Internet of Things: Current Challenges in the Quality Assurance and Testing Methods

Miroslav Bures[1][0000-0002-2994-7826], Tomas Cerny[2][0000-0002-5882-5502]

and Bestoun S. Ahmed[1][0000-0001-9051-7609]

[1] FEE, CTU in Prague, Karlovo nam. 13, 121 35 Praha 2, Czech Republic
[2] Computer Science, Baylor University, TX, USA
miroslav.bures@fel.cvut.cz

Abstract. Contemporary development of the Internet of Things (IoT) technology brings a number of challenges in the Quality Assurance area. Current issues related to security, user's privacy, the reliability of the service, interoperability, and integration are discussed. All these create a demand for specific Quality Assurance methodology for the IoT solutions. In the paper, we present the state of the art of this domain and we discuss particular areas of system testing discipline, which is not covered by related work sufficiently so far. This analysis is supported by results of a recent survey we performed among ten IoT solutions providers, covering various areas of IoT applications.

Keywords: Internet of Things; Quality Assurance; Testing Methodology; Test Strategy; Integration Testing; Security; Interoperability; Integration Issues

1 Introduction

In last two decades, the Internet of Things (IoT) solutions started to emerge from the initial pioneering visions to regular industrial solutions, which are present in our everyday lives. The lively development of these solutions brings also a number of challenges [1,2]; as common examples, we can discuss the insufficient level of standardization, legislation and quality assurance techniques, as well as security and privacy concerns [3,4,5,6]. In this paper, we focus on the quality assurance and testing techniques for the IoT domain. Despite the fact, that some of the areas are intensely covered by the literature (security and privacy are the typical representatives), in the area of systematical testing and quality assurance methodologies, much less work exists. In this paper, we present an overview of the domain and identify the areas, which we consider relevant for the further research. This analysis is supported by discussion of the specifics of IoT solutions having an impact on particular testing techniques and methods, together with a literature survey and with a survey among ten IoT solutions providers, which provided us with different, independent viewpoints on the problem discipline.

The paper is organized as follows. Section 2 analyzes principal issues of IoT solutions, leading to challenges in IoT quality assurance. Section 3 summarizes the state of the art in this domain. Section 4 presents the results of the recent survey among IoT

solutions providers. In section 5 we discuss the results and we identify the quality assurance areas, which have to be covered by a more intense research. The last section concludes the paper.

2 Principal IoT Issues with Impact on Testing Techniques

A number of discussions have been conducted regarding the IoT issues, for instance in [1,2,3,4,5,7,8]; however, during our literature survey, we have not found a systematic analysis, identifying what is the impact of these specifics to particular software testing methods and techniques. Hence, we provide such an analysis in this paper. In the following section, we identify several typical issues of IoT solutions and we number them by IDs. Next, in Table 1, we map these issues with direct consequences they have on the testing and quality assurance process.

Issue 1. From the business and economic viewpoint, competition in IoT business is having a direct impact on the conditions, in which these solutions are developed. This competition triggers a demand to lower prices of the manufactured IoT devices, as well as it creates a pressure to shorten time to market.

Issue 2. In specific applications of the IoT as the sensor networks or camera networks are, the devices can be located in places, which makes them easily accessible by an attacker; on the other hand, difficult to check by the service provider periodically. These devices can act as a vulnerable point to the entire network.

Issue 3. Another related issue is a low possibility to update certain types IoT devices. Either due to low production costs or energy consumption issues it is not possible to update some types of devices, which is typical for sensor networks. This has two consequences: (1) known security defects can be exploited by a potential attacker, and (2) inability to update the device firmware can lead to significant number of various versions of the devices used in production run of the service; these variants need to be tested, which increases the costs of the testbed and also number of variants to test.

Issue 4. The IoT devices powered by battery or solar energy lead engineers to minimize the power consumption of the device. This can lead to the implementation of lightweight authorization and security algorithms, exposing these IoT devices as a weak entry point to the whole network.

Issue 5. Compared to common web-based internet solutions, testing IoT solutions is specific from another viewpoint. When testing the web-based systems, we usually assume, that the lower physical layers (hardware, network protocols, operational systems, application servers etc.) are tested sufficiently already by supplier parties. Hence, we focus the system testing effort mainly on the application and integration levels. In IoT, the situation is utterly different. Compared to web-based solutions, there is a much more extensive variety of used standardized protocols [9]. Moreover, a number of proprietary protocols are used in the current IoT solutions. Thus, testing IoT services usually involves specific testing of the lower layers of the system; when a service involves development of the own IoT devices, we need to test also this hardware.

Issue 6. IoT devices are connected to the Internet network, which has at least two consequences: (1) number of links between connected devices will grow rapidly, and (2) weakly secured device can act as an entry point to the entire network.

Issue 7. In a number of IoT devices, the user can have low insight into the internal mechanism of a device; also, if a device is updated, the user can have low control about these updates. Combined with GPS, voice recognition or embedded cameras, this can lead to serious security and privacy threats.

Issue 8. Home-made devices not implementing industry standards can be produced and these devices can be integrated together with standardized IoT devices.

Issue 9. The dependency of the user to the network service is slowly, but constantly, growing, and this trend has to be expected to continue. In the IoT solutions, this can be especially critical in the case of medical or mission-critical services, where the reliability of the service must be ensured.

More issues can be identified; in this discussion, we tried to identify the most significant potential problems. Table 1 matches the identified issues with their consequences for the system testing processes.

After this initial analysis, let us discuss the IoT quality aspects and techniques, which are currently being researched.

Table 1. Consequences of IoT issues for testing methods.

Issues	Consequence for testing methods
1, 5, 9	Demand for comprehensive method to define efficient test strategy for IoT solutions
2, 3, 4, 6, 7	Increased demand for security testing, including privacy aspects
3, 8	Demand for more efficient methods how to select economic but representative platform variants to test
3, 5, 8	Increased demand for more efficient integration testing, if possible, automated
1, 3, 5	Test automation in general, as the number of variants seems not feasible to be tested manually
9	Testing of behavior of the IoT solutions under limited connection and various edge conditions is needed, especially for life-critical systems

3   Related Work

In the current literature, several principal areas dealing with IoT quality can be identified. We can categorize them as the following: (1) security issues, (2) user's privacy and trust issues, (3) reports on IoT testbeds and (4) other quality assurance and testing techniques not related to security, privacy, and particular testbeds. In this section, we summarize these areas.

In our literature survey, we analyzed selected 371 papers related to the categories above from the IEEExplore, ACM Digital Library, and SpringerLink databases. Papers

shorter than 4 pages, technical reports, and popular articles were excluded from the analysis. Table 2 summarizes the numbers of papers related to these categories.

Table 2. Number of papers related to principal categories.

Category	Number of papers
Security issues	261
User's privacy and trust issues	43
IoT testbeds	38
Quality assurance and testing techniques	29

In the related literature, **Security issues** are frequently discussed. A number of papers raise the concerns related to security issues, for example [3, 6, 10], and analyze the possible security problems [4, 5]. Moreover, for security testing as a standalone discipline, a number of reports can be found, as an example, we can give [11, 12]. Furthermore, a number of secure architectures on a conceptual and physical level are discussed, for instance [13, 14]. The security area is covered by live publication activity, which reflects on the importance of the issues related to IoT security.

A related topic, user's **privacy and trust** is also being frequently discussed. Concerns are raised [7, 8] and together with that, privacy-aware IoT architectures are being reported [15, 16]. In some of the studies, the privacy and trust topic is overlapping with the security issues, for instance [6, 10].

In the literature, a number of reports on various **IoT testbeds** (or test environments) can be found. Proposed architectures of these testbeds vary from standalone setups [17], distributed architectures [18], or crowd-sourcing based testbeds [19]. Some of the proposals are also based on the simulation of IoT physical devices, e.g. [20], which is a logical step due to the costs of a physical test environment.

The remaining area to discuss is **QA and testing techniques**. This area covers functional testing of IoT solutions, its integration testing, Model-Based Testing and related techniques. Due to the scope of our paper, these reports are the main subject of our interest. Here, we present the more detailed overview.

Several standard-established sub-disciplines of system testing research are spanning to the IoT testing currently. As the initial example, we can give the **Model-Based Testing**. IoT systems are being modeled by a semantic description of IoT services [21] or by several IoT-specific variants of state machines [22]. Also, UML-based models can be found; for instance, UML class and object diagrams are combined with Object Constraint Language [23]. Alternatively, UML Sequence diagrams with Π-calculus are used [24]. From these models, test cases are generated automatically, which increases the accuracy and coverage of these tests. Closely related to the Model-Based Testing, the **Model Checking** discipline has its representatives in the specific IoT context. To detect possible inconsistencies and defects in IoT models, Computation Tree Logic, CTL [25], δ-Calculus [26] or Temporal Logic of Actions (TLA) formal specification language, based on temporal logic [27] are used. The first representatives of the **runtime verification** of the IoT solutions can be found [28]. In this context, we can also

mention representatives of the **IoT reliability models**, combining the hardware and software layer [29, 30] or focusing solely on the software level [31].

As a standalone area, the IoT **protocol testing** can be identified. Variety of the methods is used here, for instance, conformance testing [32], randomness testing [33], statistical verification [34], or formal verification [35]. Previous work related to **IoT usability** testing can be also identified, for instance, an IoT-specific usability testing framework [36]. Several studies can be found discussing the **IoT performance** [37]. Generally, the performance studies focus more on the protocol level, than to the end-to-end performance of the IoT solution from the user's viewpoint.

However, according to the importance of IoT as an emerging technology, more related literature covering the topics of IoT-specific testing and quality assurance can be expected. We discuss this issue later in Section 5.

4 The Industry Survey

During the year 2017 we performed structured interviews with ten IoT solution providers, mostly large international companies. The providers varied by the particular IoT business, which included: (1) smart cars, (2) home appliances, (3) smart TVs, (4) and (5) infrastructure for IoT, meaning production of universal IoT devices, from which a final product can be built, (6) R&D, consulting and optimization of IoT solutions and (7)-(10) industrial IoT applications and sensor networks.

Table 3 presents the data related to the question "*Which of the following quality aspects of the IoT solutions do you consider the most challenging?*". The numbers in the header denote the particular IoT provider (the numbers are corresponding to the overview above). The possible answers were 3 to 1, where 3 means the highest possibility. The last column sums the answers; consequently, the discussed issues are sorted from the most significant one.

Table 3. IoT quality issues considered significant.

Issue / IoT provider	1	2	3	4	5	6	7	8	9	10	sum
Limited connection	3	3	2	3	3	3	2	3	3	3	28
Interoperability	3	3	3	3	2	3	2	3	2	3	27
Number of configurations	3	3	3	3	3	2	1	3	3	3	27
Security	3	3	1	2	3	3	2	3	3	3	26
Integration	3	1	2	2	2	3	3	3	3	3	25
Test effort focus	3	1	3	3	2	3	1	2	3	2	23
Performance	3	2	3	2	1	3	2	3	1	2	22
Privacy	3	3	3	2	2	2	1	2	1	2	21
Legislation	2	1	2	3	1	3	1	1	2	1	17

The issues were specified as follows. **Limited connection** means behavior of the IoT system under limited network connection. **Interoperability** included mutual compatibility of the IoT devices, missing or insufficient standards and a question of proprietary vs. internet standards. The **number of configurations** means the number of various configurations and types of the end nodes, making the solution hard to test on all these combinations, in software testing, this effect is called "combinatorial explosion."

Security issues cover various security breach scenarios, where IoT device serve as a weak entry point to the network, possible security breach leading to a personal harm of the user, or security breach leading to a violation of the user's privacy. Here, the area overlaps with the **Privacy**, which also covers possible misuse of collected personal data and reconstruction of user's digital portrait from various data streams. **Integration** issues include challenges how to test interactions of the individual IoT devices and their behavior in the edge cases, this area also relates to the interoperability of the devices. **Test effort focus** stood for a challenge, how to determine an efficient and specific test strategy for an IoT solution, which would determine the intensity of testing, test levels, and specific testing techniques. **Performance** issue covered behavior of the IoT solution under possible user traffic peeks and various limited conditions (e.g., a combination of the user traffic peek with a limited network connection). Finally, **Legislation** covered various issues related to the necessity to comply with local legislation, or vague definitions of the implementation rules in this legislation.

Regarding the IoT quality issues considered as significant, the results of the survey presented in Table 3 are relatively balanced; rather than pointing out a clear outlier, the data document, that the mentioned aspects are considered important by the industry representatives. Moreover, IoT quality issues considered significant varied by particular business domain of the IoT solution provider.

As the most significant issues, a behavior of IoT solution on a limited connection, interoperability and problems with a number of various versions and platform variants to test have been pointed out, closely followed by security and integration issues.

5   Discussion

Considering the related literature covering the principal IoT quality areas (Section 3, Table 2), a discussion can be made, whether integration, interoperability, platform variants and limited connection problems, shall be covered by the more intense development of IoT-specific testing and quality assurance techniques.

A question can be raised, whether the current software and system testing techniques in their generic form are insufficient to ensure proper testing of the IoT solutions. However, from our feedback from the industry survey (Table 3) as well as from our findings in the initial analysis (Table 1), the conclusion suggests, that this area is rather potential for future research.

In this section, let us further discuss three of these areas: (1) interoperability, (2) behavior of IoT solutions on a limited connection and (3) testing problems caused by a number of various versions and platform variants.

The interoperability of various IoT devices can be addressed by IoT-specific testing methods in two lines. The first line raises the current demands on automation of integration testing and simulation of parts of an IoT infrastructure. Consequences go to the Model-Based Testing discipline. Here, path-based or state-machine-based test case generation techniques can be adapted to the IoT-specific context.

The second line focuses on unit-level integration testing and raises demands to select suitable platform variants, also to generate efficient sets of input testing data for this integration tests. This generates an opportunity for the Constrained Interaction Testing discipline.

Also, the behavior of IoT solution under a limited network connection (or other solution-specific limiting constraints) raises the demands for specific integration and end-to-end testing; also, here, Model-Based Testing discipline could provide more specific methods. A possible approach could be modeling the reliability of the particular network lines in the model of the System Under Test and reflection of these specifics in a generation of special test cases addressing this problem.

Finally, a high number of platform configurations and variants to test is the domain of the Combinational Interaction Testing and Constrained Interaction testing disciplines. IoT-specific models for this problem can be created by modification of the current modeling notations (e.g. Combinational Arrays of Feature Models) to allow generation the test cases efficiently addressing the problem.

Also, overlapping with the interoperability issue, increased demand for integration testing of the IoT solutions and automation of these tests opens an opportunity for further development of integration testing frameworks, to decrease potential maintenance of automated tests, frequently reported as the major drawback of this technology [38]. In the area of front-end based automated testing, the maintenance issues are covered by previous work, e.g. [39, 40, 41]. However, this is not the case for the automated integration testing for IoT solutions.

Hence, one of the possible directions here is development of integration testing framework based on unit test framework principles; however, being technically adopted to specifics of the integration test. As an example, we can give higher support for orchestration of an integrated test, more possibilities to chain and execute conditional test steps and more flexible interruption handling of the test flow, all this features also implicitly contributing to decreased maintenance costs of the automated testware.

6   Conclusion

Despite the fact, that IoT represents the major and significant stream in the current technology development, related work addressing the topics of IoT-specific testing methods is rather limited. The industry survey presented in this paper documents the demand of the IoT solution providers for efficient testing and quality assurance methods, developed for IoT specific environment.

During our analysis, we have identified three principal areas, which can be the subject of the further research of IoT-specific testing methods: interoperability testing tech-

niques, techniques for testing of the behavior of the IoT solution under a limited network connection and techniques to efficiently reduce a high number of platform configurations and variants to test. Also, automated integration testing of IoT solutions is one of the prospective streams to be explored further.

IoT-specific Model-Based Testing is one of the suitable candidates to contribute to this area, moreover, Model Checking discipline can explore possibilities of static testing of IoT designs to minimize design errors in IoT solutions. Due to the present intensive research and development work in the IoT technology, we can expect more methods to be developed by the research community; however, currently, these areas represent further research opportunities.

Acknowledgements

References

1. Kiruthika, J. and Khaddaj, S. 2015. 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)*, IEEE, 176-179.
2. Marinissen, E. J., Zorian, Y., Konijnenburg, M., Huang, C. T., Hsieh, P. H., Cockburn, P. and Verbauwhede, I. 2016. May). Iot: Source of test challenges. In *2016 21th IEEE European Test Symposium (ETS)*, IEEE, 1-10.
3. Xu, T., Wendt, J. B. and Potkonjak, M. 2014. Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*, IEEE, 417-423.
4. Bertino, E., Choo, K. K. R., Georgakopolous, D. and Nepal, S. 2016. Internet of Things (IoT): Smart and secure service delivery. *ACM Transactions on Internet Technology (TOIT)*, *16*(4), 22.
5. Sicari, S., Rizzardi, A., Grieco, L. A. and Coen-Porisini, A. 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164.
6. Lin, H. and Bergmann, N. W. 2016. IoT privacy and security challenges for smart home environments. *Information*, *7*(3), 44.
7. Sajid, A. and Abbas, H. 2016. Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. *Journal of medical systems*, *40*(6), 155.
8. Worthy, P. and Matthews, B. and Viller, S. 2016. Trust me: doubts and concerns living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, ACM, pp. 427-434.
9. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials,* 17(4), 2347-2376.
10. Agrawal, V. 2015. Security and privacy issues in wireless sensor networks for healthcare. In *Internet of Things. User-Centric IoT*, Springer, 223-228.
11. Desnitsky, V. and Kotenko, I. 2016. Automated design, verification and testing of secure systems with embedded devices based on elicitation of expert knowledge. *Journal of Ambient Intelligence and Humanized Computing*, *7*(5), 705-719.

12. Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M. and Castedo, L. 2016. Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications. *Sensors*, *17*(1), 28.

13. Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C. and Coen-Porisini, A. 2016. A secure and quality-aware prototypical architecture for the Internet of Things. *Information Systems*, *58*, 43-55.

14. Ashraf, Q. M. and Habaebi, M. H. 2015. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, *49*, 112-127.

15. Wu, F., Xu, L., Kumari, S. and Li, X. 2017. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security. *Journal of Ambient Intelligence and Humanized Computing*, *8*(1), 101-116.

16. Chatzigiannakis, I., Vitaletti, A. and Pyrgelis, A. 2016. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. *Computer Communications*, *89*, 165-177.

17. Kawazoe, H., Ajitomi, D. and Minami, K. 2015. A test framework for large-scale message broker system for consumer devices. In *2015 IEEE 5th International Conference on Consumer Electronics-Berlin (ICCE-Berlin)*, IEEE, 24-28.

18. Rosenkranz, P., Wählisch, M., Baccelli, E. and Ortmann, L. 2015. A distributed test system architecture for open-source IoT software. In *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, ACM, 43-48.

19. Fernandes, J., Nati, M., Loumis, N. S., Nikoletseas, S., Raptis, T. P., Krco, S. and Ziegler, S. 2015. IoT Lab: Towards co-design and IoT solution testing using the crowd. In *2015 International Conference on Recent Advances in Internet of Things (RIoT)*, IEEE, 1-6.

20. Giménez, P., Molina, B., Palau, C. E. and Esteve, M. 2013. SWE Simulation and Testing for the IoT. In *2013 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, IEEE, 356-361.

21. Kuemper, D., Reetz, E. and Tönjes, R. 2013. Test derivation for semantically described IoT services. In *Future Network and Mobile Summit (FutureNetworkSummit), 2013*, IEEE, 1-10.

22. Peischl, B. 2015. Software quality research: From processes to model-based techniques. In *2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, IEEE, 1-6.

23. Ahmad, A., Bouquet, F., Fourneret, E., Le Gall, F. and Legeard, B. 2016. Model-Based Testing as a Service for IoT Platforms. In *International Symposium on Leveraging Applications of Formal Methods*, Springer, 727-742.

24. Ren, G., Deng, P., Yang, C., Zhang, J. and Hua, Q. 2015. A formal approach for modeling and verification of distributed systems. In *International Conference on Cloud Computing*, Springer, 317-322.

25. Jia, Y., Bodanese, E. and Bigham, J. 2012. Model checking of the reliability of publish/subscribe structure based system. In *2012 1st IEEE International Conference on Communications in China (ICCC)*, IEEE, 155-160.

26. Choe, Y., Lee, S. and Lee, M. 2016. SAVE: an environment for visual specification and verification of IoT. In *2016 IEEE 20th International Enterprise Distributed Object Computing Workshop (EDOCW)*, IEEE, 1-8.

27. Hillah, L. M., Maesano, A. P., De Rosa, F., Kordon, F., Wuillemin, P. H., Fontanelli, R. and Maesano, L. 2017. Automation and intelligent scheduling of distributed system functional testing. *International Journal on Software Tools for Technology Transfer*, *19*(3), 281-308.

10

28. González, L., Cubo, J., Brogi, A., Pimentel, E. and Ruggia, R. 2013. Run-time verification of behaviour-aware mashups in the internet of things. In *European Conference on Service-Oriented and Cloud Computing*, Springer, 318-330.

29. Ahmad, M. 2014. Reliability Models for the Internet of Things: A Paradigm Shift. In *2014 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW),* IEEE, 52-59.

30. Yong-Fei, L. and Li-Qin, T. 2014. Comprehensive evaluation method of Reliability of Internet of Things. In *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC),* IEEE, 262-266.

31. Behera, R. K., Reddy, K. H. K. and Roy, D. S. 2015. Reliability modelling of service oriented Internet of Things. In *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)*, IEEE, 1-6.

32. Xie, H., Wei, L., Zhou, J. and Hua, X. 2013. Research of conformance testing of low-rate wireless sensor networks based on remote test method. In *2013 Fifth International Conference on Computational and Information Sciences (ICCIS),* IEEE, 1396-1400.

33. Göhring, M. and Schmitz, R. 2015. On randomness testing in physical layer key agreement. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT),* IEEE, 733-738.

34. Bae, H., Sim, S. H., Choi, Y. and Liu, L. 2016. Statistical verification of process conformance based on log equality test. In *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC),* IEEE, 229-235.

35. Silva, D. S., Resner, D., de Souza, R. L. and Martina, J. E. 2016. Formal Verification of a Cross-Layer, Trustful Space-Time Protocol for Wireless Sensor Networks. In *Information Systems Security*, Springer, 426-443.

36. Wittstock, V., Lorenz, M., Wittstock, E. and Pürzel, F. 2012. A Framework for User Tests in a Virtual Environment. In *Advances in Visual Computing*, 358-367.

37. Batalla, J. M., Gajewski, M., Latoszek, W. and Krawiec, P. 2015. Implementation and performance testing of ID layer nodes for hierarchized IoT network. In *Asian Conference on Intelligent Information and Database Systems*, Springer, 463-472.

38. Bures, M. 2014. Automated testing in the Czech Republic: the current situation and issues. In *Proceedings of the 15th International Conference on Computer Systems and Technologies,* ACM, 294-301.

39. Bures, M. 2015. Framework for assessment of web application automated testability. In *Proceedings of the 2015 Conference on research in adaptive and convergent systems*, ACM, 512-514.

40. Bures, M. 2015. Metrics for automated testability of web applications. In *Proceedings of the 16th International Conference on Computer Systems and Technologies*, ACM, 83-89.

41. Bures, M, 2015. Model for evaluation and cost estimations of the automated testing architecture. In *New Contributions in Information Systems and Technologies*, Springer, 781-787.