

Chapter 13

Summary and Outlook

Alessandro Bassi

Five years ago, when we organised the very successful meeting “Beyond RFID: the Internet of Things”,¹ we were pioneering a new space. At that time, a global network of interconnected objects was just a very fancy and rather fuzzy concept. Today, this topic is clearly mainstream.

Cisco² and Ericsson³ have published white papers clearly showing the relevance and the importance of IoT-related technologies for their strategic offering; to mention just a few numbers, for whatever they are worth, apart from the famous forecast of 50 billion interconnected devices by 2020,⁴ Cisco foresees a related market value of \$14.4 trillion.⁵ These companies are just the tip of the iceberg: McKinsey, for instance, recently published a report⁶ estimating the IoT impact on the global GDP as between \$2.7 and \$6.2 trillion annually by 2025, an impact which is beyond that of big data. In 2012, Gartner Research identified the IoT as one of the top ten technology trends for the years to come.⁷

As members of the IoT-A consortium, we are rather proud to be at the forefront of this wave. Back in 2009, we clearly identified the main technological showstoppers for the development of a global IoT vision. The problems we faced back then were threefold.

As early developments were clearly not coherent, and showed little if any possibility of integration in bigger systems, scalability capabilities or an ability to

¹ <http://www.smart-systems-integration.org/public/internet-of-things>

² <http://share.cisco.com/internet-of-things.html>

³ <http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf>

⁴ <http://share.cisco.com/internet-of-things.html>

⁵ <http://iotevent.eu/cisco-sees-14-trillion-opportunity-in-iot/>

⁶ http://www.mckinsey.com/insights/business_technology/disruptive_technologies

⁷ <http://www.gartner.com/newsroom/id/2209615>

A. Bassi (✉)

Alessandro Bassi Consulting, 3, Avenue de Cannes, 09160 Juan Les Pins, France

e-mail: alessandro@bassiconsulting.eu

adopt strong security policies, the need was very evident: to define a common IoT ground where services, applications and products could have solid roots. This common ground is established by making different technologies talk to each other, allowing existing and new IoT-related developments to belong to the same space.

Furthermore, it is important to define a way of moving from ground-breaking ideas to real products and services.

Finally, we needed to show not only the research community but the whole community of innovators that IoT technologies can actually be used to implement their projects, providing innovation managers and architects with the necessary tools to do so.

The IoT-A project tackled the first point by upgrading existing technological developments. Communication protocols related to constrained devices were studied and extensions were proposed, tested and promoted in the appropriate standardisation fora.

As far as defining ways of moving from ground-breaking ideas to real products and services is concerned, in many formal and informal meetings we see reactions such as “what the heck?” when we explain what IoT can do for a business domain. There is a clear need for education and information that is missing at the moment. Innovation directors may have a very clear vision of what they want to achieve, but there is no way for them to understand the complexity of their challenges, to select the best architectural design patterns that can solve their issues, and to decide which technologies to use to implement a solution in practice. We see this as a vertical challenge: from a vision to a product, designing the right set of models, architectures and tools. This point was addressed by the development of the Architectural Reference Model (ARM), which includes all necessary models and design patterns for developing a real product.

Finally, after tackling both of these dimensions, as already stated, we needed to show not only the research community but the whole community of innovators that IoT technologies can actually be used to implement their projects, giving innovation managers and architects the necessary tools to do so. A silver bullet in a drawer does not solve any issues; we needed to “go out” and reach the widest possible range of most diversified audiences in order to make our work worthwhile. This book clearly addresses this third aspect of communication.

We are also aware, however, that all dimensions need further work. From the very beginning, we intended the ARM to be an iterative effort. The set of models and architectural choices will evolve, and the project partners are seeking suitable ways of making the concepts long-lasting, well beyond the project’s lifetime. What is important is that the ARM and all related developments cannot be “locked” in the sole ownership of one single organisation or group – every instrument that can promote and develop the architectural development of the IoT further must be able to use the ARM work done in IoT-A as a base.

The horizontal integration between different technologies will also require updates. As different IoT-related technologies evolve, there will be a need to develop different interfaces at any level, from device level to services. Further

investigation and efforts will be required: in particular, considering possibly revolutionary developments such as quantum technologies. Within IoT-A, we tried to provide guidelines for developments in some areas, such as protocols; however, as long-term forecasts are very often off-target, only time will tell exactly which areas will need closer attention.

Last, but certainly not least, a considerable amount of work must be done to develop sustainable security and privacy policies. Even before the IoT, RFID technologies were subject to a very negative “big brother” image. These considerations are very topical today, with the disclosure of the US government’s PRISM program, and any technology for interconnected objects may be rejected on the basis that it violates basic privacy principles. Therefore, governance schemes that on one hand are privacy-friendly, and on the other hand secure, must be agreed upon and implemented, along with widespread education on the societal benefits of IoT.

Open Access This chapter is distributed under the terms of the Creative Commons Attribution Non-commercial License, which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.