Journal of Reliable Intelligent Environments (2022) 8:223–226
https://doi.org/10.1007/s40860-022-00182-5

EDITORIAL

Intelligent environments with entangled quality properties

Carlos Rodríguez-Domínguez[1] · Aditya Santokhee[2] · Miguel J. Hornos[1]

Published online: 20 July 2022

1 Introduction

Intelligent environments (IEs) [1], and other very close disciplines, such as Ambient Intelligence (AmI) [2], Smart Environments (SmEs) [3], and even Internet of Things (IoT) [4–6], are intended to proactively improve human lifestyle in many aspects, like healthcare, social inclusion, people assistance, quality of life, lifelong learning, and intelligent and adapted transport, among others. The development of an IE that can be successfully delivered to the society is a complex challenge. So much so that it requires a multidisciplinary team that has to be not only capable of applying a combination of techniques and methods coming from Software Engineering to improve its reliability [7], but also from other Computer Science disciplines, such as artificial intelligence, ubiquitous/pervasive computing and human—computer interaction, among others, that make the resulting IE less intrusive, while being smarter, more proactive and usable for the user. All this with the ultimate goal of increasing user confidence in the IE developed [8, 9].

Therefore, IE development not only involves deploying large scale sensor/actuator networks and the use of a middleware, communication protocols, location/positioning methods, artificial intelligence techniques, smart applications, etc., but also achieving a high level of reliability, performance, usability, security, and many other quality properties. However, these quality properties are *entangled*, that is, achieving one of them usually involves either fulfilling or decreasing the level of achievement of others. For instance, developing a highly usable IE will probably mean to also develop a high-performance responsive system. However, developing a high-performance system may require reducing security checks and, therefore, the reliability of the whole system.

Those inter-relationships and balances between quality properties are difficult to address. It is particularly difficult to decide which are the most important quality properties to be fulfilled in an IE. In this last decade, some researchers of the IE field have focussed their contributions on addressing specific quality goals [10–18]. However, there are fewer contributions analyzing the interactions between those quality properties, and how they should be balanced with others in real consumer-oriented developments.

This is the reason why we have proposed this Special Issue (SI) on *Intelligent Environments with Entangled Quality Properties*. This SI was specially conceived so that the authors of papers selected from among those accepted to be presented in the 10th International Workshop on the Reliability of Intelligent Environments (WoRIE 2021)[1] could submit extended versions of their works. Nonetheless, an open call was made for other researchers who were working on topics related to the general theme addressed on this SI, even if they had not participated in the workshop, could also submit their manuscripts to it. In fact, only one of the articles included in this SI is an extension of a paper presented at WoRIE 2021. This is a pre-conference workshop held within the 17th International Conference on Intelligent Environments (IE 2021)[2] and offered as a forum to discuss not only the state of the art, trends and novel methods and techniques to improve the reliability of IE, but also other quality properties like performance, security, safety or usability. This workshop, which is gradually consolidating and covers a broad range of topics, intends to build solid bridges of collaboration between the different communities involved in IE research and development.

✉ Carlos Rodríguez-Domínguez
carlosrodriguez@ugr.es

Aditya Santokhee
a.santokhee@mdx.ac.mu

Miguel J. Hornos
mhornos@ugr.es

[1] MYDASS (Modelling and Development of Advanced Software Systems) Research Group, Software Engineering Department, Higher Technical School of Computer and Telecommunication Engineering, Campus de Aynadamar, University of Granada, 18071 Granada, Spain

[2] School of Digital Technologies, Middlesex University Mauritius, Flic en Flac, Mauritius

[1] https://www.ugr.es/~worie/2021.

[2] https://www.mdx.ac.ae/ie2021.

Consequently, this SI, which aims to expand the discussion of such exciting and challenging topics beyond the workshop, is focussed on presenting IEs that have to consider entangled quality properties and balance their degree of fulfilment to produce a quality consumer-oriented solution.

2 Contents of this special issue

Bearing in mind what is indicated in the previous section, this section contains a summary of each of the five articles that have been selected to be published in this SI from among those submitted to it. Our intention is to present here a compendium of its contents, which serves to briefly present the work addressed in each of them, as well as to encourage readers interested in the topics covered in these articles to read them and obtain more information about the research works described in them.

In the first paper, entitled *A survey on reliability and availability modeling on Edge, Fog and Cloud Computing*, Maciel et al. present the differences between these three concepts and address the modelling of certain properties (reliability and availably) on them. Cloud computing is a model that promotes ubiquitous, on-demand network access to shared computing resources [19]. Fog computing intends to bring the services intended to process data as close as possible to the devices generating those data [20], thus decreasing network latency and processing load of Cloud services. Finally, Edge computing intends to further decrease network latency and processing load by moving as many processing tasks as possible to the devices themselves [21]. Consequently, each of those computing paradigms promote a set of entangled quality properties that need to be balanced in any IE, such as flexibility, processing power, efficiency, network latency, etc. In fact, the need of balancing those properties has led most recent IEs to integrate Edge, Fog and Cloud computing paradigms within their system architectures. In that sense, the authors highlight reliability and availability as two crucial, interlinked properties that can be pursued in most systems through the integration of those paradigms. The outcomes of this paper also point out some important open challenges related to the entanglement of reliability and availability with other properties. For instance, the authors mention that Edge devices (such as those found in IoT environments) promote reliability and availability, but it is still necessary to explore how to promote security and privacy on those resource-constrained devices or how to balance those attributes with energy consumption.

In the second paper, entitled *EFSUTE: a novel efficient and survivable traffic engineering for software defined networks*, Mohammadi and Javidan propose a traffic engineering model, called EFSUTE, which intends to promote a good balance between efficiency and survivability in software defined networks (SDNs). EFSUTE monitors working and backup paths on the relevant switches of an SDN. If a link failure occurs, then the working path is declared unavailable, and the backup path is considered to manage the traffic flows. To compute the optimal paths, EFSUTE considers low congested links with shorter delays. The authors have shown through a set of simulations that EFSUTE is very efficient in comparison with other solutions, while, at the same time, it reduces the packet loss ratio, thus improving survivability. Therefore, EFSUTE is able to tackle with QoS issues, which are challenging to address in most IEs. Moreover, efficiency and survivability are a good example of entangled properties, since increasing survivability commonly involves setting up constraints and mechanisms that usually decrease efficiency.

In the third paper, entitled *Helping novice developers harness security issues in cloud-IoT systems*, Corno, De Russis and Mannella investigate security features that two popular cloud-IoT platforms offer to developers for implementing IoT-based systems, given that developing high quality and secure IoT systems are inherently challenging, due to these are complex systems with strict requirements, especially if their developers are novices. The problem is further exacerbated if these systems are designed, developed and deployed on open networks without adequate consideration for privacy and security quality properties, which should be entangled with the rest of quality properties. This study, which is inspired by a survey administered to a small group of novice developers by the researchers, finds out that novice developers often tend to overlook security considerations during the design and implementation phases of the development of IoT systems. This is due to their lack of knowledge and understanding on the features provided by cloud IoT platforms. Therefore, the authors propose a set of fourteen guidelines to better inform novice developers build more reliable and secure systems by tapping into the features offered by two prevalent Cloud IoT platforms (Amazon Web Services IoT and Microsoft Azure IoT).

In the fourth paper, entitled *Feature selection and human arm activity classification using a wristband*, Zhang et al. present a research work that investigates the potential for improving strategies and algorithms used in data pre-processing and model training/testing for wrist-worn accelerometer sensing. Recent advances in technology have facilitated the development of unobtrusive, lightweight, low-cost and power-efficient mobile wristbands which incorporate accelerometers [22, 23]. A salient feature of these devices is that they capture human activity data which necessitates classification algorithms to analyze the data. However, these are small devices with low computational power and therefore it is imperative to choose the right strategies to manage quality properties, such as accuracy and performance. Consequently, Zhang et al. claim that data pre-processing methods and optimal model selection algorithms are crucial for human

activity recognition. To begin with, they argue that it is crucial to select the feature which will contribute most to the performance of the model from a given dataset. They not only provide a list of potential benefits of feature selection [24] to maximise the classification accuracy and minimize the number of features but also critically compare feature selection and normalisation techniques. The authors investigated different techniques for data sampling frequency, feature ranking, feature scaling and sub-feature sets selection, as well as model selection strategies based on Neural Networks, Support Vector Machines, and Bayes classification algorithms. They recommend a novel plurality voting mechanism to adjust the prediction result during the model testing stage. The paper concludes that the most robust and reliable performance for human activity classification can be obtained from a combination of an individual data model together with a plurality voting mechanism.

Finally, in the fifth paper, entitled *Securing future healthcare environments in a post-COVID-19 world: Moving from frameworks to prototypes*, Vithanwattana et al. investigate pertinent security vulnerabilities and examines several existing security frameworks for eHealth and mHealth. As healthcare systems around the world have been under tremendous pressure during the COVID-19 pandemic, many healthcare services need to be moved to video, telephone or online sessions, while face-to-face sessions were significantly reduced to cater for medical emergencies or surgeries. In this scenario, it is undeniable that eHealth and mHealth systems could pave the way by offering basic medical services online in the future, given that medical devices have also been increasingly developed and deployed to monitor and record patients' health parameters. This would help medical facilities streamline their services more efficiently. However, this transformation will depend upon how successfully some of the impending security challenges are met. Consequently, the authors argue that security should be embedded from when healthcare data is collected, then transferred over the network, and stored in both on-site storage and cloud storage. This reinforces the notion that a quality framework should also support all necessary security quality properties, which are entangled, such as confidentiality, integrity, availability, non-repudiation, authentication, authorisation, accountability, auditability, and reliability [25, 26]. Thus, they propose a novel comprehensive implementation framework based on their literature review, which demonstrated that no existing framework caters for all the security requirements and healthcare environments [26]. In the end, a prototype is developed to validate and demonstrate application of their implementation framework. This study also consolidates the notion that development of reliable and secure applications depends on how successfully security properties, among other quality properties, are embedded and entangled during the development process as well as the importance of clear development guidelines.

References

1. Augusto JC, Callaghan V, Cook D, Kameas A, Satoh I (2013) Intelligent environments: a manifesto. HCIS 3:12. https://doi.org/10.1186/2192-1962-3-12
2. Ramos C, Augusto JC, Shapiro D (2008) Ambient intelligence—the next step for artificial intelligence. IEEE Intell Syst 23(2):15–18. https://doi.org/10.1109/MIS.2008.19
3. Cook D, Das SK (2005) Smart environments: technology, protocols and applications, vol 43. Wiley, Hoboken
4. Ashton K (2009) That 'internet of things' thing. RFID J 22(7):97–114
5. Li S, Xu LD, Zhao S (2015) The internet of things: a survey. Inf Syst Front 17:243–259. https://doi.org/10.1007/s10796-014-9492-7
6. Buyya R, Dastjerdi AV (eds) (2016) Internet of things: principles and paradigms. Elsevier, Amsterdam. https://doi.org/10.1016/C2015-0-04135-1
7. Hornos MJ (2017) Application of software engineering techniques to improve the reliability of intelligent environments. J Reliab Intell Environ 3(1):1–3. https://doi.org/10.1007/s40860-017-0043-0
8. Hornos MJ, Rodríguez-Domínguez C (2018) Increasing user confidence in intelligent environments. J Reliab Intell Environ 4(2):71–73. https://doi.org/10.1007/s40860-018-0063-4
9. Corno F, Guercio E, De Russis L, Gargiulo E (2015) Designing for user confidence in intelligent environments. J Reliab Intell Environ 1(1):11–21. https://doi.org/10.1007/s40860-015-0001-7
10. Augusto JC, Hornos MJ (2013) Software simulation and verification to increase the reliability of intelligent environments. Adv Eng Softw 58:18–34. https://doi.org/10.1016/j.advengsoft.2012.12.004
11. Preuveneers D, Joosen W (2016) Semantic analysis and verification of context-driven adaptive applications in intelligent environments. J Reliab Intell Environ 2(2):53–73. https://doi.org/10.1007/s40860-016-0019-5
12. Le Guilly T, Nielsen MK, Pedersen T, Skou A, Kjeldskov J, Skov M (2016) User constraints for reliable user-defined smart home scenarios. J Reliab Intell Environ 2(2):75–91. https://doi.org/10.1007/s40860-016-0020-z
13. Oguego CL, Augusto JC, Muñoz A, Springett M (2018) A survey on managing users' preferences in ambient intelligence. Univ Access Inf Soc 17(1):97–114. https://doi.org/10.1007/s10209-017-0527-y
14. Hallsteinsen S, Geihs K, Paspallis N, Eliassen F, Horn G, Lorenzo J, Mamelli A, Papadopoulos GA (2012) A development framework and methodology for self-adapting applications in ubiquitous computing environments. J Syst Softw 85(12):2840–2859. https://doi.org/10.1016/j.jss.2012.07.052
15. Benghazi K, Hurtado MV, Hornos MJ, Rodríguez ML, Rodríguez-Domínguez C, Pelegrina AB, Rodríguez-Fórtiz MJ (2012) Enabling correct design and formal analysis of ambient assisted living systems. J Syst Softw 85(3):498–510. https://doi.org/10.1016/j.jss.2011.05.022
16. Coronato A, Paragliola G (2017) A structured approach for the designing of safe AAL applications. Expert Syst Appl 85:1–13. https://doi.org/10.1016/j.eswa.2017.04.058
17. Suh YH, Lee KW, Cho ES (2018) A software framework for robotic mediators in smart environments. J Reliab Intell Environ 4(2):89–105. https://doi.org/10.1007/s40860-018-0060-7
18. Given-Wilson T, Legay A, Sedwards S, Zendra O (2018) Group abstraction for assisted navigation of social activities in intelligent

environments. J Reliab Intell Environ 4(2):107–120. https://doi.org/10.1007/s40860-018-0058-1
19. Mell P, Grance T (2011) The NIST definition of cloud computing. Comput Secur Div Inf Technol Lab. https://doi.org/10.6028/NIST.SP.800-145
20. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In: Proceedings of the first edition of the MCC workshop on mobile cloud computing (MCC'12), Helsinki, Finland, pp 13–16. https://doi.org/10.1145/2342509.2342513
21. Naha RK, Garg S, Georgakopoulos D, Jayaraman PP, Gao L, Xiang Y, Ranjan R (2018) Fog computing: survey of trends, architectures, requirements, and research directions. IEEE Access 6:47980–48009. https://doi.org/10.1109/ACCESS.2018.2866491
22. Cornacchia M, Ozcan K, Zheng Y, Velipasalar S (2017) A survey on activity detection and classification using wearable sensors. IEEE Sens J 17(2):386–403. https://doi.org/10.1109/JSEN.2016.2628346
23. Mukhopadhyay SC (2015) Wearable sensors for human activity monitoring: a review. IEEE Sens J 15(3):1321–1330. https://doi.org/10.1109/JSEN.2014.2370945
24. Guyon I, Elisseeff A (2003) An introduction to variable and feature selection. J Mach Learn Res 3:1157–1182. https://doi.org/10.5555/944919.944968
25. Yayah F (2017) A Security Framework to Protect Data in Cloud Storage. PhD Thesis. University of Southampton. Southampton
26. Vithanwattana N, Mapp G, George C (2017) Developing a comprehensive information security framework for mHealth: a detailed analysis. J Reliab Intell Environ 3:21–39. https://doi.org/10.1007/s40860-017-0038-x