Interoperability and Integration Testing Methods for IoT Systems: a Systematic Mapping Study

Miroslav Bures[1][0000−0002−2994−7826], Matej Klima[1][0000−0002−9601−8787], Vaclav Rechtberger[1][0000−0002−4127−5372], Xavier Bellekens[2][0000−0003−1849−5788], Christos Tachtatzis[2][0000−0001−9150−6805], Robert Atkinson[2][0000−0002−6206−2229], and Bestoun S. Ahmed[1,3][0000−0001−9051−7609]

[1] Dept. of Computer Science, FEE, Czech Technical University in Prague, Karlovo navesti 13, , Czech Republic
miroslav.bures@fel.cvut.cz
http://still.felk.cvut.cz
[2] Dept. of Electronic and Electrical Engineering, University of Strathclyde, 99 George Street, Glasgow, Scotland, UK
[3] Dept. of Mathematics and Computer Science, Karlstad University, Universitetsgatan 2, 65188, Karlstad, Sweden

Abstract. The recent active development of Internet of Things (IoT) solutions in various domains has led to an increased demand for security, safety, and reliability of these systems. Security and data privacy are currently the most frequently discussed topics; however, other reliability aspects also need to be focused on to maintain smooth and safe operation of IoT systems. Until now, there has been no systematic mapping study dedicated to the topic of interoperability and integration testing of IoT systems specifically; therefore, we present such an overview in this study. We analyze 803 papers from four major primary databases and perform detailed assessment and quality check to find 115 relevant papers. In addition, recently published testing techniques and approaches are analyzed and classified; the challenges and limitations in the field are also identified and discussed. Research trends related to publication time, active researchers, and publication media are presented in this study. The results suggest that studies mainly focus only on general testing methods, which can be applied to integration and interoperability testing of IoT systems; thus, there are research opportunities to develop additional testing methods focused specifically on IoT systems, so that they are more effective in the IoT context.

Keywords: Internet of Things · Testing · Verification · Integration · Interoperability · Automated testing.

1   Introduction

The Internet of Things (IoT) provides numerous advantages to its users in various application domains. However, extensive development of IoT systems in the

last decade has led to a number of reliability and security challenges [12, 32, 30]. One of the challenges frequently reported by researchers as well as industry practitioners is the integration testing of IoT systems. In contemporary IoT projects, software developers work with network specialists and electronic experts for testing; however, these parties have different backgrounds and may be accustomed to using different methods of system testing (e.g., low-level testing vs. high-level functional testing). Moreover, different expectations may also play a role; for example, in a standard software system, lower layers (e.g., network or operating systems) are usually considered to be already tested and reliable; therefore, quality engineers focus on the application itself. In the case of an IoT system, the situation might differ and lower levels might also need to be tested properly. In addition, interoperability challenges are closely associated with integration testing; different devices using a variety of protocols need to cooperate in an appropriate manner, and this reliable cooperation has to be verified. Individual devices can have numerous versions and variants, which increases the difficulty of correct and seamless integration.

Integration testing and interoperability testing of IoT systems are considered to overlap for several cases even though semantic differences and different definitions can be pointed out. However, because these terms overlap in their common usage, we decided to cover both **interoperability** and **integration** testing in the scope of this study.

As mentioned earlier, there is an increased demand for more efficient interoperability and integration testing methods. Currently, the model-based testing (MBT) discipline naturally covers the area of integration testing through methods such as path-based testing [11, 8, 10], which is typical for E2E integration tests, or combinatorial [39] and constrained interaction testing [4], which is useful in unit integration testing and optimization of system configurations. Logically, in the recent period, researchers have attempted to tailor or apply formal verification and MBT techniques for IoT systems to increase system efficiency [3]. Interoperability and integration testing has significant importance in the IoT context and mapping current methods for IoT integration testing would provide valuable information to researchers for IoT and industrial quality assurance. Unfortunately, no systematic mapping study has been conducted yet in the field of integration testing for IoT systems. Hence, we attempt to bridge this gap through this study.

The contributions of this study are as follows:

1. It gives an overview of research and development activity in this field, identifying the active parties and individuals;
2. It also provides an overview of methods and approaches that are available for IoT integration testing;
3. It identifies research opportunities and discusses possible research directions.

This paper is organized as follows. Section 2 analyzes existing mapping studies and literature surveys in the fields of integration testing, IoT testing, quality assurance and IoT integration, which justifies the motivation of this study. Section 3 explains the methodology used in this study, defines the research questions

(RQs) to be answered, and the stages through which relevant studies are identified and analyzed. Section 4 presents the answers to individual RQs and related discussions. The last section presents the analysis of the possible threats to the validity of this study and concludes the paper.

2 Motivation and Related Work

The motivation of this study is twofold. The first is the importance of integration testing in the quality assurance process of IoT solutions [12, 32] and the second is the fact that no previous systematic mapping study has addressed integration testing methods for IoT systems specifically.

In the field of general integration testing, there are several systematic literature surveys and mapping studies.

In 2007, Rehman et al. published a survey of issues and available techniques for general software integration testing [44]. Their study summarizes and classifies a variety of integration testing approaches, covering the fields of MBT, test automation frameworks, and methodological aspects; it also provides a good overview of available approaches and concepts that can be used in the definition of a test strategy. However, the study focuses on general software integration testing and is not IoT-specific. Moreover, the study was published 12 years ago; new techniques and approaches might be available now. Moreover, modern integrated software applications may change as the systems are becoming more complex and demands for their real-time or almost real-time operation have increased. This will also be reflected in integration testing methods; therefore, a state-of-the-art survey is required.

A more recent study by Shashank et al. from 2010 also focuses on the field of integration testing of component-based software systems. However, the study, published as a conference paper, is limited in terms of its sample size; rather than an extensive classification, it provides an overview of available approaches and selected examples of approaches [48]. Despite the limited extent of the study, the brief classification of the state-of-the-art methods into established MBT and software verification categories provided in this study is valid.

Another recent survey and analysis on model-based integration testing was conducted by Haser et al. in 2014 [26]. Essentially, this study is not limited to software systems; the authors discuss integration testing methods that can be applied to a broader scope of cyber-physical systems, which also covers the IoT domain. In the study, an extensive sample of 718 papers is analyzed, and conclusions are obtained for the defined research questions on software paradigms, system assessment types, and usage of non-functional requirements. However, the study is limited to model-based integration testing with limited scope of defined research questions. For the field of IoT-specific integration testing methods, a broader study is required.

In the field of testing techniques that specifically focus on IoT systems and their specifics, a recent systematic mapping study by Ahmed et al. [3] focuses on general aspects of quality and quality assurance techniques designed for IoT

systems. The scope of this study is broader than the field of integration testing and covers topics such as security, privacy, construction of testbeds, general MBT, and formal verification techniques. Integration testing is not discussed in depth in this study due to its general scope.

Another recent conference paper by Dias et al. briefly summarizes current testing tools for IoT systems; integration testing is included in the examined aspects of the problem [17]. However, the discussion is brief, and regarding the selected method in the study, all state-of-the-art methods in this field are not covered.

In 2019, Cortes et al. conducted a mapping study on software testing methods used for IoT systems [15]. The study categorizes and analyses publications discussing general testing approaches used in IoT systems. Unfortunately, the discussion of integration testing is very brief in this paper.

Another study by Garousi et al. focuses on the testing methods for embedded systems [22] (which may, to a certain extent, overlap with IoT systems discussed in this study). However, besides the fact that the field of embedded systems is not the same as the IoT field, the study focuses on general testing methods and approaches and does not concentrate on interoperability and integration testing specifically.

The most frequently addressed quality aspects of IoT systems in the last five years are security and privacy [3]. This is also clear from the availability of published literature surveys and systematic mapping studies. A meta-survey summarizing and analyzing 32 available surveys on security, privacy, and defensive mechanisms of cyber-physical systems (including IoT) was recently published by Giraldo et al. [23]. The study provides a good overview of previous works and motivates the reader to find relevant literature sources related to security and privacy problems.

Regarding the integration of IoT systems, a mapping study focusing on integration techniques and styles as well as related architectural aspects of integration was published by Cavalcante et al. [14]. However, this study does not discuss testing or quality assurance aspects of system integration.

To summarize, no current systematic mapping study is dedicated to integration testing techniques for IoT systems, discussing these techniques in the context of IoT domain and from the viewpoint of IoT quality challenges, which are frequent subjects of various reports[12, 32, 30]. This study aims to provide the missing information in this specific field.
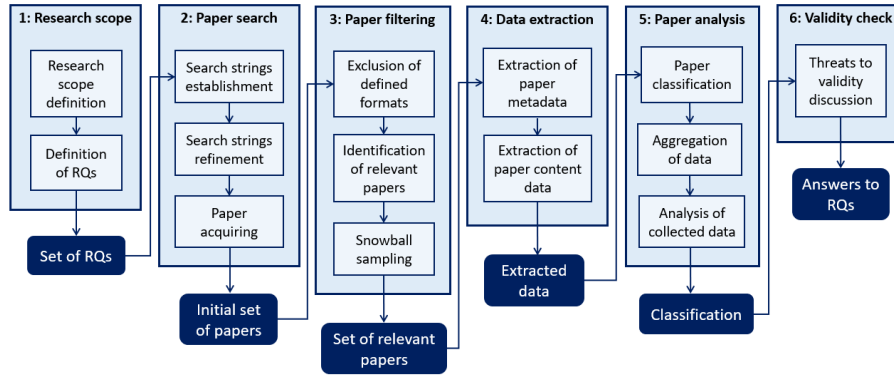
3   Methodology

This systematic mapping study follows the methodology recommendations provided by Kitchenham and Charters [33]. The process of collection and analysis of relevant studies is divided into the following six stages:

1. Research scope determination and definition of RQs to be answered in the study.

2. Search for potentially relevant papers, which includes establishment of a search strategy and acquisition of the identified papers.
3. Identification of truly relevant papers from the initial selection based on the title, abstract, full-text, and quality assessments, which includes performing snowball sampling of other relevant studies.
4. Data extraction from the remaining papers to allow further detailed analyses.
5. Classification of papers and analyses of the extracted data to answer defined RQs.
6. Validity evaluation and discussion of the possible limitations of the study.

The main stages of the methodology are depicted in Fig. 1 and described in this section.

Fig. 1. Stages of the systematic mapping study methodology followed in this study

In this study, we define seven RQs for analyzing the field of integration testing methods for IoT systems from various viewpoints:

– **RQ 1:** What is the research trend in this field in terms of the number of studies published in recent years?
– **RQ 2:** Which researchers are currently conducting active research in this field?
– **RQ 3:** Which publication media (journals and conferences) publish papers in the field of integration testing for IoT systems?
– **RQ 4:** What are the topics and subproblems currently being dealt with in the field of IoT integration and interoperability testing?
– **RQ 5:** Which testing techniques and approaches are used in this field?
– **RQ 6:** What are the current challenges and limitations in the field of IoT integration testing?
– **RQ 7:** What are the possible future research directions in this field?

We do not limit the study to a particular class or type of subproblems, or testing techniques. Hence, *RQ 4* involves informal testing techniques as well as formal and MBT techniques.

To search for relevant papers in the field of integration testing for IoT systems, we decided to use the following four established publication databases: IEEE Xplore, ACM Digital Library, Springer Link, and Elsevier ScienceDirect.

To verify the completeness of the search strings, we randomly selected a set of 30 papers as control samples, which discussed interoperability and integration testing issues of IoT systems. These control papers had to be present in the set of papers found using the search strings.

After a couple of refinement cycles, a general search string was finally established as

('Integration Testing' AND IoT) OR ('Integration Testing' AND 'Internet of Things') OR ('Interoperability Testing' AND IoT) OR ('Interoperability Testing' AND 'Internet of Things')

where the expression in apostrophes denotes the exact string to be searched at the same time. The general search string has been adopted based on particular notations used by individual databases. The timespan was determined to be 2009 to 2019.

Journal papers, book chapters, and conference papers were selected for download. In the initial stage, we also downloaded conference posters and popular magazine articles, which were subsequently filtered. The number of initially downloaded papers is presented in Table 1, column *Initial sample size*.

Once the papers were downloaded, they were filtered in several steps. First, we excluded conference posters, papers shorter than two pages, and articles from popular magazines. Subsequently, two members of our research lab independently analyzed the paper title, abstract, and full text to assess whether the downloaded papers were relevant to the examined field. This process was conducted in parallel and the results were compared; in the case of mismatch of results, the relevance of the paper was assessed in a discussion until a consensus was reached. The number of filtered papers for individual databases is presented in Table 1, column *After filtering*.

In the next step, we followed the snowball sampling process; here, we analyzed other relevant papers and articles found in the references of the filtered papers, which were not already a part of the set of filtered papers. Studies and reports found during this sampling underwent the same filtering and assessment process as the downloaded set of papers; two lab members independently analyzed the title, abstract, and full text of the papers. Those papers that were found relevant were added to the analyzed sample. The number of papers found by individual databases after this step is presented in 1, column *After snowball*.

During the data extraction and analysis phase, extracted data were independently verified by a specialist, who analyzed the set of papers and matched them with extracted metadata. A "two pair of eyes" approach was adopted for paper classification. Two specialists classified the papers independently; in the case of a mismatch, particular cases were discussed, papers were analyzed, and the final

Table 1. Numbers of papers after filtering and snowball sampling.

Source	Initial sample size	After filtering	After snowball
IEEE Xplore	384	45	53
ACM Digital Library	87	10	12
Springer Link	199	32	32
ScienceDirect	133	15	16
other databases	0	0	2
total	**803**	**102**	**115**

decision was made based on the discussion results. The final set after this phase contained 115 papers.

The narrowed selection of the papers was analyzed by publication year to answer RQ1 and by author names and affiliations to answer RQ2. Publication media were categorized by type (journal article, book chapter, conference paper, and workshop paper) and name to answer RQ3. Then, to answer RQ4, we classified the papers by categories presented in Table 2. Categories were organized in two levels: main category and subcategories. Subsequently, full text and detailed analysis of the paper content were used to answer RQs 5 to 7.

The final set of 115 papers with their metadata including abstract, category, source URL, source library, and BibTex string are available for download at *http://still.felk.cvut.cz/iot_integration_testing/*. In the folder, the list is available in CSV, OpenOffice spreadsheet, and MS Excel format.

4   Results

This section presents the results of the conducted analyses and answers to the individual RQs. Answers to each RQ are provided in a separate subsection.

4.1   RQ1: Publication Trend in Time

In the recent decade, the number of publications discussing interoperability and integration testing issues of IoT systems has constantly grown, as shown by the data presented in Figure 2.

A more significant number of publications started to appear since 2014. The growth in publication numbers from 2016 to 2019 is almost constant. When extrapolating the trend, we can expect similar growth of publications discussing interoperability and integration testing of IoT systems in the following years.
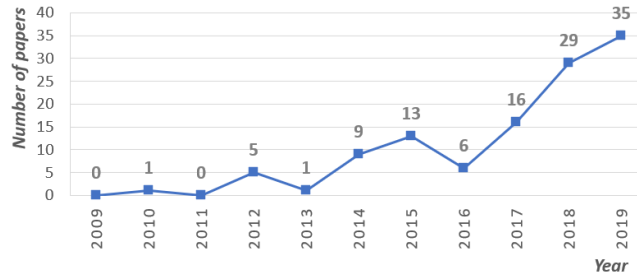
4.2   RQ2: Active Researchers

In the final set of analyzed relevant studies, eight authors emerged to be actively publishing in the field of interoperability and integration testing of IoT systems. They were Brian Pickering (University of Southampton, UK), Bruno Lima (University of Porto, Portugal), Hamza Baqa (Institut Polytechnique Paris, France),

Table 2. Categories used in the paper classification

Main category	Category short name	Category description
-	IoT quality discussion	Interoperability/integration testing included in a general IoT quality discussion
Testing methodology	Testing methodology, including	General testing methodology including interoperability/integration testing as its part
	Focused testing methodology	Methodology specially focused on interoperability/integration testing
	Formal techniques	Formal testing/verification techniques for interoperability/integration of IoT systems
	Testing methodology, applicable	General testing methodology applicable to interoperability/integration testing
	Literature review	Literature review related to IoT testing methods, which also includes interoperability and integration aspects
Testing frameworks, tools and testbeds	Testing frameworks, supporting	General testing framework directly supporting interoperability/integration testing
	Test automation framework	Specialized test automation framework directly supporting integration testing
	Testbeds	Report on IoT testbed directly supporting interoperability/integration testing
	Testing framework, applicable	General testing framework applicable to interoperability/integration testing
	Frameworks and tools overview	Overview of testing frameworks and tools applicable to integration testing
Simulation frameworks	Simulation frameworks, applicable	General IoT simulation frameworks applicable to interoperability/integration testing
	Simulation frameworks, supporting	General IoT simulation framework supporting interoperability/integration testing
-	Development frameworks	IoT systems development framework / approach / standard including interoperability/integration testing

Koray Incki (Ozyegin University, Turkey), Mengxuan Zhao (France Telecom), Michael Felderer (University of Innsbruck, Austria), Paul Grace (Aston University, UK), and Thomas Watteyne (Inria, France); they all published three studies.
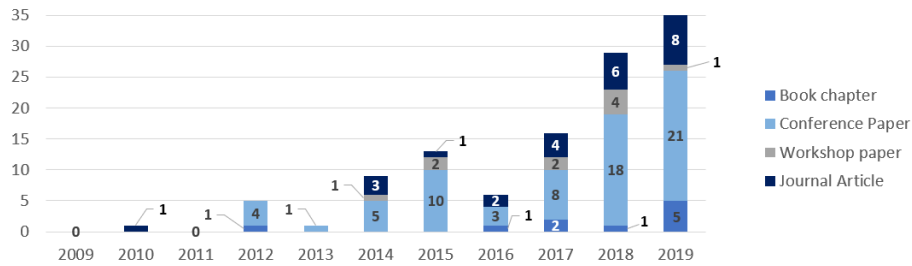
Fig. 2. Number of publications by years

No author from the analyzed set published more than three studies from 2009 to 2019, 29 authors published two studies, and 431 authors published one study. A total of 468 unique authors were found in the analyzed studies.

This analysis also points out the relative heterogeneity of the research community and absence of research mainstream in this field. However, this is a contemporary situation and might change in the near future.

4.3 RQ3: Publication Media in IoT Integration Testing

During the analysis of the papers, we analyzed four main publication media types: journal article, conference paper, workshop paper, and book chapter. Papers of conference proceedings published in a book series (e.g., LNCS by Springer) were considered as conference papers. Among the analyzed set of papers, several have been published in conferences aggregating parallel workshops; such papers were also considered as conference papers. Most papers were published in conference proceedings (61%), followed by journal articles (22%), workshop papers (9%), and book chapters (9%). Figure 3 presents more details on the publication media type by individual years of the analyzed period.

Fig. 3. Venue types by individual years

Among the media types of the published studies on interoperability and integration testing, we will start by analyzing conference papers. The analyzed

studies were published in a wide variety of conferences spanning from established conferences in system testing (e.g., IEEE Conference on Software Testing, Validation and Verification (ICST), IFIP International Conference on Testing Software and Systems, and IEEE International Conference on Software Quality, Reliability and Security (QRS)) to various forums related to IoT technology (e.g., IEEE World Forum on Internet of Things (WF-IoT), IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), and European Conference on Wireless Sensor Networks).

However, the spectrum of the conferences publishing papers focusing on IoT integration and interoperability testing is rather heterogenic, and apart from a few exceptions, we have not found a leading conference publishing more than three papers in the analyzed sample. The IEEE World Forum on Internet of Things (WF-IoT) published three papers, and the Global Internet of Things Summit (GIoTS) published two papers. The remainder of the analyzed papers were published in various unique conferences.

Regarding the journals publishing IoT interoperability and integration testing studies, the situation was found to be similar. Articles were published in a relatively wide spectrum of journals dedicated to computer systems, networks, software testing, and related areas. Three articles were published in IEEE Access and two articles in the International Journal on Software Tools for Technology Transfer. The remaining studies were published in various unique journals. The details can be found in the complete list of analyzed papers available at

   http://still.felk.cvut.cz/iot_integration_testing/.

To summarize, publication media for integration and interoperability testing studies are relatively heterogenic. Even though integration and interoperability testing are understood as established discipline in the industrial praxis, in the research world, no major journal or conferences outlies as a venue especially publishing in this specific field. This can be explained by the relative novelty of the field. However, considering that the present industry calls for more effective and systematic methods for interoperability and integration testing, the research community will very likely react to these demands, and the situation will possibly change in the coming years.

4.4   RQ4: Topics and Subproblems being Addressed

Figure 4 presents the classification of analyzed relevant studies using the categories shown in Table 2. The complete list of individual papers assigned to each category are given in the link above. In the analyzed sample, two major groups were found to be testing methodologies supporting or related to interoperability and integration testing (main category *Testing methodology* with 31 papers in total); and testing frameworks and testing tools, including test automation tools and testbeds constructed for or supporting interoperability and integration testing of IoT systems (main category *Testing frameworks, tools, and testbeds* with 46 papers in total). The analyzed set of papers also includes various IoT simulation frameworks applied to IoT interoperability and integration testing (main category *Simulation frameworks* with 12 papers in total).
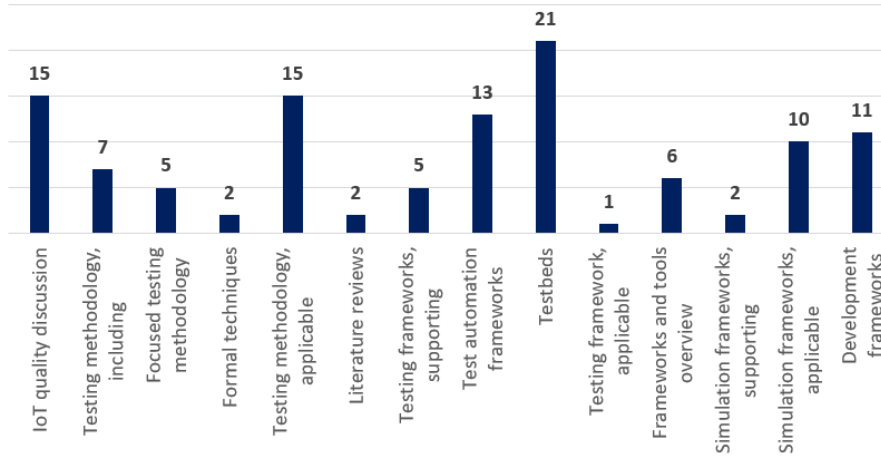
Fig. 4. Classification of analyzed studies

In the detailed categories, the largest number of analyzed studies include discussions on various IoT testbeds supporting integration testing (21 papers), followed by general IoT quality discussions (15 papers), and IoT testing methodologies applicable to integration and interoperability testing (15 papers). Interoperability and integration of IoT systems are discussed in 13 papers dedicated to IoT test automation frameworks. This topic is also the subject of 11 studies presenting various development frameworks for IoT solutions.

On the contrary, the presence of formal methods in the analyzed papers is low; only two papers focus on this topic. Similarly, only five studies present a directly focused integration testing methodology. We analyze the used techniques and approaches in section 4.5.

4.5   RQ5: Used Testing Techniques and Approaches

In the studies relevant to interoperability and integration testing of IoT systems, a variety of testing techniques and approaches have been researched and applied, from formal verifications [13] to informal crowdsourcing techniques that can be compared to exploratory testing [21].

In this study, by a testing approach, we mean (1) general approach to test design and test execution, e.g., formal verifications, Model-based Testing or informal testing, and, (2) generic testing approaches based on various test levels as unit testing, integration testing or acceptance testing, for instance. By testing techniques, we mean techniques to create test cases; for instance, combinatorial or constrained interaction testing, path-based testing, and data-flow testing.

Regarding established testing techniques, path-based testing using finite state machines (or analogous structures) as a system under test (SUT) model is discussed in five studies [53, 7, 5, 24, 19]. In addition, an SUT model based on a timed state machine has also been employed [34].

Datta et al. presented a prospective approach to semantic interoperability testing of IoT devices or services [16]. In their concept, they distinguish between syntactic and semantic interoperability to be verified during the tests. Semantic testing is also employed in a test automation framework proposed by Kim et al. [31].

Regarding the established test case notations, TTCN-3 standard by ETSI has been employed in six proposals [47, 40, 45, 53, 37, 49].

Nevertheless, established testing techniques related to IoT integration testing in the studied papers are few. In contrast, general testing approaches are discussed more intensely.

The MBT approach, in general, is explicitly discussed in several studies [2, 1, 28, 9, 5, 35, 24, 19], which mostly describe a general concept; particular testing technique, namely path-based testing, is discussed in the studies by Aicherning et al. [5], Estivill-Castro et al. [19], and Grace et al. [24].

Suggestions of formal verifications [13] and runtime verifications [27] do appear; however, for integration and interoperability testing of IoT systems, these have to be further elaborated.

Mutation testing has been used by Lu et al. for verification of RFID devices [36]; this technique can be expected to be used in future works to verify the effectiveness of developed testing techniques.

Other testing approaches include use case testing [51, 50], and, practically, exploratory testing and error guessing [21].

Several studies suggest test strategies and approaches for IoT systems that consist of general test levels (e.g., unit testing, integration testing, and acceptance testing) and approaching these test levels informally (e.g., testing of individual sensors, testing or integration, and security testing) [43, 46, 41, 18, 52, 42, 25, 38, 29, 20, 54]. These studies can be used as a basis for setting up a test strategy for an IoT system.

4.6   RQ6: Challenges and Limitations

After the analysis of the current studies in terms of interoperability and integration testing and comparing the state-of-the-art methods with the current industry demand, several conclusions can be drawn and several prospective research directions can be suggested.

The research community in the interoperability and integration testing of IoT systems seems rather heterogenic; from the analyzed studies, there is no clear leading publishing medium or author in this field focusing on this topic. This heterogeneity can be explained by a combination of several factors:

1. The field of IoT testing and quality assurance is relatively novel; despite the active production of innovative IoT solutions in the last five years, research and development of IoT-specific testing methods is currently a developing field.

2. General methods from the field of integration testing might be considered as satisfactory for testing IoT systems; thus, demand for IoT-specific interoperability and integration testing methods is not specially recognized in the research community.
3. In the research community, several research streams and subcommunities have been established, covering path-based testing, combinatorial interaction testing, constrained interaction testing, data-flow testing, and other individual basic testing techniques that can be combined to establish comprehensive integration testing methods. Hence, interoperability and integration testing itself is not considered as a subject of primary research. Instead, the focus is on primary testing approaches that can be employed for the interoperability and integration testing process.

In particular, the second and third points deserve further analysis and discussion. Regarding the second point (hypothetical low necessity to develop IoT-specific interoperability and integration testing methods, because there are general testing methods for these cases already available), it is worthwhile to analyze the situation in the current IoT systems briefly. Compared to standard software systems or relatively isolated proprietary cyber-physical systems not connected to the Internet, the situation in interconnected IoT systems might be different for a number of cases. In these systems, a more extensive set of various protocols on different networks and application levels can be integrated together, and seamless integration has to be maintained. These protocols might span from standardized protocols like WiFi, Bluetooth, IEEE 802.15.4, Z-wave, or ZigBee for low levels of the system; REST, MQTT, CoAP, or LWM2M protocols for higher levels of the system [6]; to various proprietary protocols used by individual vendors. These proprietary protocols might also contain more defects than established standards, and this fact makes smooth interoperability and integration of an IoT system more challenging.

The same applies to individual devices, where the level of standardization might be relatively low. Several attempts to standardize IoT devices and allow their interoperability have been made (e.g., ETSI GS CIM 009 or ISO/IEC 21823); however, no major standard is currently established. This is the reason for significant integration and interoperability challenges.

Therefore, the capability of previous interoperability and integration testing techniques should be revised, at the minimum; opportunities to create more effective approaches based on IoT system specifics have to be examined.

Regarding the third point, the argument that interoperability and integration testing itself might not be understood as a subject of primary research, rather as an application of primary testing approaches, there are two counter-arguments worth mentioning. First, in general system testing research, integration testing is understood as a standalone research topic, as is documented in previous mapping studies [48, 26]; in particular, the study by Haser et al. documents the broad extent of studies dedicated to integration testing of software and cyber-physical systems [26]. Moreover, another finding by a recent study conducted by Ahmed et al. [3] should be considered. Even in the discussed primary testing approaches

such as path-based testing, combinatorial interaction testing, constrained interaction testing, or data-flow testing, no specific variants of these techniques are published for IoT systems to a large extent.

Hence, to summarize, relative heterogeneity of the IoT interoperability and integration testing approaches might be explained as a result of the relative novelty of the field. Further development of IoT-specific testing techniques to cover these areas is a prospective future research direction. We analyze potential research directions further in Section 4.7.

4.7 RQ7: Future Research Directions

Regarding interoperability and integration testing methods for IoT systems, several prospective future research directions can be discussed considering the industrial needs and specifics of IoT systems.

First, specific techniques for integration and interoperability testing of IoT systems have not yet been studied extensively in the literature. The techniques might have been published under different names; for experts in the field, it might be an easy task to get an overall picture. However, for testing practitioners and researchers from other fields, getting such a picture might be more difficult.

The first future research area is handling possible combinatorial explosion problems in integration testing when considering possible configurations to test large-scale IoT systems. When various devices are integrated together in IoT systems, where these devices may vary in versions, many different system configurations can be established; flawless interoperability of devices in these variants need to be tested. The current combinatorial [39] and constrained [4] testing disciplines handle the problem on a general level. However, IoT-specific support regarding the modelling of the problem and application of general combinatorial techniques to IoT and integration testing using specific metadata from an IoT system might represent another perspective direction for future research.

Another relevant field is testing the seamless integration of various devices in an IoT system operating with limited network connectivity. Transmission of data from sensors and between actuators operating in areas with weak network signal coverage might be disrupted during the system run. Hence, in such situations, the overall functionality of an IoT system should be checked for functional correctness and transaction processing of the data, if required. To the best of our knowledge, in the testing of such reliability, current publications focus on lower levels of the system (typically network layer), and systematic methods for such tests on higher levels of an IoT system have yet to be provided.

In addition, to ensure more effective tests and also give the testing practitioners better guidance on how to construct test cases, cross-over techniques between path-based testing [8] and combinatorial interaction testing [39] for testing of close APIs in IoT systems might be researched. Using specific information and metadata from the tested system usually helps focus on the test cases more effectively, and this direction can also be explored in the case of IoT systems.

5   Conclusion

In this study, we focused on the field of integration and interoperability testing of IoT systems. The motivation was twofold: the importance of this field in the current industry and the fact that this specific area has not yet been covered by a focused, systematic literature mapping study.

In the study, we analyzed 803 papers from four major primary databases, namely, IEEE Xplore, ACM Digital Library, Springer Link, and Elsevier ScienceDirect and followed the current established recommendations for conducting mapping studies by Kitchenham and Charters [33]. After a detailed assessment of the papers and quality check, 115 papers were found to be relevant to the field.

Our results suggest that currently there are general testing methods, which can be applied to the field of integration and interoperability testing of IoT systems; therefore, there is a research opportunity to evolve more specific testing methods directly focused on IoT systems, which might work more effectively in the IoT context.

On the other hand, a number of testing and test automation frameworks that support interoperability and integration testing are being created already, and we can also find examples of individual testbeds supporting this field.

There may be several concerns related to the validity of this study. The main concern may be the exclusion of some relevant papers from the list. This possible problem was effectively mitigated by multiple-stage paper filtering and snowballing process, as described in Section 3, which also includes a thorough validity check phase.

Another possible concern may be the inclusion of irrelevant papers in the scope, which was also mitigated by the methodology (see Section 3) following well-known methods for the selection criteria as well as the "two pairs of eyes" quality check.

A limitations of this mapping study is that it analyzes papers published only in the four primary major databases (IEEE Xplore, ACM Digital Library, Springer Link and Elsevier ScienceDirect) and does not involve other possible sources such as Google Scholar, Scopus, researchgate.net or arxxiv.org, which might contain other relevant studies.

Despite these possible limitations, several prospective research directions were suggested in this study.

References

1. Ahmad, A., Bouquet, F., Fourneret, E., Gall, F.L., Legeard, B.: Model-based testing as a service for IoT platforms. In: Leveraging Applications of Formal Meth-

ods, Verification and Validation: Discussion, Dissemination, Applications, pp. 727–742. Springer International Publishing (2016). https://doi.org/10.1007/978-3-319-47169-3$_5$5, $https://doi.org/10.1007\%2F978-3-319-47169-3\_55$

2. Ahmad, A., Bouquet, F., Fourneret, E., Legeard, B.: Model-based testing for internet of things systems. In: Advances in Computers, vol. 108, pp. 1–58. Elsevier (2018)
3. Ahmed, B.S., Bures, M., Frajtak, K., Cerny, T.: Aspects of quality in internet of things (iot) solutions: A systematic mapping study. IEEE Access **7**, 13758–13780 (2019)
4. Ahmed, B.S., Zamli, K.Z., Afzal, W., Bures, M.: Constrained interaction testing: a systematic literature study. IEEE Access **5**, 25706–25730 (2017)
5. Aichernig, B.K., Bloem, R., Ebrahimi, M., Horn, M., Pernkopf, F., Roth, W., Rupp, A., Tappler, M., Tranninger, M.: Learning a behavior model of hybrid systems through combining model-based testing and machine learning. In: Gaston, C., Kosmatov, N., Le Gall, P. (eds.) Testing Software and Systems. pp. 3–21. Springer International Publishing, Cham (2019)
6. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials **17**(4), 2347–2376 (2015)
7. Amalfitano, D., Amatucci, N., De Simone, V., Riccio, V., Rita, F.A.: Towards a thing-in-the-loop approach for the verification and validation of iot systems. In: Proceedings of the 1st ACM Workshop on the Internet of Safe Things. pp. 57–63. SafeThings'17, ACM, New York, NY, USA (2017). https://doi.org/10.1145/3137003.3137007, http://doi.acm.org/10.1145/3137003.3137007
8. Anand, S., Burke, E.K., Chen, T.Y., Clark, J., Cohen, M.B., Grieskamp, W., Harman, M., Harrold, M.J., Mcminn, P., Bertolino, A., et al.: An orchestrated survey of methodologies for automated software test case generation. Journal of Systems and Software **86**(8), 1978–2001 (2013)
9. Arrieta, A., Sagardui, G., Etxeberria, L.: A model-based testing methodology for the systematic validation of highly configurable cyber-physical systems (10 2014)
10. Bures, M.: Pctgen: automated generation of test cases for application workflows. In: New Contributions in Information Systems and Technologies, pp. 789–794. Springer (2015)
11. Bures, M., Ahmed, B.S.: Employment of multiple algorithms for optimal path-based test selection strategy. Information and Software Technology **114**, 21–36 (2019)
12. Bures, M., Cerny, T., Ahmed, B.S.: Internet of things: Current challenges in the quality assurance and testing methods. In: International Conference on Information Science and Applications. pp. 625–634. Springer (2018)
13. Camilli, M., Bellettini, C., Capra, L.: Design-time to run-time verification of microservices based applications. In: Software Engineering and Formal Methods, pp. 168–173. Springer International Publishing (2018). https://doi.org/10.1007/978-3-319-74781-1$_1$2, $https://doi.org/10.1007\%2F978-3-319-74781-1\_12$
14. Cavalcante, E., Pereira, J., Alves, M.P., Maia, P., Moura, R., Batista, T., Delicato, F.C., Pires, P.F.: On the interplay of internet of things and cloud computing: A systematic mapping study. Computer Communications **89**, 17–33 (2016)
15. Cortés, M., Saraiva, R., Souza, M., Mello, P., Soares, P.: Adoption of software testing in internet of things: A systematic literature mapping. In: Proceedings of the IV Brazilian Symposium on Systematic and Automated Software Testing. pp. 3–11 (2019)
16. Datta, S.K., Bonnet, C., Baqa, H., Zhao, M., Le-Gall, F.: Approach for semantic interoperability testing in internet of things. In: 2018 Global Internet of Things Summit (GIoTS). IEEE (jun 2018). https://doi.org/10.1109/giots.2018.8534582, https://doi.org/10.1109%2Fgiots.2018.8534582

17. Dias, J.P., Couto, F., Paiva, A.C., Ferreira, H.S.: A brief overview of existing tools for testing the internet-of-things. In: 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW). pp. 104–109. IEEE (2018)

18. Eckhart, M., Meixner, K., Winkler, D., Ekelhart, A.: Securing the testing process for industrial automation software. Computers
Security **85**, 156–180 (aug 2019). https://doi.org/10.1016/j.cose.2019.04.016, https://doi.org/10.1016%2Fj.cose.2019.04.016

19. Estivill-Castro, V., Hexel, R., Stover, J.: Modeling, validation, and continuous integration of software behaviours for embedded systems. In: 2015 IEEE European Modelling Symposium (EMS). pp. 89–95 (Oct 2015). https://doi.org/10.1109/EMS.2015.24

20. Felderer, M., Russo, B., Auer, F.: On Testing Data-Intensive Software Systems, pp. 129–148. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-25312-7$_6$, $https$: $//doi.org/10.1007/978 - 3 - 030 - 25312 - 7_6$

21. Fernandes, J., Nati, M., Loumis, N.S., Nikoletseas, S., Raptis, T.P., Krco, S., Rankov, A., Jokic, S., Angelopoulos, C.M., Ziegler, S.: Iot lab: Towards co-design and iot solution testing using the crowd. In: 2015 International Conference on Recent Advances in Internet of Things (RIoT). pp. 1–6 (April 2015). https://doi.org/10.1109/RIOT.2015.7104907

22. Garousi, V., Felderer, M., Karapıçak, Ç.M., Yılmaz, U.: Testing embedded software: A survey of the literature. Information and Software Technology **104**, 14–45 (dec 2018). https://doi.org/10.1016/j.infsof.2018.06.016, https://doi.org/10.1016%2Fj.infsof.2018.06.016

23. Giraldo, J., Sarkar, E., Cardenas, A.A., Maniatakos, M., Kantarcioglu, M.: Security and privacy in cyber-physical systems: A survey of surveys. IEEE Design & Test **34**(4), 7–17 (2017)

24. Grace, P., Pickering, B., Surridge, M.: Model-driven interoperability: engineering heterogeneous IoT systems. Annals of Telecommunications **71**(3-4), 141–150 (nov 2015). https://doi.org/10.1007/s12243-015-0487-2, https://doi.org/10.1007%2Fs12243-015-0487-2

25. Guşeilă, L.G., Bratu, D., Moraru, S.: Continuous testing in the development of iot applications. In: 2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI). pp. 1–6 (2019)

26. Häser, F., Felderer, M., Breu, R.: Software paradigms, assessment types and non-functional requirements in model-based integration testing: a systematic literature review. In: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering. p. 29. ACM (2014)

27. Incki, K., Ari, I.: Democratization of runtime verification for internet of things. Computers
Electrical Engineering **68**, 570–580 (may 2018). https://doi.org/10.1016/j.compeleceng.2018.05.007, https://doi.org/10.1016%2Fj.compeleceng.2018.05.007

28. Incki, K., Ari, I.: Observing interoperability of IoT systems through model-based testing. In: Interoperability, Safety and Security in IoT, pp. 60–66. Springer International Publishing (2018). https://doi.org/10.1007/978-3-319-93797-7$_8$, $https$: $//doi.org/10.1007%2F978 - 3 - 319 - 93797 - 7_8$

29. Kaiser, A., Hackel, S.: Standards-based iot testing with open-source test equipment. In: 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C). pp. 435–441 (2019)

30. Khan, M.A., Salah, K.: Iot security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems **82**, 395–411 (2018)

31. Kim, H., Ahmad, A., Hwang, J., Baqa, H., Gall, F.L., Ortega, M.A.R., Song, J.: IoT-TaaS: Towards a prospective IoT testing framework. IEEE Access **6**, 15480–15493 (2018). https://doi.org/10.1109/access.2018.2802489, https://doi.org/10.1109%2Faccess.2018.2802489

32. Kiruthika, J., Khaddaj, S.: Software quality issues and challenges of internet of things. In: 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES). pp. 176–179. IEEE (2015)

33. Kitchenham, B., Charters, S.: Guidelines for performing systematic literature reviews in software engineering (2007)

34. Larsen, K.G., Legay, A., Miku vcionis, M., Nielsen, B., Nyman, U.: Compositional testing of real-time systems. In: ModelEd, TestEd, TrustEd, pp. 107–124. Springer International Publishing (2017). https://doi.org/10.1007/978-3-319-68270-9$_6$, $https://doi.org/10.1007\%2F978-3-319-68270-9\_6$

35. Lima, B.: Automated scenario-based integration testing of time-constrained distributed systems. In: 2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST). IEEE (apr 2019). https://doi.org/10.1109/icst.2019.00060, https://doi.org/10.1109%2Ficst.2019.00060

36. Lu, A., Fang, W., Xu, C., Cheung, S.C., Liu, Y.: Data-driven testing methodology for RFID systems. Frontiers of Computer Science in China **4**(3), 354–364 (aug 2010). https://doi.org/10.1007/s11704-010-0387-6, https://doi.org/10.1007%2Fs11704-010-0387-6

37. Makedonski, P., Adamis, G., Käärik, M., Kristoffersen, F., Carignani, M., Ulrich, A., Grabowski, J.: Test descriptions with ETSI TDL. Software Quality Journal **27**(2), 885–917 (oct 2018). https://doi.org/10.1007/s11219-018-9423-9, https://doi.org/10.1007%2Fs11219-018-9423-9

38. Medhat, N., Moussa, S., Badr, N., Tolba, M.F.: Testing techniques in iot-based systems. In: 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS). pp. 394–401 (2019)

39. Nie, C., Leung, H.: A survey of combinatorial testing. ACM Computing Surveys (CSUR) **43**(2), 11 (2011)

40. Park, H., Kim, H., Joo, H., Song, J.: Recent advancements in the internet-of-things related standards: A oneM2m perspective. ICT Express **2**(3), 126–129 (sep 2016). https://doi.org/10.1016/j.icte.2016.08.009, https://doi.org/10.1016%2Fj.icte.2016.08.009

41. Pontes, P.M., Lima, B., Faria, J.a.P.: Izinto: A pattern-based iot testing framework. In: Companion Proceedings for the ISSTA/ECOOP 2018 Workshops. pp. 125–131. ISSTA '18, ACM, New York, NY, USA (2018). https://doi.org/10.1145/3236454.3236511, http://doi.acm.org/10.1145/3236454.3236511

42. Pontes, P.M., Lima, B., Faria, J.a.P.: Test patterns for iot. In: Proceedings of the 9th ACM SIGSOFT International Workshop on Automating TEST Case Design, Selection, and Evaluation. pp. 63–66. A-TEST 2018, ACM, New York, NY, USA (2018). https://doi.org/10.1145/3278186.3278196, http://doi.acm.org/10.1145/3278186.3278196

43. Popereshnyak, S., Suprun, O., Suprun, O., Wieckowski, T.: Iot application testing features based on the modelling network. In: 2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH). pp. 127–131 (April 2018). https://doi.org/10.1109/MEMSTECH.2018.8365717

44. Jaffar-ur Rehman, M., Jabeen, F., Bertolino, A., Polini, A.: Testing software components for integration: a survey of issues and techniques. Software Testing, Verification and Reliability **17**(2), 95–133 (2007)

45. Rings, T., Poglitsch, P., Schulz, S., Serazio, L., Vassiliou-Gioles, T.: A generic interoperability testing framework and a systematic development process for automated interoperability testing. International Journal on Software Tools for Technology Transfer **16**(3), 295–313 (jun 2013). https://doi.org/10.1007/s10009-013-0281-2, https://doi.org/10.1007%2Fs10009-013-0281-2

46. Sand, B.: IoT testing - the big challenge why, what and how. In: Internet of Things. IoT Infrastructures, pp. 70–76. Springer International Publishing (2016). https://doi.org/10.1007/978-3-319-47075-7$_9$, $https://doi.org/10.1007\%2F978-3-319-47075-7\_9$

47. Schieferdecker, I., Kretzschmann, S., Rennoch, A., Wagner, M.: IoT-testware - an eclipse project. In: 2017 IEEE International Conference on Software Quality, Reliability and Security (QRS). IEEE (jul 2017). https://doi.org/10.1109/qrs.2017.59, https://doi.org/10.1109%2Fqrs.2017.59

48. Shashank, S.P., Chakka, P., Kumar, D.V.: A systematic literature survey of integration testing in component-based software engineering. In: 2010 International Conference on Computer and Communication Technology (ICCCT). pp. 562–568. IEEE (2010)

49. Sotiriadis, S., Lehmets, A., Petrakis, E.G.M., Bessis, N.: Testing cloud services using the TestCast tool. In: Advances in Intelligent Systems and Computing, pp. 819–824. Springer International Publishing (jul 2017). https://doi.org/10.1007/978-3-319-54978-1$_1$01, $https://doi.org/10.1007\%2F978-3-319-54978-1\_101$

50. de Souza, B.P., Motta, R.C., de O. Costa, D., Travassos, G.H.: An iot-based scenario description inspection technique. In: Proceedings of the XVIII Brazilian Symposium on Software Quality. p. 20–29. SBQS'19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3364641.3364644, https://doi.org/10.1145/3364641.3364644

51. de Souza, B.P., Motta, R.C., Travassos, G.H.: The first version of scenariotcheck: A checklist for iot based scenarios. In: Proceedings of the XXXIII Brazilian Symposium on Software Engineering. p. 219–223. SBES 2019, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3350768.3350796, https://doi.org/10.1145/3350768.3350796

52. Tan, T.B., Cheng, W.K.: Software testing levels in internet of things (IoT) architecture. In: Communications in Computer and Information Science, pp. 385–390. Springer Singapore (2019). https://doi.org/10.1007/978-981-13-9190-3$_4$0, $https://doi.org/10.1007\%2F978-981-13-9190-3\_40$

53. Tönjes, R., Reetz, E.S., Moessner, K., Barnaghi, P.M.: A test-driven approach for life cycle management of internet of things enabled services. In: 2012 Future Network Mobile Summit (FutureNetw). pp. 1–8 (July 2012)

54. Walker, M.A., Schmidt, D.C., Dubey, A.: Chapter six - testing at scale of iot blockchain applications. In: Kim, S., Deka, G.C., Zhang, P. (eds.) Role of Blockchain Technology in IoT Applications, Advances in Computers, vol. 115, pp. 155 – 179. Elsevier (2019). https://doi.org/https://doi.org/10.1016/bs.adcom.2019.07.008, http://www.sciencedirect.com/science/article/pii/S0065245819300348