PERSONAL DATA PROTECTION RULES! GUIDELINES FOR PRIVACY-FRIENDLY SMART ENERGY SERVICES

Research Paper

Jana Gerlach, Leibniz Universität Hannover, Hannover, Germany, gerlach@iwi.uni-hannover.de

Alexandra Scheunert, TU Clausthal, Clausthal-Zellerfeld, Germany, alexandra.scheunert@tu-clausthal.de

Michael H. Breitner, Leibniz Universität Hannover, Hannover, Germany, breitner@iwi.uni-hannover.de

Abstract

Privacy-friendly processing of personal data is proving to be increasingly challenging in today's energy systems as the amount of data grows. Smart energy services provide value creation and co-creation by processing sensible user data collected from smart meters, smart home devices, storage systems, and renewable energy plants. To address this challenge, we analyze key topics and develop design requirements and design principles for privacy-friendly personal data processing in smart energy services. We identify these key topics through expert interviews, text-mining, and topic modelling techniques based on 149 publications. Following this, we derive our design requirements and principles and evaluate these with experts and an applicability check with three real-world smart energy services. Based on our results and findings, we establish a further research agenda consisting of five specific research directions.

Keywords: Personal Data Protection, Smart Energy Services, Text-Mining, Topic Modelling.

1 Introduction

Renewable energies have become a topic of interest in recent years as they have caused severe changes in the energy sector and, in particular, in the electricity sector. The increasing digitalization of the electricity sector lays the base for customers to play a more active role, either by monitoring and adjusting their consumption or by actively engaging in the electricity market (CEER 2021). This in turn opens the door to smart energy services, such as dynamic pricing or the optimization of energy consumption (Paukstadt et al 2021). Such services, however, require large quantities and good quality of data, which is collected via advanced information and communication technologies such as smart meters and other internet of things (IoT) devices (Li et al. 2021, Guhr et al. 2020, Le Ray and Pinson 2020, Lokshina et al. 2017), usually directly at people's homes (Paukstadt et al. 2021, 2019, Chasin et al. 2020, Kappler et al. 2018). The way in which this collected data is analyzed and then shared with other parties is becoming more detailed, personalized, and hence potentially vulnerable. Consequently, this data requires increased protection (Kappler et al., 2018). However, customers will shy away from smart energy services if a certain baseline of trust in the use of their data is not established (McQuinn and Castro, 2018). Hence, it is important for smart energy service providers to ensure that customers trust the way their (personal) data is used (Le Ray and Pinson 2020, Rösch et al. 2020). The use of personal data is regulated on various levels in the European Union and in Member States. However, regulation alone does not always suffice to ensure customers trust the way their data is used (McQuinn and Castro, 2018). Barbosa et al. (2020) highlighted that there remains a lack of privacy management