ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/341312502

Towards defining Data Usage Restrictions in the Built Environment

Preprint · June 2020

DOI: 10.13140/RG.2.2.18565.58080

CITATIONS
0

READS
55

2 authors:

Gonzalo Gil
TEKNIKER
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Iker Esnaola-Gonzalez
TEKNIKER
17 PUBLICATIONS **15** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project EEPSA (Energy Efficiency Prediction Semantic Assistant) View project

Project RESPOND H2020 View project

All content following this page was uploaded by Gonzalo Gil on 12 May 2020.

The user has requested enhancement of the downloaded file.

Towards defining Data Usage Restrictions in the Built Environment

Gonzalo Gil[0000−0002−8988−4986] and Iker Esnaola-Gonzalez[0000−0001−6542−2878]

TEKNIKER, Basque Research and Technology Alliance (BRTA)
Iñaki Goenaga 5, 20600 Eibar, Spain
gonzalo.gil@tekniker.es, iker.esnaola@tekniker.es

Abstract. The building sector consumes about 40% of global energy, which is largely caused by buildings' operations. Research showed that providing users with detailed consumption and appliance-usage data may engage them in energy efficiency activities. To do so, data analytics services must be deployed by third parties. This services require huge amount of data from the users in order to offer high quality services. Nevertheless, users are reluctant to share their data especially if its private. This is the case of those measurements performed inside the buildings that describes users behaviour. In these scenarios, data sovereignty plays a key role as it provides a solution to guarantee data owners that their data is being used as they defined initially in textual contracts. In this way, the owners predisposition to exchange their data is expected to increase. In this article, focus is placed in the specification of machine-interpretable policies for built environments based on data owners' defined textual contracts. For that, domain-agnostic usage control specification IDSA approach is combined with built environment ontologies which define the resources to which usage restrictions apply. Furthermore, this approach has been implemented in a real-world home use case.

Keywords: Buildings · Ontology · Data Usage Control · Usage Policies

1 Introduction

The European Commission agreed a set of binding legislation inside the EU 2020 package in order to meet the energy sustainability and minimize the climate change. One of the spotlighted sectors regarding this package is the building sector which, according to the UNEP (United Nations Environment Programme), consumes about 40% of global energy and is responsible for 36% of CO_2 emissions in the EU. This energy consumption and specially energy peak demand, have a negative impact on operational cost and environmental aspects due to the carbon-intense generation plants that are deployed to satisfy them [3]. Certainly, demand peaks are largely caused by buildings' operations, including space and water heating, followed by appliances, cooking and lighting [2].

Demand side management activities such as load curtailment or reallocation have a huge potential to minimize these peaks, especially in the residential sector

which has traditionally been largely untapped. In this regard, the increasingly penetration of Renewable Energy Sources (RES) in the energy production side, and their combination with Demand Response (DR) programs and improvement in energy storage options, could also contribute to significantly reduce peak demands. DR can be understood as the set of technologies or programs that concentrate on shifting energy use to help balancing energy supply and demand [14], and they are introduced into the smart grids so that reliable and economical operation of power systems are ensured. However, the full capabilities of the DR are yet to be unlocked in the residential sector. This is mainly caused by the heterogeneous group of end-users that conform the residential sector, who are difficult to stay engaged with DR programs.

Research showed that providing users with historical consumption information and detailed appliance-specific consumption information contributed to the reduction of energy consumption in the residential sector [13, 9, 1]. As a matter of fact, offering usable and attractive services may further engage users with DR programs. The quality of these services depends largely on the quality and amount of data provided by the user. Additionally, shared data may also be exploited for other purposes apart from energy management, such as the development of new business models[1] including the data monetization. However, even though home occupants are aware of the benefits of these services, they may still be reluctant to share their data [11], specially if data sovereignty is not assured. In order to ensure the sovereignty of exchanged data, on the one hand, data must be controlled, and on the other, data provenance must be provided to data owners as a proof of compliance or violation of the defined usage restrictions.

Traditional access control standard XACML[2] (eXtensible Access Control Markup Language) has been established as de-facto standard for data control. However, access control mechanisms only provide control at the time of the request on provider side when the consumer requests a resource in a specific way (e.g. write or read). That is, once data access is granted, there is no control over its usage. In other words, access control is limited to past and present data restrictions and cannot cope with future control.

Usage control extends access control mechanisms by controlling how data is used and shared by the consumers once access is granted as shown in Figure 1. Moreover, usage control is not limited to the fulfillment of a set of conditions (e.g. time-based restrictions or usage purpose) for data usage or sharing. As a matter of fact, it extends to the enforcement of obligations during and after data usage. These obligations consist in a set of actions such as the anonymization of sensitive data or its deletion.

Therefore, the development of usage control solutions must face new needs [7] and challenges that are out of the scope of access control mechanisms:

- Usage Control Policies Specification and Implementation: Usage control covers not only usage conditions, but also, actions that must be enforced for

[1] https://op.europa.eu/en/publication-detail/-/publication/2d6d436e-4832-11e8-be1d-01aa75ed71a1/language-en

[2] http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

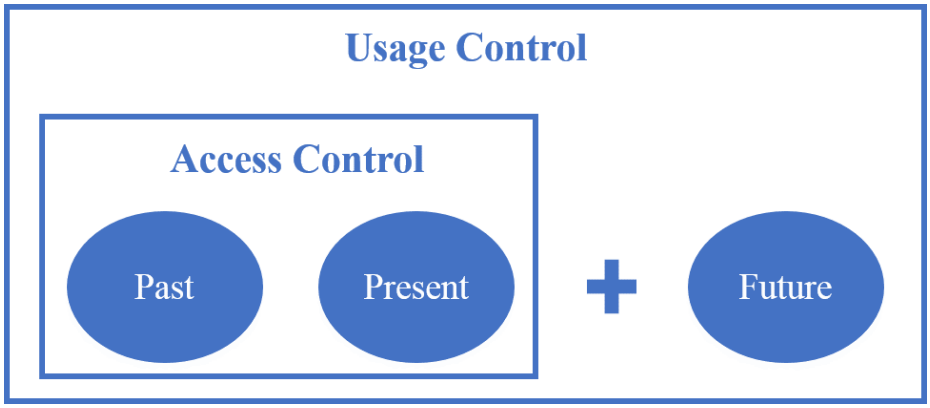

Fig. 1. Usage Control: an extension of Access Control.

compliance with the obligations defined in the usage restrictions by the provider. For that, firstly, human-readable usage restrictions must be specified as a set of conditions and obligations in a machine-interpretable formal way, secondly, formal restrictions must be translated depending on the technology and the target environment in specific implementation level policies and finally, these must be implemented in every provider connector.
- Usage Control Policies Enforcement: Usage control extends the centralized control performed by access control mechanisms in data providers side to distributed control in all those consumers that use and share providers' data. Usage control solutions must be able to enforce all the conditions and obligations that have been defined by the provider in every consumer system.
- Data Usage Tracking: Access control mechanisms enforce data control at providers infrastructure. Therefore, the provider can know how data is being requested. Nevertheless, in usage control solutions, data usage and sharing is performed in a distributed way in external platforms. Thus, usage control solutions must provide a way to track how data is being used during its life.

The International Data Spaces Association[3] (IDSA) is working on the development of a trusted open data platform where business-to-business relationships can be searched and established to provide and consume data under easily customised conditions guaranteeing data sovereignty. To reach this goal, data usage control plays a key role. Therefore, IDSA is working on the research of the challenges defined above.

Regarding usage control challenges, this article is focused on the first one referring to usage control policies specification and implementation. Therefore, its enforcement and tracking challenges are out of the scope. Likewise, usage control policies specification recognize three issues to be solved. Firstly, the assets identification. Usage control is oriented to assets rather than specific data. Assets

[3] https://www.internationaldataspaces.org/

are economic goods generated by a participant, that can classified data based on its value and usage restrictions among others. Secondly, the translation of human-readable usage restrictions into machine-readable policies which can be enrich with external information in order to be interpretable and enforceable. Thirdly, the combination of usage control ontologies with assets that can be represented using adequate domain-specific ontological terms.

In this article, focus is placed on the conversion of human-readable usage restriction specifications into machine-interpretable policies for the built environment based on ontologies.

The rest of the article is structured as follows. Section 2 introduces the challenges for formalizing the specifications of usage control restrictions in a machine interpretable way. Section 3 introduces a use case to illustrate the usage control needs in a built environment scenario. Section 4 describes the proposed approach for satisfying the identified needs. Finally, conclusions of this work are described in Section 5.

2 Usage Control Policies Specification

Traditionally, textual contracts have been enough for setting data exchange agreements between business partners. Nevertheless, in nowadays digitized world, agreements are also established between machines instead of humans, thus higher degrees of formalization are necessary for these contracts. Figure 2 represents different degrees of formalization for data exchange business contracts, from the lowest formalization to the highest formalization levels. First, the lowest level of formalization belongs to the traditional textual contracts. Second, the descriptive policies are a representation of these contracts in machine readable formats (e.g. JSON or XML). Third, formal policies extend these machine-readable policies including a consistent semantic with additional information such as usage restrictions definition and implications provided by e.g. RDFs (Resource Description Frameworks). In this way, they are interpretable by enforcement points. Fourth, enforceable policies associate usage restrictions with target environment components in a technology-dependent way in order to be executable. Finally, autonomous negotiated policies allow usage restrictions to be negotiated without human interactions.

This article, focuses on the definition of formal policies from data owners' defined textual contracts based on IDSA approach. Therefore, higher degrees of formalization are out of the scope of this article.

2.1 IDSA Approach

IDSA defines the Industrial Data Space (IDS) Information Model[4], a domain-agnostic common language for the semantic description of the participants and components within the IDS, which includes the specification of machine-interpretable

[4] https://w3id.org/idsa/core

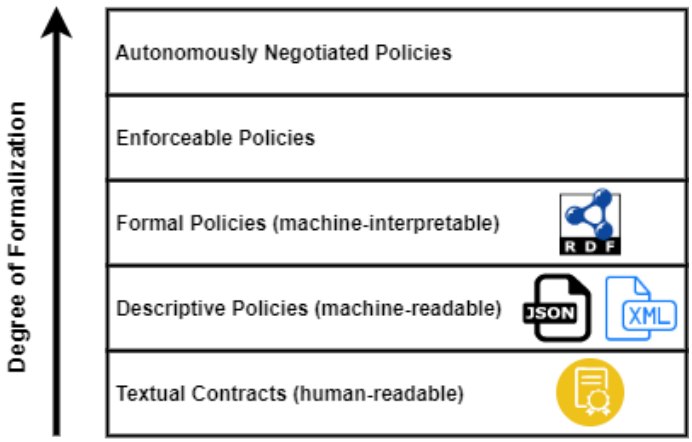

Fig. 2. Degree of formalization of business process contracts.

usage control policies. Usage control policies specification is based on the ODRL (Open Digital Rights Language) Information model 2.2[5], a W3C recommended policy expression language that provides a vocabulary and data model for the description of machine-readable contracts. Moreover, the IDS Information Model extends it towards usage control descriptions and enforcement.

IDSA define the concept of contract (*ids:Contract*), a subclass of a Policy (*odrl:Policy*), that is an abstract set of rules (*ids:Rule*) which are comprised of permissions (*ids:Permission*), prohibitions (*ids:Prohibition*) and duties (*ids:Duty*). Each of these rules describes an action (*ids:Action*) that stakeholder (*ids:Participant*) might be permitted or prohibited to do on a digital content (*ids:DigitalContent*) under certain constraints (*ids:Constraint*). This basic contract representation is shown in Figure 3.

As previously mentioned, the IDS Information Model is generic, with no commitment to any particular domain. That is, the domain knowledge has to be modelled or imported from other existing vocabularies. In this article, focus is placed on the definition of formal policies based on this IDSA usage control policies specification approach in the built environment.

3 Use Case

The RESPOND H2020[6] project aims to deploy an interoperable energy automation, monitoring and control solution to deliver DR programs at a dwelling, building and district level to neighborhoods across Europe.

The focus of this article is placed on a home located in the Aran Islands (Ireland) participating in the RESPOND project (from now on referred to as

[5] https://www.w3.org/TR/odrl-model/
[6] http://project-respond.eu/

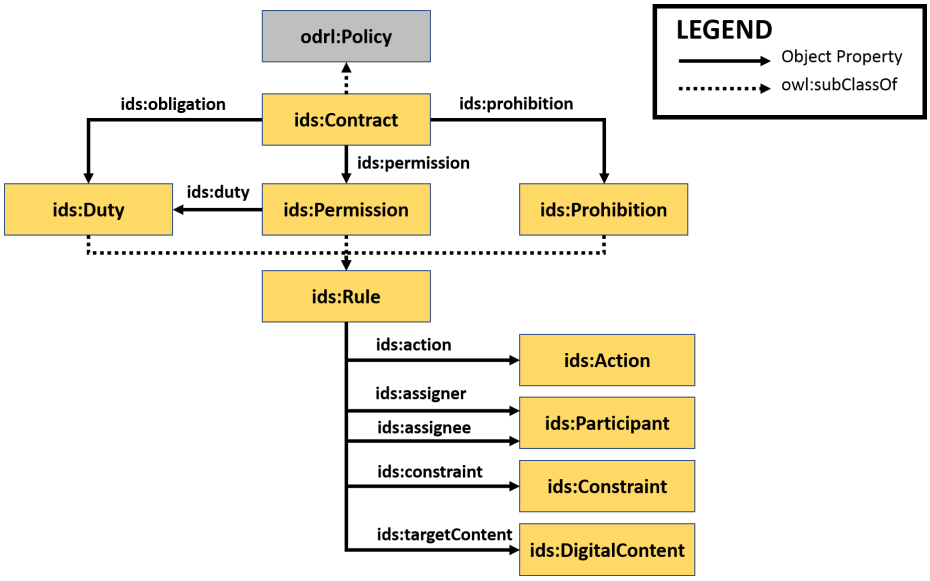

Fig. 3. IDS Policy Concept.

Aran_01). In this use case home occupants are provided with their household-related information via the RESPOND Mobile App[7] to be able to interact with the devices deployed around the home and e.g. customize the home temperature or optimize the electrical consumption. For that purpose, among other relevant data, they can visualize the electrical consumption and comfort measurements during a specific time (both raw data or summarized as aggregated data), as well as the recommended optimal electrical consumption profile. This optimal profile is obtained taking leverage of different data analytic services developed by different technology providers, including the electricity demand forecasting, renewable energy production forecasting and optimization services. For this, technology providers needs data that must be exchanged between the different stakeholders involved in this process. Therefore, some business relationships needs to be agreed.

Next, the stakeholders involved in the use case, the assets exchanged and the established agreements are described.

3.1 Stakeholders

The stakeholders identified in Aran_01 use case play different roles and, thus, they can be divided as follow:

– Owner: Person or company that owns the home or the building.

[7] http://project-respond.eu/personal-energy-performance-assistant-version-1-13-released/

- Occupant: The person who lives in the home. It may be the owner of the home or not, if it is rented. It is the data owner.
- Technology Provider: Third parties that provides hardware and/or software services. These can be classified into two different categories:
  - Data Provider: Companies that provide the service needed to obtain and exchange data with other parties. These, never use the data.
  - Data Consumer: Companies that provide data analytic services based on data consumption.

Regarding the stakeholders and their roles, Aran_01 dwellers are the owners and the occupants of the home. Energomonitor SRO[8] from the Czech Republic, TEKNIKER[9] from Spain and Institut Mihajlo Pupin[10] (PUPIN) from Serbia are the technology providers. On the one hand, even though Energomonitor provides the devices and gateways that makes and sends measurements to data consumers, Aran_01 dwellers are the owners of the data. Therefore, they have the responsibility to define textual contracts related to home data. On the other hand, TEKNIKER and PUPIN are the technology providers who exploit the data by developing analytic services that generate added value. These analytic services include the generation of optimized energy profiles electricity consumption management [6]. Moreover, TEKNIKER offers comfort services that will provide the average temperature of the home.

3.2 Assets

Assets are resources exchanged between the stakeholders. In the presented use case, assets are data, which can be classified as follows:

- Temperature: Measurements related to the temperature in the home which includes:
  - Raw data: the temperature measured by a temperature sensor.
  - Comfort data: the average temperature of all the devices of the home.
- Electrical Demand: Measurements related to the electrical energy consumed by the home which includes:
  - Raw data: the electrical demand measured by an electricity meter.
  - Aggregated data: the average value of raw data aggregated in a given period of time (e.g. 1h).
  - Forecast data: the predicted electrical demand based on 1h aggregated electrical energy demand data.
- Electrical Production: Measurements related to the electrical energy produced by deployed PV panels which includes:
  - Raw data: the electrical energy production measured by the PV panels.
  - Forecast data: the result of the execution of prediction algorithms based on electrical energy production row data.
- Electrical Optimized Profile: The optimal energy curve with views to optimizing renewable energies and minimizing demand peaks.

[8] https://www.energomonitor.com/
[9] https://www.tekniker.es/
[10] http://www.pupin.rs/

3.3 Agreements

To reach the main goal of the use case, identified stakeholders need to establish relationships between them for data exchange.

Firstly, Aran_01 is the owner and the occupant of the home. Therefore, it is the owner of the raw temperature measured every 30 seconds by several temperature sensors deployed in different rooms of the home, the raw electrical energy demand measured by the electricity meter every 5 seconds and the raw electrical production of the PV panels measured every hour. Aran_01 establishes a relationship with TEKNIKER and PUPIN for the exploitation of the data. On the one hand, TEKNIKER needs raw temperature data to provide the comfort service, and raw electrical demand for generating electrical demand aggregated data, which will be further used by TEKNIKER as an input for the electrical demand forecasting service. For that purpose, Aran_01 grants TEKNIKER raw temperature data usage for comfort purposes and electrical demand data usage for aggregation purposes, as long as this data is used before RESPOND project's ending date (i.e. 2021-01-01). Moreover, Aran_01 prohibits TEKNIKER from sharing the raw demand data. On the other hand, PUPIN needs electrical production raw data in order to provide the electrical production forecasting service. For that purpose, Aran_01 grants PUPIN raw electrical production data usage for prediction purposes. Similar to the restrictions set to TEKNIKER, PUPIN can only use the data prior to the RESPOND project's ending, and cannot share the data.

Secondly, TEKNIKER establishes a relationship with Aran_01 for comfort and forecasted data visualization, and with PUPIN for data exploitation purposes. On the one hand, Aran_01 is only allowed to use electrical demand and temperature data for mobile app visualization. Moreover, TEKNIKER forbids Aran_01 from sharing this data. On the other hand, PUPIN obtains electrical demand forecast data, in order to exploit it for providing the optimization service. Towards that goal, TEKNIKER allows PUPIN using electrical demand data only for optimization purposes, as long as it is used before the ending of the project. Finally, the sharing of this data is forbidden.

Finally, PUPIN establishes a relationship with Aran_01 for sending the results of the electrical production forecast service and the electrical optimized profile, so that they can be visualized in the mobile app. For this purpose, PUPIN allows Aran_01 visualizing electrical production and electrical optimized profile, but the sharing of this data is prohibited.

Therefore, as a result of the data exchanged between relationships Aran_01 can show in a centralized way the current comfort temperature of the home, the electrical demand and production forecast data and the optimized profile which will allow the optimization of the energy consumption in the future. Figure 4 shows the assets exchanged in every agreement between the different stakeholders.

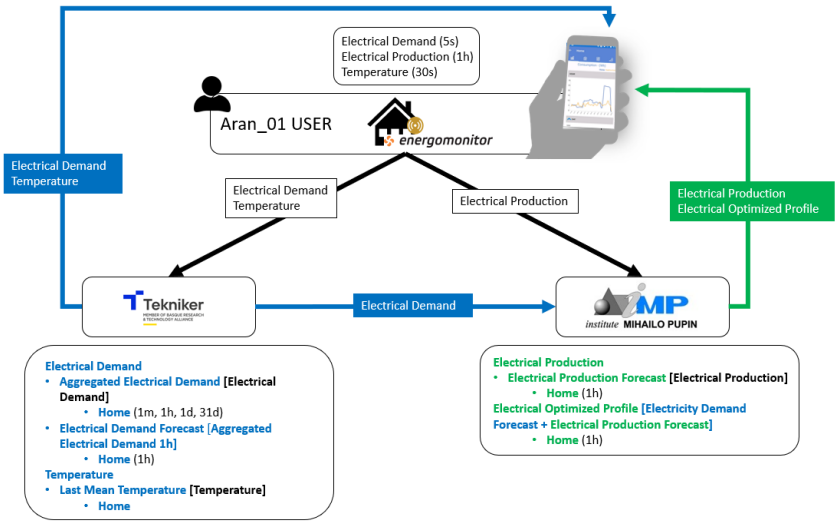

Fig. 4. Stakeholders business relationships

4 The RESPOND approach

In order to represent and formalize the use case's data usage restrictions, the IDS Information Model is used. However, as mentioned before, this ontology domain-agnostic, so and the built environment representation is out of the scope of the ontology. Therefore, in order to represent all the necessary information, the RESPOND ontology [5] is used. The RESPOND ontology's core is developed by reusing and extending three well-known ontologies: BOT[11] [12] to represent the dwelling topology, and SAREF[12] [4] and SEAS Feature Of Interest[13] [8] ontologies to represent devices, features of interest and qualities monitored and controlled by sensors and smart appliances. However, there were other RESPOND requirements that remained unsolved and a set of new axioms had to be defined to satisfy them by extending the list of appliances, observed qualities or units of measurement. Figure 5 shows the main classes and properties of the RESPOND ontology.

As part of the RESPOND project, every participant dwelling and neighbourhood is represented with appropriate ontological terms. This information remains accessible in an Openlink Virtuoso Server[14] version 07.20.3217 for its further exploitation by other services via SPARQL queries.

In order to showcase the machine-interpretable definition of formal policies, a contract between Aran_01 and TEKNIKER has been considered. This contract

[11] https://w3id.org/bot
[12] http://ontology.tno.nl/saref
[13] https://w3id.org/seas/FeatureOfInterestOntology
[14] https://virtuoso.openlinksw.com/

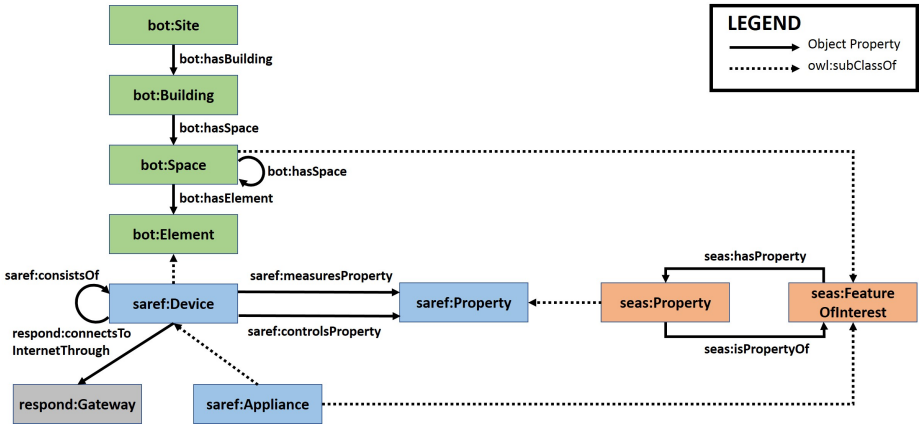

Fig. 5. RESPOND ontology's main classes and properties.

comprises two rules: a permission and a prohibition. This is represented with the following triples:

```
:contract002AZ63 rdf:type ids:Contract;
    ids:permission :permission25;
    ids:prohibition :prohibition43.
:permission25 rdf:type ids:Permission.
:prohibition43 rdf:type ids:Prohibition.
```

The permission defines that TEKNIKER can use Aran_01's demand data for aggregation purposes until the end of the project, that is, prior to the year 2021. This permission is represented with the following triples:

```
:permission25 ids:action ids:READ;
    ids:assignee :partner_TEKNIKER;
    ids:assigner :aran_01:
    ids:constraint :constraint_p25_01;
    ids:constraint :constraint_p25_02;
    ids:targetContent :aran_01_demand.
:constraint_p25_01 rdf:type ids:Constraint;
    ids:leftOperand ids:purpose;
    ids:operator idsa:EQ;
    ids:rightOperand "Aggregation Purposes"^^xsd:String.
:constraint_p25_02 rdf:type ids:Constraint;
    ids:leftOperand ids:now;
    ids:operator idsa:BEFORE;
    ids:rightOperand "2021-01-01T00:00:00Z"^^xsd:dateTimeStamp.
```

As it can be seen, the contract defined using IDS Information Model ontological terms is assigned to "aran_01_demand", which represents the electrical demand of the home Aran_01. As mentioned before, Aran_01 and the rest of the RESPOND participant dwellings are described and stored in a Triplestore. Next, a simplified RDF representation of Aran_01 is shown:

```
:irishSite rdf:type bot:Site;
    bot:hasBuilding :aran_01.
:aran_01 rdf:type bot:Building;
    bot:hasElement :aran_01_electricityMeter.
:aran_01_electricityMeter rdf:type saref:Device;
    saref:measuresProperty :aran_01_demand.
:aran_01_demand rdf:type saref:Property.
```

Regarding the second rule of the aforementioned usage restriction, it defines that TEKNIKER cannot share Aran_01's demand information and it can be represented with these triples:

```
:prohibition43 ids:action ids:DISTRIBUTE;
    ids:assignee :partner_TEKNIKER;
    ids:assigner :aran_01:
    ids:targetContent :aran_01_demand.
```

Summarizing, with the proposed approach, which is based on IDSA usage control policies specification, machine-interpretable formal policies can be defined for every relationship established between stakeholders. Moreover, these policies have been applied to the assets that are exchanged within RESPOND project. In this way, a trustworthy scenario has been defined for Aran_01. In this scenario, Aran_01 dwellers will be able to control and know how its data is being used. Moreover, they could benefit from the services provided by TEKNIKER and PUPIN such as electrical energy optimization.

5 Conclusions

Nowadays, the inefficient operation of buildings makes the building sector responsible for the consumption of about the 40% of global energy. According to recent research, this consumption could be reduced if building occupants are informed about their energy consumption and appliance-usage, as these could improve the user engagement in energy efficiency activities. The data collected by the smart home solutions could be exploited to provide users with added-value services to further engage users in this kind of activities. However, users are not eager to share their data unless data sovereignty is ensured.

Based on IDSA's domain-agnostic usage control policies specification approach, in this article textual contracts for the built environment have been translated into machine-interpretable policies taking leverage of IDS Information Model and domain-specific ontologies. This has been illustrated in a real-world home within the context of the RESPOND project. In this use case, a trustworthy environment has been developed where data usage control has been granted for every stakeholder. Such an environment is expected to increase data owners' predisposition to share their data in exchange for added-value services, thus minimizing the existing data-sharing reluctance.

5.1 Future Work

The presented work paves the way towards future research in two different aspects.

Both practice and research suggests the use of a graph-based format to capture building data, nevertheless keeping numeric data explicitly out of the semantic graph for computational performance reasons [10]. Without having the semantic representation of those numeric data, the definition of assets must be done at a quality level (e.g. temperature or humidity), thus a more fine-grained asset definition is nos possible. Therefore, stakeholders cannot specify policies at a measurement type level (e.g. raw temperature, aggregated temperature or forecasted temperature data). This research line is worth being further investigated.

The IDSA approach is limited to the semantic representation of human-readable usage control restrictions into machine-interpretable policies. Therefore, before its implementation in an specific scenario a translation must be deployed in order to be make policies enforceable based on the target environment and the specific usage control technology used. LUCON open source usage control technology is not able to translate those machine-intepretable policies into enforceable policies. In this line, LUCON will be studied in order to develop a translator which allow the implementation of technology-independent policies.

References

1. Abrahamse, W., Steg, L., Vlek, C., Rothengatter, T.: The effect of tailored information, goal setting, and tailored feedback on household energy use, energy-related behaviors, and behavioral antecedents. Journal of environmental psychology **27**(4), 265–276 (2007)
2. Agency, I.E.: Transition to Sustainable Buildings (2013). https://doi.org/https://doi.org/https://doi.org/10.1787/9789264202955-en, https://www.oecd-ilibrary.org/content/publication/9789264202955-en
3. Collins, L.D., Middleton, R.H.: Distributed demand peak reduction with non-cooperative players and minimal communication. IEEE Transactions on Smart Grid (2018). https://doi.org/10.1109/TSG.2017.2734113
4. Daniele, L., den Hartog, F., Roes, J.: Created in close interaction with the industry: the smart appliances reference (saref) ontology. In: International Workshop Formal Ontologies Meet Industries. pp. 100–112. Springer (2015). https://doi.org/10.1007/978-3-319-21545-7_9
5. Esnaola-Gonzalez, I., Diez, F.J.: Integrating building and iot data in demand response solutions. In: Proceedings of the 7th Linked Data in Architecture and Construction Workshop (LDAC 2019). vol. 2389, pp. 92–105. CEUR (2019)
6. Esnaola-Gonzalez, I., Diez, F.J., Pujic, D., Jelic, M., Tomasevic, N.: An artificial intelligent system for demand response in neighbourhoods. In: Proceedings of the Workshop on Artificial Intelligence in Power and Energy Systems (AIPES 2020) (Under Review)
7. Gil, G., Arnaiz, A., Higuero, M.: Towards assesment of existing frameworks for data usage control: Strength and limitations with respect to current application

scenarios. In: IoT Connected World Semantic Interoperability Workshop (IoT-CWSI) (2019)
8. Lefrançois, M.: Planned etsi saref extensions based on the w3c&ogc sosa/ssn-compatible seas ontology patterns. In: Proceedings of Workshop on Semantic Interoperability and Standardization in the IoT, SIS-IoT, (July 2017)
9. Peschiera, G., Taylor, J.E., Siegel, J.A.: Response–relapse patterns of building occupant electricity consumption following exposure to personal, contextualized and occupant peer network utilization data. Energy and Buildings **42**(8), 1329–1336 (2010)
10. Petrova, E., Pauwels, P., Svidt, K., Jensen, R.L.: In search of sustainable design patterns: Combining data mining and semantic data modelling on disparate building data. In: Advances in Informatics and Computing in Civil and Construction Engineering, pp. 19–26. Springer (2019)
11. Ranade, V.V., Beal, J.: Distributed control for small customer energy demand management. In: 2010 Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems. pp. 11–20. IEEE (2010)
12. Rasmussen, M.H., Pauwels, P., Hviid, C.A., Karlshøj, J.: Proposing a central aec ontology that allows for domain specific extensions. In: Joint Conference on Computing in Construction. vol. 1, pp. 237–244 (2017). https://doi.org/10.24928/JC3-2017/0153.
13. Ueno, T., Sano, F., Saeki, O., Tsuji, K.: Effectiveness of an energy-consumption information system on energy savings in residential houses based on monitored data. Applied Energy **83**(2), 166–183 (2006)
14. Warren, P.: A review of demand-side management policy in the uk. Renewable and Sustainable Energy Reviews **29**, 941 – 951 (2014). https://doi.org/10.1016/j.rser.2013.09.009

View publication stats