Energy Informatics

REVIEW

Open Access

An analysis of privacy preservation in electric vehicle charging

Andreas Unterweger[1*], Fabian Knirsch[1], Dominik Engel[1], Daria Musikhina[2], Ammar Alyousef[2] and Hermann de Meer[2]

*Correspondence: andreas.unterweger@en-trust.at
[1] Center for Secure Energy Informatics, Salzburg University of Applied Sciences, Puch bei Hallein, Austria
Full list of author information is available at the end of the article

Abstract

Electric vehicles (EVs) are gaining widespread adoption, which requires expanding the charging infrastructure. This infrastructure is part of a complex ecosystem that consists of multiple entities interacting with each other and exchanging (often personal) user data. Such a heterogeneous system with multiple participants exchanging personal data poses severe privacy risks to users. State-of-the-art literature insufficiently covers privacy aspects of charging ecosystem use cases. In this paper, a profound analysis of this ecosystem with respect to privacy is provided: First, the EV charging ecosystem and its entities are defined. Second, high-level use cases for EV charging identified in literature are analyzed and used for defining data flows within the charging ecosystem. Third, the identified use cases are compared in terms of privacy guarantees and adherence to standards. Fourth, representative implementations of these use cases are evaluated, i.e., all actors and (unintended) data flows are described and potential privacy threats are identified and visualized. It is found that privacy is not sufficiently covered by standards and implementations of EV charging use cases from literature. Furthermore, recommendations and future directions for protecting user privacy in the EV charging ecosystem are derived. In summary, stricter adherence to standards and privacy by design are suggested.

Keywords: Electric vehicle, Charging, Privacy, Analysis

Introduction

National and international legislation aiming to reduce the emission of carbon dioxide, environmental strategies (Capros et al. 2018) This results in an increasing number of Electric Vehicles (EVs) as well as a rapidly growing network of Charging Stations (CSs) which leads to new challenges for the power grid (Manbachi et al. 2016; Delgado et al. 2018).

The EV ecosystem is a complex interconnected network with diverse actors. It builds on a variety of international standards (Rives 2016; Portela et al. 2015; Sombroek 2014; Hubject 2016; OCPI 2020; Schmutzler et al. 2013), covering many aspects of data and information formats as well as exchange policies.

Within or alongside this information exchange, personal data of EV users are often collected, stored and processed by the communicating actors. This has a significant impact

on the privacy of users, as this data may allow to conclude information about user habits, their incomes and their private or family life (Langer et al. 2013). Due to the complex nature of the EV ecosystem, it requires a detailed analysis of the standards and the state-of-the-art implementations to assess or estimate the privacy impact on EV users.

Existing literature has not yet caught up with the complexity of the EV ecosystem in terms of privacy preservation. While privacy aspects of isolated Use Cases (UCs) or subsets of actors have been analyzed, an analysis of privacy preservation in the EV ecosystem as a whole, i.e., with all relevant actors and UCs, is missing.

Contributions

The contributions of this paper are fivefold. First, the EV ecosystem is described in detail for typical UCs. Second, potential privacy breaches based on the implementations of different EV UCs and data flows are discussed. We identify five potential privacy risks in the way this ecosystem is currently standardized and implemented. Third, a methodology for evaluating the privacy of data flows in the EV ecosystem is proposed. The most novel aspect of this methodology is an analysis of collusions, i.e., the privacy impact of two or more parties in the ecosystem cooperating and exchanging data. Fourth, a novel visualization of privacy guarantees in the EV ecosystem is proposed and presented.

Fifth and finally, an analysis of selected implementations of the most relevant UCs of the EV ecosystem is conducted and these UCs are compared with respect to their capability to preserve privacy of the EV users. The proposed methodology and visualization are used to do so. It is found that many UC realizations deviate from the e-mobility standards (see Fig. 1) and their privacy features are not sufficiently discussed and covered within the respective publications. We conclude our paper by providing recommendations and future directions for protecting user privacy in the EV ecosystem.

Scope

In the last decade, a lot of effort has been allocated by researchers and manufacturers to study the different challenges in the e-mobility sector. This has resulted in numerous research contributions presenting solutions which focus on specific concepts of that domain. Therefore, this work does not tend to scan all possible solutions and implementations found in literature of the different analyzed UCs. Instead, we focus on publications that reflect the data flow described in the standards for the EV ecosystem as close as possible. This ecosystem and the standards are described below in detail in the Electric Vehicle Ecosystem Section.

EV charging can happen at public charging stations, parking spaces, and homes. Each of those scenarios has its different impacts on the electricity grids. In this paper, we focus on EV charging via a network of public or semi-private charging stations. Moreover, the main business related to the ecosystem under study is electricity retail where EVs can support two use cases Grid-to-Vehicle (G2V) and Vehicle-to-Grid (V2G).

Related work

Despite growing attention from academia and industry, as well as numerous work about privacy-preserving authentication schemes (Li et al. 2014; Liu et al. 2012; Chen et al. 2015; Nicanfar et al. 2013), anonymous payment systems for EVs (Zhao et al.

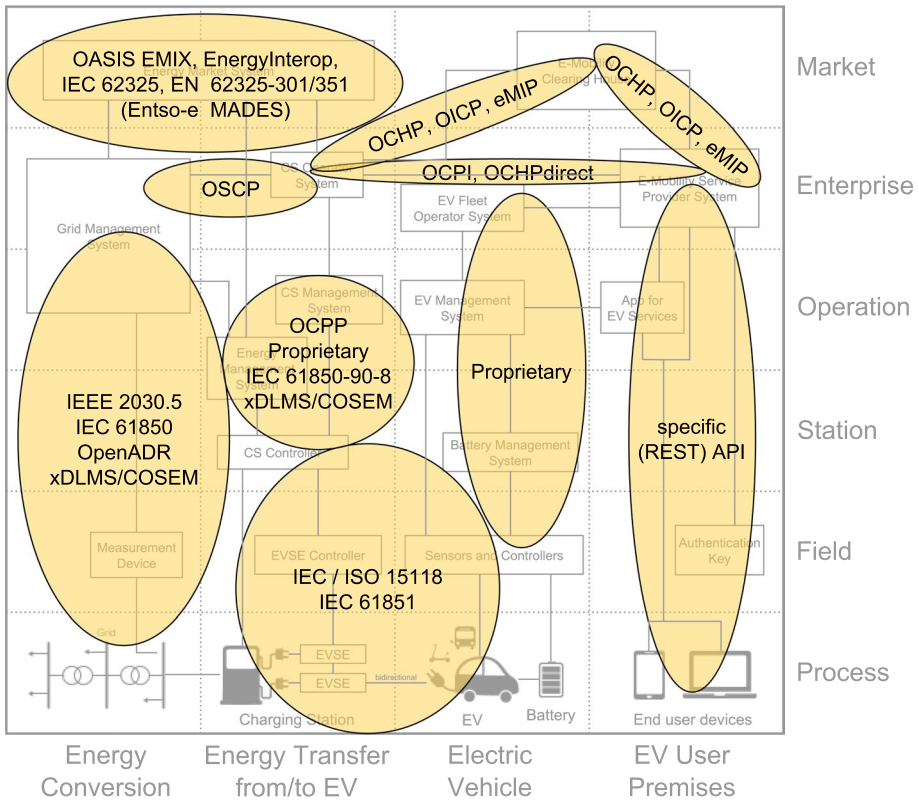


Fig. 1 A visualization of the EMSA information layer and the corresponding standards as described in Kirpes et al. (2019): The horizontal axis denotes the zones, and the vertical axis denotes the domains. The squares in the background represent the actors, systems and devices of the EV ecosystem, and the yellow circles represent the standards used by the encompassed actors, systems and devices

2014; Au et al. 2014; Gao et al. 2018; Radi et al. 2019), frameworks for reservation of charging stations (Rabieh and Aydogan 2019; Xiang et al. 2016; Liu et al. 2016), EV roaming (Mustafa et al. 2015), and grid management protocols (Han et al. 2014; Han and Xiao 2016a), there are, as of the time of writing, only a few papers (Han and Xiao 2016b; Saxena et al. 2017; Ferrag et al. 2018) on privacy-preservation considering the whole EV ecosystem.

Han and Xiao (2016b) give a high-level overview of the EV ecosystem with a focus on V2G networks. Moreover, V2G-relevant privacy issues are introduced and a number of different privacy-preserving techniques are listed. Furthermore, a set of solved and unsolved problems are pointed out. However, there is no clear mapping between all the identified privacy-relevant problems and applied privacy-preserving techniques with the different actors of the EV ecosystem and their relevant operations. In contrast, we critically analyze the data flows between the actors.

Saxena et al. (2017) discuss V2G security, including privacy, from the perspectives of the vehicle owner, vehicle, vehicle battery, electric utility provider, and billing company. Nevertheless, the authors do not consider all the actors [e.g., the the Distribution System Operator (DSO)] and well-known UCs (e.g., smart charging) in the proposed new architecture, which leads to an incomplete privacy analysis.

Ferrag et al. (2018) provide a survey on privacy-preserving frameworks in smart grids. Their scope is on the smart grid as a whole, i.e., they do not specialize on the EV related UCs. Further, the authors provide no privacy analysis and no evaluations of the discussed papers.

In our work, we analyze the EV ecosystem in detail with the major focus on the privacy preservation of the EV users' personal data. Additionally, we precisely describe the main actors and the high-level UCs of the EV ecosystem and map them on the well-known e-mobility protocols. Moreover, we suggest two different visualization approaches in the Definition of Privacy Section which can be used to analyze privacy-preserving approaches in the EV ecosystem.

Structure

This paper is structured as follows: In the Electric Vehicle Ecosystem Section, we provide an overview of the state-of-the-art EV ecosystem and derive the relevant actors and high-level UCa. In the Methodology Section, we explain how evaluate the EV literature in terms of privacy, with the Privacy Evaluation Section containing the evaluation of selected examples. Based on the results of our privacy evaluation, we provide recommendations and future directions in the Future Directions Section before concluding the paper in the Conclusion Section.

Electric vehicle ecosystem

In this section, the state-of-the-art EV ecosystem is presented, including all the main actors who participate in exchanging the EV users' personal data. Furthermore, multiple high-level UCs within the EV ecosystem are described and the corresponding interconnections between the actors of these UCs are identified. The word "actor" is used to describe any autonomous object or entity that sends and receives messages from or to other actors; this can be implemented by either stand-alone software operated by an organization or by a person (e.g., a Charging Station Managment System (CSMS) by a Charging Station Operator (CSO)) or a software embedded in a dedicated hardware device, e.g., a CS.

Overview

A thorough scan of literature and relevant reports on e-mobility (Alyousef 2021; Boucetta et al. 2021; Leviäkangas et al. 2014; Hubject 2016; OCPI 2020), clearly shows that the EV ecosystem is very complex and includes many actors and UCs. In practice, it is very rare to find one company which targets the whole ecosystem and all of its UCs. On the contrary, any one company typically focuses on few or even only one aspect. For example, one company may enable smart charging, whereas another enable asset management, billing, or roaming services.

Thus, different actors need to exchange data in order to inter-operate. As a result, a comprehensive overview of the entire ecosystem needs a holistic approach, especially with respect to privacy. For that sake, a methodology proposed in Ma et al. (2021) is followed to give a clear description of the system boundaries, actors and their roles and values in the system. Finally, the interactions among these actors according to well-known standards are shown.

For describing the EV ecosystem, the main actors and UCs are identified. Due to the focus on EV user privacy, the focus of the description is on personal data flows between the actors. To that end, many e-mobility protocols which describe such data flows have been analyzed. The protocols are extracted from (Rives 2016; Portela et al. 2015; Sombroek 2014; Schmutzler et al. 2013; Hubject 2016; OCPI 2020).

In Fig. 1, the most relevant standards and protocols of the e-mobility sector, specifically for battery-electric mobility, are presented on the information layer of the E-Mobility Systems Architecture (EMSA) model (Kirpes et al. 2019). They can be classified into six main categories with respect to their functionality:

- Communication with end user devices via a specific (REST) API,
- EV charging and automatic authorization, e.g., IEC/ISO 15118,
- Managing the CSa, e.g., the Open Charge Point Protocol (OCPP),
- Exchanging information between the CSO and the E-Mobility Service Provider (eMSP), e.g., Open Charge Point Interface protocol (OCPI),
- Roaming, e.g., the Open Clearing House Protocol (OCHP) and the Open Inter-Charge Protocol (OICP), and
- Communication with the grid operators, e.g., the Open Smart Charging Protocol (OSCP).

Figure 2 shows how the UCs cover the different components and actors in the function layer of EMSA model (Kirpes et al. 2019). A more detailed explanation of all actors and UCs follows below.

By analyzing the aforementioned protocols and the required data flows across each of these six categories, we extract the EV ecosystem as sketched in Fig. 3, where the most well-known standards for describing the required information exchange are depicted. Moreover, we extract nine high-level UCs (detailed in Section High-level Use Cases) which are denoted in brackets to identify which actors (detailed in Section Main Actors) are required to communicate for realizing the respective use case(s). The following sections address the main actors and high-levelUCs in detail.

Main actors

We identify and describe all actors which process and exchange personal data to analyze privacy risks and to evaluate privacy preservation. We distinguish the following actors:

- EV user: A person who owns and/or drives an EV. This person has to register at the eMSP of the CSOs for which they want to subscribe to in order to be able to charge using the public CSs of those CSOs. To do so, EV users initiate a service contract with an eMSP and receive Unified Identifiers (UIDs) which are stored, e.g., in an RFID card as described in Appendix . However, EV users are allowed to charge via the infrastructure of other CSO for which they are not registered.
- E-Mobility Service Provider (eMSP): An entity which grants EV users access to the charging infrastructure by issuing UIDs. The eMSP handles all communication and billing processes involving the EV users. To that end, the eMSP gathers data from CSOs and the Clearing House Operators (CHOs) it has a contract with.

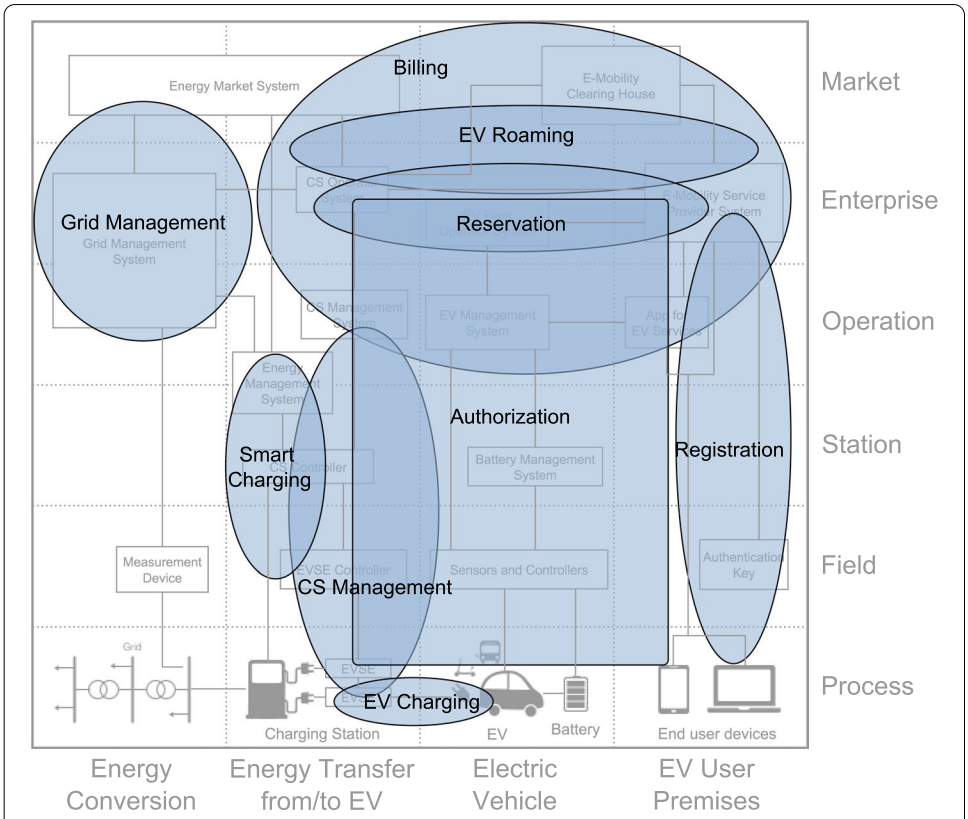


Fig. 2 Nine high-level UCs visualized on the EMSA function layer (Kirpes et al. 2019): The horizontal axis denotes the zones, and the vertical axis denotes the domains. The squares in the background represent the actors, systems and devices of the EV ecosystem, and the blue circles represent the high-level UCs with their involved actors, systems and devices

Using these UIDs, the contracted EV user has access to additional charging services via the Navigation Service Provider (NSP).

- Navigation Service Provider (NSP): An entity which provides supplementary services to EV users, e.g., location searches for available CSs, the reservation of charging connectors and routing suggestions according to EV users' preferences. The NSP usually belongs to the eMSP. Therefore, we assume the same for our representation of the EV ecosystem.
- Charging Station (CS): A hardware device which is equipped with charging connectors to deliver energy to EVs. Software is usually embedded into a CS for management purposes.
- Charging Station Operator (CSO): An entity which operates one or more CSs and allows physical access to the charging infrastructure. The CSO can directly own CSs or it can maintain CSs owned by the eMSP. The CSO manages a CS remotely by leveraging protocols, such as OCPP, in order to collect data required for billing, namely, Charge Details Records (CDRInfo).
- Clearing House Operator (CHO): An entity which enables roaming, i.e., allowing EV users to charge at CSOs which they are not subscribed to via the eMSP. The

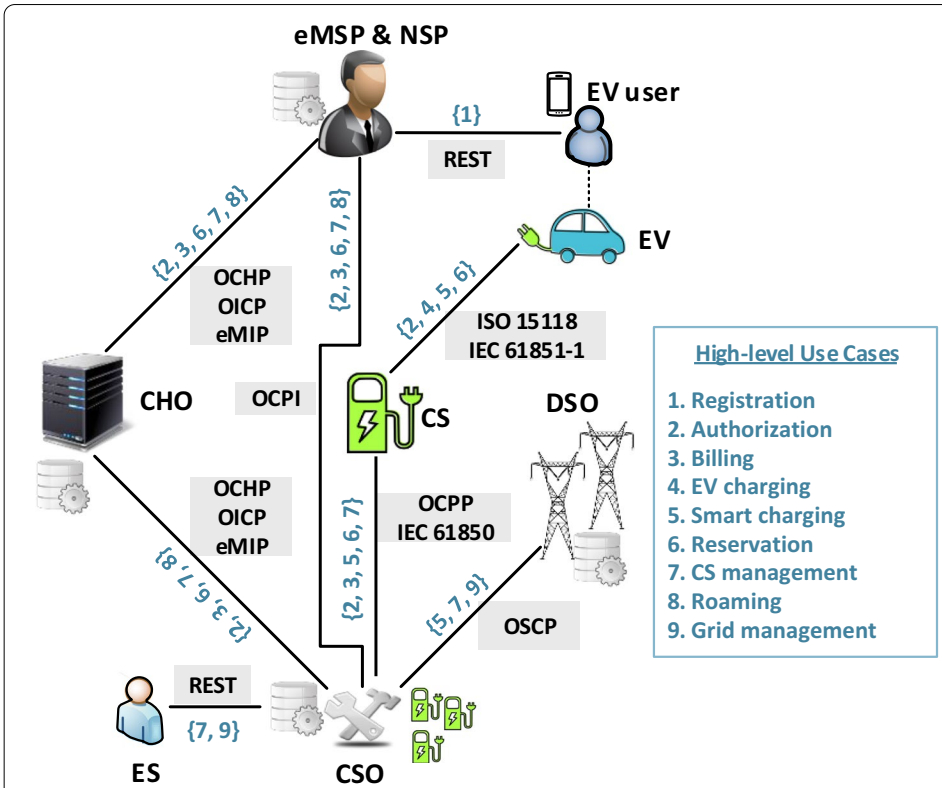


Fig. 3 Interactions among primary actors within the EV ecosystem: The actors (yellow squares) are depicted together with the data they exchange (blue arrows) as well as the corresponding standards (black arrows). Legal interactions are depicted by dashed black lines for the sake of completeness

CHO runs a software platform to facilitate mutual data exchange between eMSPs, NSPs, and CSOs.

- Energy Supplier (ES): An entity which is contracted by the CSO to deliver electricity according to contracted tariffs. In practice, this actor only measures total energy consumption of a CS and processes no direct personal data of an individual EV user.
- Distribution System Operator (DSO): An entity which offers the connection to the distribution power grid and provides information about the grid status, e.g., a 24-h forecast of available power capacity, to the CSOs.

High-level use cases

To clarify for which purposes the EV users' personal data is processed, stored, and exchanged, it is necessary to identify high-level UCs describing the interaction among the actors from Section Main Actors. Moreover, the required data flows to realize these UCs according to the e-mobility protocols/standards presented in Fig. 3 have to be identified. Inspired by Nahapiet (2017), we differentiate nine main high-level UCs:

1 Registration: Registration is the process of signing a contract between an EV user and eMSP. The EV user provides its identity information and the EV's properties as described in Appendix . After that, the EV user receive UIDs which are used for

communication with other actors. The user's personal data is stored in the database of the eMSP and is not used for communication with other actors. The request for the contract can typically be sent remotely via the eMSP's Web site, gathering only some of the personal data; otherwise, the contract is signed at the eMSP's premises.

2 Authorization: When a CS charges an EV, it needs to authenticate the user beforehand. If the user is authorized, the CS informs the CSO that it has started charging. Consequently, a bill can be issued later by the eMSP. That process is carried out using data stored in a RFID card. Authorization is handled by IEC/ISO 15118, OCPP, OCHP, OICP, OCPI, and eMIP.

3 Billing: Billing means issuing/sending an invoice to an EV user for charging. The details depend on the billing model and the type of tariffs available at the eMSP and the CHO. Billing processes are handled by IEC/ISO 15118, OCPP, OCHP, OICP, OCPI and eMIP. They mainly involve exchanging CDRInfo, i.e., data required for billing.

4 EV charging: In our work, EV charging refers only to the power ow through which the EV is charged from the grid. Discharging operations are not consid- ered as they have not gained widespread implementation yet. During charging, the Charging Point (CP) and the EV exchange only signals in order to enable the current ow between them. EV charging is supported by IEC/ISO 15118 and IEC 61851.

5 Smart Charging: Smart charging implies an instant power management by the Electrical Vehicle Supply Equipment (EVSE) controller, according to the current power grid capacity predicted by the DSO (Portela et al. 2015). It regulates the power flow into the EV based on power currently available in the grid (Alyousef et al. 2018; Alyousef and de Meer 2019), the EV's battery, the connection type, the amount of power required, etc. Data such as total required energy, arriving and/or departure time of the EV, and used power are essential data for developing advanced smart charging algorithms. Smart charging is supported by the following protocols: IEC/ISO 15118, IEC 61851, OCPI, OCPP, and OSCP.

6 Reservation: Reservation means in-advance scheduling of charging pro- cesses by remotely booking charging connectors via a NSP or a Road Side Unit (RSU). EV users can choose among available, compatible CSs via the NSP. Reservation processes may be handled by IEC/ISO 15118, OICP, OCPI, OCPP, and OCHP.

7 CS management: The management of CSs implies the technical support and configuration of the CSs by the CSO as well as the delivery of the POint Information (POI) to a eMSP/NSP directly or via a CHO. Additionally, the CSO sends aggregated data of power/energy usage to the DSO/ES so that predictions about energy usage as well as available capacity and power quality can be made. This is enabled by, e.g., OSCP, OCHP, OICP, and OCPP.

8 Roaming: The objective of roaming is to provide a smooth connection be- tween the EV users and different eMSPs, allowing an EV user to utilize any CS and to be correctly authorized and billed. To realize this UC, an exchange of CDRInfo and UIDs between the CHO and the eMSP of the user is required. Roaming can be implemented by OCPI, OICP, OCHP, and eMIP.

9 Grid management: Grid management includes the ability to control CP in terms of either capacity that is demanded from the grid or the time of use of this capacity. It

consolidates demand-supply balancing and enables peak shaving and valley filling. Schedule-based charging or smart charging can be seen as a more specific type of this use case. In order to consolidate power demand and supply, an exchange of predictions about the energy requirement is needed. This exchange relies on charging profiles (see Appendix) which are communicated between the CSO and the CSs. These profiles are built based on the users' energy requirements, forecast about the available cable capacity in the distribution grid as provided by the DSO, and the energy market given by the ES as part of a balancing group. OSCP, OCPP, and OpenADR, etc. support this UC.

From all of the nine UCs listed above, some imply only actual energy flows (UC 4), while some require processing of aggregated private data (UC 9). Taking this into account, only UCs 1–3, 5, 6 and 8 involve processing (including operations as collection, recording, organization, structuring, storage, etc. EU 2016) of direct and indirect EV user's personal data.

For the privacy analysis in this paper, we consider all actors from the descriptions above which are able to collect, process and/or possess data, independently of the physical actor being software, hardware or an individual or organization.

This consideration is independent of the physical actor being software, hardware, an individual, an organization or any combination of the aforementioned since we assume a fully automated processing of that data flow among all actors.

Methodology

This section introduces the terms privacy we well as a methodology to analyze privacy and the impact of collisions. This methodology is proposed and used for evaluating privacy for the state of the art EV charging protocols analyzed in this paper.

Definition of privacy

The term *privacy* lacks a universal definition, but generally refers to the unauthorized use, acquisition or intrusion of personal information (EU 2016). Privacy therefore only exists in the context of an individual person or legal entity (Knirsch 2017). In contrast, a security breach is the unallowed acquisition of data in contrast to a privacy breach, which is the unallowed usage of legally acquired data (Knirsch 2017). Note that some authors use the terms security and privacy interchangeably.

Privacy sensitive data is directly related to an individual or contains information about that individual. However, often the collection of fine-grained personal data is needed for a particular use case or based on statutory requirements. In addition, a single data item alone may not be privacy critical. The combination of data from various actors, however, may allow someone to learn additional information and, therefore, to breach someone's privacy.

In this paper, the terms *direct personal data* and *indirect personal data* are defined in accordance with (EU 2016). Direct personal data refers to any data item that allows to directly identify an individual without additional information (e.g., name or address, but also other information, such as hair and eye color). Indirect personal data refers to any data item that does not by itself allow the identification of an individual,

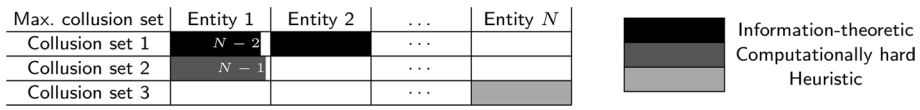


Fig. 4 Exemplary visualization of privacy guarantees for N entities and two collusion sets. Each collusion set (row) comprises of one or more entities (columns). The color of the collusion set corresponds to the level of privacy that can be achieved

but requires additional data. UIDs and numbers assigned to a person are examples of such indirect personal data items.

Collusion sets

The collection of data must be reduced to the absolute minimum needed for fulfilling a certain use case and for protecting privacy. Depending on the specific use case, finding such a trade-off between utility and privacy is highly non-trivial.

As in related work (Knirsch et al. 2018; Unterweger et al. 2016, 2019), it is assumed that all actors follow the data flow as specified in the respective protocols, but attempt to learn additional information, which in security research is referred to as *honest-but-curious* (Goldreich 2004). In an honest-but-curious model, actors may collude and exchange information to gain additional insights. In order to visualize the maximum collusion set, i.e., the maximum number of actors allowed to exchange information without breaching privacy, the methodology proposed in Unterweger et al. (2019) is used.

Such a visualization is much more concise than formal proofs or lengthy textual descriptions and thus beneficial for assessing the privacy guarantees, as well as for communication and comparison. To the best of the authors knowledge, no other comparable methodology exists to visualize collusions. The visualization is exemplified in Fig. 4. The columns list the entities (types of parties) involved in the protocol and the rows denote the different maximum collusion sets. The corresponding cells mark whether or how many instances of each entity may collude while still preserving privacy at one of the following levels:

- *Information-theoretic* Privacy cannot be breached under any circumstance, e.g., when certain parties never possess a certain data item;
- *Computationally hard* Privacy can only be breached with an enormous amount of computing power, e.g., when state-of-the-art encryption needs to be broken (Barker 2016); and
- *Heuristic* Privacy might be breached under some circumstances, e.g., for certain input data.

For example, the first row in Fig. 4 illustrates that $N-2$ instances of Entity 1 and all instances of Entity 2 may collude without breaking privacy. However, with any additional entity colluding with them, the privacy guarantees cannot be upheld. Adding another entity or one more instance of an already colluding entity to the collusion set will breach the depicted privacy guarantees.

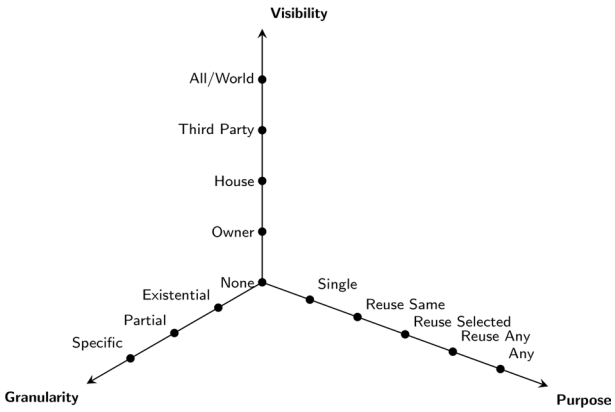


Fig. 5 Privacy dimensions as suggested by Barker et al. (2009): The three axis depict the dimensions and their possible values. The *Retention* dimension is not shown (Retention $\in$ {date, ∞})

Privacy dimensions

In Barker et al. (2009), give a formal approach towards privacy. As their approach is universally applicable, it is used in this paper. Barker et al. describe a privacy taxonomy that allows to classify data items according to their visibility, granularity, purpose, and retention. It is generally assumed that data that is collected for a particular purpose, with limited retention, at low granularity and with little visibility is more privacy-preserving than a data item that is collected for many or undefined purposes, with unlimited retention at high granularity and with wide visibility. Figure 5 illustrates the dimensions according to Barker et al. (2009).

For many applications, the retention, i.e., the amount of time data is stored, is of relevance. This is also reflected in the General Data Protection Regulation (GDPR) (EU 2016) by requiring the deletion of data after a certain amount of time. While some data items are required by law to be retained for a certain amount of time, others can be deleted immediately after processing. Barker et al.'s approach takes a retention dimension into consideration. The value of this dimension can be either a certain amount of time or *infinity*.

Note that, as opposed to collusion sets, this approach does not cover the risk of combining data items from various actors in order to gain new insights or information, especially considering the use of retained historic data.

Adaptation of Barker et al.'s methodology

While Barker et al.'s approach is universally applicable, it needs to be adapted to the specific properties and demands of the EV ecosystem. In addition, Barker et al.'s approach does not cover collusion, i.e., the cooperation of otherwise distinct parties with the purpose of exchanging data for gaining additional knowledge.

We therefore modify the approach in two ways: (i) we specify the dimensions in a way that corresponds to the actors and types of data commonly used in this ecosystem; and (ii) we combine this with the concept of collusion sets in order to additionally identify the implications of unlawful collaboration of actors.

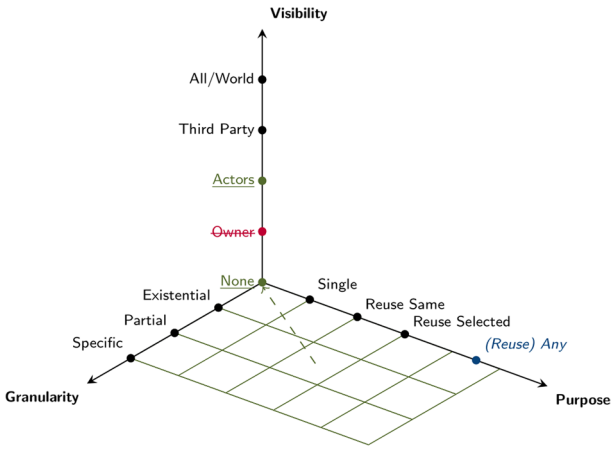


Fig. 6 Modified privacy dimensions for EV charging use cases. Green underlined values denote redefinitions, struck out red values denote removals and the purple italic value denotes the combination of two values

A modified version for the first way (i) is visualized in Fig. 6. In summary, two visibility values are removed, two purpose values are combined and two visibility values are redefined. The changes are described below and examples for both, the modified and the unmodified values, are given.

Purpose

- *Single* For example, State of Charge data sent from an EV to the CP (or sensed by CP) is used for a single purpose only, namely for the adaptation of the amount of charging power, as well as for starting and stopping the charging process.
- *Reuse same* For example, Personal Data is collected by the eMSP and reused for multiple clearing sessions with the CHO, i.e., the same data is reused at different points in time.
- *Reuse selected* For example, the Tariff Info is transmitted from the eMSP to both, the CHO and CSO. This means, that the same data is used for different purposes by different actors.
- *(Reuse) Any—combined* The values *Reuse Any* and *Any* are combined into a single value under our assumption of honest-but-curious actors (see above). Such actors are free to use collected data for any purpose (which includes the reuse any value), while fully honest actors do not reuse data for different purposes without the users' consent. For example, an aggregated form of charging profiles might be published for research purposes by the CSO.

Visibility

- *None—combined* The whole purpose-granularity plane is mapped to a single point on the visibility axis. Both, the granularity and purpose dimensions cannot practically have the value *None*. For example, the collection of data without purpose is ille-

gal (EU 2016), considering honest-but-curious actors. Similarly, a granularity of zero would mean that the data does not exist in the first place. Thus, invisible data (visibility value *None*) covers both, non-existent data as well as data collected without purpose.

- *Owner—removed* Data which is only visible to the respective owner is not visible in any protocol and can thus not be collected by any other party. This value is therefore not considered.
- *Actors* For example, the eMSP sees all personal data that it receives through the respective protocol.
- *Third Party* For example, the CSO receives user preferences from the eMSP, e.g., the individual charging profile of an EV.
- *All/World* Since honest-but-curious actors follow the defined protocol, visibility generally does not exceed the involved actors, even when collusions exist. However, some approaches may be based on data storage or data exchange concepts that allow visibility for all or the world, such as blockchain applications.

Granularity

- *Existential* For example, the unique token is used by the CSO to verify whether or not an EV is registered at the corresponding eMSP.
- *Partial* For example, the CSO may send charging data to the CHO in aggregated form. The CHO does not necessarily receive the full information, but only a partial representation of it.
- *Specific* All personally identifiable data that is collected through the defined protocols, e.g., personal data during user registration, falls into this category.

Privacy analysis

Based on the EV ecosystem as described in Section Electric Vehicle Ecosystem, we analyze in this section the potential privacy breaches and we apply both, Barker et al.'s approach (Barker et al. 2009) and an analysis of the collusion sets. The privacy of a customer is breached, if another actor can use the gathered data for an unintended purpose. The privacy analysis based on the data flows and the actors is following the approach presented in (Knirsch et al. 2015a, b).

The following five potential privacy breaches have been identified. For each privacy breach of the involved actors, the revealed data items and the potential harms are listed.

(i) **Identification of vehicle and exchange of personal data.** An EV user forwards personal data, including name, address as well as the make and the car model to the eMSP. This is intended for billing purposes. However, this information could be misused for, e.g., targeted advertisements.

- Actors involved: user, eMSP
- Data items: EV data, personal data
- Potential threats: identification of user home or work place

(ii) **Pseudonymous identification via unique token.** The EV user passes a unique token, which is issued by the eMSP upon registration, to the CSs and to the CSO for each charging operation. This allows the CSO to create (pseudonymous) statistics about the behavior of the user.

- Actors involved: user, eMSP, CSs, CSO
- Data items: token, EV data, State of Charge (SoC)
- Potential threats: identification of user habits (Knirsch et al. 2015a), tracking of user location (Langer et al. 2013) (via pseudonyms only)

(iii) **De-pseudonymization due to data exchange.** The CSO forwards data about the charging process assigned to the unique token of the customer to either the CHO or the eMSP. This can happen in an aggregated form or in high granularity. The latter allows both, the CHO and the eMSP, to learn detailed habits of the customer.

- Actors involved: CSO, eMSP, CHO
- Data items: token, charging data records, tariff information.
- Potential threats: identification of user habits (Knirsch et al. 2015a), tracking of user location (Langer et al. 2013)

(iv) **Fingerprinting the EV.** The CSs and CSO, respectively, need to adjust the parameters for charging (e.g., voltage levels, power and inlet types) for supporting smart charging on the fly for the respective vehicle. This might allow some fingerprinting about the make and model of the vehicle. This means that by comparing parameters specific to a type of vehicle to a list of known properties of vehicles, the vehicle type or manufacturer can be identified.

- Actors involved: EV, CSs, CSO
- Data items: token, EV data, SoC
- Potential threats: information about user income/social status

(v) **Profiling with smart charging.** In a setting incorporating smart charging, the DSO and CSO offer profiles to the EV and eMSP, respectively. Giving a cus- tomer the option of choosing particular profiles (i.e., preferred charging times and duration) might allow to conclude certain habits.

- Actors involved: user, CSO, eMSP, DSO
- Data items: charging profile
- Potential threats: identification of user habits (Knirsch et al. 2015a), detection of user presence at home (McKenna et al. 2012), information about home and work place (Langer et al. 2013)

These potential privacy breaches form the basis of our privacy evaluation of the EV charging. In order to mitigate these threats and in accordance with (Pfitzmann and Hansen 2010), we distinguish five privacy preservation properties, which are used for

discussing the privacy evaluation: anonymity, unlinkability, undetectability, unobservability, and pseudonymity.

Privacy evaluation

In this section, we describe the methodology for assessing the privacy aspects of papers from the literature. To do so, we first identify the privacy implications of data used in state-of-the-art EV charging implementations, protocols (Rives 2016; Portela et al. 2015; Sombroek 2014, and related work (Nahapiet 2017; Schmutzler et al. 2013). This is done by classifying the data items according to Barker et al.'s methodology (Barker et al. 2009) and by other GDPR relevant criteria, as well as by considering the potential privacy breaches described in the previous section. Data items posing significant privacy implications are used as the basis for further evaluation. Furthermore, literature on the main EV use cases is collected and some examples of in-depth analysis are presented according to the criteria described in Section Focus of Literature Selection. Finally, these examples are compared with respect to the methodologies explained in Sections Collusion Sets and Adaptation. The results are summarized in Section Privacy Evaluation Overview and shortcomings related to privacy preservation are pointed out.

Focus of literature selection

In Section High-level Use Cases we identified six UCs that process personal data directly. For all of the use case, a literature review has been conducted and the relevant papers have been categorized. For each use case one representative paper has been selected according to the following criteria:

1. The proposed solution for the respective use case adheres to one of the standards found in the EV ecosystem (as described above) or deviates by the minimum possible amount. This allows to map actors described in the paper to actors proposed in the EV ecosystem described in Section Electric Vehicle Ecosystem.
2. If multiple papers remain from the first selection, the one with the most citations per year at the time of writing has been chosen.

These criteria ensure that one representative example for each use case is provided while limiting the extent of specific per-paper details. The classification of the selected papers into UCs is presented in Table 1. The numbering of UCs is identical to the numbering in Section High-level Use Cases

Due to page limitations, we focus on the three use cases that are most common in the EV ecosystem, namely, authentication, billing, and roaming. Paper (Li et al. 2014) (UC 2) is chosen according to criterion (1), as its system model maps actors and their roles to the EV ecosystem described in Section Electric Vehicle Ecosystem besides minor deviations, e.g., the use of different names for actors. Paper (Mustafa et al. 2015) is selected as it is the only examples of roaming (UC 8) use cases that considers privacy in the proposed solutions. Subsequently, paper (Gao et al. 2018) was picked according to criterion

Table 1 Selection of literature per use case: For each of the relevant UCs, papers which incorporate them are listed

Use case	Literature
Registration (UC 1)	–
Authorization (UC 2)	Li et al. (2014), Liu et al. (2012), Chen et al. (2015), Saxena and Choi (2016), Rabieh and Wei (2017), Abdallah and Shen (2017), Nicanfar et al. (2013), Pazos-Revilla et al. (2018)
Billing (UC 3)	Gao et al. (2018), Au et al. (2014), Zhao et al. (2014), Li et al. (2019), Radi et al. (2019)
Smart charging (UC 5)	Portela et al. (2013)
Reservation (UC 6)	Rabieh and Aydogan (2019), Xiang et al. (2016), Liu et al. (2016)
Roaming (UC 8)	Mustafa et al. (2015)
Multiple	Gabay et al. (2019), Tseng (2012), Gunukula et al. (2017), Eiza et al. (2019), Yang et al. (2011), Rottondi et al. (2014), Han and Xiao (2016a), Wang et al. (2015)

Papers which incorporate multiple UCs are grouped into the *Multiple* entry

Table 2 Citations per year for the billing use case: all papers of the exemplary billing use case with their respective citation metrics according to Google Scholar as of the time of writing

References	Year of publication	Total citations	Avg. citations per year
Gao et al. (2018)	2018	82	27
Au et al. (2014)	2014	67	10
Zhao et al. (2014)	2014	7	1
Li et al. (2019)	2019	9	5
Radi et al. (2019)	2019	3	2

(2), covering the billing use case (UC 3), and it is shown in Table 2 that it has the highest number of citations per year[1].

There is no particular work on UC 1 (registration) because direct personal data of the EV user is needed to be collected and stored by the eMSP. Therefore, processing of personal data in this case must strictly follow the GDPR regulations EU 2016. However, Rabieh and Aydogan (2019) present a solution where the EV user can be identified by the eMSP only if they perform illegal actions. Nonetheless, the eMSP collects and stores direct personal data of the EV user and the registration procedure.

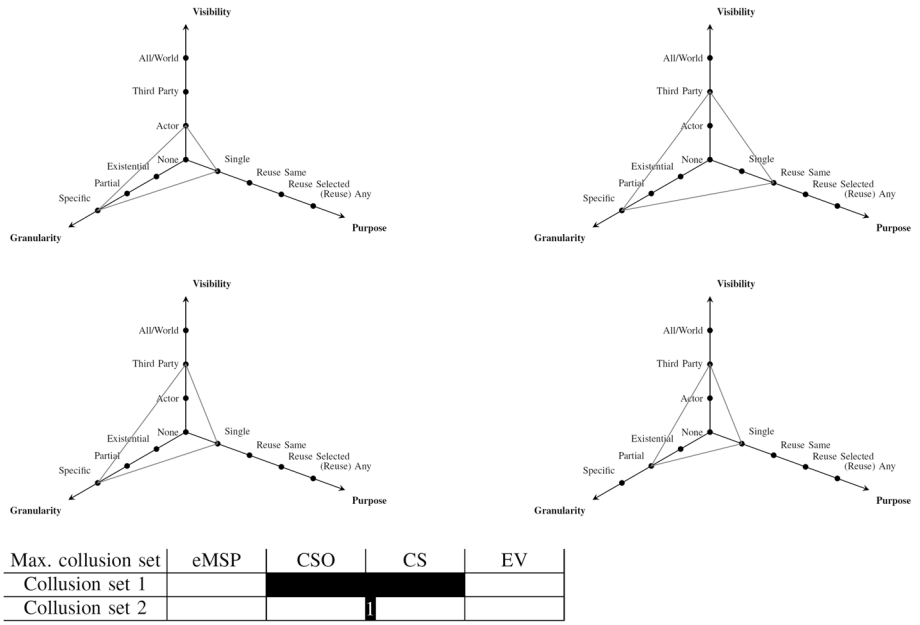
Evaluation examples

In this section, we present a detailed analysis of the three selected papers. We therefore apply the adapted approach by Barker et al. (2009) and the collusion set approach to the selected papers. We shortly describe the communication and data flows between actors and the personal data that is exchanged for each paper.

Li et al. (2014)

The authors present dynamic contactless charging and their implementation covers the authorization use case (UC 2). Their approach relies on charging pads which communicate with the EV and the eMSP. Initially, the EV registers at the eMSP, during which the

[1] The total number of citations is taken from Google Scholar at the time of writing, May 25, 2021.



Max. collusion set	eMSP	CSO	CS	EV
Collusion set 1				
Collusion set 2			1	

Fig. 7 Privacy dimensions and visualization for collusion sets for (Li et al. 2014) for data items (i) personal data/ID (top left), (ii) time (top right), (iii) location, charging parameters, amount of energy (bottom left), and (iv) aggregated energy (bottom right). Collusion set 1 refers to the mapping between the ID of the EV and its identity. Collusion set 2 refers to the potential learning of driving directions and patterns

eMSP generates a unique EV ID. This Identifier (ID) is associated with the personal data belonging to the EV owner. After this, the eMSP generates a number of session keys and nonces daily, which are used for one charging session each without repetition.

The communication flow consists of the following steps:

1 The EV encrypts its unique *ID* with the public key of the eMSP and sends it to the eMSP;
2 The eMSP decrypts this message with its private key;
3 The eMSP chooses one previously generated session keys and a nonce and sends both, encrypted with the EV's public key, to the EV;
4 The EV decrypts the session key and the nonce with its private key;
5 The EV and the CS communicate encrypted with the session key and nonce. They exchange *time*, *EV's location*, and *charging parameters*;
6 After charging, the EV sends EV *ID*, *time*, and *amount of energy* to the eMSP;
7 The CS sends nonce, *amount of energy* and *time*, encrypted with a pad-specific key, to the CSO;
8 The CSO sends nonce, *aggregated energy*, and *time* to the eMSP.

In the above steps, direct (example) and indirect private data (example) are highlighted by underlining once and twice, respecively. Indirect private data is data that requires additional information to be linked to violate privacy. In the example above, the EV ID is a pseudonym which can only be linked to an EV (and thus the corresponding owner) with the mapping database of the eMSP.

In Fig. 7, all direct and indirect private data items are depicted according to the methodology explained in Section Adaptation of Barker et al.'s Methodology. Each triangle (in gray) depicts the privacy dimensions for one data item. A larger triangle, i.e., one that is closer to the viewer, implies more privacy criticality.

Time is used by multiple actors and reused for a selected number of steps. Location, charging parameters, and amount of energy are used by multiple actors and for a single purpose. Aggregated energy is in the same category in terms of purpose and visibility, but due to being an aggregate, it has only partial granularity.

In addition, information not explicitly mentioned in the steps above can be learned: From step 5, a single CS can learn a pattern. Even though a direct identification of the EV is not possible, habits and recurring actions can be used to de-identify EVs and to match their charging session data.

The above mentioned information can be obtained by one single party. However, the protocol consists of an eMSP, multiple CS, and the EV. Note that the original paper (Li et al. 2014) implicitly assumes that all CSs are operated by the same entity, which we refer to as CSO.

Collusion set 1 consists of all CSs and the CSO. None of them possesses the ID of the EV. Thus, the collusion set provides information theoretical privacy guarantees as long as neither the eMSP nor the EV join the collusion set. Collusion set 2 consists of a single CS, which cannot derive the EV's direction, but only the presence of an EV. Adding one or multiple neighboring CS allows tracking the EV's direction and deriving patterns.

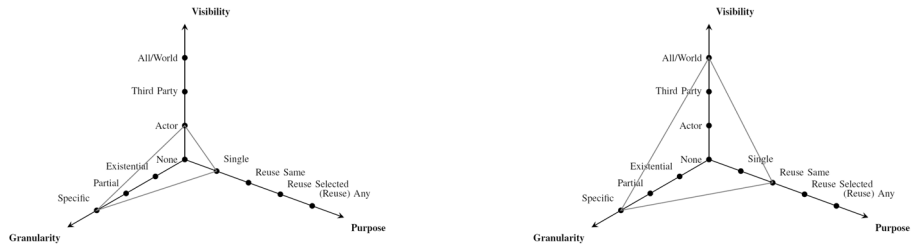
Gao et al. (2018)

The work describes a payment mechanism for peer-to-peer EV charging and covers the billing use case (UC 3). One car acts as the payee (CS and CSO in standardized notation) and another car acts as the payer (EV). The scheme uses a trusted third party, which acts like an eMSP and a blockchain for financial transactions.

The communication flow consists of the following steps:

1. The EV registers at the eMSP and provides its personal data (including verifying legal document, e.g., driver's license). The registration can be performed with multiple accounts which are signed by the eMSP.
2. When peer-to-peer charging is performed, the CS (another EV with spare battery capacity) provides an offer and its account number, which is sent directly to the EV.
3. The EV creates a blockchain transaction and initiates payment from the EV's account to the CS's account.
4. Once the payment is processed the transaction ID is sent to the CS directly to prove payment. The CS verifies the transactions and proceeds with the charging process.

In Fig. 8, all direct and indirect private data items are depicted. Personal data is handed to the eMSP during the registration process. This specific data is thus visible to the eMSP only and used for a single purpose. The account used for the payment on the blockchain is visible to all other actors in the ecosystem. The account can be reused multiple times and is directly related to one specific EV. Gao et al. (2018) point out that a new account can be used for each transaction, which enhances privacy.



Max. collusion set	eMSP	CS / CSO	EV
Collusion set 1			

Fig. 8 Privacy dimensions and collusion sets for Gao et al. (2018) for data items (i) personal data (left) and (ii) account (right). Collusion sets 1 refers to the mapping between accounts and the EV's identity. It is apparent that the collusion set is limited to the CS and the CSO and thus very small

Collusion set 1 consists of the CS and CSO. If the CS colludes with either the eMSP or the EV, the mapping between the EV and the account is revealed.

Mustafa et al. (2015)

The authors present a solution for EV charging with roaming (covering UC 8). The approach is based on a set of pseudonyms generated by the eMSP and shared with the EV. These pseudonyms are used by the EV to identify itself at remote CS. After remote charging, the CSO performs a balancing with the eMSP using the pseudonym.

The communication flow consists of the following steps:

1 The EV registers at the eMSP with its personal data. The eMSP generates a set of *pseudonyms* that are used in the subsequent steps.
2 For charging, the EV connects to a CS and sends one of its *pseudonyms*. The CS responds with a *charging time and price*, which agreed up by the EV.
3 The CS forwards this request to the CSO, which further forwards it to the eMSP. The eMSP may *grant or reject* this request given the account balance of the user.
4 If the request is granted, the EV and CS agree on the *charging parameters*.
5 After completing the charging process, the CS sends the *consumption report* to CSO which forwards it to eMSP.
6 The eMSP adjusts the account balance of the user.
7 The eMSP pays the CSO with the *pseudonym* as a reference.

The original paper distinguishes between additional actors, e.g., a tamper-proof smart card that is associated with each user. In this paper, we use the actors from Section Electric Vehicle Ecosystem, without loss of generality. Similarly, the original paper allows multiple users to share an EV. With regards to privacy, however, this additional feature does not impact the analysis and is therefore conducted for the case of one single user (which is identified by an individual smart card).

In Fig. 9, all direct and indirect private data items are depicted. The pseudonym is used by multiple parties for a single purpose and is linked to one specific EV. Both, charging time and price as well as the consumption report are reused for multiple purposes by multiple actors and contain specific information. The information whether charging is

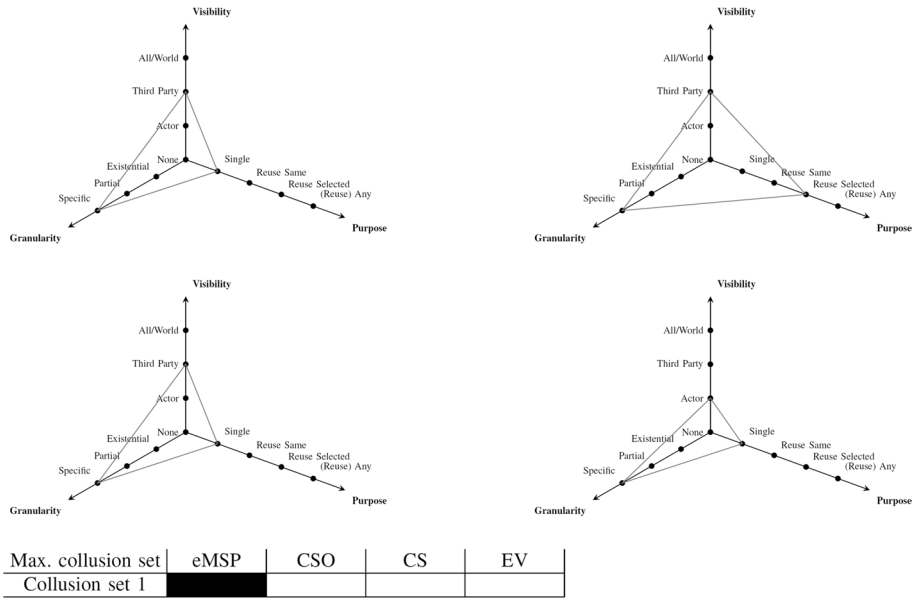


Fig. 9 Privacy dimensions and collusion sets for (Mustafa et al. 2015) for data items (i) pseudonym (top left), (ii) charging time and price/consumption report (top right), (iii) grant or reject (bottom left), and (iv) charging parameters (bottom right). Collusion set 1 refers to the mapping between pseudonyms and the EV's identity

granted or rejected by the eMSP has a single purpose and is shared by two actors, the eMSP and the CSO. This information is considered specific, since the eMSP can link this information to a particular EV. The charging parameters are used for a single purpose by a single actor and contain specific information.

In addition, information not explicitly mentioned in the steps above can be learned: The CS learns the pseudonym of the EV, but cannot link this information to one particular EV across multiple charging instances. The CSO is able to learn the location of the EV during the charging process, albeit with the same restrictions.

The eMSP initially created the pseudonym and is the only party that can link the EV to this information. If it colludes with any other party, these parties can also link the pseudonym to the EV and thus learn about the EV's behavior.

Privacy evaluation overview

We summarize the results in Table 3 and point out shortcomings related to privacy preservation.

Recommendations and future directions

In this section, we summarize our findings from the analyzed papers. First, we provide a list of recommendations based on our findings. Second, we point to future directions in the field of privacy-preserving electric vehicle charging.

Recommendations

We make four key observations with respective recommendation on the analyzed literature:

Table 3 Privacy evaluation overview: The papers and their corresponding privacy-relevant properties are listed, e.g., which personal data they treat

Paper	Use cases	Actors	Personal data	Techniques	Privacy breaches[a]	Features	Properties	Analyzed
Li et al. (2014)	Registration, Authorization	eMSP, CSO, CS, EV	Personal data, time, EV's location, charging parameters, amount of charged energy, aggregated energy	Public Key Infrastructure (PKI), one-day use pseudonym, one-day use session keys	(i) Identification of vehicle and exchange of personal data, (ii) Pseudonymous identification via unique token	Dynamic contactless charging, anonymous authentication and charging	Anonymity, pseudonymity, unlinkability (as long as only CSO, CS collude)	✓
Gao et al. (2018)	Registration, Billing	eMSP, CS, EV	Personal data, accounts	Blockchain, PKI	(i) Identification of vehicle and exchange of personal data, (ii) Pseudonymous identification via unique token	Peer-to-peer charging, the CSO and the CS play as one entity	Anonymity, pseudonymity (as long as no actors collude)	✓
Mustafa et al. (2015)	Registration, Authorization, Billing, Roaming	eMSP, CSO, CS, EV	Personal data, Charging Time slot (CTS), price, charging grant or rejection, consumption report, charging parameters	Predistributed sets of pseudonymous, tamper-proof smart cards, digital signature, PKI	(i) Identification of vehicle and exchange of personal data	Two-factor authentication, a multi-user EV charging is supported	Anonymity, pseudonymity, unlinkability (as long as no actors collude)	✓
Portela et al. (2013)	Authorization, Smart charging	DSO, eMSP, CSO, CS, EV	ID of EV user, one time charging session ID, SoC, requested amount of kilometers or energy, time of departure.	Methods: minimize, separate, aggregate, and hide one-time session key	(iii) De-pseudonymization due to data exchange, (iv)Fingerprinting of the EV, (v) Profiling with smart charging	The location remains hidden for the eMSP, the CSO cannot connect profiles of the same EV user due to one-time charging session ID	Anonymity, pseudonymity, unlinkability (as long as no actors collude)	
Rabieh and Aydogan (2019)	Registration, Authorization, Reservation	eMSP, CSO, CS, EV	Personal data, EV's data, EV's group, CTS, charging parameters	K-times anonymous authentication, one-time session key, blind signature, PKI	(i) Identification of vehicle and exchange of personal data	Anonymous authentication and charging, fair reservation mechanism	Anonymity, pseudonymity, unlinkability (as long as only CSO, CS collude)	
Gabay et al. (2019)	Registration, Authorization, Billing, Reservation	eMSP, CS, EV	Personal data, EV's data, CTS, charging station, charging fees	Zero Knowledge Proofs, blockchain smart contracts (Ethereum), pseudonymous addresses	(i) Identification of vehicle and exchange of personal data	The eMSP plays a role of the CSO as well, anonymous authentication and charging via one charging use addresses	Anonymity, pseudonymity, unlinkability (as long as only eMSP, CS collude)	

The *Analyzed* column states whether the respective paper is analyzed in detail in our paper

[a] According to the privacy breaches identified in Section Privacy Analysis

(i) **Consider collusion sets** Most papers use some sort of pseudonymization in establishing the communication among the different actors of EV ecosystem. While this preserves the privacy in the short term between parties, it only works securely as long as actors do not collude. As soon as the actor can resolve the pseudonym to personally identifiable information colludes with another actor, the privacy is broken. Thus, we recommend that collusion sets are considered when analyzing privacy guarantees. Examples for this type of analysis are provided above for multiple use case implementations.

(ii) **Consider patterns** All papers analyze privacy of single data items only. They neglect that patterns in (pseudonymized or even encrypted) data might reveal information about behavior and therefore are a potential risk for privacy. Thus, we recommend to consider which information can be extracted from communication and other patterns beyond single messages or data items.

(iii) **Consider use cases** Although there is much work about privacy-preserving frameworks and protocols, all of them focus only on a subset of UC. There is no work that covers UCs which process private data of the entire EV ecosystem, especially the registration UC. In particular, there is no work specializing on the registration use case, which initially stores and reveals personal data to the eMSP or any other trusted authority.

(iv) **Avoid trusted entities** In most of the literature on EV charging, entities or parties exist which are considered trustworthy. While this reduces the complexity and simplifies protection mechanisms, assumptions about trusted parties might not hold up in practice. Extensive use of trusted parties is a sign that some privacy aspects cannot be addressed by a use case implementation and that privacy relies solely on the trustworthiness assumption holding. To avoid this single point of failure, we recommend to use trusted parties either not at all, if possible, or in a minimalistic way, i.e., to use only one trusted party that is realistically trustworthy also in practice. To avoid further trusted entities, we recommend using privacy-enhancing technologies, see, e.g., (Unterweger et al. 2016; Knirsch et al. 2017; Erkin 2015).

(v) **Standardize** There is a lack of privacy and security standards and legal provisions for e-mobility. It is not specified which information should be communicated and which security standards need to be met in order to preserve privacy. There is currently no comprehensive legal framework in place to address all these issues. Therefore, we recommend a clear legal framework for all potential market participants to be put in place.

Future directions

Finally, we want to point out future research directions to improve the privacy guarantees of EVs charging approaches:

(i) **Use standardized names for actors** During our analysis, we found that nearly all actors or entities have different names in different papers and are sometimes combined or split. This makes comparisons of different papers hard. It would therefore be desirable if all papers used common and standardized names for their actors or clarified how their actors differ from such a standard. This paper proposes a nam-

ing example based on existing work and standards that can be used for this purpose (see Section Main Actors).

(ii) **Use a common methodology for analyzing privacy** Every paper uses slightly different methods to analyze the privacy of its proposed approach. This makes it not only hard to compare different approaches, but also hides many implicit assumptions like threat models and trusted actors. It would be desirable if all papers used one common methodology for their privacy analysis. One such methodology has been proposed in this paper. If more papers used a common methodology, they would be easier to compare, which would also make it easier to decision makers to choose an privacy-preserving EVs charging approach for implementing it in the real world.

Conclusion

This paper provided an overview of the electric vehicle charging ecosystem and its literature as well as a detailed analysis of the privacy guarantees of three representative approaches from literature for the privacy-relevant use cases. While privacy preservation is considered in all of the analyzed papers, their guarantees differ significantly, especially when considering collusion sets, where one actor who shares information with just one other actor can breach privacy completely. Similarly, patterns exposing behavioral information remain largely unconsidered in the papers and trusted parties are often used to conceal shortcomings in privacy-related implementation details. To mitigate this and to make comparisons between different approaches easier, we recommend to use a common naming convention and methodology to analyze privacy as well as to establish common standards. Common standards are desirable to enable improved as well as easier-to-understand and easier-to-compare privacy guarantees in electric vehicle charging approaches in the future.

Appendix

Data items in protocols

Data included in the RFID-card:

- Contract ID: it represents the UID of the EV user's contract. It is specified by ISO/IEC 15118 standard and depicted by alphanumeric characters.
- Token ID: it represents the UID of the user as a plain text (alphanumeric characters as well) or as a hexadecimal hash value. It is connected by many to one (M:1) relationship with the contract ID.
- Provider ID: it represent the UID of the eMSP. It is three alphanumeric characters.
- Date of expiry

EV's data:

- Vehicle inlets
- Maximum charging power

- Minimum charging power
- SoC
- Battery capacity

Personal Data:

- First name, surname, date of birth, and telephone numbers
- Address, postal code, and country
- Car data: brand, model and registration
- Contract details
- Access to home charging point

Charging preferences of an EV (user):

- Current SoC
- Expected arrival time
- Expected departure time
- Amount of required energy/number of kilometers

Abbreviations

API: Application programming interface; CDRInfo: Charge details records; CHO: Clearing house operator; CP: Charging point; CS: Charging station; CSMS: Charging Station Managment System; CSO: Charging Station Operator; CTS: Charging Time Slot; DSO: Distribution System Operator; eMIP: eMobility Protocol Inter-Operation; EMSA: E-Mobility Systems Architecture; eMSP: E-Mobility Service Provider; ES: Energy Supplier; EV: Electric Vehicle; EVSE: Electrical Vehicle Supply Equipment; ICT: Information and Communication Technology; ID: Identifier; ID: Identifiers; GDPR: General Data Protection Regulation; G2V: Grid-to-Vehicle; NSP: Navigation Service Provider; OCHP: Open Clearing House Protocol; OCPP: Open Charge Point Protocol; OCPI: Open Charge Point Interface protocol; OICP: Open InterCharge Protocol; OSCP: Open Smart Charging Protocol; PKI: Public Key Infrastructure; POI: POint Information; PSO: Parking Spot Operator; RSU: Road Side Unit; SoC: State of Charge; UC: Use Case; UID: Unified Identifier; UID: Unified Identifiers; V2G: Vehicle-to-Grid.

Acknowledgements

Not applicable.

Author contributions

FK, AU, DM and AA contributed equally to the paper, i.e., the main manuscript text, figures and related research. DE and HdM reviewed the manuscript and provided valuable feedback. All authors read and approved the final manuscript.

Authors' information

Andreas Unterweger is a senior post-doctoral researcher at the Center for Secure Energy Informatics at the Salzburg University of Applied Sciences. He holds a Ph.D. degree in Computer Science. He has published extensively about privacy in energy systems (https://scholar.google.de/citations?user=twhO16AAAAAJ&hl=en).
Fabian Knirsch is a senior post-doctoral researcher at the Center for Secure Energy Informatics at the Salzburg University of Applied Sciences. He holds a Ph.D. degree in Computer Science. He has published extensively about privacy in energy systems (https://scholar.google.de/citations?user=Sw3JdwsAAAAJ&hl=en).
Dominik Engel is the head of the Center for Secure Energy Informatics at the Salzburg University of Applied Sciences. He holds a Ph.D. degree in Computer Science. He advises Ph.D. students at the Department of Computer Sciences at the University of Salzburg. He has published extensively about privacy and security in energy systems (https://scholar.google.de/citations?user=vbczhIkAAAAJ&hl=en).
Daria Musikhina is a doctoral researcher at the Chair of Computer Networks and Computer Communications at the Faculty of Computer Science and Mathematics at the University of Passau. She holds two Master's degrees in Informatics.
Ammar Alyousef was a post-doctoral researcher at the Chair of Computer Networks and Computer Communications at the Faculty of Computer Science and Mathematics at the University of Passau, and he is now a Software Engineer and smart charging expert at TMH. He holds a Ph.D. degree in Computer Science. He has published about electric vehicle charging and related topics (https://scholar.google.com/citations?user=hm3NEZkAAAAJ&hl=de).
Hermann de Meer is the head of the Chair of Computer Networks and Computer Communications at the Faculty of Computer Science and Mathematics at the University of Passau, where he also advises Ph.D. students. He has published extensively about electric vehicle charging and related topics (https://scholar.google.de/citations?hl=en&user=ER_fzE8AAAAJ).

Funding
The financial support by the Federal State of Salzburg is gratefully acknowledged. This work is supported by the Bavarian Ministry of Economic Affairs, Regional Development and Energy and by the Zentrum Digitalisierung Bayern within the projects "Energy Management System for Integrated Business Models" (EMSIG) and "Internetkompetenzzentrum Ostbayern" (IKZO).

Availability of data and materials
Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Center for Secure Energy Informatics, Salzburg University of Applied Sciences, Puch bei Hallein, Austria. [2]Faculty of Computer Science and Mathematics, University of Passau, Passau, Germany.

Received: 22 March 2022 Accepted: 19 April 2022
Published online: 28 April 2022

References

Abdallah A, Shen X (2017) Lightweight authentication and privacy-preserving scheme for V2G connections. IEEE Trans Veh Technol 66(3):2615–2629. https://doi.org/10.1109/TVT.2016.2577018

Alyousef A (2021) E-mobility management: towards a grid-friendly smart charging solution. PhD thesis, Universität Passau

Alyousef A, de Meer H (2019) Design of a tcp-like smart charging controller for power quality in electrical distribution systems. In: Proceedings of the Tenth ACM International Conference on Future Energy Systems, pp 128–138. ACM, New York, NY, USA. https://doi.org/10.1145/3307772.3328293

Alyousef A, Danner D, Kupzog F, de Meer H (2018) Enhancing power quality in electrical distribution systems using a smart charging architecture. Energy Inf 1(1):127

Au MH, Liu JK, Fang J, Jiang ZL, Susilo W, Zhou J (2014) A new payment system for enhancing location privacy of electric vehicles. IEEE Trans Veh Technol 63(1):3–18. https://doi.org/10.1109/TVT.2013.2274288

Barker A (2016) NIST Special Publication 800-57: Recommendation for Key Management - Part 1: General (Revised). NIST. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

Barker K, Askari M, Banerjee M, Ghazinour K, MacKas B, Majedi M, Pun S, Williams A (2009) A Data Privacy Taxonomy. In: Saxton AP (ed) Dataspace: The Final Frontier: 26th British National Conference on Databases, BNCOD 26, Birmingham, UK, July 7–9, 2009. Proceedings, pp 42–54. Springer, Berlin Heidelberg. https://doi.org/10.1007/978-3-642-02843-4_7

Boucetta M, Ibne Hossain NU, Jaradat R, Keating C, Tazzit S, Nagahi M (2021) The architecture design of electrical vehicle infrastructure using viable system model approach. Systems 9(1):19

Capros P, Kannavou M, Evangelopoulou S, Petropoulos A, Siskos P, Tasios N, Zazias G, DeVita A (2018) Outlook of the EU energy system up to 2050: the case of scenarios prepared for European Commission's "clean energy for all Europeans" package using the primes model. Energ Strat Rev 22:255–263

Chen J, Zhang Y, Su W (2015) An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-grid (v2g) networks. China Commun 12(3):9–19. https://doi.org/10.1109/CC.2015.7084359

Delgado J, Faria R, Moura P, de Almeida AT (2018) Impacts of plug-in electric vehicles in the Portuguese electrical grid. Transp Res Part D 62:372–385

Eiza MH, Shi Q, Marnerides AK, Owens T (2019) Efficient, secure, and privacy-preserving PMIPv6 protocol for V2G networks. IEEE Trans Veh Technol 68(1):19–33. https://doi.org/10.1109/TVT.2018.2880834

Erkin Z (2015) Private data aggregation with groups for smart grids in a dynamic setting using crt. In: 2015 IEEE international workshop on information forensics and security (WIFS), pp 1–6. IEEE, New York City, USA. https://doi.org/10.1109/WIFS.2015.7368584

European Parliament and Council of the European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Ferrag MA, Maglaras LA, Janicke H, Jiang J, Shu L (2018) A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustain Cities Soc 38:806–835. https://doi.org/10.1016/j.scs.2017.12.041

Gabay D, Akkaya K, Cebe M (2019) A privacy framework for charging connected electric vehicles using blockchain and zero knowledge proofs. In: 2019 IEEE 44th LCN symposium on emerging topics in networking (LCN Symposium), pp 66–73. IEEE, New York City, USA. https://doi.org/10.1109/LCNSymposium47956.2019.9000682

Gao F, Zhu L, Shen M, Sharif K, Wan Z, Ren K (2018) A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Netw 32(6):184–192. https://doi.org/10.1109/MNET.2018.1700269
Goldreich O (2004) Foundations of cryptography: basic applications, vol 2. Cambridge University Press, New York
Gunukula S, Sherif AB, Pazos-Revilla M, Ausby B, Mahmoud M, Shen X (2017) Efficient scheme for secure and privacy-preserving electric vehicle dynamic charging system. In: 2017 IEEE international conference on communications (ICC), pp 1–6. IEEE, New York City, USA. https://doi.org/10.1109/ICC.2017.7997252
Han W, Xiao Y (2016) IP2DM: integrated privacy-preserving data management architecture for smart grid V2G networks. Wirel Commun Mob Comput 16(17):2956–2974. https://doi.org/10.1002/wcm.2740
Han W, Xiao Y (2016) Privacy preservation for v2g networks in smart grid: a survey. Comput Commun 91–92:17–28. https://doi.org/10.1016/j.comcom.2016.06.006
Han S, Topcu U, Pappas GJ (2014) Differentially private distributed protocol for electric vehicle charging. In: 52nd annual allerton conference on communication, control, and computing (Allerton), New York City, USA
Hubject: Open InterCharge Protocol for Emobility Service Provider. Technical report, Hubject GmbH (2016). https://www.hubject.com/wp-content/uploads/2016/06/OICP-2.1_Release-14.1_EMP_final.pdf
Kirpes B, Danner P, Basmadjian R, De Meer H, Becker C (2019) E-mobility systems architecture: a model-based framework for managing complexity and interoperability. Energy Inf 2(1):15
Knirsch F (2017) Privacy enhancing technologies in the smart grid user domain. it - Inf Technol 1(59):13–22
Knirsch F, Engel D, Frincu M, Prasanna V (2015) Model Based Assessment for Balancing Privacy Requirements and Operational Capabilities in the Smart Grid. In: Proceedings of the 6th Conference on Innovative Smart Grid Technologies (ISGT2015), pp. 1–5. Innovative Smart Grid Technologies Conference (ISGT), 2015 IEEE Power and Energy Society, Washington, D.C., USA
Knirsch F, Engel D, Neureiter C, Frincu M, Prasanna V (2015) Model-driven Privacy Assessment in the Smart Grid. 1st international conference on information systems security and privacy (ICISSP). IEEE, Angers, France, pp 173–181
Knirsch F, Eibl G, Engel D (2017) Multi-resolution privacy-enhancing technologies for smart metering. EURASIP J Inf Secur 1:1–13. https://doi.org/10.1186/s13635-017-0058-3
Knirsch F, Unterweger A, Engel D (2018) Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. J Comput Sci 33(1):71–79
Langer L, Skopik F, Kienesberger G, Li Q (2013) Privacy issues of smart e-mobility. In: 39th annual conference of the IEEE industrial electronics society, IECON 2013, pp 6682–6687. IEEE, New York City, USA . https://doi.org/10.1109/IECON.2013.6700238
Leviäkangas P, Kinnunen T, Kess P et al (2014) The electric vehicles ecosystem model: construct, analysis and identification of key challenges. Manag Glob Trans 12(3):1–9
Li D, Yang Q, An D, Yu W, Yang X, Fu X (2019) On location privacy-preserving online double auction for electric vehicles in microgrids. IEEE Internet Things J 6(4):5902–5915. https://doi.org/10.1109/JIOT.2018.2872444
Li H, Dán G (2014) Nahrstedt K Portunes: privacy-preserving fast authentication for dynamic electric vehicle charging. In: 2014 IEEE international conference on smart grid communications (SmartGridComm). IEEE, Venice, Italy, pp 920–925
Liu H, Ning H, Zhang Y, Yang LT (2012) Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid. IEEE Trans Smart Grid 3(4):1722–1733. https://doi.org/10.1109/TSG.2012.2212730
Liu JK, Susilo W, Yuen TH, Au MH, Fang J, Jiang ZL, Zhou J (2016) Efficient privacy-preserving charging station reservation system for electric vehicles. Comput J 59(7):1040–1053. https://doi.org/10.1093/comjnl/bxv117
Ma Z, Christensen K, Jørgensen BN (2021) Business ecosystem architecture development: a case study of electric vehicle home charging. Energy Inf 4(1):1–37
Manbachi M, Sadu A, Farhangi H, Monti A, Palizban A, Ponci F, Arzanpour S (2016) Impact of EV penetration on volt-var optimization of distribution networks using real-time co-simulation monitoring platform. Appl Energy 169:28–39
McKenna E, Richardson I, Thomson M (2012) Smart meter data: balancing consumer privacy concerns with legitimate applications. Energy Policy 41:807–814. https://doi.org/10.1016/j.enpol.2011.11.049
Mustafa MA, Zhang N, Kalogridis G, Fan Z (2015) Roaming electric vehicle charging and billing: an anonymous multi-user protocol. In: 2014 IEEE international conference on smart grid communications, SmartGridComm 2014, pp 939–945. IEEE, New York City, USA. https://doi.org/10.1109/SmartGridComm.2014.7007769
Nahapiet M (2017) EV related protocol overview v1.0. Technical report, ElaadNL, The Netherlands, Arnhem. https://www.elaad.nl/uploads/files/EV_related_protocol_study_v1.1.pdf
Nicanfar H, Hosseininezhad S, TalebiFard P, Leung VC, (2013) Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations. In: Proceedings IEEE INFOCOM. IEEE, New York City, pp 3429–3434
OCPI Nederland: OCPI: Open Charge Point Interface 2.2. Technical report, NKL - EVRoaming Foundation (2020). https://evroaming.org/app/uploads/2020/06/OCPI-2.2-d2.pdf
Pazos-Revilla M, Alsharif A, Gunukula S, Guo TN, Mahmoud M, Shen X (2018) Secure and privacy-preserving physical-layer-assisted scheme for EV dynamic charging system. IEEE Trans Veh Technol 67(4):3304–3318. https://doi.org/10.1109/TVT.2017.2780179
Pfitzmann A, Hansen M (2010) A terminology for talking about privacy by data minimization: anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml%5Cnhttp://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf
Portela CM, Geldtmeijer D, Slootweg H, Van Eekelen M (2013) A flexible and privacy friendly ict architecture for smart charging of evs. In: 22nd international conference and exhibition on electricity distribution (CIRED 2013), pp 1–4. IEEE, New York City, USA. https://doi.org/10.1049/cp.2013.0605
Portela CM, Klapwijk P, Verheijen L, De Boer H, Slootweg H, Van Eekelen M (2015) Oscp-an open protocol for smart charging of electric vehicles. In: Proceedings of the 23rd international conference on electricity distribution (CIRED), pp. 1–5. CIRED, Lyon, France
Rabieh K, Aydogan AF (2019) A fair and privacy-preserving reservation scheme for charging electric vehicles. In: 2019 international symposium on networks. Computers and Communications (ISNCC). IEEE, New York City, USA, pp 1–6

Rabieh K, Wei M (2017) Efficient and privacy-aware authentication scheme for EVS pre-paid wireless charging services. In: 2017 IEEE international conference on communications (ICC). IEEE, New York City, USA, pp 1–6
Radi EM, Lasla N, Bakiras S, Mahmoud M (2019) Privacy-preserving electric vehicle charging for peer-to-peer energy trading ecosystems. In: IEEE international conference on communications. https://doi.org/10.1109/ICC.2019.8761788
Rives J-M (2016) eMIP Protocol - Protocol Description. https://www.gireve.com/wp-content/uploads/2019/10/Gireve_Tech_eMIP-V0.7.4_ImplementationGuide_1.0.7_en.pdf
Rottondi C, Fontana S, Verticale G (2014) Enabling privacy in vehicle-to-grid interactions for battery recharging. Energies 7(5):2780–2798. https://doi.org/10.3390/en7052780
Saxena N, Choi BJ (2016) Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks. IEEE Trans Inf Forensics Secur 11(7):1438–1452. https://doi.org/10.1109/TIFS.2016.2532840
Saxena N, Grijalva S, Chukwuka V, Vasilakos AV (2017) Network security and privacy challenges in smart vehicle-to-grid. IEEE Wirel Commun 24(4):88–98. https://doi.org/10.1109/MWC.2016.1600039WC
Schmutzler J, Andersen CA, Wietfeld C (2013) Evaluation of OCPP and IEC 61850 for smart charging electric vehicles. In: 2013 world electric vehicle symposium and exhibition (EVS27), pp 1–12. IEEE, New York City, USA . https://doi.org/10.1109/EVS.2013.6914751.http://ieeexplore.ieee.org/document/6914751/
Sombroek V (2014) OCHP: open clearing house protocol. http://www.ochp.eu/wp-content/uploads/2013/12/130425_Open-Clearing-House-Protocol_v0_2_0.9.pdf
Tseng H-R, (2012) A secure and privacy-preserving communication protocol for v2g networks. In: IEEE wireless communications and networking conference (WCNC). IEEE, New York City, USA, pp 2706–2711
Unterweger A, Knirsch F, Eibl G (2016) Privacy-preserving load profile matching for tariff decisions in smart grids. EURASIP J Inf Secur 1:1–17. https://doi.org/10.1186/s13635-016-0044-1
Unterweger A, Taheri-Boshrooyeh S, Eibl G, Knirsch F, Küpçü A, Engel D (2019) Understanding game-based privacy proofs for energy consumption aggregation protocols. IEEE Trans Smart Grid 10(5):5514–5523. https://doi.org/10.1109/TSG.2018.2883951
Wang H, Qin B, Wu Q, Xu L, Domingo-Ferrer J (2015) TPP: traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids. IEEE Trans Inf Forensics Secur 10(11):2340–2351. https://doi.org/10.1109/TIFS.2015.2455513
Xiang Q, Kong L, Liu X, Xu J, Wang W (2016) Auc2reserve: a differentially private auction for electric vehicle fast charging reservation. 2016 IEEE 22nd international conference on embedded and real-time computing systems and applications (RTCSA). IEEE, New York City, USA, pp 85–94
Yang Z, Yu S, Lou W, Liu C (2011) P2: privacy-preserving communication and precise reward architecture for V2G networks in smart grid. IEEE Trans Smart Grid 2(4):697–706. https://doi.org/10.1109/TSG.2011.2140343
Zhao T, Chen C, Wei L, Yu M (2014) An anonymous payment system to protect the privacy of electric vehicles, pp 1–6. IEEE, New York City, USA

Publisher's Note