American Journal of Networks and Communications
2013; 2(2) : 23-27
Published online April 2, 2013 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.20130202.11

Finnish perspectives for the IOT

Johanna Virkki

Department of Electronics and Communications Engineering, Tampere University of Technology, Tampere, Finland

Email address:
johanna.virkki@tut.fi (J. Virkki)

To cite this article:
Johanna Virkki. Finnish Perspectives for the IOT, *American Journal of Networks and Communications.* Vol. 2, No. 2, 2013, pp. 23-27.
doi: 10.11648/j.ajnc.20130202.11

Abstract: The Internet of Things (IOT) means connecting people, things, and devices in order to create an omnipresent computing world. One of the most important challenges in convincing users to adopt this kind of all-around network is the protection of security and privacy in different applications. This paper presents the results of interviews conducted in a Finnish study during 8/2012-2/2013. In this research, 11 Finnish people working with different aspects of IOT development and 11 ordinary Finnish people were interviewed. The goal was to investigate their feelings on the IOT and its applications, as well as personal opinions on security and individual privacy in the IOT. Most of the answerers in this study believed that we are heading towards the IOT in the future and many IOT applications were seen tempting. However, security and privacy issues, the lack of control, and the actual need for versatile IOT applications were questioned. The people working with the IOT were found to be more critical towards the IOT than the ordinary people. An introduction of the IOT, examples of potential applications, the conducted interviews and collected answers, as well as highlights of the collected free comments are presented in this paper.

Keywords: Finland, Individual Privacy, Internet Of Things, Interviews, Security

1. Introduction

The Internet of Things (IOT) is a conceptual vision to connect things (everyday things from school buildings to coffee cups) and devices (from laptops to ovens), in order to create a ubiquitous computing world. Things will exchange data and information about the environment, while reacting autonomously to different events, influencing the environment, and creating services. This all can happen with or without human intervention. The IOT is thus the extension of the Internet to the next level, i.e., bringing the Internet to the real physical world of things. Potential examples of the versatile applications of the IOT are presented next.

Given that a growing number of people have chronic diseases and inconveniences, health-related applications of the IOT are gathering more and more attention. Potential applications include e.g. assistance and monitoring of conditions of patients inside hospitals and at home, and accident victim's medical journals that are automatically made available to the caregivers to ensure that optimal treatment can be provided. Electronic tags can be used in drugs and drug boxes can carry information on adverse effects and optimal dosage, monitor the use, inform the pharmacist when new supply is needed, know incompatible drugs, and prevent overdoses. The IOT also offers many applications to home-environment, for example automatic energy and water supply consumption, control of temperature gauges, remotely armed home security system, switching appliances on and off, etc. Possible retail applications include e.g. payment processing based on location or duration and allowing customers to pay in department stores only by walking out with the products. Customers can also receive advices in the point of sale according to customer habits, preferences, presence of allergic components, or expiring dates. Also smart cities are examples of the potential future IOT applications; for example, the citizens can monitor the pollution concentration and can receive automatic alarms when the radiation level reaches too high level, rubbish bins can send an alarm to garbage collector when they are close to being full, etc. The IOT also has many potential applications in catastrophic prevention, for example detection and warning of forest fires and earthquake, and monitoring of vibrations and material conditions in buildings and bridges [1-6].

A number of countries or districts have realized the importance of the IOT in the recovery of economic growth and sustainability. Amongst them the European Union (EU), the United States, and China are prominent examples. Thus,

companies, universities, and research institutions currently take an active part in IOT development worldwide [7].

One of the most important challenges in convincing users to adopt this kind of all-around network is the protection of security. And it is not only security, but privacy too. Concerns over security and privacy can spread wide, particularly as wireless systems can track users' personal information, actions, behaviour and ongoing preferences. Invisible and constant data exchange between things and people, and between things and other things, will occur unknown to the owners and originators of such data. The huge volumes of data that the IOT generates will have to be routed, captured, analysed, and acted upon in timely relevant ways. Working out how to do this will be no easy task. One important issue related to these different applications is the data aggregation (combining seemingly non-sensitive separate small bits of information may reveal additional, possibly sensitive information) [8]. Similar effect can occur when the data collected for one purpose is used for a different purpose, and this is done without the person's approval. As the devices and things within the IOT collect seemingly inconsequential fragments of data for their service, it should also be considered what happens when all that information is brought together, correlated, and reviewed. The sheer scale and capacity of the new technologies will magnify this problem and source suspect. Thus, security and privacy of the IOT are currently active and important research topics [2-7, 9-14].

Interesting point of view are the differences and similarities in personal thoughts of people who work with the development of the IOT and of those people, who are not yet so familiar with the concept, but are potential end users of the IOT (henceforth referred to as "ordinary people"). In this research, 22 people were interviewed in Finland during a period of 7 months, 8/2012-2/2013, in order to investigate their thoughts and feelings on the Internet and individual privacy, as well as their opinions on the IOT and its applications.

This paper is organized as follows: The introduction section introduces the concept of the IOT and gives examples of potential applications. Section 2 presents the performed interviews, including the information on the answerers and presented questions. The collected answers and examples from free comments are presented and discussed in section 3. The last section summarizes the results and presents the conclusions of this paper.

2. Interviews

For this research, 11 people working with different aspects of the IOT, e.g. radiofrequency identification, wireless networks, and wireless communication were interviewed. These answerers were chosen from different organizations (from researchers of different universities in Finland and from workers of companies on the field). Also, 11 ordinary people, working in very different areas, were interviewed. The idea of this research study is not only to compare the answers from these two different groups but to gather more versatile answers by interviewing people with different backgrounds. Thus, people of different age and people of both gender were chosen (the genders and ages of the answerers can be seen in Table 1). The personal interviews were conducted by an associate of the researcher, and they took place either at the answerers working facility, home, or at a neutral, public place. Some of the interviews were done by private e-mails between the researcher and the answerer. All these interviews thus had more flexibility than only a paper survey, as both the researcher and the answerer were able to ask for clarification. This survey had 5 questions and a possibility for free comments. Questions are listed next.

Table 1. *Genders and ages of the answerers.*

	Ordinary people	**People working with the IOT**
N of female	5	6
N of male	6	5
N total	11	11
Min. age	19	20
Average age	32	32
Max. Age	56	48

Question 1: Are you currently using social media and/or do you share pictures or personal information on yourself in the Internet?

·Yes, many times in a week

·Yes, sometimes

·No

Question 2: How much do you think a person can currently affect his/her own individual privacy in the Internet? Scale = 1-5, where

·1= A person can completely control his/her own individual privacy

·5= A person has no control over his/her own individual privacy

Question 3: What kinds of IOT applications do you see potential in your own life? What kinds of IOT applications you would not want into your own life?

Question 4: Do you believe that current Internet will grow into IOT and this kind of all-around network will come to use? What will be the schedule?

·In the near future

·During following 10 years

·During following 20 years

·Longer than 20 years

·Never

Question 5: How much do you think a person can affect his/her own individual privacy in the Internet/IOT after 10 years from now? Scale = 1-5, where

·1= A person can completely control his/her own individual privacy

·5= A person has no control over his/her own individual privacy

3. Results and Discussion

This section introduces and discusses the collected answers. All the examples of the achieved free comments are presented as direct quotes and their text is italicized.

3.1. Question 1

Social media refers to the means of interactions among people in which they create, share, and exchange information in virtual communities and networks. It allows users to share their lives in many different ways, via updates, images, voice, etc. Social media is more and more becoming a platform for the public to voice their opinion and present them to a huge audience in the Internet. Many people have chosen to make their life, at least partly, public. In Question 1, it was asked if the answerers are currently using social media and/or share pictures or personal information of themselves in the Internet. The answers to this question (shown in Fig. 1) show that 73 % of all the answers were "many times a week" or "sometimes", and 27 % of all the answers were "no". There were significantly more "no" answers among the people that work with the IOT: 91 % of the ordinary people answered "many times a week" or "sometimes", whereas among the people working with the IOT, 55 % answered "many times a week" or "sometimes". Also, in their free comments, people working with the IOT were more critical towards the use of social media.

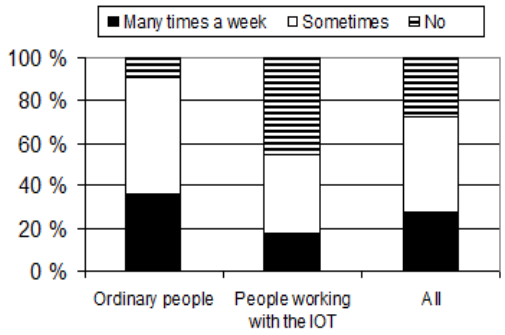

Figure 1. *Results from Question 1; Are you currently using social media and/or do you share pictures or personal information on yourself in the Internet?*

"I have not opened a Facebook or Google account, neither I am using any online photo storages or backup services, while there are benefits also. In these cases I see privacy concerns and legal complications more substantial than benefits."

"There really is no information available about what kinds of security methods they're using in many of the social media applications. Why would I want to use (with my own personal information!) something that I have no idea of?"

3.2. Questions 2 and 5

Questions 2 and 5 dealt with the feelings on how much people can currently/after 10 years affect their own individual privacy in the Internet (results can be seen in Fig. 2 and Fig. 3, respectively). According to these answers, people believe that the possibility of moving from the traditional Internet towards the IOT during the following 10 years will not significantly affect how much they can control their individual privacy in the Internet. However, some answerers from both groups do believe for a negative change, which can be seen from the differences between Fig 2 and Fig 3. The average value of all the answers to Question 2 was 2,64 and the average value of all the answers to Question 5 was 3,18. Thus, according to these results, people already feel that there is a lack of control related to the individual privacy in the Internet. This was also pointed out in the free comments. A lot of work is currently done to maintain and improve the security and privacy in the Internet, which was also mentioned.

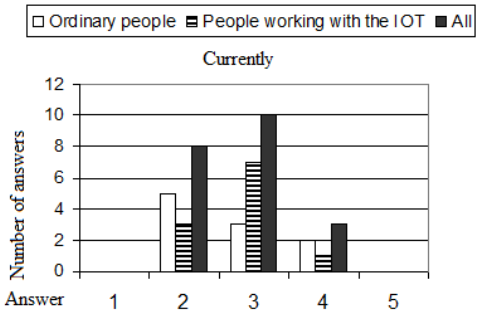

Figure 2. *Results from Question 2; How much do you think a person can currently affect his/her own individual privacy in the Internet?*

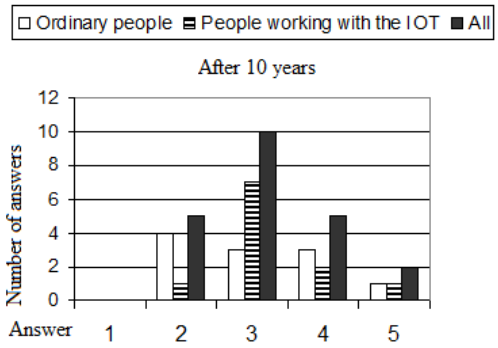

Figure 3*. Results from Question 5; How much do you think a person can affect his/her own individual privacy in the Internet after 10 years?*

"Everything you share can come public information but that is the case with old fashion communication also."

"I find the individuals privacy quite poor and therefore wish a lot higher security before IOT is everywhere more than it already is."

"Nowadays there are a lot of problems with the security. I know that they are working to improve it. I just hope that they succeed.."

"I do not want to use applications that have security risks or applications that mean I may lose my privacy. I will not want to use them in the future either, no matter how great things anyone promises."

3.3. Question 3

As was described in the first section of this paper, the range and diversity of IOT applications permeates practically through all aspects of the everyday life. Question 3 was about the IOT applications that the answerers see potential in their own life in the future, and those they would not want into their life. The most wanted applications among these answerers seem to be those related to healthcare, e.g. automatic health-monitoring. This seems reasonable, since the adjustment of the healthcare systems to the increasing number of elderly and patients with chronic diseases is one of the biggest challenges to the EU, including Finland, and the future of the public healthcare is currently a hot topic in the Finnish media.

"Monitoring of my own health and the health of those close to me"

"From personal and professional point of view, elderly people more often benefit of staying at their own home as long as possible, where this kind of monitoring can be useful."

Also, versatile applications to be used at home were seen tempting. These applications also probably are the ones most commonly mentioned with the IOT. Thus, they may be the applications that the people are the most familiar with. In general, very different kinds of applications were mentioned to be considered helpful in everyday life.

"Energy and water supplies consumption monitoring. It helps to save money."

"Cloud storage of media so that it can be accessed and used anytime and anywhere"

"Remote control of home applications"

"IOT brings lot of new possibilities for social life and business."

The lack of control was seen as the main reason why some applications were not considered desirable. It was also questioned if the cost of using different applications will be suitable. Again, negative perspectives and feelings were mentioned more often in the answers collected from the people that work with the IOT.

"Those that will help, but not cause substantial privacy concerns or other risks. This is a matter of balance, meaning that if benefits are substantial then more risks can be accepted. E.g. I am using sometimes navigation applications on the phone while knowing that the data can be tracked."

"Controlling things, like photo based recognition, or something what will happen without my knowledge."

"Systems that I cannot control or modify myself"

"I also do not want that the systems carry permanent individual information without a possibility to erase."

"I would not feel comfortable with a home alarm or smart home system connected or controllable through the Internet. Such case is especially if the authentication is not strong, e.g. based just on password and user name. Also the potential damage is essential. For example, if you can turn the heating completely off during the winter time, I would not use such application. Also you should be able to bypass locally the Internet application in case of misuse or other problems."

3.4. Question 4

In Question 4, it was inquired what people think will be the possible schedule for the current Internet to grow into the IOT and this kind of all-around network to come to use, if it will come to use. The answers to this question can be seen in Fig. 4. According to these results, 18 % of the answerers felt that this will happen during the following 10 years, 18 % during the following 20 years, and 14 % of the answerers felt that it will take longer than 20 years. In addition, two of the answerers (both working with the IOT) felt that this growing into the IOT will never happen. There was also one answerer from the group of ordinary people who felt that this will happen in the near future.

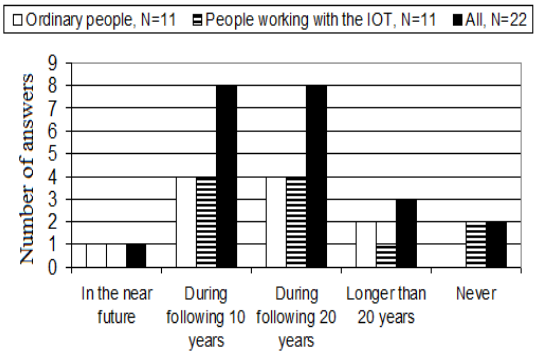

Figure 4. *Results from Question 3; Opinions on the possible schedule for current Internet to grow into IOT and this kind of all-around network to come to use.*

"It is quite hard to know the schedule. There already are applications that I think are part of the IOT. On the other hand, it seems something that will happen in the far away future. For example, now everybody has a computer and a cellular phone in Finland. This was not the case 25 years ago. I do not think they would have predicted this"

In the free comments, the IOT was seen tempting, in principle, but the necessity of the versatile applications was also questioned:

"All in all, I expect much more positive consequences than negative ones. Life becomes easier and IOT is continuously learning more and more on us, our habits, preferences and the environment we live in. However, it may also be bad for individual decision making, since IOT may decide options or make the final decision. We may trust too much on the guidance of IOT. Therefore strict personal profiles for the applications of IOT are needed. Therefore, we must be active users not lazy followers."

"Nowadays people believe that they need loads of stuff. In reality we could survive with a lot less."

In addition, it was questioned (both by the ordinary people and the people working with the IOT) if people are aware of the potential problems that may occur.

"It's scary how few people are preparing for the IOT."

"Orwell's 1984 is here."

4. Conclusion

In this research, 22 people were interviewed about the IOT in Finland. Out of the 22 answerers, 11 were working with the IOT and 11 were ordinary people, who were not yet so familiar with the concept. This paper presents the collected answers to 5 questions and highlights of the free comments. Most of the answerers believed that we are heading towards the IOT in the future. According to these answers, many future IOT applications were seen tempting, but the necessity of the huge amount of new applications was also questioned. In addition, the security risks and losing control your own individual privacy were seen as the main barriers, as was expected. The most desired applications seem to be those related to health-monitoring and applications used at home. In general, the people working with the IOT were found to be more critical towards it.

Acknowledgements

Johanna Virkki would like to thank the Helsingin Sanomat Foundation.

References

[1] Libelium, "50 Internet of Things applications", 2012. Available at: http://www.libelium.com/top_50_iot_sensor_applications_ranking (accessed 20 February 2013).

[2] The Internet of Things 2012 - New Horizons -Cluster Book 2012. Available at: http://www.Internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf (accessed 20 February 2013).

[3] Commission of the European Communities, Internet of Things — An Action Plan for Europe, 2009. Available at: http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf (accessed 19 February 2013).

[4] Internet of Things - Pan European Research and Innovation Vision-IERC 2011. Available at: http://www.Internet-of-things-research.eu/pdf/IERC_IoT-Pan%20European%20Research%20and%20Innovation%20Vision_2011_web.pdf (accessed 20 February 2013).

[5] European Commission, Information Society and Media, Internet of Things in 2020 Roadmap for the Future, 2008. Available at: http://www.iot-visitthefuture.eu/fileadmin/documents/researchforeurope/270808_IoT_in_2020_Workshop_Report_V1-1.pdf (accessed 12 February 2013).

[6] The 2nd Annual Internet of Things Europe 2010: A Roadmap for Europe' Conference Report, 2010. Available at: http://ec.europa.eu/information_society/policy/rfid/documents/iotconferencereport2010.pdf (accessed 15 January 2013).

[7] The Strategic Centre for Science, Technology and Innovation in the Field of ICT, Internet of Things Strategic Research Agenda http://www.Internetofthings.fi/

[8] D.J. Solove, '"I've got nothing to hide' and other misunderstandings of privacy" San Diego Law Review, Vol. 44, 2007, GWU Law School Public Law Research Paper No. 289.

[9] Futuretech Alert. Technology Convergence Leading To the Internet of Things, Frost & Sullivan, 2012.

[10] L. Wu and P. Shao, "Research on the protection algorithm and model of personal privacy information in internet of thing", International Conference on E -Business and E -Government, 2011.

[11] H. Feng and W. Fu, "Study of recent development about privacy and security of the Internet of Things, International Conference on Web Information Systems and Mining, 2010.

[12] D. Gessner, A. Olivereau, A.S. Segura, A. Serbanati, "Trustworthy infrastructure services for a secure and privacy-respecting Internet of Things", International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[13] V. Oleshchuk "Internet of things and privacy preserving technologies", International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009.

[14] H. Ning and H. Liu, "Cyber-physical-social based security architecture for future Internet of Things," Advances in Internet of Things, Vol. 2 No. 1, 2012, pp. 1-7. doi: 10.4236/ait.2012.21001.