Privacy Issues of Smart E-Mobility

Lucie Langer and Florian Skopik
Safety & Security Department
AIT Austrian Institute of Technology
2444 Seibersdorf, Austria
Email: {lucie.langer, florian.skopik}@ait.ac.at

Georg Kienesberger
Institute of Computer Technology
Vienna University of Technology
Gußhausstr. 27-29, 1040 Wien, Austria
Email: kienesberger@ict.tuwien.ac.at

Qin Li
School of Computer Engineering
Nanyang Technological University
50 Nanyang Ave, Singapore 639798
Email: qin.li@ntu.edu.sg

***Abstract*—The increasing adoption of Smart Grids brings about significant benefits such as enhanced efficiency and sustainability, but entails also severe threats to consumer privacy due to the possibility of establishing detailed user profiles. Existing efforts mostly focus on privacy issues in Smart Metering. However, the Smart Grid contains other important use cases whose privacy challenges have not received much attention to date. In this paper we aim to raise awareness for privacy issues in e-mobility, which will be a cornerstone application of the future Smart Grid. In particular, we study in detail the properties of privacy-relevant e-mobility use cases, the actors involved in those scenarios, and the data they exchange as part of their interaction. We investigate to which extent existing solutions can be applied to address emerging privacy challenges in e-mobility, and propose new privacy-aware design patterns.**

I. Introduction

Smart Grids are upgraded electricity networks using information and communication technology (ICT) to intelligently integrate all entities connected to them such as consumers, power plants, or distributed energy resources [1]. These enhanced electricity grids are currently being introduced in an increasing number of countries. In Europe, the roll-out of Smart Meters as part of the implementation of Smart Grids has become mandatory for all member states; by 2020, at least 80% of households must be equipped with a Smart Meter [2].

The expectations that go along with the introduction of Smart Grids pertain to overcoming the problems posed by the aging infrastructure of current power grids, and to facilitate the integration of distributed energy sources. Sustainability and efficiency of supply shall be facilitated by e.g. intelligent monitoring and self-healing abilities, as well as enhanced information flow between electricity providers and consumers [3]. However, the benefits of Smart Grids go along with several drawbacks and challenges in terms of security and privacy: a Smart Grid requires establishing an ICT network in parallel to the power grid in order to facilitate the communication of all entities involved. Apart from the security concerns that apply to an ICT network of comparable size – especially in light of its significance for the citizens' power supply –, *privacy* of the consumers is also considerably affected [4]. For example, high-frequency readings of Smart Meters can be used to establish detailed consumer profiles, including the electric appliances used in a household, waking and sleeping habits, etc. [5]. Existing work on privacy in Smart Grids therefore mainly deals with obfuscating Smart Meter readings by applying various cryptographic or statistical approaches.

However, Smart Metering is not the only application scenario within a Smart Grid where sensitive personal information of users might be exposed in an undesired way. In this paper we aim to raise awareness for privacy issues in *e-mobility*, another cornerstone application of the future Smart Grid which has not been in the focus of privacy considerations so far although it entails significant privacy issues: the concept of e-mobility foresees that a customer can charge his electric vehicle also on foreign premises while still getting billed individually. This implies that the amount of energy withdrawn as well as the identity of the vehicle or, respectively, the customer must be transparent to the energy supplier, who could use this data not only for billing purposes, but also to track customers in various unwanted ways. Thus, customer privacy is at stake due to potential misuse of sensitive motion data.

The contributions of this paper are twofold:

- *Detailed Analysis of Privacy Implications through E-mobility:* we study in detail the properties of e-mobility use cases, which involves considering the actors and the data exchanged during their communication. These use cases are the basis for an in-depth analysis of privacy implications.
- *Survey of Applicable Technologies and Required Solutions:* we investigate to which extent existing solutions can be applied to address privacy challenges of e-mobility, and propose new privacy-aware design patterns capable of mitigating privacy threats in the Smart Grid.

The remainder of this paper is organized as follows: In Section II we outline and categorise existing approaches to preserve privacy in Smart Grids. Privacy-relevant e-mobility use cases are studied thoroughly in Section III. Section IV investigates to which extent existing solutions can be applied to mitigate privacy threats in e-mobility, and proposes high-level ideas and approaches to preserve privacy in the use cases considered before. Section V concludes the paper and gives an outlook on future work.

II. Background and Related Work

Existing work on privacy aspects of Smart Grids mainly deals with Smart Metering systems since the privacy challenges are more obvious in this area than in other parts of the Smart Grid. Threats to and vulnerabilities of Smart Metering systems have been discussed for example in [6]–[8]. Data communication security controls (e.g., cryptographic functions such as encryption, message authentication codes, and digital signatures) provide standard security services in regarding confidentiality, integrity, and accountability of messages and their origin [9]. However, the aspects of privacy and potential threats [10] to customers through Smart Meter data exploitation is not fully covered yet [7]. An important official first step towards a privacy-enabled Smart Grid has been made by NIST [11], who defined challenges related to privacy protection and legal constraints.

While current efforts mainly focus on setting up strong regulatory frameworks and adapting existing privacy laws to be applicable for the Smart Grid, the adoption of technical means is still underdeveloped. Despite this fact, several sound solutions already exist which partly address the privacy challenge. First, *Anonymization of Metering Data* [12] applies the idea of separating technical data (meter readings) from customer IDs. For that purpose a third-party ID escrow company is involved. Second, *Metering Data Obfuscation* [13], [14] is about masking the own energy consumption profile with local battery buffers, e.g., from an electric car, so that one cannot infer detailed energy consumption profiles, while the overall consumption profile remains intact. Third, *Privacy-preserving Metering Data Aggregation* [15], [16], deals with the online aggregation of data from geographically co-located consumers, i.e., before readings reach the data center, so that the utility provider can still get a clear picture about the grid's state in a street or district, but not for a single customer.

Finally, instead of considering only technical aspects, SmartPrivacy ('privacy-by-design') [17] focuses on a more holistic view. This concept is an umbrella that offers the complete suite of protections to ensure data privacy. It consists of multiple measures ranging from regulatory protections to education and awareness. Notice that in contrast to these efforts, in this paper we do not focus on Smart Metering only. We argue that due to the wide acceptance of Smart Grids further privacy challenges need to be solved, such as the exploitation of motion data of e-cars.

III. E-Mobility and the Smart Grid

Enabling and supporting e-mobility is considered to be a cornerstone of the future Smart Grid due to its potential to reduce carbon emissions. After giving a brief introduction to e-mobility we describe several application scenarios in this area, focusing on the actors involved, their interactions and the data exchanged between them.

A. Introduction to E-Mobility

In this section we focus on privacy-sensitive use cases around Plug-in Electric Vehicles (PEVs), i.e. cars with an electric motor run by a battery charged with power from the electricity grid [18]. While the standard grid-to-vehicle (G2V) scenario assumes an unidirectional flow of energy from the grid to a PEV for charging purposes, the vehicle-to-grid (V2G) concept considers bidirectional energy flows between PEV and power grid, i.e. electricity is fed back to the grid during peak consumption periods. Thus, when parked, the PEV acts as a buffer absorbing excess energy (i.e. charging its battery) during off-peak hours, and providing energy (i.e. discharging its battery) during peak load hours or emergency situations such as impending power outages. Since vehicles are usually parked 95% of the time, a huge potential for load balancing opens up if we assume that any parked PEV will be connected to the grid and available both for battery recharging and discharging [18]. The utility provider may foresee a higher energy tariff for peak demand than for off-peak times in order to provide an incentive for the customer to avoid energy-intensive PEV charging during times when the electrical grid is heavily utilised.

B. Use Case Description

In general, charging a PEV starts by plugging it into an energy gateway, which may be an ordinary socket or a designated charging station. This action either directly triggers an energy flow between the grid and the PEV, or may first initiate a communication session between the PEV and the utility provider. The optional communication may include an identification of the PEV in order to grant a special tariff based on a previously arranged contract between the customer and the energy supplier.

The customer may charge the PEV either

1) at his own premises, or
2) at other parties' premises,

e.g. publicly available charging stations or private ones like friends' houses or the customer's workplace. The two scenarios of home charging and roaming can be further divided into

a) uncontrolled and
b) controlled (also called "smart") charging,

depending on whether the grid operator is able to remotely control the charging process in order to optimise grid utilisation. Controlled charging currently mostly restricts to the possibility to automatically interrupt the charging process if required during peak loads, but will in the future involve also more sophisticated ways of load management, including a user interface which allows the customer to specify his preferences and constraints for the charging process in terms of the deadline and/or the distance to be travelled the next day. Thus, in the following we will consider four different use cases:

Use case 1a: *Uncontrolled Customer-Premises Charging.*
Use case 1b: *Controlled Customer-Premises Charging.*
Use case 2a: *Uncontrolled Foreign-Premises Charging.*
Use case 2b: *Controlled Foreign-Premises Charging.*

Use case 1a refers to uncontrolled charging at home: the PEV is charged at the customer's own premises using a conventional power socket without any possibility for the grid operator to interact with the customer or the PEV, respectively. The energy costs incurred are incorporated into the total energy costs of the household. Use case 1b considers smart (i.e. demand-side managed) charging at the customer's premises, which may include separate billing of the energy consumed for PEV charging at a special tariff[1]. Use cases 2a and 2b refer to situations where the PEV roams and therefore is charged at foreign (private or public) premises, which may require an identification of the car or the customer for billing purposes.

C. Actors

Table I provides an overview of the actors involved in the four e-mobility scenarios to be analysed, including the use cases for which the respective actor is relevant.

TABLE I
ACTORS IN E-MOBILITY USE CASES.

Actor	*Type*	*Description*	*Use Cases*
PEV	device	Plug-in Electric Vehicle	1a&b, 2a&b
customer	person	PEV operator	1a&b, 2a&b
energy supplier	company	provides electric energy to customers, may offer special tariffs for PEV charging	1a&b, 2a&b
grid operator	company	monitors grid load, may require PEV to adapt amount and rate of charge	1a&b, 2a&b
charging station	device	gateway between PEV and energy grid, supplies energy for the PEV	1b, 2b
charge service provider	company	supplies charging services	2a, 2b
energy management system (EMS)	system	collects and evaluates information from all actors involved (including metering), manages charging process	1b, 2b
customer interface	system	gateway between customer and EMS, allows customer to specify his preferences and constraints for the charging process	1b, 2b

D. Interactions

In the following we describe the interactions that occur between the different actors in each of the individual application scenarios.

Use case 1a: Uncontrolled Customer-Premises Charging. The customer connects his PEV to a standard one-phase or three-phase socket at his own premises. The charging process begins immediately without any prior authentication, and terminates as soon as the plug is pulled or the PEV battery is fully charged. The grid operator has no means to control the amount or rate at which electric energy flows from the grid to the PEV. The amount of energy supplied is measured via the electricity meter in the customer's premises and is incorporated into the standard electricity bill provided by the energy supplier.

Use case 1b: Controlled Customer-Premises Charging. The customer connects his PEV to the charging station at his own premises. We assume that no PEV authentication is carried out in this scenario, i.e. *any* PEV plugged into the customer's charging station will be charged according to the tariff agreed upon by the customer and the energy supplier. The customer optionally enters his preferences for the charging process via the customer interface. The customer interface forwards this information to the EMS, which checks if any special tariff has been agreed upon by the customer and the energy supplier. The EMS calculates the amount of energy needed (either to get fully charged, or to reach the charge level specified by the customer constraints), and provides a schedule for the charging process based on feedback on the grid load provided by the grid operator. The grid operator feeds back the current grid utilisation to the EMS which may thereupon adjust the scheduling accordingly. The EMS records the amount of energy supplied to the PEV and provides the corresponding data to the energy supplier for billing purposes. The customer receives a separate bill for PEV charging issued by the energy supplier.

Use case 2a: Uncontrolled Foreign-Premises Charging. The customer connects his PEV to a charging station or a standard socket at foreign premises. The charging process begins immediately without any prior authentication of the PEV, and terminates as soon as the plug is pulled or the PEV battery is fully charged. In case of private premises, the amount of energy supplied is measured via the meter in the premise and becomes part of the standard electricity bill of the premises' owner. In case of public premises, the amount of energy supplied is measured via the meter which is part of the charging station, and the costs are settled by the customer by paying the charge service provider according to the provider's energy tariff.

Use case 2b: Controlled Foreign-Premises Charging. The customer connects his PEV to the charging station at the foreign premise and optionally enters his preferences for the charging process via the customer interface. The customer interface forwards the information provided by the customer to the EMS, which authenticates the PEV and optionally checks if any special tariff has been agreed upon by the customer and the energy supplier. The EMS calculates the amount of energy needed (either to get fully charged, or to reach the charge level specified by the customer constraints), and provides a schedule for the charging process based on feedback on the grid load provided by the grid operator. The grid operator feeds back the current grid utilisation to the EMS which may thereupon adjust the scheduling accordingly. The EMS records the amount of energy supplied to the PEV and provides the corresponding data to the energy supplier for the billing process, which may consider a special tariff provided to the customer if applicable. The customer receives a separate bill for PEV charging issued by the energy supplier. In case the charging takes place at a public charging station, the customer may be required to settle the bill immediately.

IV. Privacy Threat Analysis and Discussion

A. E-Mobility Use Case Analysis

The impact of PEV charging on customer privacy is closely related to the question whether an authentication of the PEV (or, respectively, the customer) takes place as part of the

[1] Note that for providing a separate billing account for a PEV an additional meter would have to be installed since the use of sub-meters is currently not allowed in Austria.

charging process. Table II therefore provides an overview of the different authentication requirements and the applicability of special customer-claimed tariffs within the individual e-mobility use cases.

TABLE II
CUSTOMER AUTHENTICATION IN E-MOBILITY USE CASES.

Use Case	*PEV/customer authentication required*	*Special PEV tariffs applicable*
1a: Uncontrolled Customer-Premises Charging	no	no
1b: Controlled Customer-Premises Charging	no	yes
2a: Uncontrolled Foreign-Premises Charging	yes	no
2b: Controlled Foreign-Premises Charging	yes	yes

In the following we analyse the privacy issues that arise from each of the e-mobility use cases presented in Section III.

Use case 1a: Uncontrolled Customer-Premises Charging. In this scenario no EMS is involved and no identification of the PEV is carried out. However, the grid operator and energy supplier respectively[2] can still detect that a PEV is being loaded from analysing the energy consumption profile for specific load cycles (e.g., through non-intrusive appliance load monitoring NIALM [19]). The level of difficulty of such an analysis depends on the length of the charging process and on the frequency of electricity meter reports being sent to the provider. As the time required to fully charge a battery with a capacity of 30 kWh ranges from 42 minutes to 13 hours depending on the charging mode [20], uncontrolled charging via an ordinary socket will in most cases take long enough to include a sufficient amount of metering data. Estimating the start and end time of the charging process from the energy consumption profile gives the provider information about when the customer arrives at his home as well as the approximate distance he has travelled. Moreover, the provider is able to recognise recurring patterns in the daily consumption profiles, which may indicate whether the consumer has a steady job (similar time of return on each workday), how far his workplace is away from his premises (amount of energy consumed and, thus, approximate distance travelled), or if his job requires a lot of travelling (different distances travelled during the week).

Use case 1b: Controlled Customer-Premises Charging. This scenario involves the EMS, but no identification of the PEV is carried out as we assume that all PEVs plugged into the customer's charging station will be treated equally, i.e. charged according to the tariff agreed upon by the customer and the provider. Since the use of the charging station is transparent to the provider, he knows at which time the customer arrived at home without having to analyse the energy consumption profile of the premise as in use case 1a. Thus, all privacy threats mentioned in use case 1a are applicable in this scenario as well. The customer may even deliberately provide additional information via the customer interface: from the deadline for the charging process the provider knows when the customer will leave home the next day. This information may be especially valuable for burglars, who could be informed by a maliciously cooperating provider. From the total amount of energy consumption within a certain period (e.g. one month) the provider can easily derive the number of people living in the premise, and, in particular, if the customer is the only inhabitant and the premise will thus be abandoned when he leaves. On the other hand, knowing when the customer arrives at home can be used for targeted advertising campaigns, e.g. placing cold calls which will be answered with high probability since the customer is present. This possibility may not be exploited by the provider directly, but can nevertheless be sold to other companies. In future use cases, the customer may also provide further details such as the route and distance to be travelled the next day in order to benefit from lower energy tariffs, which gives the provider additional information on the customer's whereabouts and may even disclose the customer's workplace and indicate the customer's level of income. Other privacy threats include ascertaining the customer's principal residence, which may be of interest to public authorities.

Use case 2a: Uncontrolled Foreign-Premises Charging. Uncontrolled charging at foreign premises does not involve an EMS nor an authentication of the PEV. However, it may include an authentication of the *customer* for billing purposes: At public charging stations the customer may be offered to pay by credit card or by a special customer card (i.e. a smart card or RFID card such as in the ElectroDrive Salzburg project [21], [22]). While the privacy issues of credit card use are well-known [23], the novel approach of using designated customer cards for PEV charging results in new privacy threats: the charge service provider learns the customer's identity and may be able to establish motion profiles of the customer by correlating the billing information of the charging stations. This holds particularly if the customer may only use his card when charging his PEV at specific stations (such as for [21]). The scenario of uncontrolled charging at the customer's workplace could include identifying the customer via an ID card (e.g. a staff badge which is used as an entry card within the premise) in order to allow for deducing the costs for the amount of energy used from his salary.

Uncontrolled charging at foreign premises of private individuals (i.e. friends or relatives of the customer) does usually not involve any authentication of the customer. Moreover, this scenario could have positive implications on the privacy of the premises owner since his own energy consumption profile is obfuscated by the additional load generated by the customer's PEV.

Use case 2b: Controlled Foreign-Premises Charging. This scenario involves an identification of the PEV by the EMS,

[2] Note that, in certain countries, grid operators and energy suppliers are legally identical organizations, while in other countries these might be separated. Furthermore, the question which customer-relevant information is either transparently visible to the energy supplier or is shielded by the grid operator highly depends on the actual Smart Grid architecture. In the following discussion, we therefore use the general term 'provider' to refer to both entities.

which forwards this information to the provider. Thus, the provider learns the time and place of recharging and can therefore track the customer's whereabouts. At a public charging station the customer will most probably want to charge the PEV immediately (charge-and-go), while at private premises (such as the customer's workplace) longer charging periods including load shifting and demand-side management are more realistic. In the latter scenario, the customer may therefore deliberately provide additional information via the customer interface as in use case 1b, which gives the provider detailed information on how long the customer will be away from home, thus providing an even stronger indication that the customer is not at home during that time, and therefore enabling the attacks described for use case 1b. If the customer charges his PEV at a charging station provided at his workplace, the provider may easily learn about the customer's employer. Similarly, charging the PEV at the premises of friends gives the provider valuable information about the customer's social network, which he may either use himself or sell to other companies for advertising purposes.

B. Discussion on Solutions

In the following we discuss the applicability of existing privacy protection techniques to the e-mobility use cases presented in Section III and propose novel high-level approaches to be integrated in future e-mobility architectures in order to enhance customer privacy.

Applicability of existing privacy protection techniques. As already mentioned in Section II, a commonly proposed technique to support privacy in Smart Metering is aggregation over time (i.e. several days or weeks) or space (i.e. several customers): regarding the latter approach, fine-grained metering data required for operational reasons (load management) does not necessarily have to be attributable to individual customers, but can be aggregated for example within a neighbourhood area before it is passed on to provider. This location-based aggregation of energy consumption data from geographically co-located customers can also be applied to the four e-mobility use cases introduced in Section III: for uncontrolled charging as considered in use case 1a and 2a, the application is straightforward since the PEV is just another power consuming appliance. For controlled charging, the application could be as follows: the provider must be able to control PEV charging for the sake of smart load management, but he does not have to control each PEV *individually*. Several different PEV charging stations at customer's premises may be clustered to form a pool. In this case, an EMS on cluster level serves as an interface between the provider and the single EMS of the individual charging stations within the pool. Thus, the top-level EMS implements both the load management requirements posed by the provider and the constraints specified by the customers via the EMSs of the individual charging stations. Thus, as a trusted third party the top-level EMS would manage the scheduling of the pool as a whole, while the individual charging processes within the pool would remain opaque to the provider. Likewise, time-based aggregation of a single customer's PEV energy consumption data could support a privacy-friendly billing process in use case 1b.

Besides data aggregation, another privacy-enhancing concept which could be adopted from Smart Metering is pseudonymisation of energy consumption data in terms of separating meter readings from customer identities as proposed in [12]: for load management purposes it is sufficient if the provider knows the energy consumption of a specific entity identifiable by a unique ID; he does not have to learn the customer associated with that particular ID. The link between the ID and the customer is only known to a third-party escrow organisation. This concept still requires a trusted party (namely the escrow), but can help to reduce the monopolisation of sensitive information by the provider.

Another approach proposed in [18] could be to open the electricity market also for small-scale customers by allowing them to participate in the bidding process and buy energy at acceptable tariffs without having to surrender private information on their mobility behaviour (if energy is bought for the whole household and not exclusively for e-mobility). This approach would, however, require a substantial reorganisation of the current electricity market in terms of decreasing the minimum amount to the range of several kilowatts. Moreover, the willingness of customers to participate in such a scenario would have to be analysed, and usability aspects would have to be considered. Finally, this approach is only suitable for use case 1a, since it does not prevent the necessary data exchange for controlled and foreign-premises charging.

New approaches for privacy-preserving e-mobility. As just discussed, some of the privacy-preserving techniques and approaches from Smart Metering can be transferred to the e-mobility use cases we have considered in Section III. However, the specific requirements for PEV charging go beyond Smart Metering and demand a two-tier approach of technical and organisational provisions in order to maintain customer privacy. For example, considering Table II, it would be convenient if the customer could apply special tariffs arranged with the provider without having to disclose his own identity also in a roaming scenario (use case 2a and 2b). This could be realised by a pre-paid card which would allow the customer to anonymously buy energy for charging his PEV at special rates, thus improving the concept implemented within the ElectroDrive Salzburg project, which uses personalised customer cards. Additionally, a reliable end-to-end security layer for the underlying communication system needs to be established.

The different use cases presented in Section III have shown that consumer privacy threats aggravate the more sophisticated and "smart" the charging process gets: controlled charging offers a broader attack surface than uncontrolled charging, and decreases the effort that has to be invested by the energy supplier / grid operator in order to obtain sensitive data from the customer. This is also due to the fact that the customer may get rewarded for disclosing additional information (e.g. route to be travelled the next day) by obtaining a better tariff. This trade-off between privacy and cost savings is well-known from other business branches, such as payback cards in food retailing. Consumer education and transparency is an important factor in this context: the customers should be aware of the data they provide and what it could be used for, so that they can decide autonomously how much information they are willing to share.

In order to enable such decisions without preventing the customer from using e-mobility at all, a trusted instance allowing for fine-grained access control, like the *Smart Web Grid* framework [24] is needed. Here, a service-oriented architecture incorporating a public key infrastructure and employing standards like for instance the eXtensible Access Control Markup Language (XACML) is used as a basis for a holistic information platform enabling strongly encrypted, authenticated and authorised data exchange between arbitrary stakeholders in the Smart Grid [25].

In any case, sticking to uncontrolled charging is definitely not an option for the future Smart Grid since important added values such as smart load management would be rendered void.

V. Conclusion

So far, privacy considerations for the Smart Grid have been related to Smart Meters, whose high-frequency reportings on energy consumption can be exploited to establish detailed user profiles of consumers. In this paper we have shown that significant privacy issues apply also to e-mobility, an application area that will be of paramount importance for the future Smart Grid. We have presented four fundamental e-mobility use cases and provided a comprehensive analysis of their implications on customer privacy, thus showing that e-mobility opens up a variety of surveillance possibilities which do not apply to conventional mobility. Moreover, we have shown that existing work on ensuring privacy-sensitive Smart Metering (such as obfuscating the power consumption data by applying various cryptographic or statistical approaches) can also be applied to mitigate privacy threats in e-mobility. As part of future work, detailed concepts should be established on how to bring existing as well as new privacy-enhancing solutions in e-mobility into practice. Additionally, a reliable end-to-end security layer for the underlying communication system needs to be established, and organisational measures such as consumer education need to be implemented in order to safeguard customer privacy while at the same time making the most out of the ‘Smart’ Grid.

References

[1] European Technology Platform, “Smart Grids – Strategic Deployment Document for Europes Electricity Networks of the Future,” April 2010.

[2] “Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids,” 2011.

[3] S. D. Ramchurn, P. Vytelingum, A. Rogers, and N. R. Jennings, “Putting the ’smarts’ into the smart grid: a grand challenge for artificial intelligence,” *Commun. ACM*, vol. 55, no. 4, pp. 86–97, Apr. 2012.

[4] F. Skopik, “Security is not enough! On Privacy Challenges in Smart Grids,” *International Journal of Smart Grid and Clean Energy (IJSGCE)*, vol. 1, no. 1, pp. 7–14, September 2012.

[5] E. L. Quinn, “Smart Metering and Privacy: Existing Law and Competing Policies. A Report for the Colorado Public Utilities Commision,” 2009.

[6] A. R. Metke and R. L. Ekl, “Security technology for smart grid networks,” *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[7] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, “Smart-grid security issues.” *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[8] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, “An integrated security system of protecting smart grid against cyber attacks,” in *Innovative Smart Grid Tech.*, Jan. 2010, pp. 1–7.

[9] R. DeBlasio and C. Tom, “Standards for the smart grid,” in *IEEE Energy 2030 Conference*, 2008, pp. 1–7.

[10] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, “Private memoirs of a smart meter,” in *ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, 2010, pp. 61–66.

[11] The Smart Grid Interoperability Panel Cyber Security Working Group, “Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid ,” 2010.

[12] C. Efthymiou and G. Kalogridis, “Smart grid privacy via anonymization of smart metering data,” in *International Conference on Smart Grid Communications*. IEEE, 2010, pp. 238–243.

[13] D. P. Varodayan and A. Khisti, “Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage,” in *International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 2011, pp. 1932–1935.

[14] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, “Privacy for smart meters: Towards undetectable appliance load signatures,” *International Conference on Smart Grid Communications*, pp. 232–237, 2010.

[15] K. Kursawe, G. Danezis, and M. Kohlweiss, “Privacy-friendly aggregation for the smart-grid,” in *International Conference on Privacy enhancing technologies*, 2011, pp. 175–191.

[16] F. Li, B. Luo, and P. Liu, “Secure and privacy-preserving information aggregation for smart grids,” *Int. J. Secur. Netw.*, vol. 6, no. 1, pp. 28–39, Apr. 2011.

[17] A. Cavoukian, J. Polonetsky, and C. Wolf, “SmartPrivacy for the smart grid: embedding privacy into the design of electricity conservation,” *Identity in the Information Society*, vol. 3, no. 2, pp. 275–294, Aug. 2010.

[18] P. Grahn and L. Söder, “The Customer Perspective of the Electric Vehicles Role on the Electricity Market,” in *8th International Conference on the European Energy Market*, 2011.

[19] G. Hart, “Nonintrusive appliance load monitoring,” *Proceedings of the IEEE*, pp. 1870–1891, Dec 1992.

[20] M. Faschang and F. Kupzog, “Interfacing vehicle charging systems with user and grid requirements,” *Informatik Spektrum*, vol. 36, no. 1, pp. 27–34, 2013.

[21] “Statusbericht der E-Mobilitätsmodellregion ElectroDrive Salzburg,” January 2013.

[22] A. Schuster, “Electric Mobility Model Region ”ElectroDrive Salzburg”: Scientific accompanying research activities,” in *EVS26 International Battery, Hybrid and Fuel Cell Electric Vehicle Symposium*, 2012.

[23] C. Duhigg, “What Does Your Credit-Card Company Know About You?” *New York Times*, p. MM40, May 17 2009.

[24] G. Kienesberger, M. Meisel, and A. Adegbite, “A Comprehensive Information Platform for the Smart Grid,” in *Proceedings of IEEE AFRICON 2011, Livingstone, Zambia*, September 2011.

[25] M. Jung, T. Hofer, S. Döbelt, G. Kienesberger, F. Judex, and W. Kastner, “Access control for a Smart Grid SOA,” in *Proceedings of the 7th IEEE Conference for Internet Technology and Secured Transactions*, London, UK, Dec. 2012.