An IoT Model for Coping with Trade-offs in Designing Smart Environments

Fabio Cassano, Antonio Piccinno

Dipartimento di Informatica, Universitá di Bari Aldo Moro, Bari, Italy
{fabio.cassano1, antonio.piccinno}@uniba.it

Abstract. The Internet of Things (IoT) world is composed by a huge number of different so called "smart devices" and every year new and different models are released on the mass market. Most of those devices are intended to be used by professional people or by companies. Thanks to the constant growth of the "smart objects", end users and people with low or no-knowledge of the IT-world get in touch with these pieces of technology. Those people are expected to use the smart devices "out of the box" and in a very simple and easy way so, the human-device interaction needs to be as easiest as possible. Despite of this need, end users are commonly faced with thousand of different technological standards which are hard to evaluate without a solid IT background. Thus, the comparison to understand which IoT device performs better in a particular situation become complicated. In this paper we propose a comparison of two different IoT solutions using an IoT model. The model assesses the different technical specifications of the devices and then extracts a "score" for each technological aspect. The end user can use the score to better understand the points of strength and the weaknesses of the devices.

Keywords: IoT, Smart Device, IoT model

1 Introduction

The mass market offers to expert and non-expert users thousands of different Internet of Things devices. Those devices are generally composed by sensors, electronics boards and antennas that allows them to communicate with the "outside" world. Due to the enormous number of combinations of those three components, the number of the available devices gets higher and higher. Hardware, programming, security, protocols etc. are terms that often are not clear to the end user that has to face the choice among multiple IoT devices. Indeed, the complexity of the choice increases when multiple objects can be used in multiple application contexts. Often, specific devices that are built to work in certain domains, thanks to their characteristics, can be also used in more and different contexts. For example, a temperature monitoring device for the home environment can be also used in a pharmacy store to check and control the temperature of the medicine room, using a "sink" node to transmit the data over the Internet. To correctly

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

configure an ecosystem made by multiple different devices, end users need to understand most of the device's characteristics [3,15]. This is not an easy task even for experienced people, due to the high number of different technical variables that need to be considered during this process. Thus, finding the right "trade off" between the technological aspect of the ecosystem and the different devices may be long and challenging. In literature, examples of comparing physical devices that require skills in selecting the right devices, preparing the environment settings, selecting users, identifying the tasks, etc. are reported [2,3].

In this paper we first propose a model to assess smart devices in order to give a way to assess the suitability of a specific smart device to a certain application domain. Each device characteristic can be assessed and compared in order to choose the one that best satisfies the end user needs. We also report a first validation of the model by comparing two different smart devices.

2 The IoT Device Model

The proposed model has been developed by analyzing the characteristics of a number of different devices. It is shaped as a star diagram (Figure 1). A first version has been proposed in [14,12]. The model is composed by four "macro" elements each describing a specific technological perspective of the device: Communication, Target, Data Manipulation and Development.

The first one represents the device communication element and concerns how the data are transmitted by the device. The "Target" element considers the context of use of the device, and it is associated to the device hardware implementation. The "Data Manipulation" element covers all the characteristics related to the data generated and managed by the device. Finally, the "Development" element analyses the programming characteristics of the device. "Target" and "Development" are detailed with a group of more sub-elements that help the assessment of the device.

2.1 Communication

The *Communication* element represents how the communication between the device and the external world occurs. It analyses the technical aspect of many device's characteristics, such as: the *Security*, the communication *Protocol*, and the *Destination* of the communication.

The Cryptography is an aspect related to the security of the communication. Cypher data allow them to be sent and received over the net, keeping the content safe from unauthorized users [22]. For example the elliptic cryptography is always preferred to a dictionary-based one, as reported in [18].

The Protocol is related to the application protocol in the communication. All the application protocols generate some overhead in the communication, as they add more "control" information to be sure that the data reach the receiver uncorrupted. To receive a good assessment in this element, a low-overhead protocol must be used. For example, COAP (COnstrained Application Protocol) is

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

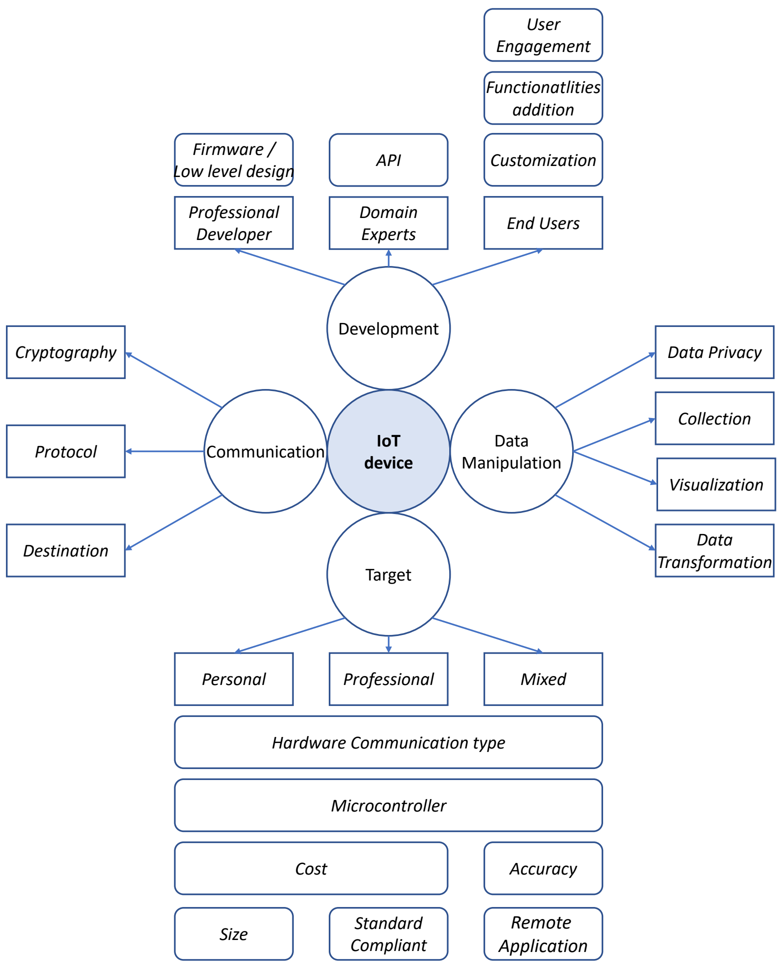

Fig. 1: The IoT device model

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

preferred to HTTP (Hyper Text Transfer Protocol) since it generates a very low overhead [21].

The Destination is related to "where" the data are sent. This is a critical aspect as it makes the difference in an IoT ecosystem when multiple similar device communicate each other at the same time. Sending the data directly to a remote server may generate excessive traffic and interference on the network, thus it is important that a coordination (such as the usage of a sink node) is present.

2.2 Target

The *Target* element represents the main usage of the device and is related to the hardware characteristics of the device. We have classified the *Target* use in three main area, according its use and/or deploy: *Personal*, *Professional* and *Mixed*. All those aspects consider, in the assessment process, the hardware characteristics, including the physical communication type. As a general guideline for the assessment process, an hardware that uses low energy to work, supports a communication type IoT-compliant (low transfer rate and low power) and is usually exploited in multiple contexts, performs better than the others [4].

The Personal element considers some technological and commercial aspects of the device such as the cost and the size, two valuable aspects in the assessment process. The Mixed element considers the cost and the possibility to use a remote application combined to the device. The Professional element assesses the accuracy of the sensor used on the device and its "IoT standard compliant".

Each of the above elements of the target perspective, share one more sub-element: Hardware communication type, Microcontroller, Cost, Accuracy, Size, Remote Application and Standard compliant. While Hardware communication type sub-element refers to the low-level technology used by the device to communicate, the Microcontroller assesses the type of the hardware used. The device cost is particularly important for personal and mixed usages, while for professionals, the accuracy in its measures should be considered. Personal devices should be small in size in order to fit everywhere, while for a mixed usage, the possibility to have a remote application is an important factor. Finally, for professionals it is imperative to use standard-compliant devices.

2.3 Data Manipulation

The *Data Manipulation* element is related to the data, from the *Data Collection* and *Data Transformation*, to the *Visualization* involving also the *Data Privacy*. This part is critical as it is the connection between the device low level sensor and the "outside world" represented by mobile applications, servers, services etc. [5].

The Data Collection is an important aspect related to how the data are temporary stored into the device. There are two different approaches to this aspect: the buffering (which is the temporary store of multiple data instances)

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

or the “immediate send”, which involve the transmission of the data as soon as it has been produced. The first one is less energy consuming [19].

The Data Transformation involves the conversion or the enrichment of the data. These kind of operations are supposed to be made on an external server rather than on the device itself.

The Data Visualization analyses the aspect of the representation of information on the device. To save energy, the device should not show anything on it, but it should send the data to a remote service. An example of visualization available on a web server is CBP, that shows home energy consumption detected by IoT devices [6,7]. CBP was also used to show collaboration among distributed team member that can be detected by IoT devices or software [8,9].

The aspect of the Data Privacy is related to the type of the data collected by the device [17]. Data integrity (the assurance of accuracy and consistency of the data) and privacy level of the people using the device are two of the most critical aspects in this element.

2.4 Development

The Development element involves the possibility of the device to be programmed by people. It has three target users: the *Professional Developers*, *Domain Expert* and *End Users*.

Professional Developers are computer-literate people that are familiar with programming languages, low-level programming and model driven testing [20]. They can read and understand the project specifications and they are able to modify it according to their needs.

Domain expert users are people familiar with the IT world. They know how to program, thus they can use the API to develop a small piece of software that is able to perform the required need.

End users are not familiar with the computer or (in general) with the technology. They are not able to program, thus they need to be supported by possibly visual paradigms (such as ATOOMA, IFTTT, Tasker or EFESTO)[16,10]. They may also have the need to collaborate each other to reach together a shared result [1].

This element has multiple sub-elements: Firmware/Low level design, API, Customization, Functionalities addition and User engagement. The former belongs to the world of Professional Developers: as their ability to program with low level languages, the source of the project and the possibility to edit the “core” of the system is essential. Domain experts, can use the API to program their solution to their own needs. End Users need to Customize and add or remove some functionalities on their own. The user engagement is important as well [11].

3 Discussion

The aim of this model is to give users a way to assess one or more different IoT devices. By the assessment the end user can detect the right trade off between

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

Level 1	Level 2	Level 3	Technology	Assessment
Communication	Protocol		HTTP	1
	Destination		Server	1
	Cryptography		N/A	0
Target	Personal	Hardware Communication	Wi-Fi	1
		Microcontroller	Arduino	1
		Cost	50€	1
		Size	Small	1
	Mixed	Hardware Communication	Wi-Fi	1
		Microcontroller	Arduino	1
		Cost	50€	1
		Remote Application	Mobile App	2
Data Manipulation	Collection		Buffer	2
	Data Transformation		N/A	2
	Visualization		No	2
	Data privacy		Ambient Data	1
Development	Professional Dev.s	Firmware Design	N/A	0
	Domain Experts	API	N/A	0
	End Users	Customization	N/A	0
		Functionalities Addition	Graphic Design	2
		User Engagement	N/A	0

Table 1: The Sonoff SC assessment table

Level 1	Level 2	Level 3	Technology	Assessment
Communication	Protocol		HTTP	1
	Destination		Sink	2
	Cryptography		None	0
Target	Personal	Hardware Communication	Bluetooth 4	2
		Microcontroller	Arduino	1
		Cost	30€	1
		Size	Small	1
	Mixed	Hardware Communication	Bluetooth 4	2
		Microcontroller	Arduino	1
		Cost	30€	1
		Remote Application	N/A	2
Data Manipulation	Collection		Immediate Send	1
	Data Transformation		N/A	2
	Visualization		LED	1
	Data privacy		Ambient Data	1
Development	Professional Dev.s	Firmware Design	N/A	0
	Domain Experts	API	N/A	0
	End Users	Customization	N/A	0
		Functionalities Addition	N/A	0
		User Engagement	N/A	0

Table 2: The Home-made device assessment table

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

all the characteristics of the devices and chose which one suits better to his/her needs. The domain experts take advantage of the model by having under control all the devices characteristics at a glance, even if they are not technical experts. This is an evolution of the work of presented in [13,14,12].

In this section we propose a comparison between two devices: the *Sonoff SC ambient analyzer* and an *home-made air and light analyzer*. The first one is an all-in-one device, which has all the required components inside the plastic case. It has an external power supply (an USB power plug) and a slot for a memory card to store all the data collected by the sensors.

The home-made air and light analyzer is composed by two parts: a Raspberry PI 3 and an Arduino board with many sensors (such as humidity, CO2, light sensors) connected to it. The communication between the Raspberry and the Arduino uses the Bluetooth 4 technology. The Raspberry can formally be connected with other Arduino boards and act as an external "sink", where all the data get collected and then sent to the external web server.

To assess all the device characteristics, we propose a score (s) from 0 to n (with $n > 0$) to assess the elements and the (optional) sub-elements of the model as follows:

- $s = 0$: the characteristic is not supported by the device;
- $[0 < s < n]$: the device partially supports the characteristic (e.g.: it adopts a technology, but a new and more performing technology is available);
- $s = n$: the device fully supports the characteristic in terms of both functionalities and recent technology.

In this assessment, for the sake of simplicity, we set $n = 2$.

Table 1 shows the assessment for the Sonoff SC ambient analyzer, while Table shows 2 the assessment of the home-made air and light analyzer has been shown. For the sake of simplicity, each element and sub-element has been named according to a "level", which is the distance from the center of the star. At a first sight, the two devices are very similar in terms of performances, price and technology. Both of them can be used in a personal and semi-professional environmental setting.

The assessment of the *Communication* element is similar. The home-made device, supporting the sink node, performs slightly better than the Sonoff and the assessment of the *Target* element is almost the same as the previous one. Thanks to the Bluetooth 4 technology, the home-made device has a better assessment than the Sonoff.

The *Data Manipulation* is performed better by the Sonoff device, thanks to the possibility to bufferize the data and the absence of any LED or display that shows the data sent. Similarly, the Sonoff device allows a little bit of personalization of the behavior of the IoT device: thanks to the graphical programming application, it is possible to define rules and send alerts to the users, if needed.

The overall results from the assessment of those two devices shows that they are almost equivalent in all the fields. The home-made device is more industry oriented, while the Sonoff is better to be used in an home environment. They

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

resides in the *End Users* element because the Sonoff SC device gives users the possibility to program alerts and functionalities.

4 Conclusion and Future Works

In this paper we have presented a model to support the assessment of a smart devices according to different dimensions. The model, has four "macro" elements: Communication, Target, Data Manipulation and Development. Each of them is then further specified. By ranking (using a discrete scale) each element, it is possible to get an overall assessment of a given IoT device. Its suitability for a specific domain is then evaluated comparing its assessed characteristics to the domain needs. We provided an example that assesses and compares two similar IoT devices that can be used at home.

In order to formally evaluate the model we are currently planning a test study with speech-therapist physicians and IoT devices.

References

1. Carmelo Ardito, Barbara Rita Barricelli, Paolo Buono, Maria Francesca Costabile, Antonio Piccinno, Stefano Valtolina, and Li Zhu. Visual mediation mechanisms for collaborative design and development. In *International Conference on Universal Access in Human-Computer Interaction*, pages 3–11. Springer, 2011.
2. Carmelo Ardito, Paolo Buono, Maria Francesca Costabile, Rosa Lanzilotti, and Adalberto Lafcadio Simeone. Comparing low cost input devices for interacting with 3d virtual environments. In *Human System Interactions, 2009. HSI'09. 2nd Conference on*, pages 292–297. IEEE, 2009.
3. Barbara Rita Barricelli and Stefano Valtolina. Designing for end-user development in the internet of things. In *International Symposium on End User Development*, pages 9–24. Springer, 2015.
4. Andrea Bartoli, Mischa Dohler, Juan Hernández-Serrano, Apostolos Kountouris, and Dominique Barthel. Low-power low-rate goes long-range: The case for secure and cooperative machine-to-machine communications. In *International Conference on Research in Networking*, pages 219–230. Springer, 2011.
5. Alessando Bianchi, Danilo Caivano, and Giuseppe Visaggio. Method and process for iterative reengineering of data in a legacy system. In *In Proceedings of Working Conference on Reverse Engineering*, pages 86–96. IEEE, 2000.
6. Paolo Buono. A low cost system for home energy consumption awareness. In *AmI (Workshops/Posters)*, 2015.
7. Paolo Buono. A circular visualization technique for collaboration and quantifying self. In *Proceedings of the International Working Conference on Advanced Visual Interfaces*, pages 348–349. ACM, 2016.
8. Paolo Buono, Maria Francesca Costabile, and Rosa Lanzilotti. A circular visualization of people s activities in distributed teams. *Journal of Visual Languages & Computing*, 25(6):903–911, 2014.
9. Paolo Buono and Giuseppe Desolda. Visualizing collaborative traces in distributed teams. In *Proceedings of the 2014 International Working Conference on Advanced Visual Interfaces*, pages 343–344. ACM, 2014.

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).

10. Federico Cabitza, Daniela Fogli, Rosa Lanzilotti, and Antonio Piccinno. Rule-based tools for the configuration of ambient intelligence systems: a comparative user study. *Multimedia Tools and Applications*, 76(4):5221–5241, 2017.
11. Danilo Caivano, Fabio Cassano, Daniela Fogli, Rosa Lanzilotti, and Antonio Piccinno. We@ home: A gamified application for collaboratively managing a smart home. In *International Symposium on Ambient Intelligence*, pages 79–86. Springer, 2017.
12. Danilo Caivano, Fabio Cassano, Rosa Lanzillotti, and Antonio Piccinno. Towards an iot model for the assessment of smart devices. In *Advanced Visual Interface (Workshops/Posters)*. Springer, In print.
13. Danilo Caivano, Fabio Cassano, and Antonio Piccinno. Eud4sh: A eud model for the smart home. In *International Symposium on Ambient Intelligence*. Springer, In print.
14. Danilo Caivano, Fabio Cassano, and Antonio Piccinno. Wip: a model for assessing iot devices. In *4th International Conference on Smart Computing*. Springer, In print.
15. Danilo Caivano, Daniela Fogli, Rosa Lanzilotti, Antonio Piccinno, and Fabio Cassano. Supporting end users to control their smart home: design implications from a literature review and an empirical investigation. *Journal of System and Software*, In print.
16. Giuseppe Desolda, Carmelo Ardito, and Maristella Matera. Efesto: a platform for the end-user development of interactive workspaces for data exploration. In *Rapid Mashup Development Tools*, pages 63–81. Springer, 2016.
17. Wenbo He, Xue Liu, Hoang Nguyen, Klara Nahrstedt, and Tarek Abdelzaher. Pda: Privacy-preserving data aggregation in wireless sensor networks. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 2045–2053. IEEE, 2007.
18. Vivek Kapoor, Vivek Sonny Abraham, and Ramesh Singh. Elliptic curve cryptography. *Ubiquity*, 2008(May):7, 2008.
19. Joongheon Kim. Energy-efficient dynamic packet downloading for medical iot platforms. *IEEE Transactions on Industrial Informatics*, 11(6):1653–1659, 2015.
20. Beatriz Pérez Lamancha, Macario Polo, Danilo Caivano, Mario Piattini, and Giuseppe Visaggio. Automated generation of test oracles using a model-driven approach. *Information and Software Technology*, 55(2):301–319, 2013.
21. Tapio Levä, Oleksiy Mazhelis, and Henna Suomi. Comparing the cost-efficiency of coap and http in web of things applications. *Decision Support Systems*, 63:23–38, 2014.
22. Kai Zhao and Lina Ge. A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pages 663–667. IEEE, 2013.

Proc. of Fifth International Workshop on Cultures of Participation in the Digital Age - CoPDA 2018
Castiglione della Pescaia, Italy, May 29, 2018 (published at http://ceur-ws.org).