11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Selecting Privacy Solutions to Prioritise Control in Smart Metering Systems

Juan E. Rubio[a], Cristina Alcaraz[b], and Javier Lopez[c]

[a] *Student*
[b] *Senior Postdoctoral researcher*
[c] *Full Professor*

NICS
Network, Information and Computer Security Lab

Introduction

- Smart Grid provides several benefits due to:
  - Accurate monitoring for operators.
  - Detailed consumption reports for users.

- However, privacy is at risk when analysing energy readings, being able to draw conclusions about the life of homeowners.

- Still, the energy supplier needs to know:
  - The electricity consumption of all customers in an area at any time.
  - The overall consumption of every single customer over the billing period.

Introduction: Privacy Enhancing Technologies

- Privacy-preserving techniques must be implemented to prevent the Energy Service Provider (ESP) from checking the current energy consumption of a single customer.

- Privacy Enhancing Technologies (PETs):
  - Trusted Computation
  - Verifiable Computation
  - Cryptographic Computation
  - Anonymisation
  - Perturbation

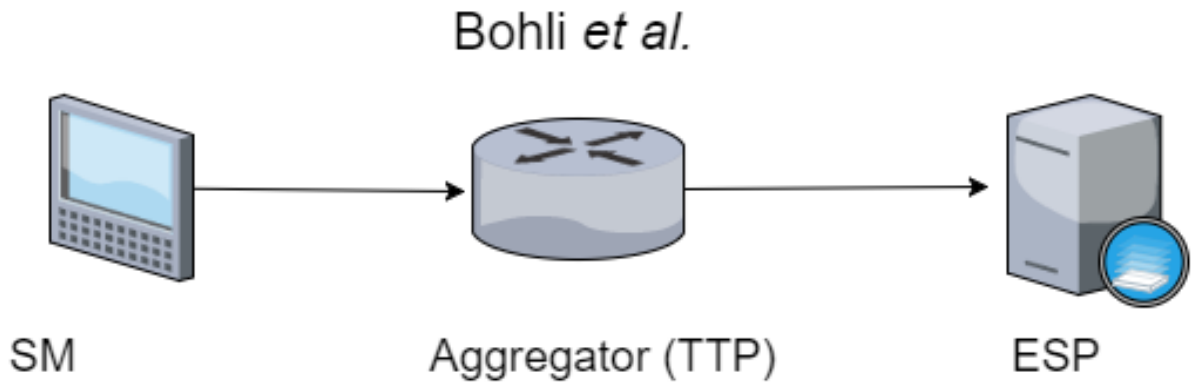
- At the same time, it is important to care about performance (e.g., not saturating net communications or running complex protocols).

Control requirements

- **Real-time Performance:** absence of operational delays.
  - Speed
  - Storage
  - Communication overhead
  - Synchronisation
- **Dependability:** avoidance of frequent and several faults.
  - Fault-tolerance
  - Aggregate error
- **Sustainability:** compatibility with future needs.
  - Configurability
  - Maintainability
- **Survivability:** capability to address malicious or deliberate attacks.

Analysis of Privacy Techniques: Trusted Computation

- **Bohli *et al.***: a Trusted Third Party (TTP) aggregates all readings from a set of Smart Meters (SMs) to inform the ESP in real time and also sum up individual consumption to compute the bill.



- **Lemay *et al.***: a Trusted Platform Module (TPM) isolates the bill calculation in the smart meter, being possible to prove to the ESP that all components are trustworthy and security has not been compromised.

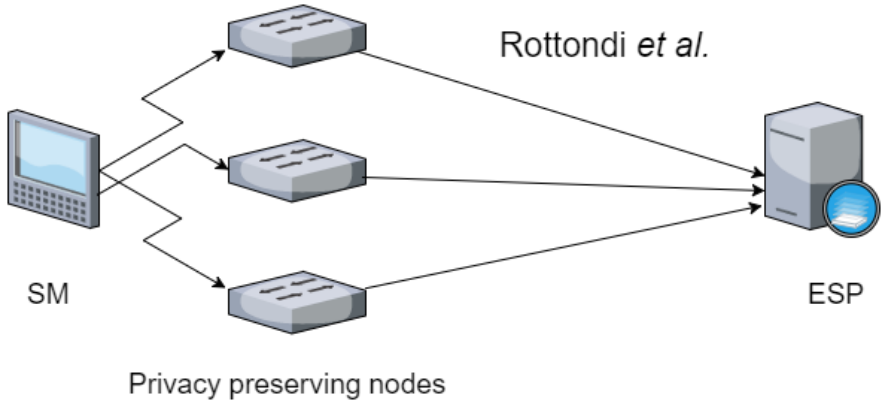
Verifiable Computation techniques

- **Molina-Markham *et al.***: Zero-Knowledge (ZK) protocol that allows a prover (i.e., the smart meter) to demonstrate the knowledge of a secret (the power readings needed to compute the bill) to the verifier (i.e., the ESP).
  - Therefore, the client can compute the bill without revealing the electricity usage.

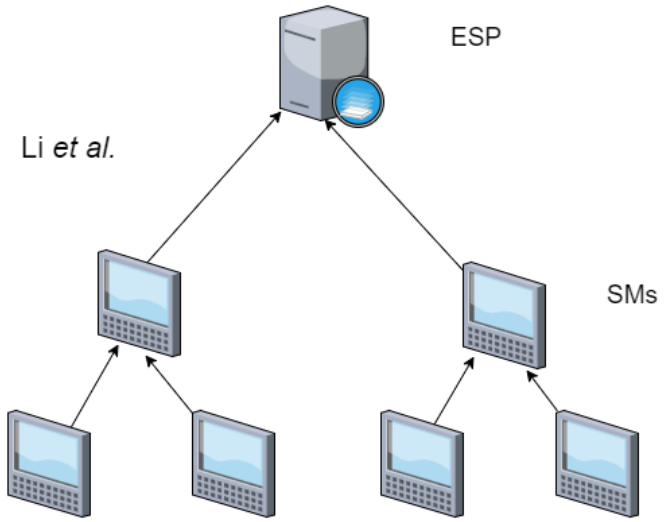
- **Jawurek *et al.***: plug-in Privacy Component (PC) between the SM and the ESP that captures all data and sends the latter signed commitments along with the final bill calculation to prove its correctness.

Cryptographic Computation techniques

- **Rottondi *et al.***: a secret (i.e., the energy usage information) is divided into shares that are distributed among Privacy-Preserving Nodes (PPNs).
  - The provider cannot reconstruct the measurements until it collects, at least, a defined number of them.



- **Li *et al.***: smart meters are placed in a tree topology:
  - Each smart meter encrypts its usage data and pass it to its parent, which aggregates it with the rest of the children.
  - Ultimately, the root node sums up the information for the ESP.

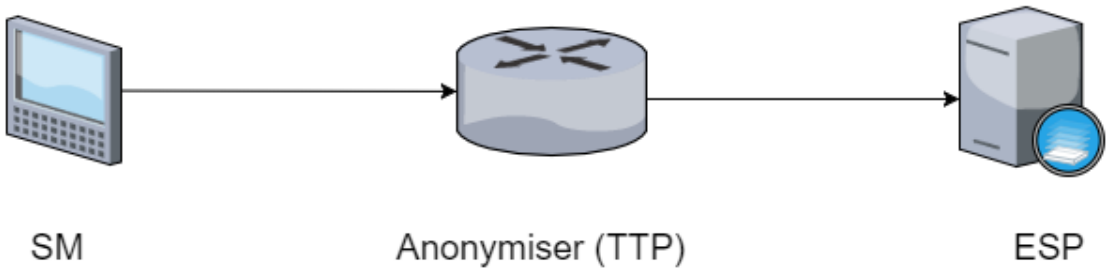


Anonymisation techniques

- **Efthymiou *et al.***: division between two kinds of data generated by the SM:
  - high-frequency measurements transmitted to the ESP to perform monitoring operations
  - low-frequency metering data intended for billing.
- Since the high-frequency has to be pseudoanonymised, they are sent to an escrow, whereas the low-frequency data is transmitted to the ESP.

- **Petrlic:** a trusted third party issues pseudonym certificates for the SMs, which are used to encrypt and sign power readings without performing any aggregation.

Petrlic *et al.*



Perturbation techniques

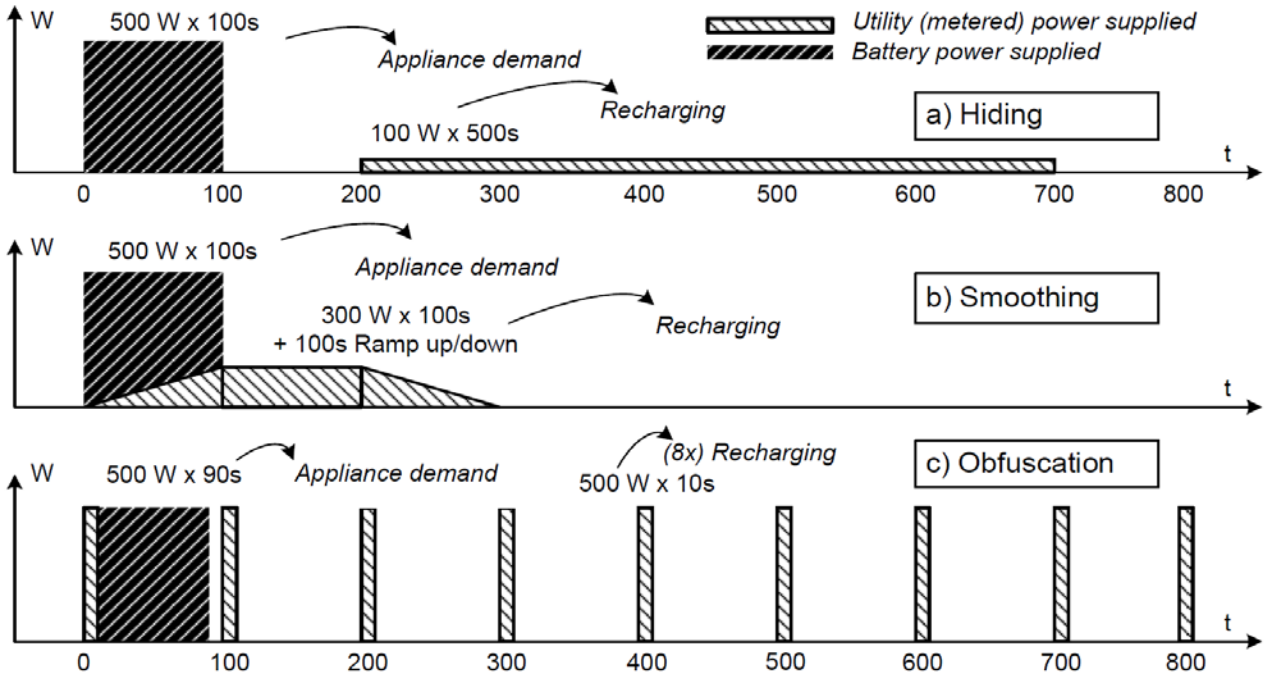
- **Lin *et al.***: semi-trusted storage system which securely stores all the encrypted data from meters in an area, supporting two types of operations:
  - When performing load monitoring operations, the ESP can only access a sum of several SMs' readings in a single time unit.
  - When performing billing operations, it is only possible to query the sum of readings from a single SM over a time period.

- Random noise is introduced in the stored data, so the aggregation can be considered accurate with a given probability.

Batteries approaches

- **Kalogridis *et al.***: based on hiding the electricity consumption through a re-chargeable battery, that changes the actual energy usage curve to avoid the exposure of sensitive data.

- This solution does not depend on special architectures and is compatible with other additional mechanisms.



Discussion: privacy properties

- Communication model
  - SM ⟶ Third party ⟶ ESP: introduction of an intermediate element to aggregate data.
  - SM ⟶ ESP: data processing at source, by means of a TPM or a battery to mask the real power usage.
  - Other approaches: spanning-tree of SMs.
- Type of aggregation of power measurements
  - Data aggregation over a time period for a single meter to support billing operations
  - Spatial aggregation over a set of SMs to comply with monitoring operations
- Security measures
  - Symmetric encryption to transmit data from SM to TTP
  - Asymmetric encryption to encrypt and sign measurements
  - Use of hardware-protected storage to perform remote attestation
  - Homomorphic encryption to aggregate data without revealing individual measurements
  - Introduction of noise in the readings through pseudorandom numbers
  - Load signature moderation

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

✓ Efficient operations ~ efficient operations, many steps
✗ Complex operations that require high computational capabilities

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

✓ Consumption data is stored in a third party

✗ The smart meter saves all the energy measurements locally

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓								

✓ Only one message per billing period between the SM and ESP

~ Only one message from SM to the ESP per billing period, but permanent transmission of data between SM and TTP

× Frequent communication between SM and ESP

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

✓ No need to aggregate data with synchronisation

✗ Energy readings from smart meters have to be gathered simultaneously

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

✓ The technique is easily configurable and can extent its functionality

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓								

✓ Tolerance against failures

~ Fault-tolerant depending on a threshold of failures

× Not fault-tolerant

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

✓ Accurate energy measurements
✗ Presence of noise in the consumption data

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

✓ Effective mechanisms to front external attacks

Discussion: control requirements

PET / Control Requirement	Trusted Computation		Verifiable Computation		Cryptographic Computation		Anonymisation		Perturbation	Batteries
	Bohli et al.	Lemay et al.	Molina-Markham et al.	Jawurek et al.	Rottondi et al.	Li et al.	Efthymiou et al.	Petrlic	Lin et al.	Kalogridis et al.
Speed	✓	~	×	~	~	~	~	~	✓	✓
Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
Comm. overhead	~	✓	~	✓	~	~	~	~	×	~
Synchronisation	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Configurability		✓			✓			✓		
Maintainability		✓			✓			✓		
Fault-tolerance	✓	✓	✓	✓	~	✓	✓	✓	×	×
Aggregation error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resilience	✓	✓				✓	✓	✓	✓	

Conclusions and future work

- Smart Grid raises several privacy issues with respect to the analysis of consumption data, which can lead to obtain information about the user habits.
- Several privacy solutions proposed in literature have been classified and analysed, focusing on aspects like their architecture, data aggregation and security.
- In addition, we have assessed the suitability of these techniques in terms of control, in order to find a trade-off between security and automation.
- Future work is proposed to include more techniques and define a more precise taxonomy of privacy and control requirements to systematically recommend a solution for grid operators.