# Chapter 88
# Privacy-Preserving Aggregation in the Smart Grid

**Georgios Karopoulos**
*National and Kapodistrian University of Athens, Greece*

**Christoforos Ntantogian**
*University of Piraeus, Greece*

**Christos Xenakis**
*University of Piraeus, Greece*

## ABSTRACT

*The introduction of information and communication technologies to the traditional energy grid offers advantages like efficiency, increased reliability, resilience, and better control of demand-response, while on the other hand poses customers' privacy at risk. By using information collected by a smart meter, an attacker can deduce whether a house is empty from its residents, which devices are being used, residents' habits and so on. In order to cope with such cases, many privacy-preserving aggregation solutions have been proposed that allow aggregation, while at the same time protect individual readings from attackers. In this book chapter, the authors provide a critical review of such methods, comparing them and discussing advantages and disadvantages.*

## INTRODUCTION

Traditional energy grid infrastructure is being upgraded into a smart grid. The smart grid is the result of the modernization of the existing energy grid in such a way that customers, as well as utilities, have the ability to monitor, control, and predict energy usage. To this end, the EU has plans to replace at least 80% of its electricity meters with smart ones by the year 2020 (European Commission, 2009). Moreover, according to a US report (The Edison foundation, 2014), the smart meter installations in the USA have reached 50 million of devices as of July 2014.

The advantages of the smart grid in a large scale are national energy independence, emissions control, and global warming combat. In the grid operator/utility level it enables more granular defini-

DOI: 10.4018/978-1-5225-8897-9.ch088

tion of pricing policy, better capacity and usage planning, increased resilience and protection against cyber- physical attacks, while it provides more flexibility to energy markets. Regarding customers, the smart grid will enable them manage actively their energy usage, control energy bills, and be involved as renewable energy producers.

Despite the numerous benefits from its adoption, the smart grid comes with several security and privacy concerns. In the smart grid, customers need to frequently share information on energy usage with the utility, something that exposes them to privacy invasions. In the proposed book chapter, the authors will study energy metering data aggregation in the Advanced Metering Infrastructure (AMI) and its privacy implications. An indicative example of the latter is an attacker that observes energy usage reports of a smart meter, in order to infer when nobody is in the house.

In the past few years, several privacy-preserving billing and metering data aggregation schemes have been proposed. The idea behind these schemes is to use cryptographic tools, like homomorphic or traditional symmetric/asymmetric encryption, so that smart meters transmit measurements to utility providers in a secure manner. In order not to overwhelm utility servers with excessive traffic, aggregators are used, which are nodes that aggregate consumption data for a geographic area before sending the result to the utility operator. Privacy- preserving aggregation approaches need to protect customers from third parties, that wish to gain access to their consumption data, but also aggregators, since they cannot always be considered trusted. Moreover, such schemes need to meet several other requirements to be considered appropriate for the smart grid, like security and scalability.

The rest of this book chapter is organised as follows. In the next section, the authors present a reference architecture for privacy-preserving aggregation, the security model and requirements. Next, existing work in privacy-aggregation in the smart grid is categorised and presented in detail. Also, a discussion regarding findings from the analysis and comparison of the aforementioned proposed schemes is provided, followed by conclusions of this study.

## BACKGROUND

In this section, the authors present a generic smart grid architecture that will assist in the analysis of the privacy-preserving aggregation schemes. Next, the authors will present the considered security model for consumption aggregation, and the requirements that derive from it.

### Architecture

Regarding metering data transmission, there are mainly two types found in the literature that operate in parallel (WELMEC, 2010; Efthymiou & Kalogridis, 2010):

- **High Frequency:** Where readings are collected every 15 minutes (this is common practice for electricity meters), and
- **Low Frequency:** Where readings are collected for longer periods for billing purposes (every week or month).