Testing the Internet of Things

Michael Felderer[1] and Ina Schieferdecker[2]

[1] University of Innsbruck, Innsbruck, Austria
michael.felderer@uibk.ac.at
[2] Fraunhofer Institute FOKUS & TU Berlin, Berlin, Germany
ina.schieferdecker@fokus.fraunhofer.de

Internet of Things (IoT) is achieving wide application and playing a more and more significant role in todays smart world. It is designed to make objects sensed and controlled remotely across network infrastructure, building integration of the physical world into information networks. The IoT connects every device with the internet for switching information and co-working with other devices. It extends and expands the communication between human and human, human and machine, or machine and machine, where a machine can be any physical entity [1]. In Gartner's 2015 Hype Cycle for Emerging Technologies [2] — which illustrates how a technology stacks up against others in terms of maturity — the Internet of Things (IoT) is presented at the peak of the curve with high expectations as the new digital business paradigm that will offer fundamentally new ways for service- and value creation and extends previous approaches to manage eternal networked systems [3].

The different application domains and scenarios of the IoT are enormous and will impact all areas of our daily lives [4]. Typical application scenarios are the transportation and logistics domain (i.e. intelligent decisions on routing of products), healthcare domain (i.e. personalize patient care) and smart cities, homes and factories (i.e. energy savings and property protection, Industry 4.0) [5–7]. Gartner estimates there will be 50 billion connected devices by 2020 [8]. Such massive-scale interconnections are built on multiple levels of technology support, from physical devices, to communications, to data, and to applications, which are heterogeneous by nature but are glued dynamically with various middlewares. To link and share everything as promoted by IoT, the scale and complexity of the system have been greatly increased.

Consequently, quality assurance of the IoT system faces new risks and threatens that are hardly addressed by conventional approaches. Furthermore, with the emergence of the IoT and its characteristics, the environment for software engineers radically changes related to development and delivery of high quality and error-free IoT software applications. Hence, software quality assurance and software testing activities must meet these new requirements and be adapted to be compliant with the new and rapidly changing environment caused by the IoT. Marwah and Sirshar [1] even claim that software quality assurance in the IoT can be seen as a new era in research.

Due to the architecture, IoT systems are constructed in a rather different way from traditional software systems. A common IoT system would be built on the foundation of collaboration among various components at various levels and involve components from hardware elements to top-level programs. Test and validation ensuring correct functionality, workflow control, resilience to attacks, data authentication, and client privacy for such a complex system requires great efforts and novel approaches. Test perspectives vary as different levels and qualities are concerned in IoT. For instance, at device-level, connectivity, energy and network transport between devices are main issues threatening to correctness and performance of IoT systems. The cloud-level involves most test perspectives including functionality, performance and security. At the mobile-level testing is more focused on mobile application correctness over any network in the whole lifecycle scenarios. Finally, end-to-end testing takes all previous levels into consideration to validate the whole systems. Due to the complexity, the importance of data and the need for testing of several level (including the device, cloud and mobile level), especially model-based testing [9, 10] and risk-based testing [11, 12] approaches are well-suited to support quality assurance of IoT applications.

This special track on Testing the Internet of Things serves as a platform for researchers and practitioners to present approaches, results, experiences and advances on all level of IoT testing, i.e., device, cloud, mobile and end-to-end testing level. The objective of the Testing the Internet of Things track was to establish a fruitful and meaningful dialog among systems practitioners and with systems engineering researchers in embedded systems, cyber-physical systems, and the Internet of Things on the challenges, obstacles, results (both good and bad), and lessons learned associated with the massive deployment of Internet of Things solutions in various safety- and security-critical environments.

In the special track two papers, one by Foidl and Felderer [13] and another one by Ahmad et al. [14] are presented.

Foidl and Felderer [13] present data science challenges to improve quality assurance of IoT applications. Due to the massive amount of data generated in workflows of IoT applications, data science plays a key role in their quality assurance. Therefore, the authors present respective data science challenges to improve quality assurance of Internet of Things applications. Based on an informal literature review, they outline quality assurance requirements evolving with the IoT grouped into six categories (Environment, User, Compliance/Service Level Agreement, Organizational, Security and Data Management) and present data science challenges to improve the quality assurance of Internet of Things applications in four categories (Defect prevention, Defect analysis, User incorporation and Organizational) derived from the six quality assurance requirement categories.

Ahmad et al. [14] present Model-Based Testing As A Service (MBTAAS) for testing data and IoT platforms. To manage things heterogeneity and data streams over large scale and secured deployments, IoT and data platforms are becoming a central part of the IoT. MBTAAS responds to the fast growing demand to systematically test such IoT and data platforms. For this purpose, MBTAAS combines model-based testing techniques and service-oriented solutions. Besides the approach itself, the authors also present experiments with MBTAAS on FIWARE, one of the EU most emerging IoT enabled platforms.

References

1. Marwah, Q.M., Sirshar, M.: Software quality assurance in internet of things. Int. J. Comput. Appl. **109**(9), 16–24 (2015)
2. Gartner: Gartner's 2015 hype cycle for emerging technologies identifies the computing innovations that organizations should monitor. Technical report, Gartner (2015)
3. Issarny, V., Steffen, B., Jonsson, B., Blair, G.S., Grace, P., Kwiatkowska, M.Z., Calinescu, R., Inverardi, P., Tivoli, M., Bertolino, A., Sabetta, A.: CONNECT challenges: towards emergent connectors for eternal networked systems. In: 14th IEEE International Conference on Engineering of Complex Computer Systems, ICECCS 2009, Potsdam, Germany, 2–4 June 2009, pp. 154–161 (2009)
4. Santucci, G., L.S.: Internet of things in 2020 - a roadmap for the future. Technical report (2011)
5. Vermesan, O., Friess, P.: Internet of Things-from Research and Innovation to Market Deployment. River Publishers Aalborg (2014)
6. Lee, I., Lee, K.: The internet of things (iot): Applications, investments, and challenges for enterprises. Bus. Horiz. **58**(4), 431–440 (2015)
7. Foidl, H., Felderer, M.: Research challenges of industry 4.0 for quality management. In: Felderer, M., Piazolo, F., Ortner, W., Brehm, L., Hof, H. (eds.) Innovations in Enterprise Information Systems Management and Engineering, vol. 245, pp. 121–137. Springer, Switzerland (2016)
8. Evans, D.: The internet of things - how the next evolution of the internet is changing everything. Technical report, Cisco Internet Business Solutions Group (IBSG) (2011)
9. Schieferdecker, I.: Model-based testing. IEEE Softw. **29**(1), 14 (2012)
10. Felderer, M., Zech, P., Breu, R., Büchler, M., Pretschner, A.: Model-based security testing: a taxonomy and systematic classification. Softw. Test. Verification Reliab. **26**(2), 119–148 (2016)
11. Felderer, M., Schieferdecker, I.: A taxonomy of risk-based testing. Int. J. Softw. Tools Technol. Transf. **16**(5), 559–568 (2014)
12. Felderer, M., Wendland, M.F., Schieferdecker, I.: Risk-based testing. In: Margaria, T., Steffen, B. (eds.) ISoLA 2014, Part II, LNCS 8803, pp. 274–276. Springer, Switzerland (2014)
13. Foidl, H., Felderer, M.: Data science challenges to improve quality assurance of internet of things applications. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II, LNCS 9953, pp. 707–727. Springer, Switzerland (2016)
14. Ahmad, A., Bouquet, F., Le Gall, F., Legeard, B., Fourneret, E.: Model-based testing as a service for data fiware generic enablers. In: Margaria, T., Steffen, B. (eds.) ISoLA 2016, Part II, LNCS 9953. Springer, Switzerland (2016)