J. E. Rubio, C. Alcaraz, and J. Lopez, "Selecting Privacy Solutions to Prioritise Control in Smart Metering Systems", *The 11th International Conference on Critical Information Infrastructures Security* vol. 10242, pp. 176-188, 2017.
NICS Lab. Publications: https://www.nics.uma.es/publications

Selecting Privacy Solutions to Prioritise Control in Smart Metering Systems

Juan E. Rubio, Cristina Alcaraz, Javier Lopez
Department of Computer Science, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
{rubio,alcaraz,jlm}@lcc.uma.es

Abstract

The introduction of the Smart Grid brings with it several benefits to society, because its bi-directional communication allows both users and utilities to have better control over energy usage. However, it also has some privacy issues with respect to the privacy of the customers when analysing their consumption data. In this paper we review the main privacy-preserving techniques that have been proposed and compare their efficiency, to accurately select the most appropriate ones for undertaking control operations. Both privacy and performance are essential for the rapid adoption of Smart Grid technologies.
Keywords: Smart Grid, Data Privacy, Control, and Metering

1 Introduction

In comparison with the traditional electric grid, the Smart Grid (SG) enables a more accurate monitoring and prevision of energy consumption for utilities so they can adjust generation and delivery in near real-time. Users also receive detailed consumption reports that can help them to save money by adapting their power usage to price fluctuations. The Advanced Metering Infrastructure (AMI) is a smart metering system that makes this possible by processing a huge data collection generated at a high frequency [14]. This information can then be analysed to draw surprisingly accurate conclusions about customers.

In order to preserve privacy, consumption data should not be measured. However, this is not feasible: the energy supplier needs to know the sum of the current electricity consumption of all its customers (or a group of them concentrated in a certain region) primarily to perform monitoring operations and Demand Response. Secondly, the supplier also needs to collect attributable information to know the total consumption of a single customer over a given time period (e.g., a month), in order to calculate the bill. As a result, privacy-preserving techniques must be implemented to prevent the Energy Service Provider (ESP in the following) from checking the current energy consumption of a single customer.

There does not seem to be a clear difference in research between protocols that address privacy when metering for billing and those which concern metering for monitoring the grid and handling Demand Response. Even though some of the surveyed protocols enable both operations, this paper divides them into those which principally concentrate on providing privacy when carrying out billing operations and those which focus on the monitoring tasks. However, it is equally useful to assess not only how user privacy is protected but also the impact of these mechanisms on the performance of the collection and supervision systems (e.g., not saturating net communications or running hard time-consuming protocols).

The techniques discussed here make use of the traditional Privacy Enhancing Technologies (PETs) [8], [13]:

- **Trusted Computation (TC)**: the Smart Meter (SM) itself or a third party is entrusted to aggregate consumption data before it is sent to the energy supplier.
- **Verifiable Computation (VC)**: the smart meter or a third party calculates the aggregated data and sends proof to the provider to ensure its correctness.
- **Cryptographic Computation (CC)**: by using secret sharing or homomorphic cryptographic schemes, so the provider can only decrypt the aggregate of consumption data.
- **Anonymization (Anon)**: removal of the smart meter identification or substitution with pseudonyms.
- **Perturbation (Pert)**: random noise is deliberately added to the measurements data while keeping it valid for control purposes.

In this paper, we present a description and analysis of some of the most representative solutions that address privacy in the context of smart metering, emphasising their effects in control and supervising tasks. In addition, other privacy technologies based on the use of batteries (denoted as *Batt* in the tables) to mask the energy usage will also be considered. The aim is to guide both customers and grid operators in the search for techniques that fit their needs while balancing both privacy and control.

To accomplish the analysis, all techniques are presented as follows: In Section 2 the privacy and performance properties analysed in the solutions are introduced. In Section 3 the techniques are categorised according to the PETs they integrate and their suitability for billing and monitoring operations, and then they are analysed. Conclusions and future work are discussed in Section 4.

2 Privacy and Automation Properties

Currently, numerous approaches related to data privacy in SG [20], [6], can be found but not all of them consider aspects related to the efficient management of the real demand. To do this, it is necessary to consider a set of essential properties concerning not only privacy but also data monitoring itself, so as to find a desirable trade-off between security and automation. For example, privacy schemes must ensure the user's privacy and security in the supervision tasks without producing disruptions or delays in the data collection processes. Given this and the need to preserve the consumption data and its availability for the control, the following lines describe the set of essential properties needed to select the most suitable privacy techniques for SG environments.

To organise the intrinsic features of the privacy in relation to the control, it is first necessary to consider the main control requirements defined in [2]. Any control system in charge of supervising specific areas must take into account: the performance in real time (privacy solutions must not interfere with the monitoring tasks), sustainability in terms of maintainability and configurability, and dependability and survivability in relation to reliability and security. Based on these criteria, the goal is to define the different properties related to the privacy that can affect the monitoring tasks, and therefore the requirements of automation.

Real-time Performance: addresses the operational delays caused by the processing of information, application of techniques and the transference of the data to control utilities. When handling this control requirement with respect to the features of the privacy solutions, these fundamental properties should be considered:

- **Speed**: as some protocols discussed in this paper have not been implemented, speed cannot be measured in quantitative terms. An estimation can be made by counting and considering all the communication and cryptographic steps required to run it.
- **Storage**: subject to the excess of operations and the massive storage, which can require extra resources to maintain meter values.
- **Communication overhead**: the excess of communication and the data transference rate (e.g., for synchronisation) may hamper the data recollection and the supervision of the area.
- **Synchronisation**: it focuses on the time when data streams are being sent from the producer (i.e., the smart meter) to the consumer (i.e., the energy service provider). Whereas certain protocols may require all data producers to send it at the same time, in others the data producers send it independently of each other. It must be noted that the use of synchronisation increases the complexity of the protocol.

Sustainability: defined as "that development that is able to meet the needs of the present without compromising the ability of future generations to meet their own needs" in [4]. Namely, the privacy techniques must not provoke compatibility problems, conflicts or errors; and for this, it is necessary to consider aspects related to the configuration, maintainability and updating of the techniques.

- **Configurability**: related to the easy way to carry out not only the commissioning and setup phase of the PETs but also their configurability throughout its life-cycle.
- **Maintainability**: this property comprises updating and upgrading measures, where the updating or upgrading process must not imply a reduction in the control tasks.

Dependability: can be defined as "the ability of the system to properly offer its services on time, avoiding frequent and several faults" in Al-Kuwaiti *et al.* [1], and includes reliability and security as main properties. However, we only address the reliability since the security is already part of the privacy solutions. In this category, we consider:

- **Fault-tolerance**: some of the protocols discussed here may be robust enough as to bear unlimited software and hardware failures or just a certain number of them (or no failures at all).
- **Aggregate error**: a protocol can be considered as exact or noisy depending on the presence of errors in the aggregated data that are a result of metering failures or a consequence of applying perturbation to preserve privacy.

Survivability: capability of a system to fulfil its mission and thus address malicious, deliberate or accidental faults in a timely manner. It also includes security against external attacks, which is briefly analysed in Section 3.1. However, for the purposes of the work presented here, where we prioritise control, **resilience** is specifically studied, which allows the system to continue its services when part of its security is compromised.

On the other hand, it is essential to take into account the mode of configuration of the nodes and the data management. Depending on the scenario, the communication model can vary, as it defines how smart meters (producers) are connected to utilities (e.g., for control). There are different communication models, from distributed systems to hierarchical or decentralised systems composed of aggregators or trusted third parties. In addition, and related to the communication model, it is also important to take into account the type of commissioning and setup needed to specify the group management, and data spatial distribution to determine how the data subsets are aggregated spatially (over a set of data producers) or temporally (over a set of one data producer's data items).This feature is also known as the aggregate function.

3 Selecting Techniques: Analysis and Discussion

In this section, the privacy-reserving metering solutions are assessed. The current literature has been reviewed to provide the most discussed techniques of each of the PETs presented in the introduction, resulting in ten protocols. Firstly, an introduction to their main architecture and privacy features is given, and then a discussion is proposed to compare the efficiency of each one accord-

ing to the control requirements indicated in Section 2. Note that since most of the techniques lack a real implementation, the comparison is done based on an estimation of the properties in each solution.

3.1 Analysis of Privacy Techniques

As introduced, this subsection gives a brief overview of the main solutions proposed in the literature, focusing on the aggregation and communication model that they put into practice, along with the underlying security. Techniques are classified into those which are mainly suitable for monitoring and those that address privacy when performing billing operations. Finally, all these characteristics are presented in Table 1, where the solutions appear, ordered by their implemented PET.

Among the **privacy techniques for billing operations**, the following solutions have been considered: Bohli *et al.* [3] propose a model where a Trusted Third Party (TTP) is introduced to aggregate (i.e., sum all smart meters' readings) before sending them to the ESP. Specifically, SMs transmit their data through an encryption channel to the TTP, which sums up individual consumption for each smart meter at the end of the billing period and also informs the ESP about the current status of that part of the grid. It can be considered efficient as it uses symmetrical encryption (usually AES) and robust since it can detect the presence of fake groups (i.e., sets of SMs controlled by the ESP that emit default values in order to isolate the real customer's consumption). However, it introduces some communication overheads due to the permanent data submitted by SMs to the TTP to monitor the electricity consumption of a certain area.

Molina-Markham *et al.* [15], to the contrary, describe a Zero-Knowledge (ZK) protocol that allows a prover (the smart meter in this case) to demonstrate the knowledge of a secret (the power readings needed to compute the bill) to the verifier (the ESP) without revealing the electricity usage or the ability to under-report it. In addition to this, neighbourhood gateways are placed between the SMs and the ESP to relay aggregated power readings corresponding to an area without disclosing any particular origin, enabling Demand Response operations by this means. Zero-Knowledge protocols are computationally expensive, although the communication between the SM and the ESP takes place only once per billing cycle.

Jawurek *et al.* [7] also specify another Zero-Knowledge protocol for billing based on Pedersen commitments [17]. It introduces a plug-in Privacy Component (PC) between the SM and the ESP that intercepts consumption data and sends the provider signed commitments and the final calculation together with the random parameters used to create the Pedersen commitments from individual measurements. Taking advantage of the homomorphic property of this schema, the ESP can effectively check the bill validity computing the calculation on the received commitments, which result in a new commitment of the bill amount and random numbers presented. It is worth commenting that the PC is invisible to the SM and it calculates the final price. Also, it does not have

to be trustworthy, since the VC protocol itself ensures a correct bill calculation, and therefore it can be implemented easily with no special hardware-protected components.

Lemay *et al.* [10] propose isolating the bill calculation in the smart meter by using a Trusted Platform Module (TPM). More specifically, its architecture is composed by independent virtual machines intended to perform diverse applications like billing or Demand Response. A hypervisor controls the access to the hardware (hence the power measurements) and integrity and confidentiality are guaranteed through remote attestation, which proves to the provider that the hardware and software being used are deemed as trustworthy. To achieve this, the device includes hardware-protected storage, cryptographic modules and other tamper detection components. In terms of control requirements, this solution reduces the amount of information transmitted between SM and ESP, as all data processing (i.e., the bill calculation) occurs at the point of the origin of the data. The TPM also allows the service provider and the customer to run their own applications relying on the strong isolation that virtualisation technology provides.

Likewise, Kalogridis *et al.* [9] define the concept of 'load signature moderation' to shape the electricity consumption so it does not expose any sensitive data. They propose the introduction of a decentralised energy production system within the household, so power can be dynamically drawn from re-chargeable batteries and other energy storage and generation devices. Thus, actual energy usage curves can be changed, hidden, smoothed, obfuscated or emulated. This solution protects against attackers that have a physical control over the SM and does not depend on specific grid architectures or trust relationships, while being compatible with other additional mechanisms and enabling grid monitoring. However, it requires extra computation when the battery is almost charged or empty, in order to keep masking the consumption and hence preserving privacy.

As for the **privacy techniques for monitoring operations**, we hightlight the Efthymiou *et al.*'s work [5]. They establish a division between two kinds of data generated by the SM. On the one hand, high-frequency measurements (e.g., collected every 15 minutes) transmitted to the ESP to perform monitoring operations over a set of SMs, which have to be pseudoanonymised due to the information they provide about a user's private life. On the other hand, low-frequency metering data (e.g., collected monthly) that is attributable for billing purposes. An identification is assigned to each type: HFID (High-Frequency ID) and LFID (Low-Frequency ID), respectively. Whilst high-frequency data is sent to an escrow with the HFID and remains unknown to the ESP, low-frequency data is disclosed publicly and is linked to LFID. The escrow can be queried by the ESP to verify the connection between a HFID/LFID pair. Its principal disadvantages are the complex setup process and the strong data privacy policy the escrow has to comply with.

Petrlic *et al.* [18] propose an anonymisation technique that uses a trusted third party. It issues pseudonym certificates to the SMs, which are used to encrypt and sign power readings. This data is relayed by the TTP once it

verifies the signature and removes any identifiable information, subsequently forwarding it to the ESP. Therefore, no aggregation is performed, and a TPM is assumed to be present in the household. This is for calculating the bill at the end of the month, while still being able to detect manipulations of the meter through remote attestation. However, the solution has some overheads because of the permanent data delivery between the SM and the TTP.

Rottondi *et al.* [19] propose introducing Privacy-Preserving Nodes (PPNs) between the SMs and the ESP that, according to a central configurator, aggregate data based on space (for a set of SMs spread in an area) and time (for a single SM) depending on the need and access rights. Privacy is preserved with the use of a secret sharing scheme: a secret (i.e., the energy usage information) is divided into shares that are distributed among the nodes, so that the ESP cannot reconstruct the measurements until it collects, at least, a defined number of them. Exploiting the homomorphic properties of this scheme, the data can be aggregated in the PPNs and then delivered to the ESP without revealing individual measurements. This architecture is resilient against faulty or compromised PPNs as long as the number of healthy ones is above a certain threshold.

Li *et al.* [11], to the contrary, suggest an architecture where the smart meters are placed in a tree topology. Each smart meter, beginning with the leaves, encrypts its own individual electricity measurements and passes them to its parent, which aggregates them with the rest of the children using the Paillier homomorphic cryptosystem [16]. A collector is placed as the root node to ultimately aggregate the data for the ESP. Thus, no inner-node can access any individual measurements and the ESP can only obtain the sum of them. The complexity derives from the creation of the tree prior to running the protocol. Its height should be small enough to reduce the hops and its nodes should not have too many children to avoid excessive computation and communication load.

Lastly, Lin *et al.* [12] propose a semi-trusted storage system which securely stores all the data from meters in an area. The Load Monitoring Center (LMC) can only access a sum of meter readings from several SMs in a single time unit. On the other hand, the ESP can only take the sum of readings from a single SM over a time period. As a result, both load monitoring and billing operations are supported. It is important to remark that random noise is introduced in the sum of encrypted readings from a set of SMs. Thus, LMC obtains an approximate aggregation that can be considered accurate with a given probability. A TPM is used to compute remote attestation and generate the pseudorandom numbers needed for the measurements encryption. One drawback that this approach has is the continuous communication that occurs between the ESP or LMC and the SMs in order to regenerate these numbers to decrypt the readings.

In the remainder of this paper, all these solutions are closely studied and compared with each other to decide on how they fit the expected control requirements for such a critical infrastructure as the Smart Grid.

Table 1: Main features of the surveyed privacy techniques

Implemented PET	**Trusted Computation**		**Verifiable Computation**		**Cryptographic Computation**		**Anonymization**		**Perturbation**	**Batteries**
Privacy Technique	[3] Bohli *et al.*	[10] Lemay *et al.*	[15] Molina-Markham *et al.*	[7] Jawurek *et al.*	[19] Rottondi *et al.*	[11] Li *et al.*	[5] Efthymiou *et al.*	[18] Petrlic	[12] Lin *et al.*	[9] Kalogridis *et al.*
Communication model	SM → Aggregator (TTP) → ESP	SM (TPM) → ESP	SM → Aggregator → ESP	SM → PC (Privacy Component) → ESP	SM → PPN (Privacy-preserving node) → ESP	Tree of smart meters with a collector in the root	SM → Escrow → ESP	SM → Anonymiser (TTP) → ESP	SM → Storage System → ESP, LMC	SM (LSM+Power Router) → ESP
Setup and commissioning	Symmetric keys exchange required	Asymmetric keys generation for attestation	Asymmetric keys for commitments signing	Privacy component installation in the household required	Secret sharing scheme parameters initialization	Aggregator tree construction+ distribution of encryption keys	Setup needed to establish respective attributable and anonymous data identities	Initialization of certificates with the TTP required	Key generation at TPM	No setup phase. However, additional resources (Battery, LSM, power router) required
Aggregate function	Arbitrary subsets of meters, individual consumption for each meter	Monthly consumption data aggregation	Arbitrary subsets of meters, individual consumption for each meter	Monthly consumption data aggregation per SM	Customizable space and time aggregation complying with privacy and consumer policies	Arbitrary subsets of meters	Arbitrary subsets of meters, individual SM data items along time	Arbitrary subsets of meters submitting real-time consumption data to the TTP	Subsets of meters in an area, individual consumption data per SM	No aggregation performed, no specific architecture or trust relationship required
Security	Symmetrical encryption to transmit data from SM to ESP	Remote attestation, Hardware-protected storage, encrypted and signed measurements	Homomorphic encryption of data	Homomorphic encryption of data, commitments signing for authentication	Secret sharing scheme	Homorphic encryption to aggregate data, asymmetric encryption for signing	Pseudo-anonymisation of data, assumed encryption for setup phase	Asymmetric encryption of data and signing using pseudonym certificates	Encryption of data in the storage system using pseudo-random numbers	Load signature moderation (no encryption performed)

3.2 Discussion: Privacy vs. Control

In Section 3.1, the ten solutions considered in this paper have been introduced, and their main features have been described. Regarding their architecture and implemented PET, some aspects can be pointed out.

On the one hand, with respect to the PETs applied, it is noteworthy that some of the protocols often combine more than one privacy-enhancing technology. The clearest example is trusted computation, through establishing a trust in a third party (e.g., Efthymiou *et al.* [5] with the escrow) or embedding the SM in a TPM to securely perform the cryptographic operations (like Petrlic *et al.* do to calculate the bill with an anonymisation mechanism). Regardless of the trust assigned to these parties or devices, most of the techniques opt to introduce an element between the SM and the ESP in order to intercept the communication and optionally perform an aggregation (e.g., a privacy component in Jawurek *et al.* [7]). Apart from this approach, there are other solutions that prefer to process all data at source, as specified in Lemay *et al.* [10] through a TPM or by using a battery to mask the real power usage, like the solution of Kalogridis *et al.* [9]. The technique of Li *et al.* [11] still performs an aggregation of multiple SM readings without involving any third party, securely routing the data through a spanning-tree with a homomorphic scheme. With respect to the aggregation of power measurements, it is performed over a time period for a single meter only in solutions that pursue billing operations, as do Jawurek *et al.* [7]. On the other hand, some solutions only aggregate data spatially to comply with monitoring operations, as is the case of Li *et al.* [11]. There are also approaches, such as Rottondi *et al.* [19], that are able to aggregate measurements in space (over a set of SMs) and time (for each SM over a billing period) following the rules of a central configurator.

Aside from analysing how these solutions contribute to privacy when measuring power readings, a study of how they behave in terms of control and automation procedures must be done, as stated in Section 2 and reflected in Table 2. All considered features of the privacy techniques (denoted as FPT, defined in section 2) are evaluated. Beginning with their **speed**, a technique can be considered as fast when its underlying cryptographic scheme is not complex and it does not imply taking several computational steps (e.g., aggregating, encrypting, and signing). In this sense, Bohli *et al.* [3], Lin *et al.* [12] and Kalogridis *et al.* [9] are fast due to the use symmetrical encryption, modular additions and a load signature moderator, respectively. Other solutions like Molina-Markham *et al.* [15] are far less efficient because of the Zero-Knowledge protocol that requires high computational capabilities. Other techniques are somewhat competent but require various operations. These are marked with a $\backsim$ in Table 2.

When **storage** is considered, the techniques discussed are positive as long as the smart meter does not hold consumption data or if all this information, used for aggregation, is stored in a third party (e.g., the PC in Jawurek *et al.* [7]). For this reason, the solution of Lemay *et al.* [10], for example, cannot be considered as such, as it saves all measurements on the TPM. As for **communi-**

cation overhead it is related to the frequency of data delivery and the number of messages transmitted between the SM, an eventual third party and the ESP. Here, a solution has been treated as efficient if there is only one message and it occurs once per billing period, between the SM and the ESP (so only some techniques for billing meet this requirement, for example Lemay *et al.* [10]). An intermediate level of overhead can be conceived when the SM contacts the ESP once, but it is always transmitting data to a third party to accomplish monitoring operations or that frequency depends on customisable aggregation rules (denoted as $\backsim$). A protocol is inefficient when there is a frequent communication between the SM and the ESP, like Lin *et al.* [12].

Concerning **synchronisation** between all parties involved to relay data, only Rottondi *et al.* [19] require the privacy-preserving nodes to gather measurements from a set of smart meters simultaneously, which can be considered negative from the perspective of performance.

With regards to **sustainability** features, three of the surveyed techniques offer the possibility to extend their functionality which makes their solutions more configurable to fit both customer and utility needs. In the case of Lemay *et al.* [10] their local TPM virtualisation system is able to implement new virtual machines with different purposes. In Rottondi *et al.* [19], configurability is achieved through the central configurator, which can adapt to new aggregation and privacy policies. Both of these solutions are maintainable for the same reason, as is the approach of Petrlic *et al.* [18], which contemplates remote TPM updates to integrate new mechanisms and fix possible errors.

Most of the techniques described **tolerate unlimited failures** when taking measurements with the help of a third party or because of the underlying protocol features. One exception is Lin *et al.* [12], where the LMC needs the meters to reply with their blind factors used for decrypting data. Also, Kalogridis *et al.* [9] has not been considered as fault-tolerant because a failure in the power routing system leaves all the real measurements exposed. A special case is Rottondi *et al.* [19], whose secret sharing scheme makes it possible for the ESP to reconstruct the data as long as it has a minimum number of them spread across all the privacy-preserving nodes. As a result, it is fault-tolerant depending on the number of working nodes. As to the presence of error in the aggregated data, Lin *et al.* [12] perturbation protocol is the only one which introduces noise in the measurements (in particular when aggregating data spatially).

Lastly, it is worth commenting on the **resilience** of these techniques. Some of them include in their papers a brief description of response to certain attacks. For example, Bohli *et al.* [3] explains the detection of fake groups of SMs; Lemay *et al.* [10] suggest remote attestation and tamper-proof components to protect against malicious software and physical attacks; Li *et al.* [11] mention the resistance to dictionary attacks against ciphertexts; Efthymiou *et al.* [5] propose sanctioning nodes when a power theft is detected, by temporarily lifting their anonymity; and Petrlic *et al.* [18] is resistant against false data injections and also includes software integrity attestation, which is also presented in Lin *et al.* [12] due to the use of TPMs. The trust given in this device turns out to be the main problem of this approach: what is executed within the TPM is

Table 2: Control requirements for surveyed privacy protocols

Implemented PET		**TC**		**VC**		**CC**		**Anon**		**Pert**	**Batt**
CR[a]	**FTP**[b]	[3]	[10]	[15]	[7]	[19]	[11]	[5]	[18]	[12]	[9]
Performance	**Speed**	✓	∽	×	∽	∽	∽	∽	∽	✓	✓
	Storage	✓	×	×	✓	✓	×	✓	✓	✓	✓
	Comm.	∽	✓	∽	✓	∽	∽	∽	∽	×	∽
	Sync.	✓	✓	✓	✓	×	✓	✓	✓	✓	✓
Sustainability	**config.**		✓			✓			✓		
	maint.		✓			✓			✓		
Dependability	**Fault-tol.**	✓	✓	✓	✓	∽	✓	✓	✓	×	×
	Agg. error	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Survivability	**Resil.**	✓	✓				✓	✓	✓	✓	

the responsibility of the ESP, which can always run code to transfer sensitive information. Therefore, some auditing processes have to be performed by third parties in order to check the software and its possible vulnerabilities.

In light of the comparison in Table 2, it is noticeable that TC is the PET that tends to show a better behaviour when performing control in smart metering. In particular, we can highlight Lemay *et al.* [10], which provides more benefits due to the efficient handling of measurements in the TPM. Nonetheless, Petrlic *et al.* [18] also demonstrates suitable capacities for power consumption and control management, and also involves trust in a third party and with the use of a TPM, as stated at the start of this comparison. Alternatively, Bohli *et al.* [3] and Efthymiou *et al.* [5] are similar solutions to the ones commented earlier, which present a lower complexity due to the use of symmetric encryption and pseudoanonymisation, respectively. To sum up, a good approach for designing privacy solutions is the combination of PET solutions of the kind: TC and Anonymisation.

4 Conclusions and future work

Despite it being accepted that accurate readings provided by smart meters improve Demand Response control and help customers fulfil their needs, it also raises several privacy issues. New techniques must be implemented to prevent other parties involved in the Smart Grid infrastructure from accessing personal consumption data that leads to the extraction of life patterns. We have conducted a concise analysis to classify some of the most relevant solutions considering different criteria: their implemented PET, their suitability for billing or monitoring purposes and other factors, like the aggregation and architecture type, that affect how privacy is preserved. Moreover, since automation efficiency also has to be considered, we have compared the main control requirements expected for these protocols. Future work will involve defining a more precise taxonomy of the privacy and control features of each of these protocols to systematically find the best solution depending on the needs of customers and grid operators. Also, it would be interesting to implement real prototypes of these solutions to perform a quantitative comparison.

ACKNOWLEDGEMENTS

The second author receives funding from the *Ramón y Cajal* research programme financed by the Ministerio de Economía y Competitividad. In addition, this work also has been partially supported by the same ministry through the research project PERSIST (TIN2013-41739-R), by the Andalusian government through the project FISSICO (P11-TIC-07223) and by the European Commission through the H2020 project NECS (H2020-MSCA-ITN-2015- 675320).

References

[1] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein. A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability. *Communications Surveys & Tutorials, IEEE*, 11(2):106–124, 2009.

[2] C. Alcaraz and J. Lopez. Analysis of requirements for critical control systems. *International Journal of Critical Infrastructure Protection (IJCIP)*, 5:137–145, 2012.

[3] J.M. Bohli, C. Sorge, and O. Ugus. A privacy model for smart metering. In *Communications Workshops (ICC), 2010 IEEE International Conference on*, pages 1–5. IEEE, 2010.

[4] Brundtland Commission et al. Our common future, chapter 2: Towards sustainable development. *World Commission on Environment and Development (WCED). Geneva: United Nation*, 1987.

[5] Costas Efthymiou and Georgios Kalogridis. Smart grid privacy via anonymization of smart metering data. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 238–243. IEEE, 2010.

[6] Soren Finster and Ingmar Baumgart. Privacy-aware smart metering: A survey. *Communications Surveys & Tutorials, IEEE*, 16(3):1732–1745, 2014.

[7] M. Jawurek, M. Johns, and F. Kerschbaum. Plug-in privacy for smart metering billing. In *Privacy Enhancing Technologies*, pages 192–210. Springer, 2011.

[8] M. Jawurek, F. Kerschbaum, and George Danezis. Sok: Privacy technologies for smart grids–a survey of options. *Microsoft Res., Cambridge, UK*, 2012.

[9] Georgios Kalogridis, Costas Efthymiou, Stojan Z Denic, Tim A Lewis, and Rafael Cepeda. Privacy for smart meters: Towards undetectable appliance load signatures. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 232–237. IEEE, 2010.

[10] Michael LeMay, George Gross, Carl A Gunter, and Sanjam Garg. Unified architecture for large-scale attested metering. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 115–115. IEEE, 2007.

[11] Fengjun Li, Bo Luo, and Peng Liu. Secure information aggregation for smart grids using homomorphic encryption. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 327–332, 2010.

[12] H.Y. Lin, W.G. Tzeng, S.T. Shen, and B.S.P. Lin. A practical smart metering system supporting privacy preserving billing and load monitoring. In *Applied Cryptography and Network Security*, pages 544–560. Springer, 2012.

[13] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan, and A. Nejadpak. A survey on smart grid metering infrastructures: Threats and solutions. In *Electro/Information Technology (EIT), 2015 IEEE International Conference on*, pages 386–391. IEEE, 2015.

[14] R. R. Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar. A survey on advanced metering infrastructure. *International Journal of Electrical Power & Energy Systems*, 63:473–484, 2014.

[15] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*, pages 61–66. ACM, 2010.

[16] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptology—EUROCRYPT'99*, pages 223–238. Springer, 1999.

[17] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Advances in Cryptology—CRYPTO'91*, pages 129–140. Springer, 1991.

[18] Ronald Petrlic. A privacy-preserving concept for smart grids. *Sicherheit in vernetzten Systemen*, 18:B1–B14, 2010.

[19] C. Rottondi, G. Verticale, and A. Capone. Privacy-preserving smart metering with multiple data consumers. *Computer Networks*, 57(7):1699–1713, 2013.

[20] H. Souri, A. Dhraief, S. Tlili, K. Drira, and A. Belghith. Smart metering privacy-preserving techniques in a nutshell. *Procedia Computer Science*, 32:1087–1094, 2014.