A Semantic Policy Language for Usage Control

Ines Akaichi[1,*], Sabrina Kirrane[1]

[1]Institute for Information Systems & New Media, Vienna University of Economics and Business (WU), Vienna, Austria

Abstract

Usage control involves the encoding and enforcement of policies regarding future data use in the areas of data protection, intellectual property management, and secrets management. Proposed policy languages are either too specific or too general in their ability to express usage policies. In this paper, we propose the Usage Control Policy language and show how we can encode usage control specific requirements using deontic rules and fine-grained conditions.

Keywords

Usage Control, Policy Specification, Semantic Web, Knowledge Representation

1. Introduction

Modern decentralized solutions, such as the *Internet of Things (IoT)* and *distributed knowledge graph applications*, face a variety of legislative challenges (e.g, *data protection legislation* and *copyright legislation*) regarding data and digital asset management. In addition, according to Pretschner et al. [1], data owners are reluctant to share their data with decentralized solutions, as often they have no control over how their data are used. Technologies that aim to address these challenges, which are usually classified as usage control, aim to ensure that data consumers handle data according to usage policies stipulated by data owners.

Herein, we focus on policy-based usage control, in the context of which we use machine-readable policies to express the requirements for future data usage and mechanisms to enforce the respective usage policies. These policies need to be able to encode normative statements, mainly permissions (respectively prohibitions) and obligations (respectively dispensations) related to the use of data. The different deontic constructs can specify the conditions in which data may be used or in which actions need to be taken.

Various semantic policy languages have been proposed that could potentially be suitable for expressing usage control, as they support deontic concepts in their core design. The Open Digital Rights Language (ODRL)[1] was originally proposed to express licenses. In addition, attempts have been made to generalize the ODRL model to express other policies [2], such as data protection according to the General Data Protection Regulation (GDPR). ODRL allows constraints to be expressed as simple assertions that can also be combined using logical operators (e.g., and, or). However, ODRL and existing derivatives do not provide concrete guidance for

SEMANTICS 2022 EU: 18th International Conference on Semantic Systems, September 13-15, 2022, Vienna, Austria

*Corresponding author.

ines.akaichi@wu.ac.at (I. Akaichi); sabrina.kirrane@wu.ac.at (S. Kirrane)

0000-0002-6020-5572 (I. Akaichi); 0000-0002-6955-7718 (S. Kirrane)

[1]ODRl, https://www.w3.org/TR/odrl-model/

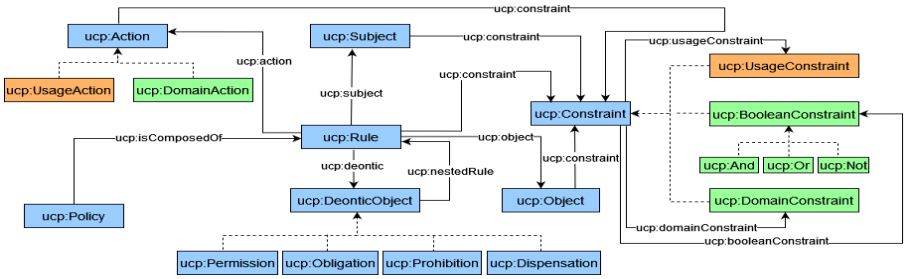

Figure 1: A Core Model for Usage Control Policy Language[2]

the specification of granular semantic conditions such as temporal (e.g., on a monthly or hourly basis), spatial (e.g., on an organizational or country level), cardinality and similar conditions that are needed to express usage policies. Although, Rei [3] can be used to encode general policies (e.g., access control, privacy, conversation, etc.), as per ODRL, Rei does not support fine-grained conditions and relies primarily on existing domain ontologies to express conditions.

In this paper, we build on these two policy languages to propose a first version of the Usage Control Policy language (UCP) that is built on top of domain independent ontologies that feature deontic concepts and fine-grained constraints governing the use of data. Additionally, our language has support for classes of enforcement that are derived from deontic concepts and which are important for making correct policy decisions.

2. Use Case

Our use case is inspired from the IoT domain pertaining to a smart city, where residents make use of multiple smart objects, such as smart homes, cars, parking lots, etc. We assume that marketing companies are interested in the data produced by these smart objects in order to revise new or adjust existing marketing strategies. Thus, the manufacturers of these objects may host or use data sharing platforms whereby data resulting from the use of smart objects are shared with both their customers and various third parties. Consequently, these platforms could offer subscribers the ability to download data relating to smart objects or their users.

3. The UCP Language

In this initial version of the UCP language, we focus on supporting the encoding of simple usage policies that could be used for ex-ante compliance checking, for instance. Other approaches to policy compliance checking may be the use of an ex-post approach. In the former approach, we assume that marketing companies encode their usage request in a knowledge graph and submits this request to the usage control framework, which is provided by the manufacturers and is responsible for determining if usage is permitted, prohibited, or if usage is subject to specific obligations that need to be fulfilled by marketing companies. This is performed by looking for exact matches or matches that are based on simple subsumption reasoning between the subjects, objects, actions, and constraints of the usage policy and the usage request.

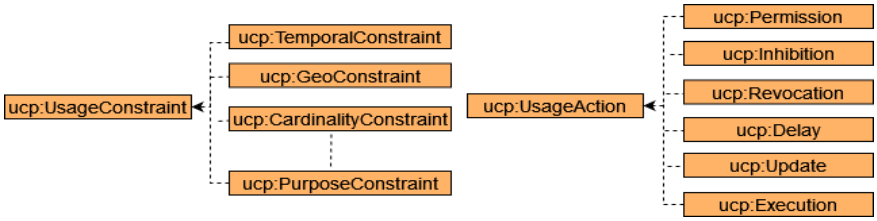

Figure 2: An Instantiation of Usage Control Constraints and Actions[2]

A Core Model for Usage Control. Our model design is informed by our extensive literature review regarding the specification and enforcement of usage control policies [4] and the work of [2] and [3]. In Figure 1, we present the core model of our policy language, which is based on deontic constructs that allow policies to be expressed as what an entity can/can not do and should/should not do with the data in terms of actions. In the proposed model, a `Policy` is made up of a set of `Rules` that encode `Permissions`, `Prohibitions`, `Obligations`, or `Dispensations`. Each `Rule` is associated with an `Action` that is performed by a `Subject` on a target `Object`. A `Rule`, a `Subject`, an `Object`, and an `Action` can also be constrained by one or more `Constraints`. In addition, the model supports *nested rules* that can express nested requirements, which are needed to encode regulatory requirements, such as those set forth by the GDPR [2].

Usage Actions and Constraints. Following the approach proposed by Kagal et al. [3], `Action` has two subclasses: speech acts and domain actions. Speech acts allow conversation policies between agents to be described, among other things. Whereas, Domain actions are actions on the objects in the domain. In our context, we replace speech acts by `UsageActions`, which will allow usage control specific actions to be described, also called classes of enforcement. Classes of enforcement are actions that can prevent undesired system events by changing the behavior of a system. According to our survey on usage control [4], there could be up to six different classes of enforcement, which we present in Figure 2. `Permission` and `Inhibition` allow or prohibit requests for data usage; `Revocation` revokes access in the event of policy violations or revocation of consent; `Delay` delays an attempted usage request until the corresponding obligations are fulfilled; `Update` modifies certain data values after access is granted in order to protect data privacy; and `Execution` executes actions such as sending notifications to data owners.

Following the approach in [3], `Contraint` has two subclasses: `DomainConstraint` and `BooleanConstraint`. `DomainConstraint` describes simple assertions from the domain. While, `BooleanConstraint` allows constraints to be joined together with operators, `AND`, `OR` and `NOT`, to create complex constraints. We extend `Constraint` by adding the class `UsageConstraint`. The new class allows usage specific constraints to be expressed, i.e, under which conditions data can be accessed/used. Based on existing literature [1], few usage control constraints are already identified, such as temporality, geolocation, purpose, and cardinality, as we show in Figure 2. We plan to enhance the expressiveness of these constraints by including other ontologies and vocabularies that can express the different classes with increased granularity.

[2]Green: concepts from[3]; Blue: concepts from [2]; Orange: our contribution

A Model Instantiation. In the following, we demonstrate how to use our proposed Usage Control Policy Language to express examples of policies (P) inspired by our use case. We assume that usage policies could be expressed by the manufacturers and/or the users of the smart objects in order to inform marketing companies under what conditions the data produced can be used. In order to encode our policy examples, we use the Turtle syntax.[3]

P1. *Only subscribed marketing companies are allowed to download power consumption data. They must keep the downloaded data for a maximum of 6 months.* This policy can be described as a rule that is linked to a deontic permission (that includes a nested rule obligation), a constraint (a subscribed marketing company), a subject (the marketing company), an object (power consumption data), and an action (to download). To encode this policy, we begin by expressing a simple permission describing the right to download data by a marketing company.

```
<http://example.com/mcp#Perm_MarketingCompDownloading>
  a <http://example.com/ucp#Permission> .
```

The constraint that describes a subscribed marketing company is a domain constraint that we define as an RDF statement, which is matched with the knowledge graph that describes the marketing company.

```
<http://example.com/mcp#IsSubsribed>
  a <http://example.com/ucp#DomainConstraint> ;
  ucp:subject <http://example.com/mcp#MarketingCompany> ;
  ucp:predicate <http://www.w3.org/1999/02/22-rdf-syntax-ns#type> ;
  ucp:object <http://example.com/mcp#Subscriber> .
```

The obligation to store data for a limited period of time is described as follows.

```
<http://example.com/mcp#Oblig_MarketingCompStoring>
  a <http://example.com/ucp#Obligation> .
```

The obligation involves a time constraint describing the limited duration for storing data.

```
<http://example.com/mcp#For6Months>
  a <http://example.com/ucp#TemporalConstraint>.
```

The storing duration is expressed using the *OWL-Time*[4] concepts: `TemporalEntity` and `GeneralDurationDescription`. In our model, `time:TemporalEntity` and `ucp:TemporalConstraint` can be modeled using the `owl:sameAs` property.

```
<http://example.com/mcp#For6Months>
  time:hasDurationDescription <http://example.com/mcp#Duration6Months> .
<http://example.com/mcp#Duration6Months>
  a <http://www.w3.org/2006/time#GeneralDurationDescription> ;
  time:months 6.0 .
```

The permission rule, which encapsulates the above definitions, is described as follows.

```
<http://example.com/mcp#Rule_MarketingCompDownloading>
  a <http://example.com/ucp#Rule> ;
  ucp:subject <http://example.com/mcp#SubscribedMarketingCompany> ;
  ucp:object <http://example.com/mcp#PowerConsumptionData> ;
  ucp:action <http://example.com/mcp#ActionMarketingCompDownloading> ;
  ucp:constraint <http://example.com/mcp#IsSubsribed> ;
  ucp:deontic <http://example.com/mcp#Perm_MarketingCompDownloading> .
```

[3]The respective namespaces are used to identify our UCP ontology *ucp:<http://example.com/ucp#>*; the marketing company policy (MCP) onotlogy *mcp:<http://example.com/mcp#>*; the time ontology *time:<http://www.w3.org/2006/time#>*; and the owl ontology *owl:<http://www.w3.org/2002/07/owl#>*.

[4]OWL-Time, https://www.w3.org/TR/owl-time/

The obligation clause that is associated with the permission is described with the following rule.

```
<http://example.com/mcp#Rule_MarketingCompStoring>
  a <http://example.com/ucp#Rule> ;
  ucp:subject <http://example.com/mcp#MarketingCompany> ;
  ucp:object <http://example.com/mcp#PowerConsumptionData> ;
  ucp:constraint <http://example.com/mcp#For6Months> ;
  ucp:action <http://example.com/mcp#ActionMarketingCompStoring> ;
  ucp:deontic <http://example.com/mcp#Oblig_MarketingCompStoring> .
```

The permission is further linked to the associated obligation rule.

```
<http://example.com/mcp#Perm_MarketingCompDownloading>
  ucp:nestedRule <http://example.com/mcp#Rule_MarketingCompStoring> .
```

P2. *Subscribed marketing companies are allowed to download power consumption data for aggregation purposes only.* The encoding of the respective permission follows the same pattern as for the other policy. In this policy, the constraint is a `PurposeConstraint` that is encoded as a simple assertion.

```
<http://example.com/mcp#ConstraintUsagePurposes>
  a <http://example.com/ucp#PurposeConstraint> ;
  ucp:usageConstraint <http://example.com/mcp#AggregationPurposes> .
```

4. Conclusion and Future Work

In this paper, we proposed the UCP language, used to express usage control policies. In future work, we plan to examine the suitability of several fine-grained conditions that we have mentioned in this paper. In addition, we plan to introduce the states of deontic concepts into our model, for example to monitor the life cycle of obligations in order to check whether they are fulfilled or not by the end users. More generally, we aim to study the expressiveness requirements of various obligations and conditions and how they can be efficiently structured into various Description Logic policy profiles with well understood semantics and complexity.

Acknowledgments

This work is partially funded under the Marie Skłodowska-Curie grant agreement No 860801 and FWF together with netidee SCIENCE programmes as project number V 759-N.

References

[1] A. Pretschner, M. Hilty, D. Basin, Distributed usage control, Commun. ACM 49 (2006).
[2] M. D. Vos, S. Kirrane, J. Padget, K. Satoh, Odrl policy modelling and compliance checking, in: RuleML+RR, Springer International Publishing, Cham, 2019.
[3] L. Kagal, T. Finin, A. Joshi, A policy based approach to security for the semantic web, in: The Semantic Web - ISWC 2003, Springer, Berlin, Heidelberg, 2003.
[4] I. Akaichi, S. Kirrane, Usage control specification, enforcement, and robustness: A survey, 2022. URL: https://arxiv.org/abs/2203.04800.