in *Proc. IEEE Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Jul. 2017, pp. 69–76.
[78] E. Cavalcante *et al.*, "On the interplay of Internet of Things and cloud computing: A systematic mapping study," *Comput. Commun.*, vols. 89–90, pp. 17–33, Sep. 2016, [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366416300706

BESTOUN S. AHMED received the B.Sc. degree in electrical and electronic engineering from the University of Salahaddin-Erbil, in 2004, the M.Sc. degree from University Putra Malaysia, in 2009, and the Ph.D. degree in software engineering from University Sains Malaysia, in 2012, where he was a Research Fellow with the Software Engineering Research Group. He was as a Senior Lecturer with the University of Salahaddin-Erbil. He spent one year doing his postdoctoral research with the Swiss AI Lab, Istituto Dalle Molle di Studi sull'Intelligenza Artificiale, Switzerland. He was an Assistant Professor with the Department of Computer Science, Czech Technical University in Prague. He is currently with the Department of Mathematics and Computer Science, Karlstads University, Sweden. His current research interests include combinatorial testing, search-based software testing, computational intelligence, and quality assurance for the IoT software systems.

MIROSLAV BURES received the Ph.D. degree from the Faculty of Electrical Engineering, Czech Technical University in Prague, where he is currently a Researcher and a Senior Lecturer in software testing and quality assurance. His research interests include model-based testing (process and workflow testing, and data consistency testing) efficiency of test automation (test automation architectures, assessment of automated testability, and economic aspects), and quality assurance methods for the Internet of Things solutions, reflecting specifics of this technology. In these areas, he also leads several R&D and experimental projects. He is a member of Czech chapter of the ACM, CaSTB, ISTQB Academia work group, and participates in broad activities in the professional testing community.

KAREL FRAJTAK received the B.S. and Ph.D. degrees from Czech Technical University (CTU) in Prague, Czech Republic, where he was an Engineer. He is currently a Researcher with the Software Engineering Group, CTU in Prague. His research interest includes model-based testing area and explores possible combinations and synergies between model-based testing and exploratory testing techniques to find more efficient methods of automation of the current testing processes.

TOMAS CERNY received the B.S. degree from Czech Technical University, the M.S. degree from Baylor University, and the Ph.D. degree from the Faculty of Electrical Engineering, Czech Technical University in Prague, Czech Republic. He was an Engineer with Czech Technical University and the Faculty of Electrical Engineering, Czech Technical University in Prague. He is currently an Assistant Professor of computer science with Baylor University, where he conducts research on aspect-oriented programming, security, and software engineering mostly related to distributed architectures including SOA, MSA, or the IoT.