Human-Centric Internet of Things. Problems and Challenges

Ekaterina D. Kazimirova
AO Kaspersky Lab
Moscow, Russia
e-mail: Ekaterina.Kazimirova@kaspersky.com

***Abstract* — The paper analyzes the Internet of Things from the perspective of designing a new ecosystem for humans. Both the opportunities and the threats are analyzed. It is concluded that Internet of Things platforms will eventually integrate all aspects of human life, creating a new information environment that will help people to achieve maximum self-fulfillment and significantly greater life expectancy.**

Keywords - Internet of Things; Industrial Internet of Things; neuromorphic computing; affective computing.

I. INTRODUCTION

Technology is rapidly changing our lives. The evolvement of the Internet of Things (IoT) is a major new technology trend that is changing the principles on which the relationship between people and things has been based for hundreds of years. It is creating a new environment, where people are surrounded by "living" things. Like any radically new environment, it has both opportunities and dangers in store for us. Naturally, we cannot identify all the benefits and risks of the various development scenarios from the current observation point, but we should certainly try, because this will help to crystalize the principles on which the Internet of Things platforms that are now emerging should be based. Tomorrow, these platforms will be our new habitat. In this paper, we look at some of the problems and issues associated with the Internet of Things as a new ecosystem.

Our idea is that, in order for a secure and truly useful human-centric Internet of Things to be built, IoT platforms should from the outset be developed to integrate the most important areas of human life, to include a comprehensive set of features related to caring for people's health and supporting them in their self-development and leisure, rather than simply resolving individual problems (that is, making it more convenient to control specific sets of things).

In this paper, we look at the current state of the Internet of Things, as well as its development prospects, from different viewpoints, including that of security. This is an extensive subject area and we do not undertake to address all the issues. This article is an attempt to outline the problem and the main approaches for addressing it.

The paper is structured as follows. In Section II, we discuss the Internet of Things as a new environment, and in Section III, briefly discuss IoT and IIoT security. Conclusions and future work are indicated in Section IV.

II. INTERNET OF THINGS AS A NEW ENVIRONMENT

A. Internet of Things Today

Although the Internet of Things is a universally recognized global trend, it has not yet evolved as a generally accepted practice, nor as a unified set of technologies, methods and approaches, nor as a new environment for people to live in. Humanity may be able to break through the new technological barrier but is as yet unable to see what is beyond the line of the horizon.

For now, it is clear that:

- Things will have built-in microchips or RFID tags.
- Things will connect to humans via the Internet.
- People will use mobile apps to control things remotely, such as turning off a forgotten iron from the office.
- Hopefully, things will be able to adapt to people's needs [1].

The first multifunctional personal assistants have the potential to evolve into fully-fledged advisors to humans, to the point of playing a role in forming their life strategies (existing intelligent personal electronic assistants include Amazon Echo [2], Google Assistant [3], and Azuma Hikari produced by Vinclu Inc [4]). These are only the first signs of global changes in the information environment.

B. Internet of Things as a Dream

Many amazing phenomena that people only used to dream about and describe in tales have come to pass – such as the magic bowl of water or crystal ball reflecting things that are happening far away, which has come to life as television and the Internet; the magic flying carpet from oriental stories, which has become the airplane, etc. Note that in fairy tales, things could talk and interact with people in various other ways, helping them or interfering with their plans. It is possible that we have now approached one of the last "fairy-tale" technological barriers – that is, lifelike things that can speak and understand speech, and interact with people in other ways. The right conditions for breaking through that barrier will soon be in place, including the emerging Internet of Things, speech recognition and affective computing.

C. Internet of Things as a New Ecosystem

Such gadgets as smart power outlets, irons, backpacks, etc. are already available on the market. However, it is no

 ISBN: 978-1-61208-576-0

coincidence that the European Commission's strategy is based on the human-centric Internet of Things [5]: things should not just have some attributes of intelligence and remote monitoring support (e.g., checking from the office whether the TV set at home is off) – they should eventually make up a new ecosystem centered around humans, who are surrounded by "living", self-aware and context-oriented things. We believe that the role of things in such an ecosystem will go beyond satisfying the simple needs of humans – intelligent things will also become people's advisers, monitor their physiological condition, suggest solutions and scenarios of successful actions (which reminds us of Ariadne's thread from the Ancient Greek myth).

Importantly, things and robots, which are also a form of things (i.e., various artificial personal assistants), are already becoming capable of displaying emotions themselves and, in the near future, will be able to detect emotions in humans – based on their tone of voice, facial expressions, skin reactions, etc. While so far people have been the only sentient and cognizant creatures around, in the future the very environment in which they live will be cognitive and capable of making decisions on its own. We believe that this functionality will be implemented gradually in the process of building IoT platforms.

Note that monitoring the psycho-emotional and physiological status of people has the potential to extend human life: by avoiding functional overload, we can optimize the activity of our organisms and reduce their wear and health risks.

Creating a friendly environment can also be seen as an independent task: imagine walking along the platform waiting for your train, with the pillars smiling at you as you pass them.

D. Changing the Technological Landscape

From the technology viewpoint, there are several major objectives, the primary of which is to create a technological platform that would enable a human-centric Internet of Things to be built.

Consumer IoT platforms should integrate various facets of life – people's need for comfort, emotional support, finding a work and leisure balance, caring for their health. With the help of smart personal assistants, people may be able to optimize not only their everyday affairs, but also their life strategies. Cognitive technologies involved in the dialog between people and machines will help individuals to compensate their cognitive shortcomings and achieve maximum self-fulfillment.

Neuromorphic computing [6][7] is seen as an important element of the computing base for such platforms, since a) it is the intelligence implemented in a thing that makes it truly intelligent, and b) the digitization of everything will result in skyrocketing volumes of data that will need to be handled, and it is best to process part of the data locally (using embedded microchips), rather than in the cloud.

Naturally, information security will be of crucial importance for such systems.

III. SECURITY

The problem of protecting information in IoT must be addressed in an entirely new way, since this is about creating and protecting an ecosystem that will accumulate all kinds of diverse information about people.

In fact, it would be fair to say that people themselves will be integrated into information flows. Clearly, it is essential to maintain the security of data on their health, behavior, future plans and emotional state. Even today, experts emphasize the importance of safeguarding information stored and processed by IoT devices – such as medical data [8]. As technology evolves, such information sometimes becomes too accessible. The new IoT reality and new technologies that provide protection for that reality should develop hand-in-hand.

For Industrial Internet of Things (IIoT), on the contrary, the nearly complete absence of people from industrial processes (humanless technologies) will be an important factor. It remains to be determined in what measure and form humans should be involved in automated industrial processes and the control of their safety and security.

IV. CONCLUSIONS AND FUTURE WORK

The Internet of Things is not simply a range of comforts but a new ecosystem that should be centered around people.

Going forward, different categories of the Internet of Things will be increasingly connected, shaping an integral environment, the essence of which will be in creating a living and thinking space around humans. It should be designed to ensure that people do not simply live in comfort but reach maximum self-fulfillment and the longest lifespan possible.

In the process of building this living and thinking space we are going to face new challenges:

- How can people avoid being lost in the world of things: if the environment becomes more intelligent than its users, how can they keep it under their control?
- How will things interact with each other - what should be the main principles of device-to-device communication?
- How autonomous will those smart things be in making decisions? Should they be allowed to make decisions proactively? How can we make sure that they will behave the way they should?

We believe that further research should be focused on finding answers to these fundamental questions.

Problems associated with protecting the IoT and IIoT ecosystems are different in some essential ways. While in the former case, protection is needed for extremely personalized information flows, in the latter, it is humanless industrial zones that will need to be protected.

ACKNOWLEDGMENTS

The author is grateful to Andrey Lavrentyev, Michael Gusev and Evgeny Volovich for fruitful discussions.

 ISBN: 978-1-61208-576-0

REFERENCES

[1] N. Gershenfeld, R. Krikorian, and D. Cohen, “The Internet of Things,” Scientific American, vol. 291, Issue 4, pp. 76–81, Oct. 2004.

[2] What is Amazon Alexa? Available from: https://developer.amazon.com/alexa 2017.06.28

[3] Meet your Google Assistant. Available from: https://assistant.google.com/ 2017.06.28

[4] Azuma Hikari. Official Site. Available from: http://gatebox.ai/hikari/en/ 2017.06.28

[5] Public Report from the Workshop on the Exploitation of Neuromorphic Computing Technologies, Brussels, Feb 2017. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=43537 p. 13 2017.06.19

[6] The issues of the “Workshop on the Exploitation of Neuromorphic Computing Technologies” of European Commission. Available from: https://ec.europa.eu/digital-single-market/en/news/workshop-exploitation-neuromorphic-computing-technologies 2017.06.24

[7] S. Furber and K. Meier “Neuromorphic Computing in the Human Brain Project”, The issues of Innovation Workshop Exploitation of Neuromorphic Computing Technologies Feb. 2017, Brussels. Available from:

http://ec.europa.eu/information_society/newsroom/image/document/2017-8/1_furber_steve_and_meier_karlheinz_CDA4E45F-EF31-6FBF-1642BB9BAB97CEF4_43088.pdf 2017.06.19

[8] S. Lozhkin “Hospitals are under attack in 2016” Available from: https://securelist.com/hospitals-are-under-attack-in-2016/74249/ 2017.06.19

 ISBN: 978-1-61208-576-0