Privacy Enhancing Technologies for the Smart Building Domain

Stephan Cejka · Felix Knorr · Lukas Krammer · Daniel Lechner

Abstract – In today's building automation systems, high amounts of data are collected in order to optimize costs and reduce energy consumption. Some of these data can directly or indirectly be related to an individual person, leading to a possible privacy infringement. Therefore, special care has to be taken in order to protect personal data and privacy. Furthermore, the use of personal data is restricted by law. This article addresses some of the issues and gives possible solutions. As privacy issues introduced by Smart Meters are tightly connected and have been heavily discussed in literature, this work will use them as the main example for describing privacy preserving solutions.

1. Introduction

Major objectives of the building automation domain are cost optimization and energy consumption reduction. By utilizing accurate occupancy information, the energy efficiency can be improved, for example, by effectively controlling the heating, ventilation and cooling (HVAC) systems and lighting. Occupancy has traditionally been detected using sensors, but it was shown that high frequency Smart Meter data also allow that. This is problematic in terms of privacy as these data necessarily are transmitted to the outside of the customer's sphere ([1, 2]).

2. Personal Data in the Smart Building

Studies show that the building sector accounts for up to 40 % of the overall energy consumption, thus savings in this area can have a high impact. For optimization purposes, various types and high amounts of data are collected and processed in a Smart Building (e.g., HVAC, lighting and shading, access, elevators, security, fire detection and metering data), some of those possibly infringing the privacy of a person and thus requiring compromises on their collection and their processing. Once these data can be related to an identifiable person, they become personal data, imposing legal restrictions on how to use them. Processing of personal data is lawful only if (i) it is in accordance with the law, (ii) pursues a legitimate purpose, and (iii) is necessary in a democratic society in order to achieve the legitimate purpose.

3. Smart Metering

Even customers that are not living in a Smart Building are affected by the introduction of Smart Meters into their homes. In difference to traditional Ferraris meters that have only been read out once a year, new Smart Meters may transmit the current consumption in intervals of only 15 minutes. It makes a big difference from perspective of privacy, if just an annual consumption of 2,500 kWh or a consumption of 0.5 kWh within 15 minutes is known. Legally or regulatory specified low intervals of measuring and processing energy consumption allows for big insights into private homes and habits of their inhabitants, i.e., when they were home or which appliances were used. Appliances show characteristic power consumption patterns and can therefore be identified if the meter is read out sufficiently often. As a result, profiles of individual behavior can be derived. Fewer readouts could at least identify sleep and absence phases, still problematic if such data is available, e.g. to robbers. Furthermore, data could be used by third parties, e.g., for targeted advertising, insurance, or to identify health problems.

Doubts about the compliance of Smart Meters with the European Convention on Human Rights delayed their introduction in the Netherlands for two years. In 2014, 200,000 Smart Meter have already been in use in Austria; it is legally required for grid operators to equip 95 % of their customers until 2019. Beside a general data protection act, since 2013 special regulations addressing privacy in Smart Metering are active in Austria. One effect is that fines have fewer premises in this domain than in the general act, such that sanctions can be imposed easier. For other kinds of a building's data these regulations are not applicable; furthermore there is no other special act in existence for those.

4. Selected Privacy Enhancing Technologies

The finding of appropriate technical and legal solutions for privacy is one of the key tasks. Privacy issues and countermeasures in Smart Metering have heavily been addressed by literature and will also serve as main example in this work. Depending on the type of data, some of the approaches can also be used for other arising data in the Smart Building.

4.1 Data Minimization

Only the minimum of personal data required to fulfill the contract shall be collected. Any processing of data needs to be necessary and proportional. In this domain, the goal can be achieved by reading out personal data rarer. Compromises are necessary as the

Stephan Cejka · Felix Knorr · Lukas Krammer · Daniel Lechner
Siemens AG Corporate Technology,
Research in Digitalization and Automation,
Siemensstraße 90, 1210 Vienna, Austria
stephan.cejka@siemens.com

grid operator relies on short-time feedback to know the status of the grid.

4.2 Opt-In

End users should be able to decide about the installation of a Smart Meter. However, a certain percentage of households have to be equipped by law; hence an opt-in solution is not possible. Austria allows for limited opt-out as long as the goal of 95% of all households being equipped with Smart Meters is not affected. An explicit opt-in is necessary for extended functions requiring readouts more often than once a day (e.g., for dynamic tariffs). For the current Austrian legal situation, an explicit declaration of consent is required for use of personal data exceeding the Smart Metering privacy regulations.

4.3 Data Anonymization

It should always be sought to get along with anonymized or pseundonymized data only, such that it is not possible to backtrack to the end user. In anonymized data, all identifying elements are purged. Even though the grid operator needs to know the current status of the network, it is not necessary to map all high frequency meter data to an end user. For billing, the connection to the customer is of course necessary, but those data can be transmitted in a very low frequency.

4.4 Data Aggregation

It is often sufficient to process aggregated data from more than one measuring point only. For example, a transformation substation could aggregate the minimum and maximum voltage or the sum of the current flow of all connected households not imposing the individual measurement values.

4.5 Data Security and Technical Data Protection

Communication to the outside of the customer's sphere has to be protected against unauthorized access, interception and modification by third parties. It needs to be ensured that devices remove data after a defined time and tenants cannot access data of earlier inhabitants or neighbors. Access to personal data at authorized parties should be restricted to only those employees that are required to read data. Thus, every access – local data base readouts, data exports, as well as remote maintenance – needs to be logged.

4.6 Data Sovereignty and Earmarking

End users should be able to decide what their data is used for. Authorized people shall use personal data only for the defined objectives, they must not link such data with other data and they must not pass them over to third parties. All accesses of third parties shall only be allowed with the permission of the end user. Therefore, landlords, insurance companies, employers, etc must not have access to this information; it is even denied by Austrian law to use such data in administrative or civil cases.

4.7 Data Obfuscation

In comparison to previous mentioned solutions, this approach involves the customer only. The intention is to mask energy usage by flattening the consumption curve, for example, by strategically charging and discharging energy storages or by changing the photovoltaic feed during appliance's use. Other solutions add noises to the consumption curve by randomly powering devices with high energy consumption (e.g. a water boiler) on and off.

4.8 Minimal and Local Data Storage

Data shall only be kept as long and as detailed as they are required for the objective they have been collected for. Furthermore, data should be retained in a local place only, without a transmission to the operator's central data bases if not necessarily required there – most types of Smart Building data usually fall into this category.
For Smart Meter data a transfer is usually required since the grid operator is interested in the current state. A full view on the grid including a central storage of the collected individual consumption data on the operator's site is however not necessary, for example, when using automated secondary substations that react on grid problems by themselves (cf. [3]). Some approaches even move the procedure of factorization into the customer's sphere, thus only requiring transmitting the accumulated energy costs.

4.9 Data Control and Customer Incentive

Transparent and objective access to the collected data is an important aspect, notably as Smart Meter systems are introduced to enhance energy efficiency and consumption. Customers are entitled to receive information about their energy consumption as an incentive to save energy. Necessary is therefore a web site that enables the end user to monitor his data and to see immediate effects of changing habits. It has to comply with safety standards and data protection regulations in relation to the access rights, i.e., authentication and encrypted connection. Direct access for third parties needs to be prohibited.

5. Outlook and Conclusion

While Smart Meter privacy issues have heavily been discussed in literature and special data protection acts have been implemented in Austria, special acts for other data in Smart Buildings are not available. Besides Smart Meters, data generated by various sensors also allow the detection of occupation phases of inhabitants. In the future, this will necessarily required to be addressed by research and laws. However, some suggested approaches for privacy in Smart Metering can be applied to other kind of personal data as far as feasible. Generally, the legal base for data protection is about to be changed as the new EU General Data Protection Regulation will come into effect in 2018.

Acknowledgements

The presented work is conducted in the "Building Profiling for Energy Management (BProfEM)" project, funded and supported by the Austrian Research Promotion Agency (FFG).

References

1. Cejka S (2016) Privacy by Design & Smart Metering. University term paper, in german.
2. Cejka S (2017) Vorschläge für Datenschutz und Privatsphäre bei Smart Metern und deren Umsetzung im österreichischen Recht. Jusletter IT, February 2017, in german.
3. Faschang M, Cejka S, Stefan M, Frischenschlager A, Einfalt A, Diwold K, Pröstl Andren F, Strasser T, Kupzog F (2016) Provisioning, deployment and operation of smart grid applications on substation level. Computer Science - Research and Development. doi:10.1007/s00450-016-0311-x