Ethical issues of monitoring sensor networks for energy efficiency in smart buildings: A case study

Available online at www.sciencedirect.com

ScienceDirect

Energy Procedia 134 (2017) 337–345

Procedia Engineering

www.elsevier.com/locate/procedia

9th International Conference on Sustainability in Energy and Buildings, SEB-17, 5-7 July 2017, Chania, Crete, Greece

Ethical issues of monitoring sensor networks for energy efficiency in smart buildings: a case study

Ylenia Cascone[a], Maria Ferrara[a], Luigi Giovannini[a], Gianluca Serale[a,]*

[a]*Politecnico di Torino, DENERG, TEBE Research Group, corso Duca degli Abruzzi 24, Turin, 10129, Italy*

Abstract

The development of Internet of Things (IoT) based sensors has become crucial for analyzing and optimizing the energy-performance of buildings. However, researchers and professionals should be prepared to deal with the social and thus ethical issues arising from the use of such technologies. Based on a real case-study, we present a detailed analysis of the networks of stakeholders and the consequent ethical issues related to the implementation of energy and IEQ sensors network in an Italian university campus. Alternative scenarios for eliminating or reducing the criticalities related to security and privacy issues are proposed.

Peer-review under responsibility of KES International.

Keywords: sensors; Internet of Things, ethics; privacy; security; monitoring; energy; idoor environmental quality; control

1. Introduction

Nowadays, sensor-based technologies for the monitoring of energy consumption and Indoor Environmental Quality (IEQ) are becoming a key element for the Heating Ventilation and Air Conditioning (HVAC) systems sector in buildings. Given their necessity to ensure a comfortable environment, sensors are becoming a crucial issue also for energy efficiency [1,2]. In recent years, since the major building technologies (e.g., system efficiencies, envelope insulation, etc…) are reaching their maximum performance physical limit, expectations of further disruptive improvements in the energy performance of buildings are related to sensor-based technologies. On one hand, such

* Corresponding author. Tel.: +39-090-4546; fax: +39-011-090-4499.
E-mail address: gianluca.serale@polito.it

1876-6102
Peer-review under responsibility of KES International.
10.1016/j.egypro.2017.09.540

systems can monitor occupancy and correct bad behaviors. On the other hand, if connected through the Internet to data repositories and weather forecasts, they can improve the system performance by anticipating climate actions with predictive controllers [3] and correct inefficiencies by means of a comparison with good practice benchmarks. Furthermore, present sensor technologies are very cost effective, as the cost reduction of electronic items and the diffusion of wireless networks have dramatically cut down investment and installation costs. This is particularly true in historical buildings, where retrofitting actions are not always possible or economically feasible [4]. Moreover, in existing public buildings, energy savings can be achieved by designing low CapEx ICT-based services to monitor and control environmental conditions, energy loads and systems operation.

A study by Fraunhofer Institute for Building Physics [5] pointed out that an intelligent sensor-based regulation of the heating system can ensure higher energy savings than any other building technology. Furthermore, the study highlighted that 24% of savings are to be ascribed to occupant monitoring and 7% to weather forecast [6], and that high energy savings were achievable by raising awareness about the energy consumption issues in public building occupants. For this reason they designed a monitoring network capable of collecting and communicating coarse energy consumption information in large public buildings. Pesola et al. [7] dealt with remote monitoring of municipality buildings, designing multi-criteria metrics capable of addressing the needs of every stakeholder.

Recently, similar studies were carried out also at Politecnico di Torino. In particular, the projects “Smart Energy Efficient Middleware for Public Spaces” (SEEMPubS) and “WiFi4Energy” dealt with wireless sensor networks for energy management in educational buildings. A tangible result of this project is the setting up of the “Politecnico di Torino Living Lab”, an office that aims at monitoring real time data concerning energy consumption. Politecnico di Torino consumes about 5000 t.o.e of primary energy every year, corresponding to an energy bill of about 4 M€/year. Energy-saving opportunities can thus produce important reductions of operative costs. Nowadays, the sensors network consists in smart meters measuring the power (thermal, electrical, water consumption) absorbed at different levels. Furthermore, in the period 2010-2012, 70 additional IEQ sensors recorded data in different environments (offices, corridors, lecture halls). The purpose was to gain additional knowledge from energy and IEQ monitoring in order to infer some rules driving the energy consumption.

In the “SEEMPubS” project, the idea was to monitor environmental and energy data in real time and to control the operation of lighting and HVAC systems, in order to ensure both energy efficiency and environmental comfort. With regard to lighting, several control logics were adopted according to the use of the rooms, but they were mainly based on occupancy detection coupled with manual control. The lights were programmed to be switched on only in presence of occupants and dimmed to integrate daylighting or to achieve visual comfort. With regard to the heating strategy, a lower set point temperature was maintained during unoccupied hours, and the heating system’s switch off was anticipated when the power from lighting and electrical devices exceeded the heating power’s need [8]. Moreover, in the “WiFi4Energy” project, carbon dioxide sensors were also installed.

The present work focuses on critical ethical aspects related to sensor-based technologies for monitoring the buildings energy consumption and IEQ. The sensors network experiences carried out at Politecnico di Torino were used as case studies to analyze the ethical issues concerning the monitoring of public spaces. The authors of this paper consider it important to specify that they were not directly involved in the above mentioned projects and monitoring experiences (contacts are listed in the acknowledgment of the present paper for interested readers). Firstly, this paper provides a scheme and a framework of stakeholders involved in activities of monitoring public spaces of a university. Secondly, some interviews to the main actors involved in those projects were carried out to identify the main drawbacks and ethical issues that were perceived. Thirdly, the highlighted ethical issues were analyzed in depth and compared with similar case studies from the literature. Eventually, possible alternative scenarios were proposed and their consequences were outlined.

2. Description of the stakeholders’ network involved in the monitoring campaign

Figure 1 represents the Politecnico di Torino network of stakeholders involved in the process described in this paper. The key actors are highlighted in the figure with different colors: yellow boxes indicate the policy-makers, blue boxes define the sensors main users, the technology providers are identified with orange boxes and the purple box indicates a possible short circuit in the system (the so called villains represent actors that should not be present, but which still represent an actual threat to the system). Arrows indicate the main direction of communication while

double arrows indicate two-way communications. Colored lines are used to indicate different critical aspects and paths that concern ethical issues. These aspects will be better explained in the following sections.

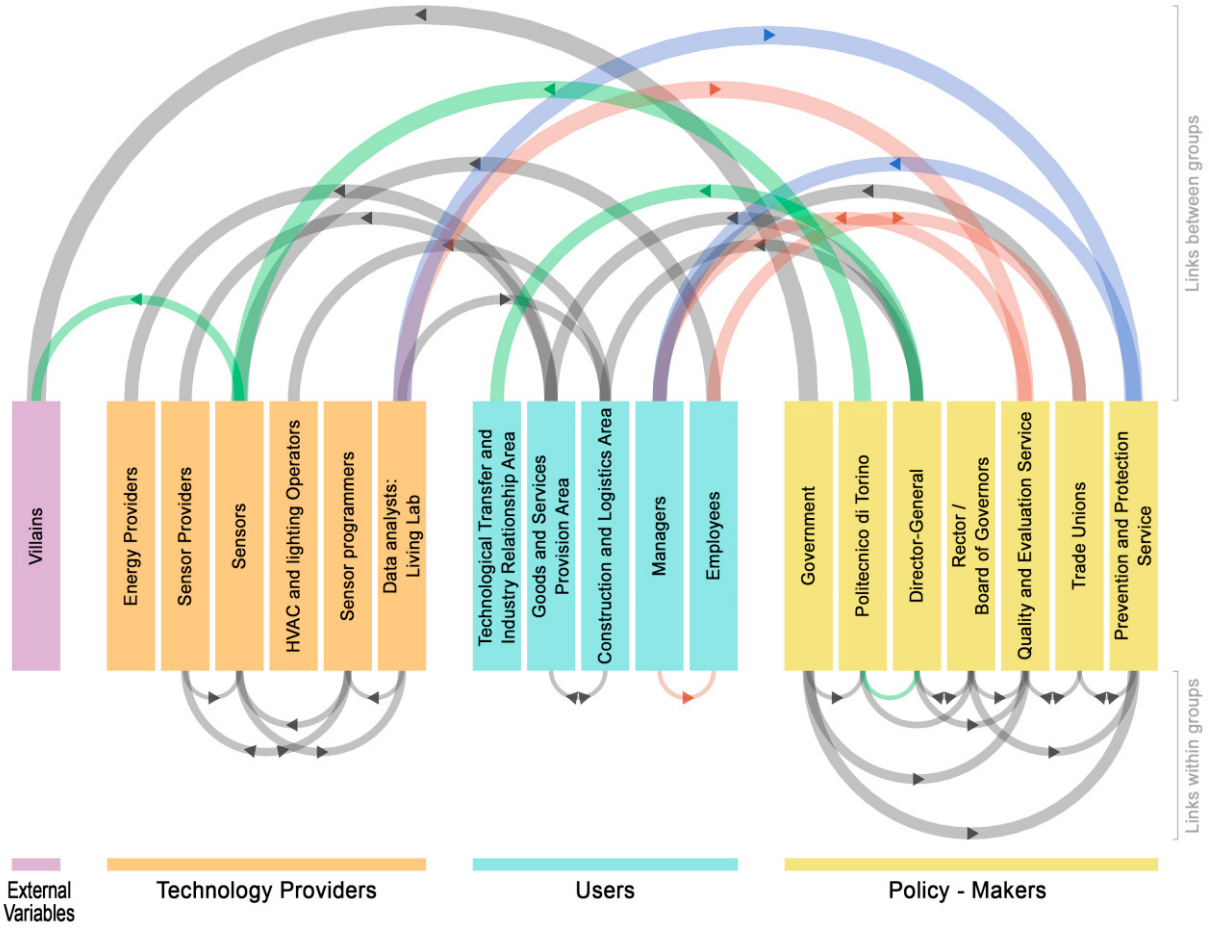

Fig. 1. A framework of the stakeholders' network.

The highest level of policy makers is represented by local or national Governments and the institution Politecnico di Torino, as they affect the entire network with their laws and internal regulations (e.g., laws on computer crimes, privacy, hygiene in work places). Politecnico di Torino is represented by its *Board of Governors*, *Rector* and *Director-General*. The Rector directly controls the office of *Prevention and Protection Service*, and he shares with the *Director-General* the responsibilities on the office of *Quality and Evaluation Service*. Those two offices have the function of policy makers in terms of control and drawing up of internal regulations. The *Director-General* is also engaged in the control of some administrative areas involved in the process as users. Trade Unions represent the users in front of the policy-makers and dialogue with the various actors involved.

The leading role of users is taken by the Employees of Politecnico di Torino. This class represents indistinctly all the different figures that actively work inside the institution. Those which cover responsibility positions on other employees are defined Managers. The main administrative areas involved in this process are the *Construction and Logistics Area* and the *Goods and Services Provision Area*. The former plans with *Living Lab* the positioning of sensors and acts on HVAC and lighting systems, modifying their set points and regulation logics according to the sensors' measures, while the latter represents the area that pays the electricity bills of the university. *Technological Transfer and Industry Relationship Area* could also be indirectly involved.

The Living Lab is both a user of the data retrieved from sensors, and the office that coordinates the technology providers involved in the process. In particular, these ones are the Sensor Providers (e.g., whom guarantees the sensor hardware) and Sensor programmers (e.g., whom decides the acquisition mode, the ICT code used inside the network, the sampling time). HVAC and lighting systems Operators follow the instructions provided by the *Goods and Services Provision Area* in terms of system regulation. Energy Providers are the actors who, supplying energy services to the Politecnico di Torino, earn money.

3. Ethical issues identified in the case study

Some of the main actors involved in the "WiFi4Energy" and "SEEMPubS" projects were interviewed to point out the main ethical issues of monitoring sensor networks for energy efficiency in smart buildings. Those actors represent the various stakeholders directly or indirectly involved in the projects. On the one hand, interviews to professors and researchers allowed the main scopes of the projects and the difficulties encountered to be outlined. On the other hand, brief interviews to the staff of Politecnico di Torino indirectly involved in the monitoring campaign were carried out to understand their opinion concerning possible ethical issues. The various opinions were merged in the present paper, which was submitted to the approval of the people involved in the interviews to ensure correctness and consistency of the information herewith reported with their opinions. An additional question regarding health issues was identified through literature analysis.

The first problem regarded the privacy theme. Data on IEQ retrieved by means of CO_2 sensors, as well as data from the operation of the dimming lighting sensors, could provide information on the occupancy of offices and could be potentially used to control the presence of people in their working place. Even though the employees working in the offices hosting the sensors were not compelled to follow a strict working time, they perceived the presence of sensors as a potential threat (Figure 2a). Moreover, in addition to monitoring their working schedule, the presence of sensors could also potentially identify bad or even illegal behaviors of the occupants, for example by detecting people smoking indoors. As highlighted by [9] and [10], the privacy issue in the context of smart spaces is related to a matter of trust on who handles the data (both people and software), in order to prevent the disclosure of data to third-parties. Even though several explanations on how the sensor network worked were provided to inform the end-users, the lack of trust in the fact that the sole interest of the project was the improvement of the energy efficiency eventually led to its interruption. Another issue that emerged in the "WiFi4Energy" project was the fact that the sensors indirectly allowed the quality of workplaces to be verified. The possibility of identifying criticalities, such as non-compliances to health standards and regulations (e.g., minimum levels of daylighting), could be considered as a benefit for the employees. However, the presence of sensors was perceived as a threat by those stakeholders who were responsible of guaranteeing a good quality of the workplaces (Figure 2b). Although the presence of sensors could indeed be beneficial to promote actions for the improvement of the workspaces, this could happen only in relation to the will of spotting criticalities and taking action to correct them.

Another issue that can be identified in the Internet of Things (IoT) context regards security. If not well-protected, the sensor network can become a weak point through which unauthorized access can become a threat to the secrecy of data. Sensible data that need protection range from personal data of people working and studying in Politecnico di Torino to information and results on ongoing researches and patents (Figure 2c). Due to the limited computing power of IoT technologies, the direct application of traditional Internet security protocols is recognized as not feasible [11], and hence security and privacy in the context of IoT are still a challenge [12]. Moreover, most of the security efforts are concentrated at the levels of application and network, but proper hardware protection is often lacking [13]. In addition, information on the occupancy of offices could pose a threat to the security of physical places, for it could foster the occurrences of theft.

An additional problem that can be highlighted is the potential threat that the wireless sensor networks pose to the health of the occupants. The use of Wi-Fi devices is becoming more and more common, and there is a growing concern about the possible long-term health effects of the exposure to the radiofrequency radiation (RF) signals. According to the Precautionary Principle [14], when an activity poses a potential threat to harm human health or the environment, precautionary measures should be taken even if some cause-effect relationships are not yet completely proven. There is a vast literature on the effects of RF on both animals and humans, and a review by the International Commission on Non Ionizing Radiation Protection (ICNIRP) highlighted that, from the few studies which

performed an adequate exposure assessment, health-related effects were not found [15]. The only identified health effect relates to an increase in body temperature, although this increase is insignificant for the levels of exposure to wireless networks [16]. A recent study by Pachón-García et al. [17] on the emissions of Wi-Fi networks in a typical indoor place highlighted that the radiation coming from this technology is however not negligible, even though all the recorded values were well below the threshold of 61 V/m set by the ICNIRP guidelines [18]. However, the health risk is still an open question, and research in this field is still ongoing. Further studies are still necessary to verify whether, and to which extent, RF waves emitted from Wi-Fi devices affect human health. Some investigations suggest that some effects could exist [19,20,21].

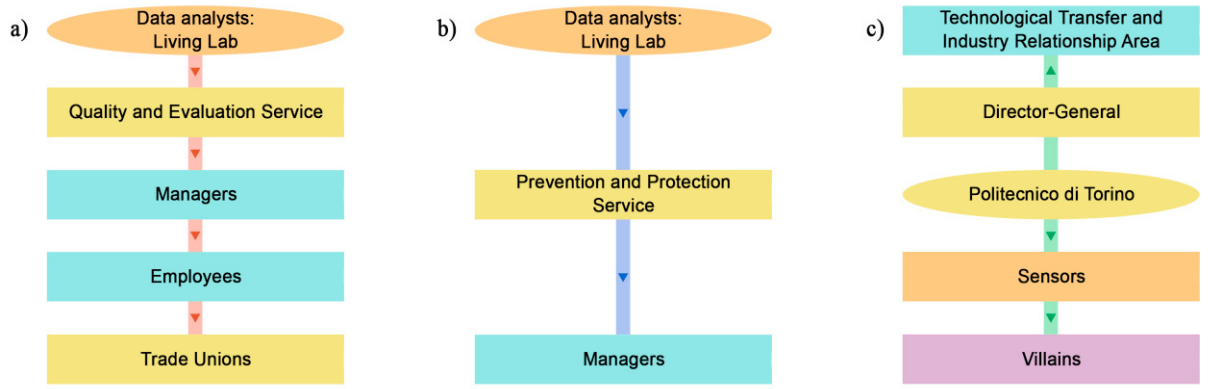

Fig. 2. Critical paths of main ethical issues: (a) privacy of the employees; (b) quality of workplaces; (c) security of the data.

4. Discussion

This section tries to suggest possible alternative scenarios that are able to mitigate or address the ethical issues highlighted in the previous part of the paper. In this work, alternative scenarios are proposed only for the two major ethical issues highlighted by the stakeholders of the projects. In particular, those are the drawbacks related to the privacy issues and those concerning security. The proposed solutions are based on a critical discussion of the outcomes of various scientific papers addressing similar situations.

4.1. Alternative scenarios for the privacy issues

Even though the potential energy savings achievable by means of ICT sensor technologies are undeniable, the present study highlights how the open ethical issues related to the privacy theme exist. From the interviews carried out it was clear that the occupants were mostly afraid that the gathered data could disclose potential bad habits in the working space. This information was not directly collected by the IEQ sensors, but it was possible to indirectly retrieve it (e.g., monitoring whether an office was occupied or not or if someone was smoking in it). The two questions to be asked are therefore the following:

- How are the collected data used?
- Who has access to the collected data?

The current scenario does not provide an exhaustive answer to these questions. Indeed, some sensible data about the occupants' behavior in their workplace were stored and no actual guarantee about their possible use was given to them. In the present study, some alternative scenarios are elaborated and then analyzed to reveal their strengths and weaknesses, including additional ethical issues they may raise.

A first alternative scenario could imply the elaboration of the collected data according to the so called Differential privacy (DP). As explained by Chau and Little in [9], DP is an evolution of the common practice of data

aggregation. Based on the idea of ensuring that the probability of getting any outcome remains the same whether or not any individual participates, DP relies on complex algorithms that randomize and add noise to the functions that use the collected dataset in order to mask the effects of individual participation. In this way, data relative to a given user cannot be retrieved. Hence, the privacy of the single person is safeguarded, as no personal data are disclosed in any part of the procedure. Although the privacy of the user is protected, DP does not get along well with the smart space concept. Indeed, smart spaces need to adapt their performance to each collected datum; and so, to be efficient, disaggregated data are necessary. In DP, local adaptation of the system performance is intrinsically not possible. Moreover, privacy issues in this scenario are not completely solved, but only shifted from an individual to a group dimension. Mantelero in [22] pointed out that group analysis of the collected data can still affect the single user. The analysis of DP aggregated data may in fact bring the policy-makers to decisions that pertain to the single user too. For example, if misbehavior in a group of users is detected from the DP data analysis, the responsible for that given misbehavior cannot be detected, and the possible countermeasures would influence the entire group. The collective dimension of data protection is a relatively new ethical topic, developed simultaneously to the big data analysis advancements, and about which a debate is still ongoing to determine its boundaries and its rules. One partial response would be that these data have necessarily to be managed by a completely trusted entity [9], but it is clear that this is a non-exhaustive answer, since another actor is added to the process and the question of ownership of the data is added [23].

An alternative way to protect the privacy of the users would be the application of the concept known as K-anonymity to the collected data [24]. This privacy safeguarding strategy aims at protecting the identity of the person whose information is disclosed. This result is achieved by defining which attributes of the user may be used to reveal his identity (name, age, location, etc…) and generalizing the values relative to these attributes so that identification of any specific person is no more possible. In this way, even if k-anonymized sensitive information is released, smart space occupants remain protected by anonymity. The privacy of the single user is generally well protected with the k-anonymity strategy, as no identification is usually possible. Unfortunately, smart spaces provide multiple data releases over time, all relative to the same group of people (the occupants), which means that composition or intersection of these multiple dataset may reduce the size of the anonymizing set. In fact, by monitoring the evolution of the dataset over time, it might finally be possible to reveal the identity of the single user through the changes that occur in the single attribute categories. Generally, K-anonymity works better than DP for smart spaces, but it also implies a reduction of precision in the collected data, and the probabilistic privacy protection strategy can again severely degrade the performance of the system, as well as the achievable energy savings. Furthermore, the considerations on group privacy regarding the first alternative scenario remain valid in this second scenario too.

According to the recent *General Data Protection Regulation* (GDPR) (Regulation (EU) 2016/679) [25], measures that meet the principle of data protection by design should be implemented. Both the first and the second alternative scenarios comply with widespread guidelines inside the privacy safeguard research field [26], according to which data should be aggregated or anonymized unless it is strictly necessary to do otherwise, and they should be systematically associated to the users' identities only when and where it is strictly necessary. In the analyzed case study the occupants were mostly concerned that environmental data could be indirectly used to detect (and disclose to their superiors) their working time or misbehavior. This situation is obviously a privacy violation, as the users were not informed of such a use of IEQ data. A third alternative scenario follows a completely different strategy, i.e. that of informed consent of occupants. If the users are informed about this possibility of the use of IEQ data and have given their consent, the privacy violation is partially solved. If the employer is paying his employees to fulfil a task and follow previously agreed rules, does he have the right to monitor whether or not they are misbehaving and breaking these rules? This is a topic of broad and current interest, about which the international debate is still on-going and a univocal answer is not possible yet. Therefore, only a partial response to this question is possible, that is to say that the use of monitored IEQ data may be always possible when the informed consent is given by the user and no fundamental human right is violated [27]. In [27], comparing the traditional village model to the global village one, the author analyzed the following statement and its possible consequences: "…openness is a virtue, in any case, what does an honest man have to fear." In other words, why should an honest employee be worried about the fact that his actions in the workplace are monitored? Well, this can raise two major issues, whose effects on the employees may be very serious. The first issue is of psychological nature; psychologists have shown [27] that if

someone knows (or thinks) that he is being monitored, he no longer dares to express his natural feelings, above all joy and anger. These feelings are then completely suppressed on the workplace. This means that monitoring the users' activity, even prior their informed consent, may not be a privacy issue, but has a disruptive effect on the personal dimension of the employee, changing his nature and preventing him from being free to express himself. Even though only few studies address the problem, this one, brought to the extreme, may be considered a violation of the human rights. The second issue is strictly linked to the above one, and related to the concept of objectification of the worker. By monitoring his employees, the employer might finally end up looking at them no more as people performing a task, but only as instruments that he can exploit to reach his goals. This is a very serious issue, which must not been underestimated as it results form a long history of debate concerning workers' rights, Only with great efforts and trade union battles this mentality, typical of the great plants of the end of XIX century, has finally been discarded, and laborers have started to be considered as human beings and not only as means for making money. Now, if this mentality takes roots again, the human rights of the employees may be subjected to risks of being reduced. For all the issues it may raise, such a position has to be analyzed very carefully, taking into account also the effects it may generate.

4.2. Alternative scenarios for the security issues

Both human-to-machine and machine-to-machine communications are offered through IoT devices. However, the more the IoT devices are deployed, the greater the related information system is at risk, and several security properties may need to be satisfied, such as confidentiality, integrity, authentication, authorization, and freshness of data [11]. Security requirements may directly involve the data gathered from the sensors (if sensible), as well as the controlled access to other resources, such as the IoT network layer. In this context, the main questions to be asked concerning security are:

- Why should data be protected?
- Who should take the risk of security system fail?

As already mentioned, in the "SEEMPubS" and "WiFi4Energy" projects, the data were not sensitive by themselves. However, they should be protected due to the information that can be indirectly derived from them. For this reason, alternative scenarios addressing security issues should provide solutions covering both physical and virtual space security risks.

Concerning physical spaces, the knowledge about space occupancy may lead not only to privacy problems, but also to security problems, as thieves may enter the monitored smart spaces when they know that they are not occupied. Alternative scenarios addressing this issue should avoid the possibility of exactly identifying the space to which data are related. Therefore, it is possible to find synergies between some scenarios related to privacy issues and those concerning security, as the above presented "Differential privacy" and "K-anonymity" scenarios could be implemented for providing solutions also to security problems. However, as mentioned above, such scenarios imply reducing the details of the collected data and thus reducing the potential energy saving based on space monitoring.

Moreover, concerning the virtual space, data should be protected because they may become a "doorway" for other sensitive data that are stored and shared within Politecnico di Torino network. Based on this concept, it is assumed that the more doorways connecting sensors and the Internet (here intended as the virtual space) are opened, the more the system is likely to be attacked. Therefore, alternative scenarios should limit the number and increase the protection of such doorways, given that most of IoT devices are limited in terms of CPU, memory capacity and battery supply. It seems therefore impossible to directly apply standard conventional security protocols of the Internet, and research is still working to define appropriate IoT security protocols [11].

A first extreme scenario, where no doorways to an external network are opened, can be identified as a no wireless and no remote internet storing of data scenario. This scenario seems to be completely secure with regard to virtual security risks, as there is no direct link between data and the rest of the network. On one hand, all the sensors are connected through cables to a dedicated server placed in a secure room, so that external attacks from the wireless network are avoided. Due to the robustness of the cabled network, the only possibility to have access to data is to enter into the secure room and get data from the server. On the other hand, also the possible attacks from the internet

are avoided by using no cloud technologies. However, this scenario presents a criticality due to the higher cost to build a wide cabled network, in particular in historical and existing buildings. Moreover, users could need the possibility to have access to the data also from remote, and the absence of cloud communication would limit this necessity. In particular, one prerogative of the analyzed research projects was that all the partners, inside and outside Politecnico di Torino, could have access to the data and remotely work on it.

In order to limit the number of doorways between the sensor network layer and that of Politecnico di Torino, one a second scenario could be defined. The server where data are stored may be an external server that is managed by a third party entity who is responsible for the security risks concerning data. In this way, part of the risk is transferred to a third party and the virtual space of other sensitive data within the Politecnico di Torino's network is protected. The remote access to data remains possible for all the project partners. However, it must be recognized that the third party owner of the external server may not be a fully trusted entity, and therefore other unexpected security risks related to confidentiality may occur. Authentication and authorization procedures may be implemented in order to limit such risks.

5. Conclusions

The development of IoT-based sensors has become crucial for analyzing and optimizing the energy-performance of buildings. However, several social and thus ethical issues may arise from the use of such technologies. The present paper reported the main ethical issues identified in the design and installation of sensor networks for the monitoring of energy consumption and IEQ in an Italian university campus. Far from providing exhausting and conclusive answers to the analyzed problems, this study supplies an overview on the major issues that are likely to be encountered, i.e. data security and privacy, and on possible ways to solve them. Future work could combine the different alternative scenarios herewith presented to simultaneously address more than one ethical issue.

Acknowledgements

Special thanks to prof. Gian Vincenzo Fracastoro, Laura Blaso, Emanuele Norata, Riccardo Tomasi and Giovanni Carioni for their support in this research through the sharing of their opinions and information about the analyzed research projects. For the project SEEMPubs interested readers can refer to "https://ec.europa.eu/digital-single-market/en/news/seempubs-maximum-energy-savings-minimum-intervention-historic-buildings", while for the project "WiFi4Energy" to "http://www.wifi4energy.polito.it/". A special thanks also to prof. Norberto Patrignani, because the present paper was conceived thanks to his PhD course "Computer Ethics" held at Politecnico di Torino.

References

[1] Ahmad MW, Mourshed M, Mundow D, Sisinni M, Rezgui Y. Building energy metering and environmental monitoring – A state-of-the-art review and directions for future research. Energ Buildings 2016; 120:85–102.
[2] Fabrizio E, Ferrara M, Monetti V. Smart heating systems for cost-effective retrofitting. In Pacheco-Torgal F, Granqvist C, Jelle B, Vanoli G, Bianco N, Kurnitski J, editors. Cost-effective energy efficient building retrofitting. Materials, technologies, optimization and case studies. Amsterdam: Elsevier - Woodhead Publishing; 2017. p. 277-302.
[3] Fiorentini M, Wall J, Ma Z, Braslavsky JH, Cooper P. Hybrid model predictive control of a residential HVAC system with on-site thermal energy generation and storage. Appl Energ 2017; 187:465-479.
[4] Capozzoli A, Grassi D, Piscitelli MS, Serale G. Discovering knowledge from a residential building stock through data mining analysis for engineering sustainability. Energ Proc 2015; 83:370-379.
[5] Kersken M, Sinnesbichler H.. Simulation study on the energy saving potential of a heating control system featuring presence detection and weather forecasting. Internal report of Fraunhofer Institute 2013.
[6] Zhao L, Zhang J, Liang R. Development of an energy monitoring system for large public buildings. Energ Buildings 2013; 66:41–48.
[7] Pesola A, Serkkola A, Lahdelma R, Salminen P. Multicriteria evaluation of alternatives for remote monitoring systems of municipal buildings. Energ Buildings 2014; 72:229–237.
[8] Aghemo C, Virgone J, Fracastoro GV, Pellegrino A, Blaso L, Savoyat J, Johannes K. Management and monitoring of public buildings through ICT based systems: Control rules for energy saving with lighting and HVAC services. Front Arch Res 2013; 2:147–161.
[9] Chau JC, Little TDC. Challenges in Retaining Privacy in Smart Spaces. Procedia Comput Sci 2013; 19:556–564.
[10] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comp Sy 2012; 28:583–592.

[11] Nguyen KT, Laurent M, Oualha N. Survey on secure communication protocols for the Internet of Things. Ad Hoc Netw 2015; 32:17–31.
[12] Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. 2014. Security, privacy and trust in Internet of Things: The road ahead. Comput Netw 2014; 76:146–164.
[13] Hernandez G, Arias O, Buentello D, Jin Y. Smart Nest Thermostat: A Smart Spy in Your Home. In: Proceedings of Black Hat 2014. Las Vegas. p. 1–8
[14] Various Authors, 1998. Wingspread Statement of the Precautionary Principle. Racine, WI (USA).
[15] ICNIRP, 2009. Exposure to high frequency electromagnetic fields, biological effects and health consequences (100 kHz–300 GHz). Oberschleißheim (Germany).
[16] World Health Organization. 2006. http://www.who.int/peh-emf/publications/facts/fs304/en/ [web Doc].
[17] Pachón-García FT, Fernández-Ortiz K, Paniagua-Sánchez JM. Assessment of Wi-Fi radiation in indoor environments characterizing the time & space-varying electromagnetic fields. Measurement 2015; 63:309–321.
[18] ICNIRP. Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). Health Phys 1998; 74:494–522.
[19] Avendaño C, Mata A, Sanchez Sarmiento CA, Doncel GF. Use of laptop computers connected to internet through Wi-Fi decreases human sperm motility and increases sperm DNA fragmentation. Fertil Steril 2012; 97:39–45.
[20] Choy JT, Brannigan RE. Re: Use of Laptop Computers Connected to Internet Through Wi-Fi Decreases Human Sperm Motility and Increases Sperm DNA Fragmentation. Eur Urol 2012; 62:1196–1197.
[21] Çiğ B, Nazıroğlu M. Investigation of the effects of distance from sources on apoptosis, oxidative stress and cytosolic calcium accumulation via TRPV1 channels induced by mobile phones and Wi-Fi in breast cancer cells. Biochim Biophys Acta 2015; 1848:2756–2765.
[22] Mantelero A. Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection. Comput Law Secur Rev 2016; p. 1–18.
[23] Molina-Solana M, Ros M, Ruiz MD, Gómez-Romero J, Martin-Bautista MJ, 2017. Data science for building energy management: A review. Renew Sust Energ Rev 2017; 70:598–609.
[24] Sweeney L. K-anonymity: A Model for Protecting Privacy. Int J Uncertain Fuzz 2002; 10:557–570.
[25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union L 119 2016. p. 1–88.
[26] Rottondi C, Verticale G, Capone A. Privacy-preserving smart metering with multiple data Consumers. Comput Netw 2013; 57:1699–1713.
[27] Poullet Y. Data protection legislation: What is at stake for our society and democracy? Comput Law Secur Rev 2009; 25:211–226.