Survey on Privacy-Preserving Techniques in Smart Grids

Alexander Pötzsch
Technische Universität Dresden
alexander.poetzsch@mailbox.tu-dresden.de

Abstract*— *The smart grid offers a lot of advantages compared to today's electricity grid regarding efficiency and operating costs. Unfortunately the smart grid contains likewise a great threat to privacy of consumers. Analyzing the consumption of consumers can reveal sensitive information.

This survey gives an overview of the most recent approaches to protect consumer privacy. It starts with a comparison between today's electricity grid and the smart grid. Further a simple model of a smart grid is presented and privacy threats are discussed. In the main part of the paper the most recent approaches to privacy protection are discussed.

***Index Terms*—Smart Meter, Smart Grid, Privacy**

I. Introduction

Today's electricity grid is a broadcast grid. Within it, there are few energy suppliers producing electricity for many consumers. The grid has only one flow direction of electricity, from the suppliers to the consumers. To calculate the energy demand of the consumers, forecast models are used. But these forecast models are limited in their precision and because electricity shortages are undesirable, producers usually provision more production capacity for higher demands. Storing electrical power for such an event is expensive and therefore not common.

If the energy demand is higher than the average, peaker plants are activated to meet the needs of more electricity. Peaker plants are usually running on fossil fuels. Activating them is not only expensive but an additional environmental pollution [1].

With the debate about climate change and the rising awareness for greenhouse gas, there is a desire to avoid fossil fuels and replace them with renewable energy sources. The use of renewable energy lets the traditional electricity grid face new challenges. Energy production with renewable energy sources (e.g. solar and wind) are dependent on weather conditions and hence shows a strong volatility. Furthermore energy production plants which use renewable energy sources are often small and widely distributed. Even consumers can become producers e.g. if they have solar panels on their roof and feed overproduced power into the electricity grid. This combination of producer and consumer is also referred to as prosumer.

The structure of the electricity grid will shift from a few large energy suppliers to many small energy suppliers.

In order to meet these challenges the idea of a smart grid was proposed. A smart grid adds a flow of information between producers and consumers in addition to the existing electricity flow. Communication between producers and consumers can help to determine the actual energy demand. With the knowledge of the actual demand, alignment of plant capacities to the actual consumption patterns is possible. Therefore over-provisioning of production capacity can be prevented and consequently wasting of resources and money. The production of electricity will be overall more efficient. However a strong linkage of the electricity grid and information technologies is necessary. The dangers that information technologies bring along will be integrated into the electricity grid. Gathering data that violates the privacy of consumers will be a serious threat.

Data about the consumption can reveal a lot of private information [3]. The purpose of this survey is to provide an easy to understand overview of recent approaches to protecting consumer privacy. The remainder of the paper is structured as follows: In section II the smart grid model used in this paper is presented and possible privacy threats in smart grids are discussed. Section III is a discussion about possible measures in metering for billing. In section IV measures in metering for operation are discussed and section V concludes the paper.

II. Background

A. Smart Grid Model

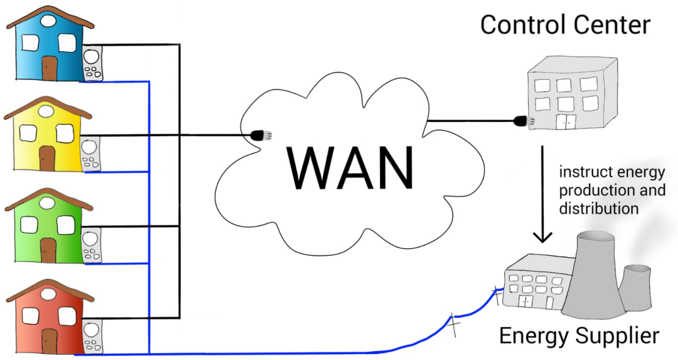

Fig. 1. Model of a smart grid with four consumers and one control center. Each consumer has their own metering device. Metering devices and control center communicate via WAN.

Besides the traditional electricity grid, a smart grid has an information network and needs more agents than the simple producer and consumer scheme. The model of a smart grid, used in this paper, introduces two new agents. Figure 4 shows an illustration of the smart grid model.

The first new agent is a device for metering. Like an ordinary meter the device measures the power consumption on the consumer side. Additionally it is the communication end point on the consumer side. It can send the real time consumption as well as a sum of consumption over a period of time. The metering device is connected to the HAN (home area network) of the consumer to be able to communicate. The HAN of the consumer is connected to the WAN (wide area network) of the town, which is used by all agents to communicate.

The second new agent is the control center (CC). It collects the data of all consumers and evaluates them. Based on the data the CC instructs the energy supplier how much electricity is needed and how it needs to be distributed. For billing the accounting center can either be included in the CC or the CC forwards the data for billing to the responsible office.

Additionally the model used in this paper assumes that not more data is communicated than vital to operate the smart grid. Furthermore communication channels are considered to use encryption and can handle transmission failures.

B. Metering Device Setup

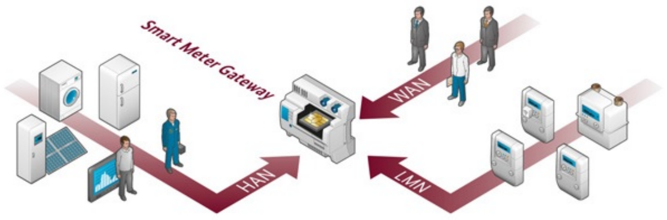

Fig. 2. Local metering infrastructure according to the BSI. Source: BSI "Das Smart-Meter-Gateway" [4]

There is no worldwide consistent standard for a metering device. Different countries have their own suggestions of structure, layout and functioning of a metering device. In any case a metering device must be able to measure the consumption and communicate with the CC. This paper adheres to the definitions of the BSI (German Federal Office of Information Technology) standard as an example for a structure of a metering device.

According to the BSI standard a metering device is constructed with two distinct components. The smart meter (SM) for the actual metering and the smart meter gateway (SMGW) for communication. Figure 2 shows an illustration of the BSI standard with multiple SMs connected to one SMGW. The crucial point of this design is that the SMs are completly separated from the communication to the HAN. Multiple SMs can be connected to the SMGW in a local metrological network (LMN), however the SMs can only communicate with the SMGW. Agents outside of the LMN cannot communicate directly with the SMs. All communication is handled by the SMGW, making it the interface to the SM.

For this paper the One-Box-solution for the metering device is assumed. This means exactly one SM is connected to exactly one SMGW and both are installed together in one metering device. In this paper subsequently the One-Box-solution is addressed as smart meter (SM).

C. Privacy Problems Caused by Smart Meters

The main innovation of the smart grid is the communication between the SM and the CC. For this purpose the SM aggregates data about the real-time consumption of the consumer and sends them to the CC or stores them for later forwarding. This data can be used to reconstruct private information about the consumer as discussed in [6]. The capabilities of reconstructed information range from simple day routine profiles (sleep, work, eat routines) to more sensitive and derived information e.g. religious believes [7].

In the best case private information of the consumers is used for targeted advertising. But in worse scenarios they can be used for blackmailing, burglary or other ways to harm the consumer.

A crucial factor to reconstruct private information is the sampling frequency of the SM. For instance, it is possible to determine what device is in use when the SM processes the electricity consumption every few minutes. However if the SM processes the electricity consumption monthly, only deviation of the average monthly consumption can be determined (e.g. a very low monthly consumption because of a vacation).

As mentioned in section I, one of the main targets of a smart grid is the alignment of production capacities to the actual demand with the use of data of the real-time consumption. Therefore SMs have to process the electricity consumption and communicate the data on a high frequency, which benefits the reconstruction of private information.

A second important factor is the attribution of the data to a consumer. To violate the privacy it is not sufficient to create a consumption profile. It must be possible to attribute this profile to a consumer.

Since a high frequency is mandatory to gain advantage of a smart grid, measures to protect privacy focus on preventing the attribution of data. For operation of a smart grid it is not necessary to know exactly who is consuming a certain amount of electricity. It is rather vital to know the exactly consumption in an area of consumers.

The CC receives all consumer data to operate the smart grid. As a consequence, it is most likely a privacy threat. In this paper the CC is considered as honest but curious. This means that the CC obeys protocols and behaves as intended. But it tries to learn more about consumers from all received data. Therefore, it must be prevented, that the CC can learn anything about consumers from the received data. If a CC learns enough about consumers to create personal profiles, a serious privacy violation happens.

III. Metering for Billing

Metering for billing can be subdivided in billing with a simple tariff and billing with a complex tariff.

A simple tariff has a fixed price per billing unit (commonly kilowatt hour). Usually the consumption is summed up and communicated to the energy supplier once over a long period of time e.g. once every year. Because of this long time span it is not possible to reconstruct sensitive private information about the consumer. For that reason the privacy is considered protected in simple tariffs. This extends to smart grids if the consumption for billing is equally processed and communicated to the CC.

Complex tariffs do not have a fixed price per billing unit. It is possible to link prices to the day time or the CC communicates current prices based on supply and demand. To bill such dynamic prices it is necessary to process the consumption of a consumer more frequently and therefore privacy has to be considered.

The first possible measure to protect privacy is the integration of a trusted third party (TTP). The TTP receives the data from the SM, calculates the sum and communicates the result to CC for billing. The second possible measure is the use of a trusted platform module (TPM), making the SM a trusted agent. The SM does all the calculation and only communicates the result to the CC.

Both measures are not exclusively useful for metering for billing. Because of the resemblance of billing with dynamic prices to real-time metering for operation, TTP and TPM approaches are used in metering for operation, too. Therefore their details are discussed in section IV.

The main difference between metering for billing and metering for operation is the point in time the CC needs the data. For billing the CC needs the data only once in the billing cycle while for operation the CC needs real-time data. That implies for metering for billing that the consumer data has to be stored until the CC needs it. For a TTP approach there are two possibilities to store the consumer data. Either the TTP stores the data for all consumers or each SM stores all data for its consumer. In a TPM approach only the last option is possible, since the SM does all the calculation.

Eventually for metering for billing it has to be decided which agent to trust. Either all trust is put into the SM or a TTP is appointed. Either way the consumer privacy is protected from the CC.

IV. Metering for Operation

In metering for operation the focus is on the real-time electricity consumption to provide electricity more efficiently. Therefore, a high frequency of processing the consumption is necessary. But monitoring the electricity demand must not violate the privacy of consumers.

To protect the privacy in metering for operation typically anonymization or pseudonymization is utilized. With anonymization, features that help identify a consumer are removed, meaning the consumption data cannot be linked to a consumer. For pseudonymization these features are not removed but replaced by an alias. Hence it can be possible to link consumption data to a consumer after pseudonymization, if the data is analyzed extensively.

Subsequently approaches are discussed that remove or replace features of identification using a trusted third party (TTP), securing SM with trusted platform modules (TPM) or aggregating SMs. In the last section IV-D, an approach is discussed that aims to avoid the emergence of features of identification using rechargeable batteries.

A. *Trusted Third Party*

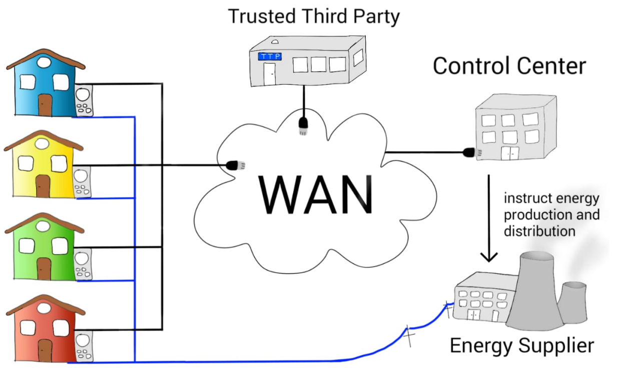

Fig. 3. Model of a smart grid with an additional trusted third party (TTP). The TTP is connected via WAN. It can participate in the communication between smart meters and control center.

The trusted third party (TTP) is an additional agent trusted by all other agents. It accesses sensitive information that can be used to violate the privacy of consumers. Therefore the TTP has to be secure and trustworthy.

There are different possibilities to include the TTP into a smart grid. As a computation center the TTP receives the data from all SMs and does all necessary computation, e.g. prepares bills as mentioned in section III. The SM sends data only to the TTP, which keeps the data secret, and the CC receives only the finished bills. The consumer and the CC put all the trust in the TTP, that data is kept secret and bills are generated correctly. Riella et al. [8] discuss an approach that implements a computation center TTP via cloud computing using SGX containers for secure computation.

If the data has to be processed by the CC the TTP can act as concealment. The TTP can provide pseudonyms or resources that SMs use for their communication to conceal their identities. He et al. present an approach of a TTP providing blinding factors for a group of SMs [9]. When a SM prepares its message for the CC it uses the blinding factors in its calculations to encrypt the message. The TTP sends a key to the CC for decryption of SM messages. However this key does not decrypt a single message. The decryption key of the CC can only decrypt the sum of the messages of one blinding factor group. Hence the identity of a single SM is hidden in the blinding factor group. In this scheme He et al. use an intermediate agent between SMs and the CC. Therewith the CC cannot link a message to a SM.

It is also possible that the TTP participates in the communication as an intermediate communication node between SMs and CC. The TTP then removes or replaces all information about the SM and shields it from the CC.

Ambrosin et al. discuss another approach with a verification center [10]. The verification center is a TTP that examines if the SMs work as intended. In the scheme presented by Ambrosin et al. the SMs do not communicate directly with the CC. Instead SMs communicate among each other and a SM uses a random number of other SMs as intermediate hops to send data to the CC. Therefore the identity of a SM is hidden from the CC. SMs create a log of their actions. To ensure that the SMs work as intended and to detect a malicious SM, the verification center examines the log of each SM. In this scheme the TTP does not participate in the real-time communication of CC and SMs, but rather becomes a supervising authority that detects and communicates unintended behavior afterwards.

Adding a TTP to the smart grid is a possibility, if all other agents in the smart grid do not trust each other. Thereto it is necessary, that all agents agree to one TTP. However it is important to keep in mind, that this is only shifting the problem of who to trust. This is very relevant if the TTP becomes malicious.

B. Secured Smart Meters

SMs must be protected from attacks, since they are measuring sensitive data and are connected to the Internet. Furthermore attackers can have physical access to the SM and manipulate it or perform side channel attacks. Side channel attacks aim for collecting information from sources which are byproducts of function of the SM, e.g. measuring electromagnetic radiation, power analysis or timing attacks [11].

Commonly metering devices are sealed physically to detect manipulation. However, because the SM is connected to the internet new possible threats must be considered and it becomes necessary to protect the SM itself. Enhancing the security of SMs was the goal of the SPIDER-project, a german incorporation of many partners to develop a secure SM [12]. The result of the project was a prototype with an integrity self test.

In many approaches for security in smart grids it is a common premise that a SM includes a trusted platform module (TPM). A TPM is a chip that expands a computer system with additional security functions. It was designed by the trusted computer group and standardized in 2009 (ISO/IEC 11889). One of the two important components of a TPM is a persistent and volatile storage for keys. The other important component is a cryptographic processor which includes a random number generator, an RSA key generator, SHA-1 hash generator, and an encryption-decryption-signature engine. Besides generation of keys a TPM can be used to store data securely and bind it to the TPM. Furthermore remote attestation offers a third party the possibility to verify that the software of the SM has not been changed. Zhao et al. [13] discuss the TPM in detail and consider a SM as trusted SM if it has an TPM and behaves as intended. In addition to protect the privacy of the consumer they arrange the SMs in a ring network.

Another approach is to implement the function of the SM directly into hardware using application-specific integrated circuits (ASICs) or field programmable gate arrays (FPGAs). Hardware-based functions are faster in computation and more difficult to manipulate. Nath et al. [14] show that ring oscillators physically unclonable functions (RO PUFs) can be implemented into FPGAs and used in SMs. RO PUFs are one way functions that are unique per chip. That implies that two different chips with the same input do not produce the same response. Furthermore one chip does not produce the same response for two different inputs. Nath et al. utilized these features to develop an authentication scheme for agents in a smart grid.

Instead of using an additional chip or implementing functions in hardware, it is also possible to use trusted execution environments (TEEs). A TEE is a secure and isolated area on the processor. Karopoulos et al. [15] discuss TEE and show that it provides similar features like TPM with secure storage, secure attestation and secure critical applications. With the omission of a dedicated security chip, TEE provides a more flexible alternative to hardware-oriented approaches. Unlike TPM, later updates and bug fixes are possible.

It is important to secure the SM and there are numerous approaches to accomplish it. The concrete implementation depends on many factors like costs or national laws. It must be considered that the SMs are likely provided by the CC. For the CC mainly the correct functioning of the SMs and protection against outside attackers is important. If a customer can not obtain a SM from an independent source, they can not assume their privacy to be protected against the CC. Standards and laws to regulate the hardware implementation can limit the influence of the CC on the SMs. Additionally other measure have to be taken to protect consumer privacy. However, in many schemes for privacy protection in smart grids, SMs are considered to be provided with a TPM.

C. Aggregation of Smart Meters

Unlike metering for billing, where it is important to know the exact consumption of one consumer, it is sufficient in metering for operation to know the consumption of a group of consumers. Therefore it is possible to aggregate the data of a number of SMs. Hereby the real time consumption of a consumer can be hidden inside the group.

According to the smart grid model, the SM encrypts the data and sends it to the CC. Commonly for aggregation a homomorphic encryption is used. With homomorphic encryption the encrypted data can be added and after decryption the correct result is recovered, just like adding up the unencrypted data.

The encrypted data of the SMs is added and send to the CC. The CC receives only the encrypted result and knows the real time demand of a certain area but not the individual consumption of each consumer. To decrypt the sum of the individual consumptions the CC needs a key, which is usually a sum of all individual SM keys. The CC can not recover individual SM keys from its key, just like it can not recover individual consumptions from the sum.

Lin et al. [16] present a SM aggregation scheme with Fogs. A Fog is an access point for a number of SMs to the internet. As access point it receives the encrypted data from each SM, calculates the sum and forwards it to the CC. In their scheme they consider Fogs as potentially malicious, since they are publicly accessible. Therefore the aim of the scheme is to offer protection even if the access point for SMs is malicious.

Instead of homomorphic encryption Ni et al. [17] propose a scheme that uses encryption based on the decisional Diffie-Hellman assumption. In this scheme the SMs form a ring network to generate a noise to encrypt their data. The CC recovers the sum of the noise of the SMs and can therefore decrypt the sum of the SM data. The SMs send their data to the access point, which collects and adds the data before it forwards the sum to the CC.

The aggregation approach can be combined with a TTP. Instead of an access point in the communication infrastructure to the CC doing the aggregation, a TTP can aggregate the SM data alongside its other functions. Or alternatively the TTP can provide the resources for homomorphic encryption. In the scheme in section IV-A He et al. use the TTP as concealment for SMs [9]. The TTP provides blinding factors for the SMs to use homomorphic encryption. An intermediate agent called aggregator then aggregates the SM messages and forwards the sum to the CC.

Aggregation of SMs is a viable option to enhance privacy, because individual metering data can be hidden in a larger group of consumers. Moreover it can be integrated into other approaches to combine the benefits.

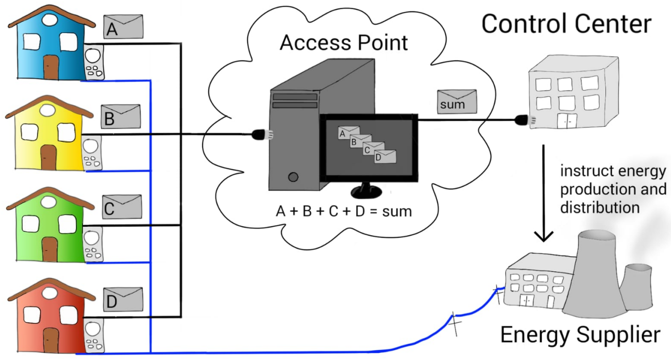

Fig. 4. Smart grid model with aggregation of smart meters. The smart meters encrypt their data and send them to the access point. It calculates the sum and forwards to the control center. The control center decrypts the sum of the encrypted messages and obtains the sum of the smart meter data.

D. Battery Approach

The previous methods have all in common that they try to disguise features that can lead to identification of the consumer. With the battery approach it is the aim to avoid the emergence of data that can reveal information about the consumer. A rechargeable battery is installed between the consumer's electric circuit and the SM. The battery is supposed to shape the consumption of the consumer and therefore no information can be extracted from the consumption data.

Ideally the battery would cover the entire consumption of the consumer and charge when no electricity is consumed otherwise. Hence only a constant consumption can be detected when the battery charges and no consumption otherwise. With the amount of batteries required, this is only a possibility for detached houses. For apartment buildings the battery approach becomes a considerable challenge. Furthermore it assumes the consumption can be predicted. However information about the consumer can still be recovered from this consumption pattern. It indicates when electricity is consumed (no consumption is metered, battery is used). When the consumer does not use any other device, the battery charges. Hence a consistent consumption is metered.

Charging and discharging the battery must be implemented in a feasible way that does shape the real consumption. It has to be considered that the battery must not fully charge after it was used for a short amount of time. Hereby the real consumption is not concealed but delayed. This causes some kind of memory effect, which means the battery remembers the real consumption and reveals it at a later point in time to the SM. Another important consideration is that a fully discharged battery must not charge continuously to the maximum without a break. During the charging time the consumption is not concealed. The real consumption is added to the consumption of the charging battery, which is easy to separate. It is important that the charging and discharging of the battery shapes the consumption so much that no information about the real consumption can leak.

One approach is to use charging and discharging the battery likewise to shape the consumption. Hossain et al. [18] discuss the use of a modified AFSO algorithm (artificial fish swarm optimization) to decide whether the battery should charge or not. Based on the current state of charge and the real consumption the algorithm decides the charging and discharging of the battery.

Another approach is to use only the discharging of the battery to shape the consumption and charge it with some other source of electricity. Giaconi et al. [19] discuss a scheme which assumes renewable energy sources on the consumer side, e.g. solar panels. Discharging the battery shapes the consumption. The renewable energy source on the consume side is used to charge the battery, hence the consumption the battery handles disappears completely from the metering of the SM.

The battery approach is suitable to avoid the emergence of data that can be used to violate the privacy of the consumer. However it depends heavily on the availability of efficient batteries and their expense.

V. Conclusion

The smart grid and the use of smart meters offer a lot of opportunities. Unfortunately they offer likewise opportunities to violate the privacy of consumers. It is important to implement measures that protect the privacy of consumers sufficiently. This survey presented an overview of the most recent approaches to protect consumer privacy. Properties of metering for billing as well as measures to protect consumer privacy during metering for billing were discussed. Privacy challenges of metering for operation were presented, followed by a discussion of approaches to meet these challenges. Trusted third parties, approaches to secure smart meters, aggregation of smart meters and the battery approach were discussed.

Discussed approaches offer the possibility to improve the privacy protection of consumers. However, most approaches need improvement. The use of a trusted third party is more a shift of the problem than a solution. In approaches to secure the smart meter with hardware implementation, the control center has a strong influence, if the control center provides the smart meter for the consumer. The battery approach depends on availability of efficient batteries and their expanse.

In the current state of research, aggregation of smart meters seems to be the most viable option to protect consumer privacy. It can be combined with other approaches to even improve privacy protection.

The smart grid is in early stages of its development. It is important to have reliable privacy protection, when the smart grid is widely deployed. Therefore it is important, that further research is done to find reliable and secure privacy protection measures.

References

[1] Z. F. et al., *Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities*. IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 21–38, 2013.

[2] S. Finster and I. Baumgart, *Privacy-Aware Smart Metering: A Survey*. IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1088–1101, 2015.

[3] M. R. A. et al., *Smart Meter Data Privacy: A Survey*. IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2820–2835, 2017.

[4] *Das Smart-Meter-Gateway*. Bundesamt für Sicherheit in der Informationstechnik – BSI, BSI-Bro18/332, p. 1-44, 2018.

[5] C. F. et al., *Open and Secure: Amending the Security of the BSI Smart Metering Infrastructure to Smart Home Applications via the Smart Meter Gateway*. in Smart Energy Research. At the Crossroads of Engineering, Economics, and Computer Science, vol. 495, C. Derksen and C. Weber, Eds. Cham: Springer International Publishing, pp. 136–146, 2017.

[6] E. L. Quinn, *Privacy and the New Energy Infrastructure*. SSRN Journal, 2009.

[7] M. A. Lisovich and S. B. Wicker, *Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems*. vol. 1, no. 1, p. 10, 2009.

[8] R. J. R. et al., *Securing Smart Metering applications in Untrusted Clouds with the SecureCloud Platform*. in Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems - W-P2DS'18, Porto, Portugal, pp. 1–6, 2018.

[9] D. H. et al., *Privacy-preserving data aggregation scheme against internal attackers in smart grids*. Wireless Networks, vol. 22, no. 2, pp. 491–502, Feb., 2016.

[10] M. A. et al., *Despicable me(ter): Anonymous and fine-grained metering data reporting with dishonest meters*. in 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, pp. 163–171, 2016.

[11] I. M. et al., *Security of Smart-Meters against Side-Channel-Attacks (SCA)*. p. 10, 2019.

[12] K.-O. D. et al., *Integritätsmessung von Smart Meter Gateways*. p. 12, 2016.

[13] J. Z. et al., *Privacy Protection Scheme Based on Remote Anonymous Attestation for Trusted Smart Meters*. IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3313–3320, Jul., 2018.

[14] A. P. D. N. et al., *Hardware-based novel authentication scheme for advanced metering infrastructure*. in 2016 IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit (OIS), Dayton, OH, USA, pp. 364–371, 2016.

[15] G. K. et al., *Towards trusted metering in the smart grid*. in 2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Lund, Sweden, pp. 1–5, 2017.

[16] X. L. et al., *Data Privacy Protection in Smart Grid*. in Privacy-Enhancing Fog Computing and Its Applications, Cham: Springer International Publishing, pp. 67–85, 2018.

[17] J. N. et al., *EDAT: Efficient data aggregation without TTP for privacy-assured smart metering*. in 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, pp. 1–6, 2016.

[18] M. B. H. et al., *Enhanced Smart Meter Privacy Protection Using Rechargeable Batteries*. IEEE Internet of Things Journal, vol. 6, no. 4, pp. 7079–7092, Aug., 2019.

[19] G. G. et al., *Smart Meter Privacy With Renewable Energy and an Energy Storage Device*. IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 129–142, Jan., 2018.