IoT Applications in Smart Cities: A Perspective Into Social and Ethical Issues

Conference Paper · June 2018

DOI: 10.1109/SMARTCOMP.2018.00034

3 authors:

Francesca Righetti
Università di Pisa

Carlo Vallati
Università di Pisa

Giuseppe Anastasi
Università di Pisa

IoT Applications in Smart Cities: a Perspective into Social and Ethical issues

Francesca Righetti, Carlo Vallati, Giuseppe Anastasi*
Department of Information Engineering
University of Pisa
Pisa, Italy
{name.surname}@ing.unipi.it

***Abstract*—The possibility of interconnecting any kind of device to the Internet is driving the adoption of the Internet of Things (IoT) paradigm also in a city environment. Many IoT applications are making the Smart City concept real, offering advanced services to citizens and city administrators. This evolution relies upon a seamless exchange of information among different systems. Exchanged data includes personal and/or critical information, thus requiring proper handling in order to avoid security and privacy issues. At the same time, recent developments in robotics are fostering the realization of autonomous agents (e.g., cars, buses, drones) that do not require human intervention. In the city of the future, many services will rely on autonomous agents. Also, autonomous agents (e.g., robots) will become more human alike, and will be able to show emotions. Therefore, they will replace humans in many city activities. In this paper, we first overview the expected evolution of IoT applications and, then, we briefly analyze the security, social, and ethical issues that are foreseen in a Smart City context.**

***Index Terms*—Smart City, Internet of Things, Autonomous Agents, Emotional Robots**

I. Introduction

The evolution of the Internet of Things (IoT) can be compared to the evolution of smartphones. Initially, only some technology enthusiasts owned a smartphone, while nowadays almost every person has one and, apparently, nobody can live without it. Similarly, some years ago, having a thermostat or a light bulb connected to the Internet was not so frequent. Recently, the benefits deriving from remotely reaching our "things", for remote control or configuration, are becoming clear even to common users who started to acknowledge the need to have smart objects.

The power of the IoT does not only consist in remote control. Another important benefit of connecting objects is the possibility for smart objects to access any kind of information through the Internet, information that can be exploited to improve the service offered to end-users. For example, a thermostat connected to the Internet could download weather information in order to optimize its power consumption, based on the actual and expected temperature. At the same time, in the city environment, anemometer, pluviometer, humidity and temperature sensors, could be deployed in parks and gardens areas, and their measurements could be exploited by sprinklers to make irrigation more efficient (e.g., disabling the irrigation when unnecessary), thus avoiding waste of water.

According to [1], the IoT is rapidly evolving. In 2013, there were about 5 billion of connected objects, however their number is expected to increase up to 50 billion by 2020. The city environment represents a context that can particularly benefit from the mass adoption of IoT devices. Indeed, the spread of low-cost and low-energy devices, along with the improvement in wireless communication, is already allowing a rapid deployment of sensors and actuators in many different city environments. Sensors and actuators are the building blocks of the so-called *cyber-physical systems* [2] that can offer innovative services to the citizens, thus improving their quality of life. Moreover, cyber-physical systems can guarantee a more efficient management of the city, thus reducing costs [3] and improving its sustainability.

The deployment of multiple cyber-physical systems in different application domains will ultimately create an ecosystem in which a large amount of heterogeneous data will be produced [4]. In many cases, collected data may include personal data about citizens. Also, data could be used to infer information about their life (e.g., habits, preferences, and health status). Other data may refer to critical infrastructure. Therefore, privacy and security issues cannot be neglected and, needless to say, they become more and more relevant as the number of deployed sensors and actuators increase. Hence, a proper handling of data, as well as appropriate regulations about data management, are required.

In the city of the future many objects will be autonomous agents (e.g., autonomous cars, buses, and vehicles) connected to the Internet and communicating according to the Machine-to-Machine (M2M) paradigm. This will pave the way to the so-called *Internet of Autonomous Things*. Autonomous agents will be able to carry out many activities without any human intervention (e.g., autonomous driving). This will change radically our way of living and moving. Moreover, autonomous agents will become more and more intelligent and will be able to show emotions. Thus allowing them to replace humans in many activities.

The increasing utilization of IoT devices and autonomous agents eventually will enable a number of benefits in terms of advanced services, better quality of life, increased efficiency,

* Giuseppe Anastasi is also affiliated with *Smart Cities & Communities National Lab.*, CINI, Italy

978-1-5386-4705-9/18/$31.00 ©2018 IEEE
DOI 10.1109/SMARTCOMP.2018.00034

environmental sustainability. At the same time, it may introduce a number of security, social and ethical issues. In this paper, we intend to analyze the IoT technology for future cities from two different perspectives. On one hand, we highlight the benefits that can potentially derive for citizens from using IoT applications in an urban environment. On the other hand, we also try to emphasize potential issues that may come from using such new technologies. Social and ethical issues are often neglected by researchers and technologists, when designing their solutions. This paper aims at stimulating a discussion among researcher to make them aware that such issues should never be neglected when developing technical solutions.

The rest of the paper is organized as follows. Section II reviews the main IoT-based applications for Smart Cities. Section III and IV describe further evolutions of the urban ecosystem in order to include autonomous agents and emotional robots. Section V highlights some security, social, and ethical implications of this evolution. Finally, Section VI concludes the paper.

II. IoT Applications for Smart Cities

The number of IoT applications for smart cities is progressively growing up. More and more cities are deploying sensors and actuators to instrument potentially all the activities that are carried out in the city. These devices communicate typically through wireless links and create a sort of capillary network pervading the city. Environmental monitoring, traffic monitoring, smart parking, smart surveillance, participatory sensing are just some of the most common applications already used in many cities. Below we provide a brief overview of these applications, highlighting their benefits for the citizens and the community, but also emphasizing their potential threats. Due to space limitations, we just consider a limited number of applications.

Air Quality and Environmental Monitoring. Air quality represents a serious threat for the public health, the environment and, ultimately, the economy of a country. Poor air quality results in poor health, premature deaths, as well as in damages to ecosystems, crops, and buildings. Obviously, the effects are more serious in urban areas, where the majority of the population resides. Therefore, almost all cities rely on air quality monitoring systems. Currently, air quality is typically monitored through large and expensive sensing stations, installed at some strategic locations that measures parameters such as particulate matter (PM), Ozone (O3), Carbon Dioxide (CO2), Nitrogen Dioxide (NO2). This allows an accurate monitoring, but limited to specific areas. In the future, as the cost of sensors will become affordable by single citizens, air quality sensors will be privately owned, thus allowing a fine-grained air quality monitoring of urban areas.

In addition to air quality parameters, other environmental parameters are also monitored, including temperature, humidity, wind speed and directions, meteorological data, etc. Based on this information, it is possible to forecast the air quality in advance, in a specific area, and inform the population, especially people affected by respiratory illness. Systems of this kind can have a structure like in Figure 1. Using a similar approach, sensors can be used to monitor wastewater, especially during heavy rain, and predict the risk of flooding so as to timely alert the population. Air quality and, more generally, environmental monitoring, relies on collecting data generated by sensors and analyzing them to take rational decision (e.g., limit the vehicular traffic in case of high level of air pollution). Due to the nature of the collected data, they do not require special handling procedures. However, decisions made on environmental data (e.g., air quality forecast, prediction of flooding) should be made with great accuracy and diffused with caution, as they may have a potentially strong impact on citizens and their behavior.

Fig. 1. Air Quality.

Traffic monitoring. Real time monitoring of urban traffic is crucial to avoid jams, maintain a controlled level of congestion, and ensure that the level of air pollution is kept below the threshold imposed by regulations. Traffic monitoring can be carried out taking two different approaches. The former consists on deploying traffic-intensity sensors capable of measuring the number of cars/vehicles entering or exiting the city. Typically, they are deployed at the main entrances of the city and buried under the asphalt, as shown in Figure 2. The alternative approach consists in using cameras that monitor the flow of vehicles entering/exiting the city. Images generated by cameras are, then, processed to infer information about the traffic intensity. In both cases, data about traffic intensity in the different areas of the city are made available, in real time, to city managers who can take timely and appropriate decisions, if necessary. Also, information about traffic can be diffused to citizens, who can thus select the less congested path to reach their destination. Indeed, many applications including Google Maps already implement this service. Finally, the analysis of traffic data can also be used by city administrators and managers to plan alternative mobility solutions, investigate the correlation between air quality and traffic intensity in specific areas of the city; etc. Traffic data are typically anonymous. However, if they are generated through cameras deployed in certain points of the city, the collected information may include personal data such as number plates. Hence, data must be anonymized, by removing any personal information, before storage and analysis, in order to avoid privacy issues.

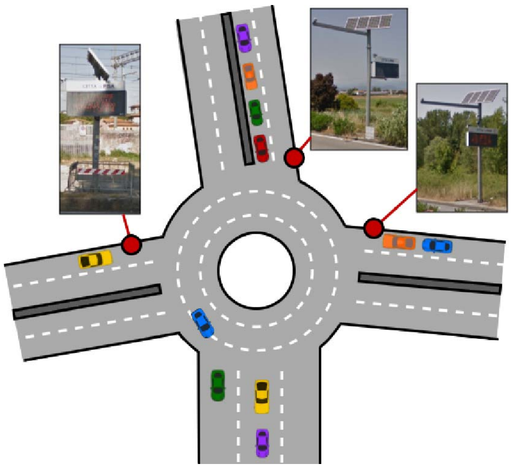

Fig. 2. Traffic Monitoring.

Smart Parking Management. Smart parking-management systems are complementary to traffic monitoring and aim at managing efficiently traffic flows by informing citizens on where to go when they look for a parking lot. This avoids traffic in areas where all the parking lots are busy. A possible approach to smart parking management is shown in Figure 3. The status of each parking lot is monitored through a dedicated sensor and the collected information is periodically sent to a server on the cloud. An alternative approach consists in using cameras to infer the status of parking lots. In both cases, the collected data are used to generate a real-time map of the parking area that can be made available to drivers, through a specific app on their smartphone. This way, drivers can be guided towards the closest (free) parking lot, thus saving time, reducing fuel consumption (and air pollution). As for traffic monitoring, the approach based on cameras requires preliminary data anonymization to prevent privacy issues.

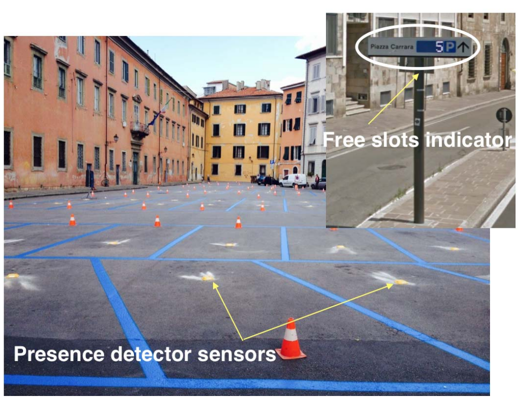

Fig. 3. Smart Parking.

Smart Surveillance. Urban security is a key requirement in modern cities and citizens are typically very sensitive to security. Smart surveillance is nowadays used in all cities, based on cameras deployed in almost all corners of the city. Some cameras are deployed by police and used for real-time and continuous monitoring of the most critical areas, while some others are private cameras deployed by private organizations (e.g., banks, shops) to prevent possible crimes. In principle, through an accurate and capillary deployment of small cameras it would be possible to monitor the entire city. Data collected by cameras can be stored and/or analyzed in real time, trough intelligent algorithms, to detect or prevent crimes. While this is beneficial for urban security, nevertheless it introduces a sort of modern Big Brother in our daily life that may compromise the privacy of citizens. In this context, deciding the right tradeoff between security needs and right to privacy of citizens is a very challenging task. People are very sensitive to urban security and crime prevention; at the same time, they are very jealous about their personal privacy. Therefore, appropriate rules need to be introduced to regulate this, very critical, field.

Participatory Sensing. All the previous applications and services rely on *institutional sensors*, i.e., sensors deployed either by a public institution (e.g., municipality, environmental protection agency, police department) or a private organization (e.g., banks, shops). However, nowadays everyone owns a smartphone, which is a powerful device equipped with a camera and many other sensors, such as GPS, gyroscope, accelerometers, compass, microphones, and many others. Therefore, citizens can use their personal smartphone to acquire information on the surrounding environment and upload them to the city cloud platform, where data can be stored and analyzed. This direct involvement of users (citizens) can enable a potentially large number of applications/services, ranging from simple notification of critical situations (e.g., malfunctioning systems, car accidents, misbehaviors, crimes, etc.) to *participatory sensing* applications, such as cooperative air-quality monitoring through private sensors owned by citizens. As above, since information is often collected through cameras, privacy issues must be carefully considered when dealing with this kind of applications.

Smart Homes/Buildings. The trend observed for cities also applies to homes and buildings. Future homes/buildings will be more and more equipped with interconnected sensors and actuators to monitor and control any activity inside the building. Most of activities (e.g., switching lamps on and off) will be automated based on information collected by sensors and/or preferences expressed by the user or inferred by the system itself. Ideally, this should increase user's comfort and reduce energy consumption. Commercial solutions for smart homes are already available on the market, or under development. Some of these solutions relies on cameras for detecting user activities and take decisions. Therefore, it has been already observed that sentences such as "the walls have ears" are no longer a way of saying; instead, they have become a reality [6]. Of course, this reality is not acceptable for many users who believe that (i) privacy cannot be traded off with energy efficiency, and (ii) comfort cannot be separated by privacy.

III. Towards the Internet of Autonomous Objects

All the applications considered in the previous section rely on a large number of sensors deployed in the city, whose generated data are then stored in the city Cloud platform and processed to take rational decisions, typically by city administrators and managers. The city of the future will also include autonomous agents, i.e., systems that can take decisions autonomously, thus enabling autonomous management and administration. In such a scenario, which could be referred to as the *Internet of Autonomous Things*, autonomous agents will interact each other exchanging data of different nature, through the Internet, to implement coordination and optimization processes without requiring human intervention. This paradigm has the potential to dramatically change future cities. For instance, a simple autonomous system can be deployed to manage efficiently the traffic lights, combining together data from traffic monitoring, air quality and smart parking that could be analyzed to regulate the traffic lights timing.

In the future, the number of autonomous systems will increase more and more, enabling additional synergies. Cars and buses will drive autonomously, and their integration into a larger IoT system will improve the efficiency of their decision-making processes as they can exploit also environmental and traffic information retrieved from other systems. Future autonomous taxi vehicles, e.g., offered through drones [7], will decrease urban traffic and, hence, its environmental impact. Autonomous cars will revolutionize the way of living of people, as the latter ones will have the opportunity to employ the time taken for driving in other tasks. Some of them will use this time to work even more. Some others will exploit this extra time for reading (electronic) newspapers, watching a movie, etc. Needless to say, the internal organization of cars will change.

From the previous examples, it clearly emerges that the utilization of autonomous systems in a city context (but also in other contexts) introduces a number of problems. First, since decisions are taken without any human intervention, security and privacy requirements on data exchanged by autonomous agents will become even more relevant. For instance, a security attack to an autonomous car may have very serious consequences on the safety of people. Also, autonomous agents bring in the problem of *responsibility* [5]. In case of a damage caused by an autonomous agent (e.g., an autonomous car), who is responsible for that? Its owner? Its vendor? Its designer? And who responsible in case of a misbehavior due to a security attack?

In the city of the future autonomous agents (i.e., robots) will replace humans in many activities. Robots are already used in many scenarios where the human presence is impossible or unsafe (e.g., the inspection of hazardous environments). Figure 4 shows Walkman, an anthropomorphic robot developed by University of Pisa in cooperation with the Italian Institute of the Technology and other research institutions, that has been, recently, used to check the status of buildings after an

Fig. 4. Walkman.

earthquake in Central Italy. Robots will be used in the future also to replace human workers in factories or in other contexts, for example in the assistance of elderly people in their homes. Figure 5 shows Jobot, an autonomous worker robot developed at the University of Pisa, that can be instructed to carry documents and other stuffs, e.g., in an office environment, from one office to another. There are examples of hotels where robots carry out reception services and clean rooms [8]. In the future, it will be possible to conceive a city full of robots that will be employed for works that are currently done by humans, e.g., streets repair, concierges, assistance.

Fig. 5. Jobot.

This futuristic scenario is considered controversial. From one hand, it will lead to the reduction of the number of jobs, thus creating social and economic problems, and raising ethical issues for technology makers. On the other hand, such future technology is expected to create new jobs and integrate seamlessly with human workforce. We can think, for instance, to an hotel in which receptionists and waiters are robots, while the rooms cleaning is still performed by humans jointly with robots, as in this case, the job requires human experience and perception.

IV. Futuristic Perspectives: Emotional Robots

Emotions are embedded in our everyday use of technology. Recently, Facebook has integrated emotions to its interface, thus allowing users to add a reaction to posts, e.g., love, sadness, anger, wonder. However, the explicit user intervention is required to specify her/her feeling or emotions. In future pervasive IoT systems, we can think of new smart objects/agents that will be able to detect human emotions with the help of artificial intelligence, thus enabling the Emotional IoT.

Systems deployed around us, e.g. in a city or home environment, will learn to catch the meaning of our emotions, and exploiting an adaptive user-device communication, they will respond based on user's feelings. The IoT is going to exploit human's emotions also into its applications and devices. For instance by tracking daily mood swings and detecting the impact of emotions on users patterns, IoT applications can change their behavior based on experts' recommendations on what is best to do with individuals with a certain state of mind. Information about mood and emotions can eventually be shared with other systems or even with friends, thus suggesting possible human interactions, e.g. because they share the same mood or have compatible feelings.

Smart watches and, more generally, wearables devices will represent the foundation for this emotional technology as they can collect and track users' emotions and feelings. Specifically, they will help in continuously evaluating the physical state of people and their physical fitness. This data will allow to coordinate users' daily habits for instance to avoid stressful situations, unnecessary anxiety and detect in advance potential health problems. Emotional sensing will help individuals that are in need of care (e.g. children, elderly) and those who suffer from autism, ALS (Amyotrophic Lateral Sclerosis) and other specific health conditions. With the help of this technology, they will be able to communicate their emotions. However, existing sensors that can extract physiological signals associated to emotions (e.g., hearth rate, skin conductance, blood volume pressure, etc.) often require invasive technologies (e.g., electrodes), and hence may not be easily accepted by people.

Fig. 6. FACE.

In order to overcome this issue, researchers are developing innovative techniques to understand emotions by analyzing facial expressions (e.g., through cameras) avoiding invasive devices. Figure 6 shows FACE (Facial Automation for Conveying Emotions) [9], a social android built by a team of researchers at the University of Pisa. It is able to emphatically interact with people through non-verbal communication. By using a set of sensors integrated in its head, FACE is able to analyze facial expressions and gestures of its interlocutors, and infer their emotional states. Based on the inferred emotional state, FACE establishes a non-verbal communication with its interlocutor by means of facial expressions and gestures. Specifically, it is able to reproduce facial expressions corresponding to some basic emotional states: Hanger, Disgust, Fear, Happiness, Sadness and Surprise. Due to its simplified facial expressiveness, FACE has been originally conceived for facilitating the interaction with people having deficit in understanding human emotions, like subjects with Autism. Recently, it was also the main ”actress” of a very special video, released by 20th Century Fox [10].

Emotional Technology may have many applications in the city of the future. In this context, it could be exploited to extract emotions from citizens by means of cameras already deployed in the city (e.g., for surveillance). The detection of emotions could be used to detect critical situations. For instance, a smart camera could identify a robbery by detecting a high level of fear of people in a certain area and alert the police automatically and timely. In addition, we can imagine that in the city and/or home of the future many objects around us will be able to detect the emotional state of their users, and react consequently. Hence, the way of communication will be revolutionized. For the same reason, the development of these emotional technologies will imply a number social and psychological issues. In addition, these technologies will have to include extreme security and privacy measures by design, as it will be highlighted in the next section. This will be essential considering the extreme sensitivity of the emotional data, whose diffusion could have devastating psychological effects on the users.

V. Security Social and Ethical challenges

As the IoT become more and more pervasive and evolving towards the *Internet of Autonomous and Emotional Things*, IoT devices are expected to gather a very large amount of data that will be shared among heterogeneous systems of city of the future. This data will be used to take decisions on the citizens and the city environment. Having millions of devices that produce data transmitted over the Internet poses a number of challenges in terms of security, and raises social and ethical implications. As technology evolves faster than the legal and moral frameworks, a future IoT governance should be created to manage the growing technology and the implications of its usage [5].

Citizens and users should become aware that every IoT device, given the fact that it is connected to the Internet, is exposed to attacks by malicious users that can exploit programming and design vulnerabilities, such as, weak encrypted communication protocols, simple passwords or outdated software versions. The security aspect in IoT systems is of crucial importance, especially in a Smart City environment. It allows to avoid data stealing, privacy violations or worst the malfunctioning of the system itself which could arise situations that pose a threat to human lives. Malicious users could target, for instance, traffic lights: the timing system can be hacked by injecting forged data to temper with the regular schedule, for example to force red lights to stay on for longer periods, thus causing traffic jams on a certain city area. Attacks could also target air quality or environmental monitoring systems. By injecting malicious air quality data, the attacker can refrain people from going in some areas of the city. In a waste-water monitoring system, instead, fake data could be injected to trigger fake alerts.

If we also consider future autonomous agents, even more serious security implications arise for the public safety. Imagine a city in which cars are driven autonomously, if some hacker can take control of them, she/he could drive them whenever she/he wants, potentially putting humans in danger. Security problems can be handled by enforcing security in the design of IoT systems. However, even the most secure systems could be weakened by the human component that is, in most of the cases, involved for ultimate control and configuration. For this reason, users should be made aware of proper practices for IoT device configuration, for instance by changing every default password and selecting strong ones. Such traditional solutions, however, are unfit to handle the social and ethical implications that the future Internet of Autonomous Things will arise. The enabling factor of such systems is indeed data sharing, which enables effective functioning of autonomous agents and allows their coordination, especially in the complex scenario of the Smart City. The data shared across different systems can be extremely sensitive, containing personal information that citizens are not willing to share, or that can violate their privacy. Even data that, at first sight, could seem meaningless, can represent a threat for human safety and privacy.

Nowadays, thanks to pervasive sensing devices, there is the possibility to acquire and store efficiently an enormous amount of data, i.e., exploiting cloud architectures. Data can be analyzed and merged using data mining techniques, which allow to detect users behaviors and expose their habits and personal preferences. Those insights can be of interest to the public administrations (to plan the city development) or to the marketing division of companies (to develop new products or to make targeted advertising). However, how can citizens' rights to privacy be enforced?

As highlighted in [5], the IoT will intensify the tradeoff between individual privacy and the exploitation of personal information to improve the efficiency of public services along with their safety and security. For this reason, it is mandatory to handle the privacy and ethical issues, especially considering that some of the IoT systems, even in the context of a Smart City, will deeply invade our personal sphere. These actions have to be implemented before autonomous IoT systems will become popular in order to include in them privacy rules and moral frameworks to be applied for the management of data. For instance, in traffic monitoring and in smart parking systems, when cameras are adopted, our movements around the city will be tracked through the number plate of our cars. The data regarding our movements could be transferred to the systems of different companies automatically without user's consensus. For this reason it is of crucial importance to have rules, clearly defined by laws, that are imprinted on those systems to regulate the diffusion of personal data and impose transparency in the data management processes and analysis. With smart surveillance systems this requirement is even more important, as very sensible information can be acquired, e.g., how much time we spend in shops, with whom, our preferences etc.

The freedom of citizens could be jeopardized if personal data is easily distributed and shared. Technology has no ethics, especially future autonomous systems that can share personal data, whenever an advantage for the system or the users is detected. For this reason, in order to make citizens more comfortable in sharing their data, thus making Autonomous IoT systems accepted by humans, a novel legal framework should be developed for determining the appropriate behavior of the systems and for defining the persons responsible and accountable for their correct behavior.

VI. Conclusions

The IoT systems will greatly impact the quality of lives in future cities. They will integrate our daily lives and change the way we live the city and its services seamlessly, without us even notice. Such pervasive technology, however, will be characterized by many potential threats as highlighted in this paper. In particular, new security and privacy threats will arise, thus requiring future actions by both legislators and technicians. The collection end exploitation of emotional data by IoT systems will also arise other social and ethical issues that have to be handled properly in order to allow citizens to enjoy their lives with the aid of future technology.

References

[1] J. Chase, "The Evolution of the Internet of Things", Strategic marketing, Texas Instruments, Dallas, 2013.

[2] P. Vlacheas et al., "Enabling smart cities through a cognitive management framework for the internet of things," in IEEE Communications Magazine, vol. 51, no. 6, pp. 102-111, June 2013.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," in IEEE Internet of Things Journal, pp. 22-32, Feb. 2014.

[4] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, pp. 1645-1660, 2013.

[5] F. Berman and V. G. Cerf, "Social and ethical behavior in the internet of things". Commun. ACM 60, pp. 6-7, January 2017.

[6] J. Bohn, V. Coroama, M. Langheinrich, F. Mattern and M. Rohs, "Social, economic and ethical implications of ambient intelligence and ubiquitous computing," in W. Weber, J. Rabaey, E. Aarts (Eds.), Ambient Intelligence, Springer, 2005, pp. 5-29.

[7] "REINVENTING URBAN MOBILITY", Volocopter. [Online]. Available: https://www.volocopter.com/en/. [Accessed: 28-Feb-2018].

[8] M. Rajesh, "Inside Japan's first robot-staffed hotel," The Guardian. [Online]. Available: https://www.theguardian.com/travel/2015/aug/14/japan-henn-na-hotel-staffed-by-robots. [Accessed: 28-Feb-2018].

[9] D. Mazzei et al., "The FACE of autism," 19th International Symposium in Robot and Human Interactive Communication, Viareggio, 2010, pp. 791-796.

[10] "The FACE robot from Research Center "E. Piaggio" casted by the 20th Century Fox," UNIPINEWS, 30-Aug-2016. [Online]. Available: https://www.unipi.it/index.php/english-news/item/8261-the-face-robot-from-research-center-e-piaggio-casted-by-the-20th-century-fox. [Accessed: 28-Feb-2018].