A Comprehensive View on Quality Characteristics of the IoT Solutions

Miroslav Bures\textsuperscript{1,2\{0000–0002–2994–7826\}}, Xavier Bellekens\textsuperscript{2\{0000–0003–1849–5788\}}, Karel Frajtak\textsuperscript{1\{0000–0003–4133–2805\}}, and Bestoun S. Ahmed\textsuperscript{1\{0000–0001–9051–7609\}}

\textsuperscript{1} FEE, Czech Technical University in Prague, Czech Republic
\{miroslav.bures,frajtak,albeybes\}@fel.cvut.cz
\textsuperscript{2} School of Design and Informatics, Abertay University, UK
x.bellekens@abertay.ac.uk

Abstract. Categorization of quality characteristics helps in a more effective structuring of the testing process and in the determination of properties, which can be verified in the system under test. In the emerging area of Internet of Things (IoT) systems, several individual attempts have been made to summarize these aspects, but the previous work is rather heterogenic and focuses on specific subareas. Hence, we consolidated the quality characteristics into one unified view, which specifically emphasizes the aspects of security, privacy, reliability and usability, as these aspects are often quoted as major challenges in the quality of contemporary IoT systems. The consolidated view also covers other areas of system quality, which are relevant for IoT system testing and quality assurance. In the paper, we also discuss relevant synonyms of particular quality characteristics as presented in the literature or being used in the current industry praxis. The consolidated view uses two levels of characteristics to maintain a suitable level of granularity and specificity in the discussed quality characteristics.

Keywords: Internet of Things, Quality Characteristics, Quality Assurance, Testing.

1 Introduction

To measure the quality of a System Under Test (SUT), various quality characteristics are being employed as standard industry practice, for instance, \textsuperscript{13,21,13}. These characteristics are covering various quality aspects of the SUT, spanning from the presence of defects in SUT functionality to broader issues, ranging from usability and maintainability to the testability of the systems \textsuperscript{2}.

The importance of these characteristics lays in several functions:

1. They serve as managerial tools to measure the quality of SUT and contribute to making the quality assurance process more effective;
2. They emphasize different quality aspects besides the simple presence of software defects. Hence, they lead system engineers to focus on aspects like testability, maintainability, scalability or another, which are not directly quantified by the presence of defects explicitly reported by the testing teams. However, these can have a significant impact on project or product success or failure;

3. They help setting-up an efficient test strategy for particular SUT, but most importantly they help managerial decisions regarding the quality aspects that are important and inform on which techniques shall be employed to prove SUT quality;

4. Considering the fact that the security and privacy are discussed as the main challenges of the current IoT solutions [20,9], proper quality characteristics may help reducing cyber–security and privacy risk by revealing flaws and reducing the attack surface by ensuring that the correct operations are executed.

In the software testing and quality assurance industry, several sets of quality characteristics have been established and used. As an example, we can give ISO/IEC 9126, later replaced by ISO/IEC 25010:2011 [18] or TMap Next [2]. As IoT systems differ from web-based software enterprise systems in a number of points it also brings several challenges specific to IoT infrastructures [20,9], it is, therefore, relevant to revise these quality characteristics and quality metrics for IoT systems and to capture their specificities. A first attempts has already been made [25,21,11,7,16,10,23,14,11,12,8,4,27], however these classifications focus specifically on heterogenic areas of IoT systems, applications and viewpoint on the system quality. Hence, a more consolidated system is required, discussing the particulars of IoT domains and their intrinsic nature.

Generally, we need to distinguish between quality characteristics and quality metrics. Quality characteristic is a general category, describing a particular viewpoint on the SUT, which can be used in the test planning, test strategy or test reporting. It is not defined by a particular formula which employs particular elements and quantities form the SUT model or facts from the test management process. Differently, quality metric is usually expressed as a formula, in which various facts from the testing process or SUT model is used (e.g. number of executed test cases, number of found defects, number of requirements covered by test cases, measured times in the tests and others). Also, elements of SUT models used for test design purposes can be used (e.g. various metrics capturing structural test coverage).

In this paper, we attempt providing a unified classification of quality characteristics specifically dedicated to IoT architecture, ranging from the availability to the cyber–security and usability of the systems.

The remainder of this paper is organised as follows; Section 2 broadly introduces work on quality characteristics and metrics, while in Section 3 we provide a unified classification of quality characteristics focusing on IoT systems. Section 4 records selected points related to the consolidation process. The last Section concludes the paper.
2 Related Work

Currently, a set of individual attempts to categorize quality characteristics for IoT systems can be found, most of them focusing on a specific area or aspect of IoT systems, or not sufficiently focusing on the physical level of an IoT system. In this chapter, we discuss these works.

The TMap Suite (previously TMAP Next) is the body of knowledge for professional testers, created by Sogeti corporation, summarized quite an exhausting list of quality characteristics with the selection of these characteristics relevant to IoT testing [1]. However, as the major background of the company is in software testing, this list does not reflect some important networking and physical layer aspects of IoT systems. We can find these characteristics covered by other authors.

A quality model targeting cloud service called Cloudqual was defined by Zheng et al. [28]. This model is used to represent, measure, and compare the quality of the cloud service providers. It contains six quality dimensions in total — one subjective, i.e., usability, and the others objective — availability, reliability, responsiveness, security, and elasticity. Empirical case studies on three storage clouds were conducted. Similarly, the trust of cloud service providers is calculated using the proposed novel trust model based on past credentials and present capabilities of a cloud resource provider by Manuel [23]. Quality characteristics discussed in these studies related to the IoT cloud services can be used in the classification of these characteristics for general IoT systems.

Data quality metrics in pervasive environments were defined by Li et al. [21] and applied on real-world data sources to demonstrate the feasibility of the metrics. Previous data quality characteristics in database applications were not applicable to pervasive environments and the metrics proposed in QoC research were either unobservable or unadaptable to application requirements. Three metrics were redefined for pervasive environments, namely currency, availability and validity, to quantitatively observe the quality of real-time data and data sources.

Regarding the security area, which is being frequently discussed as one of the most significant IoT challenges [20,9], individual studies can be found. As an example, a study by Islam and Falcarin [17] can be given. The authors identified security requirements through asset-based risk management process to describe the security goal. Security of the IoT platform is one of the most important requirements, and the results of this study are applicable here.

Various security metrics are used to quantify the degree of freedom from a possibility of suffering damage or loss from a malicious attack. These key metrics have been defined by Abbadi [3]. Security and usability assessment of several authentication technologies are analyzed and summarized by Solie [27].

The applications of IoT bring new possibilities of what the user can achieve and experience. A subjective user’s satisfaction with the application — quality of experience, QoE — will become new quality metrics the operators will have to consider. Ikeda et al. propose a framework of scalable QoE modeling for explosively increasing applications [16]. They defined two sets of metrics — physical
metrics emerging in the IoT architecture and metaphysical metrics demanded by users.

The quality of the data at the device and network level is also covered by the literature. Banerjee and Sheth explore challenges in interpreting and evaluating the quality of data at informational and application levels \[5\]. Authors propose solutions of at the different OSI layers to understand the factors affecting the quality of the system.

Cloud applications can scale up on demand (elasticity) depending on the application load. This characteristic is discussed in the study by Han et al. \[14\]. In this study, elastic scaling approach making use of cost-aware criteria to detect and analyze the bottlenecks of the cloud-based applications along with adaptive scaling algorithm for cost reduction was presented.

The nature of the IoT platform where devices (especially mobile devices) are dynamically joining or leaving the network creates new issues in enforcing QoS of such platform. Gomes et al. discuss this scalability characteristic and propose a new approach for resource allocation focusing on the performance of the system when participants disconnect \[12\].

Another relevant characteristic, an information flow efficiency is explored in supply chain management by Badenhorst et al. \[4\]. A conceptual framework of indicators and data-oriented metrics to evaluate the efficiency of information flows in supply chains are introduced in this study.

Also testability of an IoT system, especially testability by automated tests shall be considered as a quality characteristics. Previous attempt to define metrics for automated testability has been done for web applications \[7,8\], relevant for automated tests using the web-based user interface of the SUT. As IoT systems provide web-based user interfaces in many cases, this proposal can be applicable also to IoT context.

As the individual works discussed in this section focus rather on the IoT specific areas, on certain segments of the whole IoT platform, or does not reflect the quality aspects of IoT system in their full spectrum, a consolidated view has to be created to cover the whole spectrum of the IoT quality characteristics.

### 3 Proposed Classification

In the proposed classification, we merged several relevant proposals \[28,21,17,16,5,14,11,12,3,4,27\] into one unified view, which we enriched by several own suggestions of quality characteristics relevant for the IoT systems.

In the proposal, we followed several design principles:

(I) We added a physical device layer aspect to the classification, as this aspect becomes especially relevant in case of the IoT systems.

(II) We focused in special detail on Security, Privacy and Usability aspects, as these areas are considered as being critical for the IoT domain \[20\].

(III) We tried to minimize possible overlaps and duplications in the final proposed classification.
In this paper, we deliberately focus on quality characteristics instead of more detailed quality metrics. The reasons are the following: (1) the quality metrics might be too specific considering particular subdomain of IoT systems so that generalization might be not possible, and (2) much more SUT modelling information shall be required, making such attempt being out of the scope of the conference paper. Hence, in our consolidation, we abstracted some of the quality metrics from a subset of surveyed work (for instance [3,16]) to the quality characteristic without biasing the original purpose and meaning of the metric.

Table 1 presents this consolidated view. Regarding the level of granularity, we decided to use two levels: main level quality characteristic (in Table 1 by bold) and second-level quality characteristic, being a subcategory of the main level (in Table 1 by italics, indented).

For several quality characteristics, synonyms have been used in the investigated literature. Also, due to our experience, several synonyms are used in the industry praxis. We put these synonyms to the footnote with a citation to the source paper (or a comment that the synonym is our suggestion based on the industrial praxis). The last column of the Table 1 presents the origin of the suggested quality characteristic. Word own in this column indicates that the quality characteristic is our suggestion based on the industrial experience and quality characteristics defined in test management methodologies for traditional software systems.

Table 1: Proposed unified classification of IoT systems Quality Characteristics

| Quality Characteristics | Description                                                                 | Origin  |
|-------------------------|-----------------------------------------------------------------------------|---------|
| Accessibility           | The extent to which the system can be handled by users with specific needs. | own     |
| Availability            | Availability of the provided service or particular data supplied as the part of the service. | [28,21] |
| Device lifespan expectancy | What is the estimated lifetime of a single HW device?                       | own     |
| Elasticity              | The ability of the system to provide particular service on demand during a time interval. | [28]    |
| Installability          | What is the estimated lifetime of a single HW device?                       | [1]     |
| - Ease of deployment    | Effectiveness and efficiency with which the application can be deployed to devices of the system. | own     |
| Quality characteristic | Description | Source |
|------------------------|-------------|--------|
| Interoperability<sup>3</sup> | Capability of the system, product, or device to interact with another system, product or device or to interchange data with it. | own, [1] |
| Maintainability | Effort needed to perform various maintenance tasks of the deployed system. | [1] |
| - Replaceability | Effectiveness and efficiency with which an invalid unit or device of the system can be replaced | own |
| - Updateability | Effectiveness and efficiency with which a unit or device be updated to the latest version. | own |
| - Performance | The extent to which the system is able to handle a certain amount of data and concurrent user/device traffic. | own |
| Privacy | The extent to which the system maintains access to the user data corresponding to defined access rights by all involved parties and the extent to which the system prevents abuse of the user data | [1,17] |
| - Randomness | The extend to which the cryptographic algorithm used for protection generated random numbers (i.e. entropy size, or the randomness of the seed). | [17] |
| - Data privacy<sup>4</sup> | The extend to which the data is safely stored with appropriate measures (i.e. Encryption). This can also include the location of storage. | [1,17] |
| - Data Transmission | The extend to which the data is vulnerable to a replay or a Man in the Middle (MITM) attack. The extent to which the data being transmitted is encrypted with an appropriate algorithm. | [17] |
| - Access Control | The extend to which the user has access to data, and the data he and others can modify. | [17] |

<sup>3</sup> also Compatibility [1]
<sup>4</sup> also Confidentiality [1] or Data Store [17]
| Quality characteristic          | Description                                                                                                                                         | Source |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| – **Non-Repudiation**          | The extent to which the system can guarantee that the data has not been modified                                                                    | [17]   |
| – **Proof of Transaction**     | The extent to which a transaction can be proven to be from a user and the extent to which this user can be identified by other users if the data is leaked. | [17]   |
| **Reliability**                | The extent, in which the system is free from hardware and software defects, or other defects, which can lead to system failures.                     | [11, 28] |
| – **Data quality**             | Is the quality of the data provided by the system on the various levels (device, network, computing, and user interface) sufficient to enable correct run of the service? | [16, 5, 21] |
| – **Functional Correctness**  | What is the error rate of the system in the sense of functional defects affecting the system processes and the procedures handling the data stored in the system? | own    |
| – **Up-to-dateness**           | Are the data obtained from the system or device actual enough to enable correct operation of the service?                                             | [21]   |
| – **Trustworthiness**          | The extent to which the data provided by the system are trusted by its’ users.                                                                     | [23, 21] |
| **Resource utilization**       | The extent to which the resources required by the system were used in relation to the accuracy and completeness with which users of the system achieve their goals. | [1]    |
| – **Estimated energy efficiency** | How long can the device operate without a power source? Does the device have a backup power source? Can it switch to passive mode when not needed?         | own    |

5 also Correctness (our suggestion)
6 also Precision [21] or Data Integrity [5]
7 also Data validity (our suggestion)
8 also Efficiency [1]
| Quality characteristic | Description | Source |
|------------------------|-------------|--------|
| Responsiveness<sup>9</sup> | The extent to which the system handles a request within a required time interval. | [28] |
| Satisfaction | The extent to which user needs are satisfied when the system is used in a particular operation. | [4] |
| Scalability | The extent to which the system can adapt to new operational conditions, as the deployment model, size of processed data, user traffic conditions, added or removed devices and others. | [14,11,12] |
| Security | The extent to which the system protects its data so that any other party accessing to the system is given a level of access to this data, which is appropriate to the particular level of authorization. | [12,8,3] |
| – Attack Surface | The number of interfaces provided to the user to access data and their associated security. | [3] |
| – Given Sense of Control | The extent to which the user has access to control the device/application and the associated data collected and shared with the third party. | [3] |
| – Flaws vs Time | The number of critical flaws found over a period during a review or after deployment. | [3] |
| – Data Timeliness | The extent to which the data are backed up and can be retrieved by the users and/or forensic investigators. | [4] |
| – Data Provenance | The extent to which the data is guaranteed to be provided by a trusted source. | own |
| – Security Compliance | The extent to which a system is compliant with a given security standard fit for its purpose (i.e. Critical infrastructure, Military, General Public). | [3] |
| Testability | The extent how easy is to design and conduct tests for the system, especially automated tests. | own |

<sup>9</sup> also Time–behavior [4]
| Quality characteristic     | Description                                                                                                                                                                                                 | Source |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Usability                 | The extent how easy, efficient, and enjoyable the interface of the system is to use and how efficiently the user interface contributes to support of the tasks user has to perform in the system.                          | [1,28,27] |
|                           | - **Subjective Satisfaction**                                                                                                                                                                                | 27     |
|                           | The extend to which a user is satisfied with both the software and its interface.                                                                                                                                 |        |
|                           | - **Rate of User Error**                                                                                                                                                                                    | 27     |
|                           | The extend to which the user encounter errors on the system or is required to perform an error action (i.e. reset a password, back-end error).                                                            |        |
|                           | - **Speed to Learn**                                                                                                                                                                                        | 27     |
|                           | The time required by the user to learn about the software and intrinsic characteristics. This can relate to the time for the user to perform an easy, medium or hard action with a software.                        |        |
|                           | - **Support of Secure Behavior**                                                                                                                                                                             | own    |
|                           | The extend to which the security notifications and control are both enjoyable and understandable by a lay user. The user interface contributes to the cyber-situational awareness of the user. |        |

4 Discussion

In this section, discuss several issues related to taken approach and related questions.

Regarding the selection of the resources, to compile the presented consolidated view, we preferred works which are also consolidating the previous ideas, for instance, summary by Li et al. [21], which aggregates a set of previous works as [6,19,26,24,25].

During the creation of the presented consolidated view on IoT systems Quality Characteristics, interpretation of particular items may be different by individual authors. As an example, Availability can be discussed: this characteristic is described as ”Uptime percentage of cloud services during a time interval” by Zheng et al. [28], or as a ”Availability of the data sources, measured by a ratio of the number of attributes available to the total number of attributes” by Li et al. [21]. In such cases, we consolidated the metric to more general one, as, in the example of Availability was ”Availability of the provided service or particular data supplied as the part of the service”. Another example of this generalization is the Data quality, where Li et al. [21] understands this characteristic to cover
all layers of the SUT spanning from physical layer to the user interface layer, whereas Ikeda et al. [16] discuss this characteristic in context of the IoT devices. Similarly, we unified a concept of *scalability* understood differently by various authors [14,11,12].

In case of *Resource utilization* and *Efficiency* suggested by TMAP [1], these two categories seem rather overlapping, even if not equivalent. Hence, we decided to merge these both categories into final *Resource utilization*, as this characteristic express the idea better.

In another situation, we decided to add more specific quality characteristic, than was reported in works dealing with this topic previously. The example is *Accessibility*. In [1] and [28], *Accessibility* is implicitly understood as a part of *Usability*, however, according to the common understanding of these two concepts, for instance [15], our suggestion is to distinguish these two categories.

We made also generalization in case of *Confidentiality* suggested by TMAP [1] — we included this characteristic as a subtype of *Privacy* category, named as *Data Privacy*, as we merged this characteristic with *Data Store* suggested by Islam et al. [17].

A discussion can be made, if suggested *Up-time* subcategory of the *Reliability* does not duplicate *Availability*. As the *Up-time* related to particular IoT devices in the sense of their reliability, whereas *Availability* category describes the overall availability of the system, we decided to keep these two characteristics separated.

In the proposed categorization we decided to exclude characteristics metrics related to test coverage levels [2] as well as metrics for assessment of efficiency of test cases, for example [10,22]. Such metrics might be discussed in the context of testing process efficiency, however, does not directly relate to the quality characteristics of SUT (a relevant exception would be, when an automated test suite was considered as an SUT).

Another point can be raised regarding a question, if proposed two–level categories are appropriate to organize the discussed quality characteristics. In the current categorizations, only one level list is usually used, for instance [18] or [2]. However, specific focus on physical layer aspects, security, privacy, reliability and maintainability of an IoT system led us to the identification of more relevant subcategories, which justify the proposed two–level structuring.

5 Conclusion

The usage of quality characteristics contributes to the better structuring of the testing process, helps in the test reporting and acts as a check–list for the test engineers aiding decision which quality aspects of the SUT to test. For these reasons, we consider it useful to provide a comprehensive view of the quality characteristics for the IoT systems, focusing on the specifics of these systems. As the previous work discusses rather individual areas of IoT systems and particular subareas of system quality, in this paper we provide a consolidated view. This effort involved extensive discussions arising from an attempt to consolidate the particular terminology used by various authors; we summarize this discussion
In the proposed classification we emphasized specific characteristics of the IoT system. Namely, we reflected physical device layer more intensely in comparison to standard software quality characteristics, for instance, and we focused in special detail to Security, Privacy and Usability aspects, as these areas are considered as being critical for the IoT domain. This focus makes the proposed IoT characteristics more relevant to IoT systems, compared to a case, when standard software quality characteristics would be used in testing of an IoT solution.

Acknowledgements

This research is conducted as a part of the project TACR TH02010296 Quality Assurance System for Internet of Things Technology.

References

1. TMap: a set of quality characteristics for IoT testing. [http://www.tmap.net/wiki/quality-characteristics#TitleLink](http://www.tmap.net/wiki/quality-characteristics#TitleLink) accessed: 2019-08-09
2. van der Aalst, L., Roodenrijs, E., Vink, J., Baarda, R.: TMap NEXT: business driven test management. Uitgeverij kleine Uil (2013)
3. Abbadi, Z.: Security metrics what can we measure? In: Open Web Application Security Project (OWASP), Nova Chapter meeting presentation on security metrics, viewed. vol. 2 (2011)
4. Badenhorst-Weiss, J.A., Maurer, C., Brevis-Landsberg, T.: Developing measures for the evaluation of information flow efficiency in supply chains. Journal of Transport and Supply Chain Management 7(1), 1–13 (2013)
5. Banerjee, T., Sheth, A.: IoT quality control for data and application needs. IEEE Intelligent Systems 32(2), 68–73 (Mar 2017). [https://doi.org/10.1109/MIS.2017.35](https://doi.org/10.1109/MIS.2017.35)
6. Bu, Y., Gu, T., Tao, X., Li, J., Chen, S., Lu, J.: Managing quality of context in pervasive computing. In: Quality Software, 2006. QSIC 2006. Sixth International Conference on. pp. 193–200. IEEE (2006)
7. Bures, M.: Metrics for automated testability of web applications. In: Proceedings of the 16th International Conference on Computer Systems and Technologies. pp. 83–89. ACM (2015)
8. Bures, M.: Model for evaluation and cost estimations of the automated testing architecture. In: New Contributions in Information Systems and Technologies, pp. 781–787. Springer (2015)
9. Bures, M., Cerny, T., Ahmed, B.S.: Internet of things: Current challenges in the quality assurance and testing methods. In: Kim, K.J., Baek, N. (eds.) Information Science and Applications 2018. pp. 625–634. Springer Singapore, Singapore (2019)
10. Bures, M., Cerny, T., Klima, M.: Prioritized process test: More efficiency in testing of business processes and workflows. In: Kim, K., Joukov, N. (eds.) Information Science and Applications 2017. pp. 585–593. Springer Singapore, Singapore (2017)
11. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems 25(6), 599–616 (2009)
12. Gomes, R., Bouloulakis, G., Costa, F., Georgantas, N., Da Rocha, R.: Qos-aware resource allocation for mobile iot pub/sub systems. In: International Conference on Internet of Things. pp. 70–87. Springer (2018)

13. Guceglioglu, A.S., Demirors, O.: Using software quality characteristics to measure business process quality. In: International Conference on Business Process Management. pp. 374–379. Springer (2005)

14. Han, R., Ghanem, M.M., Guo, L., Guo, Y., Osmond, M.: Enabling cost-aware and adaptive elasticity of multi-tier cloud applications. Future Generation Computer Systems 32, 82–98 (2014)

15. Henry, S.L., Abou-Zahra, S., Brewer, J.: The role of accessibility in a universal web. In: Proceedings of the 11th Web for All Conference. pp. 17:1–17:4. W4A’14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2596695.2596719

16. Ikeda, Y., Kouno, S., Shiozu, A., Noritake, K.: A framework of scalable qoe modeling for application explosion in the internet of things. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). pp. 425–429 (Dec 2016). https://doi.org/10.1109/WF-IoT.2016.7845393

17. Islam, S., Falcarin, P.: Measuring security requirements for software security. In: 2011 IEEE 10th International Conference on Cybernetic Intelligent Systems (CIS). pp. 70–75 (Sept 2011). https://doi.org/10.1109/CIS.2011.6169137

18. Jung, H.W., Kim, S.G., Chung, C.S.: Measuring software product quality: A survey of iso/iec 9126. IEEE software (5), 88–92 (2004)

19. Kim, Y., Lee, K.: A quality measurement method of context information in ubiquitous environments. In: Hybrid Information Technology, 2006. ICHIT’06. International Conference on. vol. 2, pp. 576–581. IEEE (2006)

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

21. Li, F., Nastic, S., Dustdar, S.: Data quality observation in pervasive environments. In: 2012 IEEE 15th International Conference on Computational Science and Engineering. pp. 602–609 (Dec 2012). https://doi.org/10.1109/ICCSE.2012.88

22. Li, N., Li, F., Offutt, J.: Better algorithms to minimize the cost of test paths. In: Software Testing, Verification and Validation (ICST), 2012 IEEE Fifth International Conference on. pp. 280–289. IEEE (2012)

23. Manuel, P.: A trust model of cloud computing based on quality of service. Annals of Operations Research 233(1), 281–292 (Oct 2015). https://doi.org/10.1007/s10479-013-1380-x

24. Manzoor, A., Truong, H.L., Dustdar, S.: On the evaluation of quality of context. In: European Conference on Smart Sensing and Context. pp. 140–153. Springer (2008)

25. Neisse, R., Wegdam, M., Van Sinderen, M.: Trustworthiness and quality of context information. In: Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for. pp. 1925–1931. IEEE (2008)

26. Sheikh, K., Wegdam, M., Van Sinderen, M.: Middleware support for quality of context in pervasive context-aware systems. In: null. pp. 461–466. IEEE (2007)

27. Sollie, R.S.: Security and usability assessment of several authentication technologies. Master’s thesis (2005)
28. Zheng, X., Martin, P., Brohman, K., Xu, L.D.: CloudQual: A quality model for cloud services. IEEE Transactions on Industrial Informatics 10(2), 1527–1536 (May 2014). https://doi.org/10.1109/TII.2014.2306329

Paper accepted at

Urb-IoT 2018
3rd EAI International Conference on IoT in Urban Space

November 21-23, 2018, Guimares, Portugal

http://urbaniot.org/full-program/