A Systematic Exploration on Challenges and Limitations in Middleware Programming for IoT Technology

Pedro Taveras, Pontificia Universidad Catolica Madre y Maestra, Santo Domingo, Dominican Republic

ABSTRACT

In a distributed environment, such as IoT, the requirement for constant sensing and actuating from a diverse source of devices increases the complexity and therefore, the operational cost of the software required to keep the system running. The article covers the conceptual and technological aspects, together with a series of previous experiences, findings, and literature that constitute the essence of the body of knowledge related to the issues and challenges for developing middleware that supports the IoT domain’s independent functionality. The article provides the foundation to understand the challenges faced in the development of IoT middleware, focusing on five sensitizing elements, namely, IoT evolution, architecture, security, middleware, and programming. The systematic exploration on limitations for IoT software development revealed the need for programming methods and language abstractions to cope with the demands of IoT scenarios, specifically to deal with the challenges of massive communications, limited infrastructure, and multiplicity of devices.

KEYWORDS

Internet of Things, IoT, IoT Architecture, Microservice Model, Middleware Programming

1. INTRODUCTION

Developing IoT based products is a complicated task, regardless of whether the product is an autonomous vehicle, a smart home appliance or a factory automation system. IoT-based products contain thousands, if not millions, of embedded lines of codes. And many of these products and the systems and software that control them are critical from a security point of view. Therefore, programmers must be confident that the software code that controls these devices is 100% accurate and responds in the manner and speed intended. The consequences can be dire if these were not so. Additionally, many of these products must be certified or the product design flow must follow a standard process of industrial certification. Progressively, there is increasing pressure for companies to design IoT enabled devices and products more quickly and economically, while maintaining the highest level of security and performance. However, there are known problems and limitations faced in

DOI: 10.4018/IJHIoT.2018070101

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
software development for IoT middleware, using models and tools that are not adequate to achieve the computational performance level demanded by a robust IoT middleware. Considering that developing IoT software does not necessarily mean to create an algorithm for an object to be intelligent, but rather to connect it to the network and thus integrate it with the world of information. This integration allows to scale a solution, and thus add more value to the end user, and can even change a business model. The cloud and big data are part of this ecosystem. The cloud and all its services make the IoT possible because of its low costs in relation to its size and the possibility of scaling. On the other hand, big data makes the IoT truly useful in being able to have distributed solutions that can be analyzed comprehensively and thus obtain statistics and probabilities to predict possible situations.

Nonetheless, defining IoT is a fuzzy task. IoT is the result of the integration and evolution of different technological and social fields (IEEE, 2016). Some researchers attempted to address IoT features to find the ground for its definition and facilitate the understanding of the subject. In this sense, Haller (2010) asserted that all the different definitions of the term “Internet of Things” agree that the concept is linked to the integration of the physical world with the digital world of the Internet. The term “thing” in IoT refers to the daily physical objects that we normally handle, equipped with sensors, identifiers, and an Internet Protocol (IP) address. These objects are electronic devices with basic computational features, which are capable of communicating with other objects with similar characteristics, are appointed as “things.” The “things” can access resources from the outside world through a collection of procedures (software pieces) that can be called from anywhere on the Internet. As shown in Figure 1, this mechanism for invocation, a resource called service, is completely independent of the platform used and the programming language in which the system is implemented. These resources may offer a middleware that function as a direct interface to a given endpoint (computer, sensor, device) or network resources that act as proxies, possibly providing additional levels of aggregation and abstraction (Haller, 2010).

IoT, in general, is an area that poses significant challenges. From the technical point of view, it is necessary to provide a reliable system with adequate efficiency, security, and performance capabilities (Commission of the European Communities, 2008). In this domain, security and reliability have a double connotation. They are related to a nascent technology but are also part of the requirements of the architecture that should make this technology usable and exploitable, and understanding how the computational properties (constructs) of this technology can contribute to expanding the current knowledge about IoT middleware programming and design. Therefore, the first step is to understand that an IoT is a nascent technology (Fischer et al., 2016). Moreover, the second step, is to understand that it is a product of the convergent evolution of other computational developments called enablers (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015). Academic and practitioners’ literature, considered as seminal, contextual, and recent, were examined to provide the supporting evidence and

Figure 1. IoT architecture (RoboQ, 2018)
The Vertical-Cavity Surface-Emitting Laser: A Key Component in Future Optical Access Networks
[www.igi-global.com/chapter/vertical-cavity-surface-emitting-laser/36331?camid=4v1a](www.igi-global.com/chapter/vertical-cavity-surface-emitting-laser/36331?camid=4v1a)

Internet of Things: Privacy and Security Implications
[www.igi-global.com/article/internet-of-things/179894?camid=4v1a](www.igi-global.com/article/internet-of-things/179894?camid=4v1a)