2015 Euromicro Conference on Digital System Design

Consumer-centric and Service-oriented Architecture for the Envisioned Energy Internet

Søren Aagaard Mikkelsen and Rune Hylsberg Jacobsen
{smik,rhj}@eng.au.dk
Department of Engineering, Aarhus University

***Abstract*—The Energy Internet is the vision of performing intelligent automation in the smart grid using Internet-based technologies. This vision complies with embracing the residential domain into the smart grid, since it facilitates the reuse of the existing Internet connection in the home. Stakeholders such as Energy Service Companys (ESCOs) and Distribution System Operators (DSOs) can then acquire meter data from residential homes, where the residential consumer can gain potential cost savings by using their services. However, residential consumers have concerns about their privacy when metering devices monitor home appliance usage that potentially can reveal their habits without their consent. This paper discusses architectural design challenges and presents a consumer-centric system architecture with incentives for the residential consumers, ESCOs and the DSOs to participate. The architecture is based on a Service-Oriented Architecture (SOA) using web services that follow the Representational State Transfer (REST) architectural style. The ESCOs provide intelligent automation through home-oriented and grid-oriented web services that optimise for the residential home and DSO, respectively. The consumer can control the privacy enforcement through a Home Energy Management System (HEMS) that negotiates the information content of the meter data with a management entity in the cloud. OAuth 2.0 is adapted for the consumer to authorise web services to access meter data from the management entity.**

***Keywords*-smart grid, data privacy, web services**

I. Introduction

The residential domain has been estimated to be responsible for 28% of the global electric energy consumption [1] and therefore represents a great potential for reducing CO_2 emissions. This has resulted in that DSOs have deployed smart meters and Internet of Things (IoT) companies have established a position in residential market with focus on home automation for energy efficiency based on meter data. On one hand, residential consumers (RCs) who grant access to their meter data can benefit from gaining knowledge about the energy usage and get recommendations for potential cost savings through DSOs' and ESCOs' analytics tools. On the other hand, data sent to the ESCO or DSO can reveal personal information about the residents' behaviour.

For getting the RC engaged in the smart grid, it is necessary to have a consumer-centric system architecture. A system that collects near real-time data from smart meters and smart devices, must allow full consumer control of the information disclosed from the residential home.

By using recent advances in Internet technology, this paper presents a consumer-centric and SOA that embraces the RCs, the ESCOs and the DSO. This solution forms a *Energy Internet* [2] and is based on having RESTful Home-oriented Services (HoSs) and Grid-oriented Services (GoSs) deployed in the cloud. The privacy of the RC is enforced at two stages. First stage includes a HEMS that acquired meter data in the Home Area Network (HAN). The information from meter data is negotiated between a home agent and a grid agent located on the HEMS and in the Management Services (MS), respectively. Data stored in the MS can be accessed by ESCOs and the DSO through a Authentication & Authorisation Service (AAS) using OAuth 2.0 (OAuth2).

The paper is structured as follows. Section II presents the related work. Section III argues about challenges and goals we believe the consumer has. Afterward, it gives a conceptual view of our proposed architecture with focus on the protocols that send sensitive information. Section IV gives a comparative evaluation of the architecture. The conclusion and the future work are presented in Section V.

II. Related Work

Gustavsson [3] presented one of the first smart grid architectures using agent-based systems. The load management in their system is based on negotiating device agents, service agents, and utility agents. These concepts are reused by Fhom [4]. Their architecture has a comprehensive virtualized multi-agent platform targeting the smart meter that incorporated Privacy Enhancing Technologies (PETs). Instead of the stakeholders' individual goals, [5] addresses the cohesion. They present a plugin-based middleware communication bus for supporting the diversity of home automation protocols. Others [6], [7] take advantages of the inherent ability of a SOA to support multiple business cases. For a thorough review on Multi-Agent System (MAS) and SOA the reader is referred to [8].

Privacy issues have been previously studied in cloud-based smart grid architectures [9], [10], [11], [4], [12]. Recently, the focus have been intensified with usage of a cloud infrastructure as a platform for storing data and providing services [13]. The authors in [14] provide six privacy practices for developers to follow when designing cloud-based architectures for the smart grid. The research presented in [10] introduces a personal cloud for a virtual home in a consumer-centric architecture. Service providers are able to access the data through privacy mechanisms (e.g. aggregation), whereas the DSO can access the raw data in the database. However, in this architecture the Infrastructure as a Service provider become a trusted party.

978-1-4673-8035-5/15 $31.00 © 2015 IEEE
DOI 10.1109/DSD.2015.50

This encompasses some risks since the physical location of data is not constrained to a fixed location. Uncertainty about the physical location of the data enhances the risk for exposure.

In our proposed architecture the meter data are physically stored in the residential homes and are in control of residents. The architecture combines a MAS and an Internet-based SOA by using software agents to provide individualised privacy enhancements, while supporting interoperability and multiple business cases for the other stakeholders.

III. Architecture

A. Design Challenges

To generate a future-proof solution, an architecture must permit for changeable business cases [15]. It is especially important if the market penetration should depend on the consumer's acceptance of the system and not on public support or demand. For instance, the European Directive 2009/72/EC [16] demanded the deployment of smart meters should cover at least 80% of all consumers by 2020. A similar strategy for embracing the residential domain is hard to imagine for at least two reasons:

- Demand response of home appliances has not been considered as a part of the electrical system until recently. International standards exist, however it is still uncertain how the current smart home appliances should adapt to them. In contrast, smart metering systems have gone through a lot of standardisation effort on an international scale, thus creating well-defined interfaces for metering companies.
- The lifetime of home appliances varies much more than smart meters. The transition between a "non-intelligent" home appliance and an intelligent home appliance might be long. Consumers cannot be enforced to upgrade their equipment without compensation. A smart meter has an expected lifetime of 15-20 years and is owned by the DSO.

Current trends in IoT [2] show that ubiquity and interconnection between consumer devices are predominant factors for success. Today, it is possible to have high computational power, support for multiple networking protocols and have a large data storage on small embedded devices. This enables them to act autonomously without forwarding operations to more powerful devices. The consumer will be able to delegate objectives to these devices with minimum support. In some situations, it might actually be unfeasible with human assistance, e.g. if a heat pump should follow an indoor climate strategy based on price policy. Furthermore, in order to operate the electric grid based on meter data from residential homes, it is necessary to do calculations on assembled data sets that are associated to the same nodes in the electric grid (feeder, substation, etc.). The trends show that a cloud platform seems to be the most feasible choice, because of its capabilities of being scalable, shareable, flexible and reliable [17].

The consumer's expectations and concerns are key-factors for a successful deployment. Many consumers have little or no notion about what the smart grid is [18]. This insecurity is further intensified by the uncertainty about data security and privacy protection [11]. Hence, we believe that a simple system where the consumer is in control of his data delegation, will provide a more trustworthy solution.

B. Assumptions and Goals

The overarching goal of the presented system is two-fold. From the DSO side it is to perform global intelligent automation to optimise the stability and life expectancy of the electric grid. From the residential side it is to take advantage of global intelligent automation and perform intelligent automation with the aim to minimise the energy costs and energy usage for the RC. For fulfilling this goal, the proposed system architecture is based on the assumption that the RC is the key enabler for facilitating this [19]. From the consumer's point of view, we believe that the consumers would like to have the following:

- **Portability**: The liberty to choose ESCOs for handling data storage and processing.
- **Adaptability**: The possibility to participate voluntarily in adapting their energy usage to more preferable times.
- **Privacy**: The choice in choosing the desired level of privacy and the control of the physical location where their data are stored.
- **Opt-out**: An easy way for opting out of the contract to the DSO and ESCO, if they do not want to participate.
- **Autonomy**: A system that requires minimal of effort for participating.

To create a market which is profitable for the DSO, ESCO and the RCs require further considerations. There are still uncertainties on how other energy technologies will emerge and support the operation of the smart grid on a residential level. For instance, what will be the market penetration of electric vehicles, solar panels, residential batteries and windmills in future? Before technologies mature, it is difficult to believe in a market which embraces the residential domain will be initiated by DSOs. Therefore, it is necessary to have a system architecture that allows for new markets to emerge, but also support the transition in between them.

C. System Model

The system model, presented in Fig. 1, encompasses a HEMS that uses the existing Internet connection in the residential home and a number of web services in the cloud. All services are based on the *separations of concerns principle* where the services can be assembled dynamically. To ensure reusability and connectivity, the system adapts to the REST [20] architectural style. It provides a homogeneous and stateless interface for all services.

Services associated with the optimisation of each residential home are called *home-oriented*, while services associated with the optimisation of the electric grid are called *grid-oriented*. In contrast to other system models, our proposed model is constructed without a *trusted* data aggregator [21]. Aggregating systems are typically created around trusted subsystems that negotiate on behalf of a group of residential homes and

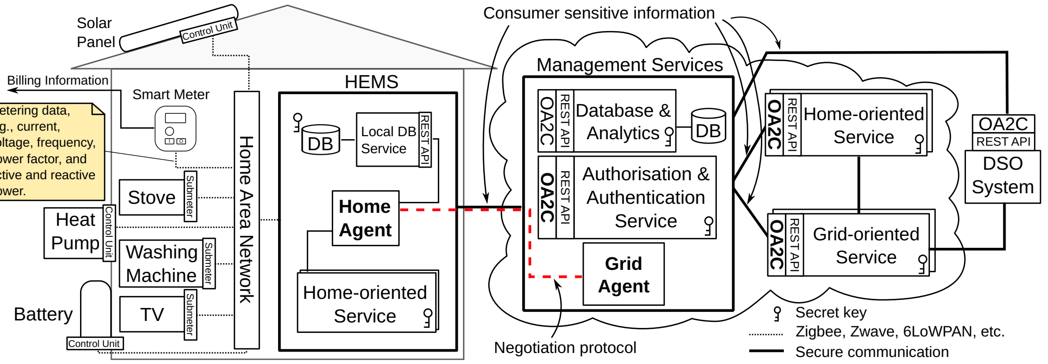

Fig. 1. Conceptual view of the system model.

optimise locally within the grid, e.g. systems based on a virtual power plant or a microgrid system.

The main entities in the architecture are the HEMS, the MS and services (HoSs and GoSs). They do the following:

HEMS is a controlling hub. It attaches to the HAN and connects the smart devices (smart meter, heat pump, battery, etc.). All metering data obtained within the HAN are encrypted and stored in the Local Database Service (LDS). The home agent and grid agent negotiate electricity price and “’information” for a number of future time slots.

MS is the central entity in the system. It authenticates and authorises for data access. It enables ESCOs to publish HoS for the RCs. The RCs can subscribe to these, which generate an access token that authorises the service to access meter data from the Database & Analytics (DB&A) or the LDS with a specific scope and duration.

HoS and GoS are standalone and OAuth2 compliant (OA2C) web services that operate for the RC’s and DSO’s advantage, respectively. The HoSs provide services that can do energy optimisation by applying direct load control on e.g. a battery, heat pump or solar panel. These can either be hosted in the cloud or locally on the HEMS. The GoSs receive information about the state of electricity grid from the DSO system and the aggregated meter data from the MS.

D. Adversary Model

In the architecture, it is assumed that the HEMS manufacturers are benign, i.e. the HEMS will act in the residential consumer’s best interests by following the protocol and only share meter data with the consumers’ consent. The meter data obtained from HAN are assumed to be legit and the communication within the HAN is considered secure. How this is secured is beyond the scope of this paper. Furthermore, we assume the AAS only will authorise access to the consumer’s meter data given the consumers’ consent and stores confidential information securely. The service providers operating the DB&A, home- and grid-oriented services located in the cloud are considered to be honest-but-curious adversaries that follow the OAuth2 protocol over HTTPS, but might remember all the data being sent. The DSO is also considered an honest-but-curious adversary that cannot learn less than what he obtains from the billing information. Moreover, the price policy given by the DSO to the RC is assumed to be the “’best” (in context of lowest electricity price based on the avaliable information that can ensure grid stability with high probability). For all adversaries it is assumed they cannot break cryptographic primitives.

E. Negotiation Protocol between HEMS and MS

The purpose of the data exchange between HEMS and MS is to give more near real-time information about the state of the electric grid. This facilitates services to calculate better prediction models about needed demand than already obtained from the billing information. The sampling period T_b of the billing information is typically from hourly to monthly depending on the tariff scheme for the RC. Since these data are used for billing, the data transfer is often required to be sent through a dedicated communication channel e.g. Advanced Metering Infrastructure (AMI), thus beyond the scope of what the HEMS can protect.

Assuming the DSO will receive the billing information with a sampling period T_l from the main meter without aggregation, this can be considered the minimal boundary for the information content I_l for consumption and production data. As shown in Fig. 1, the home agent receives meter data from the individual smart devices. The smart meter has the potential to extract additional data which are not obtained when the DSO is getting the billing information. Information like active power, reactive power, voltage, current, power factor and frequency with a sampling period T_{sm} (typically $T_{sm} = 20s$) provides additional information that can be exploited to violate privacy. Furthermore, the submeters on the home appliances and the control units with a sampling period T_{sub}, the information content for all meters I_h will follow the inequality $I_h \geq I_l$.

A bargaining game between the home agent and the grid agent can e.g. be based on the necessary data granularity and meta information the grid agent must require for identifying behavioural patterns. This can be identified in two ways: by identifying the appliance or by identifying the usage pattern of the appliance. Hence, the bargaining game can happen on two levels: on (1) *intra-appliance* level, i.e. consumption pattern within a cycle of its usage (washing machine has water pumping, washing, spin drying) and (2) *inter-appliance*, i.e. the order which appliances are used (e.g. washing machine → tumble dryer). Assuming the grid agent is only interested in the aggregated demand with $> I_l$, the meter data on *intra-appliance* level can provide knowledge about the true appliance usage for a given T_{sm} [22].

A privacy metric for determining data granularity could be based on the classification efficiency, e.g. the F-score [22]. This can be used to identify appliances such that the data granularity T_{sm} can be adjusted based on the outcome of the bargaining game. The F-score has the benefit of being more “’palpable” for the RC than e.g. the entropy. The RC will be aware of the appliances that can be derived from the information sent, thus generating more privacy awareness. However, using the F-score has drawbacks because it will depend on the implementation of the feature extraction and classification algorithm.

F. Authorisation Protocol between MS and Services

The authorisation protocol between the MS and the ESCO's services is based on the OAuth2 framework [23]. The AAS is a central place for RCs, ESCOs and DSOs to authorise specific access to each other's data through a token system.

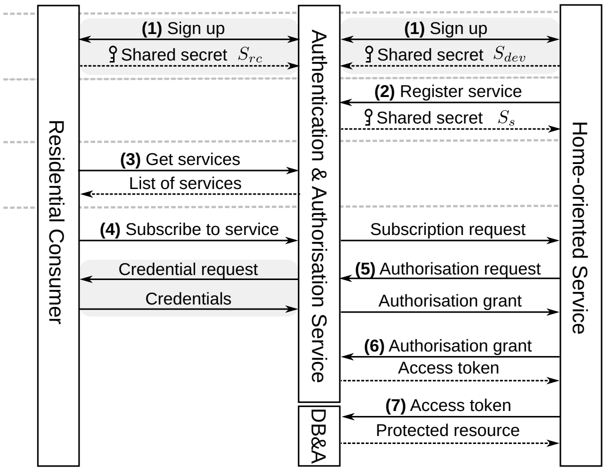

Fig. 2. A high-level view of the OAuth2 authorisation protocol (5-7) with amendments for capturing the authentication process (grey boxes) and acquiring services (2-4). Grey lines indicate new manual interactions.

The authentication and authorisation procedure are illustrated in Fig. 2, where the protocol phases are indicated by $(\cdot)$. It shows a successful authentication and authorisation cycle between RC and the HoS. It is similar for the DSO and the GoS, but for the sake of brevity, we only present the scenario between the RC and HoS. It is assumed that the protocol is executed over a secure HTTPS connection between the RC and AAS, but also the AAS and the HoS/GoS (services) to prevent man-in-the-middle attacks. Furthermore, it is assumed the HEMS and the AAS have been authenticated, authorised and can exchange data. The phases are:

(1) A sign up procedure between the RC and the AAS, where the RC proves his identity by a digital signature scheme (e.g. by a national wide authentication service and/or through a two-factor authentication service) and exchange a shared secret S_{rc}. Similar sign up procedure is required for the developer wanting to register a service. They also exchange a shared secret S_{dev}.

(2) The ESCO registers a service after he is authenticated. It provides the Uniform Resource Identifier (URI), application name, and meta information about the categories it applies to. Furthermore, it provides its admission requirements to other services. The AAS generates a shared secret S_s for the service that it must append to all messages henceforth. It is used to identify the authenticity of the service.

(3) The RC requests for a list of services registered at the AAS. These services are listed based on keywords or categories that match the RC's preference.

(4) The RC subscribes to a service by accepting the admission requirements, and the service gets notified.

(5) For the service to acquire an authorisation grant, it can request the AAS to request permission from the RC through an authorisation code. The AAS will require both authentication of the RC, but also the acceptance of the access conditions (defining data scope, duration) from the RC. The RC never shares his credentials with the service. Furthermore, instead of sending an authorisation grant back to the service (as shown in Fig. 2), the AAS can send the access token directly to the service.

(6) An authorisation grant received by the service can be exchanged with an access token through the AAS. The access token is opaque for the service and specifies scope and duration of access granted by the RC. Furthermore, it can be a self-contained access, e.g. JSON Web Token (JWT). This can provide the DB&A with all authorisation information which can be verified directly on the DB&A. The access token should be stored securely at the service, in order to reduce the risk of compromising the RC.

(7) With the access token, the service can request access to the DB&A. The DB&A validates the access token and if it is valid, it sends a representation of the protected resource to the service.

The logical separation of the resource service (DB&A) and the authorisation service (AAS) provides portability for the RC. It allows for different actors to host them. For instance, the AAS could be hosted by a cooperation between DSOs in a grid region. The individual DSO could host the DB&A itself, thus providing a single point of access for all RCs. Furthermore, the OAuth2 protocol allows for customised authorisations for each single ESCO. This facilitates a possible switch between different ESCOs without losing data history and without having to remember new credentials. The RCs can also revoke data sharing by invalidating the token. The service will then be required to refresh the token, which the RC can accept.

IV. Comparative Evaluation

In the following, the proposed architecture is compared with work with similar objectives. Table I shows the comparison between the existing architectures against the assumptions and goals listed in Section III-B.

TABLE I
Comparative evaluation of proposed architecture.

	Portability	Adaptability	Privacy	Opt-out	Autonomy
SG/SH [6]	✓				✓
VHome [10]	✓	✓	*	✓	✓
Proposed architecture	✓	✓	✓	✓	✓

* Partly, do not give the RC physical control of data storage.

In [6] the privacy is not integrated at the RC level and requires a trusted third party to support this. The system cannot adapt if the RC does not want to share meter data. VHome [10] incorporates privacy by having a personal cloud that allows stakeholders to access through a privacy preserving mechanism. However, the RC is not physical in control of what data he shares, thus the RC implicit trust the Infrastructure as a Service (IaaS). In our proposed architecture, the data is first stored locally in the homes. Based on user preference for privacy and price offered by the DSO, meter data are negotiated to be stored in the DB&A.

V. Conclusion and Future Work

A consumer-centric and service-oriented architecture has been proposed based on five goals we believe the consumer would require for participating a market with a DSO and ESCOs. The architecture has been constructed in compliance with identified design challenges and related work. From this, the paper presents a system model that comprises a HEMS, management services and ESCO's services. It takes a different approach than typically cloud-based solutions by giving the residential consumer physical control of data storage locally and data delegation globally. The HEMS integrates with HAN and stores meter data from submeters and the smart meter in the residential home. The management services handle data authorisation and data authorisation based on consumer preferences. For enforcing privacy, the paper gives a high-level description of a negotiation protocol between the home agent and grid agent. Moreover, it adapts the OAuth2 protocol to the architecture for authenticating and authorising the residential consumers, ESCOs and DSOs. Last, the architecture is evaluated against the goals previously defined and compared to architectures with similar objectives.

Future work will include design of JWT in the OAuth2 procedure for ESCO to comply in given architecture. Furthermore, an evaluation of the protocol between the home and grid agent to negotiate data attributes and granularity should be performed.

Acknowledgement

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 317761.

References

[1] EEA Report No 6/2008., "Energy and environment report," 2008.

[2] N. Bui, A. Castellani, P. Casari, and M. Zorzi, "The internet of energy: a web-enabled smart grid system," *Network, IEEE*, vol. 26, no. 4, pp. 39–45, July 2012.

[3] R. Gustavsson, "Agents with power," *Commun. ACM*, vol. 42, no. 3, pp. 41–47, Mar. 1999.

[4] H. S. Fhom, N. Kuntze, C. Rudolph, M. Cupelli, J. Liu, and A. Monti, "A user-centric privacy manager for future energy systems," in *2010 International Conference on Power System Technology*. IEEE, Oct. 2010, pp. 1–7.

[5] M. Albano, L. Ferreira, T. L. Guilly, and M. Ramiro, "The ENCOURAGE ICT architecture for heterogeneous smart grids," *encourage-project.eu*, no. July, pp. 1383–1390, 2013.

[6] K. Kok, S. Karnouskos, D. Nestle, and A. Dimeas, "Smart houses for a smart grid," *IET Conference Proceedings*, January 2009.

[7] R. H. Jacobsen and S. A. Mikkelsen, "Infrastructure for intelligent automation services in the smart grid," *Wireless Personal Communications*, vol. 76, no. 2, pp. 125–147, 2014.

[8] P. Vrba, V. Marik, P. Siano, P. Leitao, G. Zhabelova, V. Vyatkin, and T. Strasser, "A review of agent and service-oriented concepts applied to intelligent energy systems," *Industrial Informatics, IEEE Transactions on*, vol. 10, no. 3, pp. 1890–1903, Aug 2014.

[9] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds," *2011 IEEE 4th International Conference on Cloud Computing*, pp. 582–589, Jul. 2011.

[10] R. P. Singh, S. Keshav, and T. Brecht, "A cloud-based consumer-centric architecture for energy data analytics," in *Proceedings of the Fourth International Conference on Future Energy Systems*, ser. e-Energy '13. New York, NY, USA: ACM, 2013, pp. 63–74.

[11] J. Polonetsky and C. Wolf, "How Privacy (Or Lack of It) Could Sabotage the Grid," 2009.

[12] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 981–997, Fourth 2012.

[13] M. Yigit, V. C. Gungor, and S. Baktir, "Cloud computing for smart grid applications," *Computer Networks*, vol. 70, pp. 312 – 329, 2014.

[14] S. Pearson, "Taking account of privacy when designing cloud computing services," *2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, pp. 44–52, 2009.

[15] F. Li, W. Qiao, H. Sun, H. Wan, J. Wang, Y. Xia, Z. Xu, and P. Zhang, "Smart Transmission Grid: Vision and Framework," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 168–177, Sep. 2010.

[16] The European Commission, "Directive 2009/72/EC of the European Parliament and of the council of 13 July 2009," *Official Journal of the European Union*, vol. 2008, no. June, 2009.

[17] K. Maheshwari, K. Birman, J. Wozniak, and D. V. Zandt, "Evaluating Cloud Computing Techniques for Smart Power Grid Design Using Parallel Scripting," in *2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*. IEEE, May 2013, pp. 319–326.

[18] IndEco Strategic Consulting, "Smart grid consumer engagement: lessons from North American utilities," , Tech. Rep., 2013.

[19] W.-H. Liu, K. Liu, and D. Pearson, "Consumer-centric smart grid," in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, Jan 2011, pp. 1–6.

[20] R. Fielding, "Architectural styles and the design of network-based software architectures," Ph.D. dissertation, University of California, 2000.

[21] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," in *2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*. IEEE, Dec. 2009, pp. 711–716.

[22] G. Eibl and D. Engel, "Influence of data granularity on smart meter privacy," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 930–939, March 2015.

[23] D. Hardt, "The oauth 2.0 authorization framework," Internet Requests for Comments, RFC Editor, RFC 6749, October 2012, .