PrivEnergy – a Privacy Operator Framework Addressing Individual Concerns

Christine Tex
Karlsruhe Institute of Technology
Karlsruhe, Germany
christine.tex@kit.edu

Philipp Hertweck
Frauenhofer IOSB
Karlsruhe, Germany
philipp.hertweck@iosb.fraunhofer.de

Martin Schäler
Karlsruhe Institute of Technology
Karlsruhe, Germany
martin.schaeler@kit.edu

Klemens Böhm
Karlsruhe Institute of Technology
Karlsruhe, Germany
klemens.boehm@kit.edu

ABSTRACT

The energy transition is a core challenge of today's society. Data-driven services are necessary to encourage households to participate in this transition, but have to respect the individual privacy concerns of the data owners. To facilitate this, we propose a framework of data-perturbation operators. We give an overview over our framework and argue that our framework is a valuable foundation to address individual privacy concerns of households.

CCS CONCEPTS

• **Security and privacy** → **Privacy protections**; *Pseudonymity, anonymity and untraceability*; *Human and societal aspects of security and privacy*; *Usability in security and privacy*; • **Information systems** → *Information systems applications*; • **Mathematics of computing** → Time series analysis;

KEYWORDS

Smart Meter, data perturbation, individual privacy concerns

1 INTRODUCTION

The transition from fossil energy sources to renewables, like wind or solar, is a fundamental concern of our society. One important issue is user acceptance, including acceptance by private households. To encourage them to participate and invest in the transition, data-driven services that help to save energy, i.e., money, are a key factor. Some data-driven services are distributed by nature. An example is coordinated appliance scheduling: Think of variable energy prices and a set of households trying to optimize the appliance schedules globally, among all households. In general, distributed services are organized as shown in Figure 1. There, load profiles are exchanged. As load profiles contain various private information, privacy concerns of the households regarding their neighbors have to be respected. This issue is known as *owner privacy*. For distributed services, the conventional solution from literature is secure multi-party computation (MPC). However, MPC and similar solutions mainly assume (implicitly) that all households have the *same* privacy concerns. But this is not the case. For instance, some households may have restrictions, while others are generous.

e-Energy '18, June 12–15, 2018, Karlsruhe, Germany
2018. ACM ISBN 978-1-4503-5767-8/18/06…$15.00
https://doi.org/10.1145/3208903.3212048

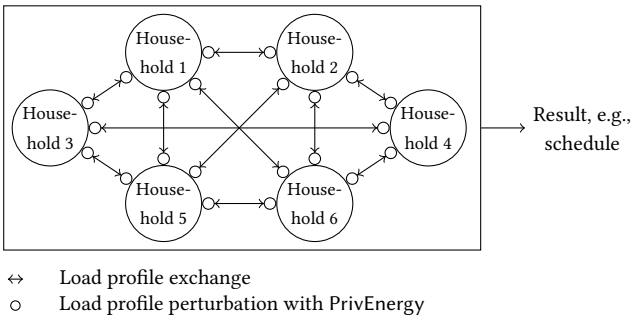

Figure 1: Architecture of data-driven, distributed services.

Data perturbation has been touted as a means to ensure privacy and allow for data exchange at the same time. Thus, we propose the data-perturbation framework PrivEnergy to comply with individual privacy concerns. The framework consists of data-perturbation operators dubbed *privacy operators* for load profiles. Examples are addition of noise or temporal aggregation. These operators are freely combinable. Thus, the framework is a means to implement data-driven services, such that they preserve privacy. In literature, to specify individual privacy concerns, there exist the Pufferfish [3], the Blowfish [1] and the InPaCT [4] framework. However, they are declarative in nature, and our framework can be a way to implement them.

Challenges. Designing the privacy-operator framework is subject to two challenges: (A) completeness of the operator set and (B) combinability of the operators including (B.1) algebraic properties and (B.2) privacy of operator combinations.

A. Completeness. Related work proposes a wide range of categories of techniques to ensure privacy [6, 7]. An example is so-called *data masking*. Most categories target at hiding different private information, i.e., privacy concerns, in the data, such as appliance usage behavior. There is not a single category that covers all information. Thus, our framework itself should cover all categories.

B. Combinability. As households may want to protect *different* kinds of information, the framework must allow combinations of operators. However, while individual techniques to ensure privacy

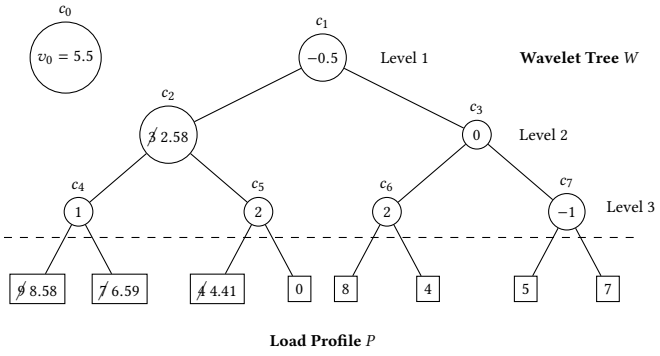

Figure 2: Load profile in Haar wavelet representation [8], before and after application of *AddNoiseGauss* with Parameters $\sigma = 2.7$ and $\phi = 2.7$.

are relatively well understood, their combinations are not. Thus, allowing combinations of operators raises two sub-challenges:
B.1. Algebraic Properties It is desired to have operators with well-defined algebraic properties, such as associativity and commutativity, to apply them in any order.
B.2. Composite Privacy The effects of combinations of privacy operators regarding the privacy level provided must be quantifiable.

Contributions. In this paper, we give an overview of a privacy-operator framework addressing these challenges. It has known algebraic properties and privacy levels of operator combinations, and is complete in the above sense. Our specific contributions are:

- In the introduction, we have motivated the framework as well as its usefulness for the implementation of data-driven services such that they preserve owner privacy. We have done this with the example of distributed services.
- We sketch our framework, say how we achieve completeness and explicitly define one operator of our framework exemplarily.
- We outline how we address the combinability challenge.

2 PrivEnergy FRAMEWORK

We now explain the data representation used to realize the framework, say how we achieve completeness, and show exemplarily how operators are defined and applied to load profiles.

Data Representation. To implement privacy operators, the Haar wavelet representation of load profiles (cf. Figure 2) is widely used [8]. The reason is that it represents the on/off switching of appliances – a main privacy concern of households – very well. We use this representation as well.

Completeness. Many techniques to ensure privacy of load profiles exist. According to [6, 7], they all fall into the categories listed in Table 1. As Table 1 shows, we cover each category either with at least one operator or on top of our framework. Thus, our framework is complete. We adopt operators already defined in literature, and also propose a new operator, namely *WeakPeak*.

Definition and Application of Operators – Example. Operators are defined coefficient-wise. For illustration, see Definition 2.1 for the definition of *AddNoiseGauss*. Whenever applying an operator, we traverse the wavelet tree and apply the operator to every coefficient. Afterwards, we retransform the wavelet tree in a load profile. See Figure 2 for an example of an operator application and the resulting, perturbed, load profile.

Table 1: The PrivEnergy operator set.

Category	Operators	Covered
Anonymization	- (on top)	✓
Individual Measurement Perturbation		
– Load Signature Moderation	*WeakPeak*, *DeNoise*	✓
– Data Masking	*AddNoiseGauss*, *AddNoiseLaplace*	✓
Aggregation		
– Temporal Aggregation	*TempAgg*	✓
– Spatial Aggregation	- (on top)	✓

Definition 2.1 (*AddNoiseGauss*$_{\sigma,\phi}(c)$ [2, 5])**.** *Let c be a coefficient and $c.v$ the value of c. For $\sigma, \phi > 0$, let $I = \{c : c \in W \text{ and } |c.v| \geq \sigma\}$ and $\rho = \frac{|P|}{|I|}$. Then*

$$c.v \leftarrow \begin{cases} c.v + \mathcal{N}(0, \phi\sqrt{\rho}) & \text{if } c \in I \\ c.v & \text{otherwise.} \end{cases}$$

3 ADDRESSING COMBINABILITY

In this section, we outline how we address the combinability challenge. Namely, we say how to achieve algebraic properties and how to evaluate composite privacy.

Achieving Algebraic Properties of the Framework. As mentioned, associativity and commutativity of the operator set is desired. Associativity is already given, as the combination of operators is a function composition, which is associative. However, commutativity is not given. For instance, *AddNoiseGauss* is not commutative with itself. We propose to modify the operators by adding new parameters to the operators to achieve commutativity.

Composite Privacy. Composite privacy has to be evaluated in two ways. First, we have to prove that every individual operator preserves privacy. Second, we have to combine operators and quantify how the privacy level changes. We propose to measure privacy by using well-known experimental privacy attacks in the first place.

4 CONCLUSIONS

Data-driven services encourage households to participate in the energy transition, but raise individual privacy concerns. To counter this, we propose the PrivEnergy framework of privacy operators. We motivate the framework and its usefulness with the example of data-driven, distributed services, and give an overview of it. In future work, we use our framework for the actual implementation of data-driven services which preserve privacy.

5 ACKNOWLEDGEMENT

This work was partially supported by the Federal Ministry of Education and Research (BMBF; ref. nb. 02K15A024).

REFERENCES

[1] X. He, A. Machanavajjhala, and B. Ding. 2014. Blowfish Privacy: Tuning Privacy-Utility Trade-Offs Using Policies. In *SIGMOD*. ACM.

[2] S. Kessler, C. M. Flath, and K. Böhm. 2015. Allocative and Strategic Effects of Privacy Enhancement in Smart Grids. *Information Systems* (2015).

[3] D. Kifer and A. Machanavajjhala. 2012. A Rigorous and Customizable Framework for Privacy. In *PODS*. ACM.

[4] F. Laforet, E. Buchmann, and K. Böhm. 2015. Individual Privacy Constraints on Time-Series Data. *Information Systems* (2015).

[5] S. Papadimitriou et al. 2007. Time Series Compressibility and Privacy. In *VLDB*. VLDB Endowment.

[6] N. Saputro and K. Akkaya. 2014. On Preserving User Privacy in Smart Grid Advanced Metering Infrastructure Applications. *Secur. Commun. Netw.* (2014).

[7] F. Skopik. 2012. Security is not enough! On Privacy Challenges in Smart Grids. *SGRE* (2012).

[8] X. Xiao, G. Wang, and J. Gehrke. 2011. Differential Privacy via Wavelet Transforms. *IEEE TKDE* (2011).