Developing an Ontology to Enhance Semantic Interoperability in IoT Environments

Maria Cornejo-Lupa
Electrical and Electronics Engineering Department
Universidad Católica San Pablo
Arequipa 04001, Peru
maria.cornejo.lupa@ucsp.edu.pe

and

Ana Aguilera*
Escuela de Ingeniería Informática
MEDING Interdisciplanary Center
Universidad de Valparaíso
Valparaíso 2340000, Chile
ana.aguilera@uv.cl

and

Irvin Dongo
Electrical and Electronics Engineering Department
Universidad Católica San Pablo
Arequipa 04001, Peru
Univ. Bordeaux, ESTIA INSTITUTE OF TECHNOLOGY
Bidart 64100, France
ifdongo@ucsp.edu.pe

Abstract

Semantic Technologies for the Internet of Things provide opportunities to improve interoperability, considering the multidimensional challenges. This study proposes the development of an enhanced ontology that integrates different ontologies in the IoT domain, including key aspects such as interoperability, security, privacy, energy efficiency, and ethics. A formal methodology for ontology design and construction was used in four phases: ontology requirements, design, construction, and evaluation. As a result, an enhanced ontology called IoTO++ was built. This five-module ontology improves operational efficiency in IoT environments. Furthermore, it facilitates the automation of data-driven decisions and actions, thereby enabling faster adaptation to changing environments. The validation emphasizes competence and quality criteria. OQuaRE framework was also used considering the quality model and metrics. IoTO++ achieves 100% in modularity and testability. In the rest of the subcategories it exceeds 89%, demonstrating its maintainability.

Keywords: IoT, Interoperability, Semantic, Ontology.

*Corresponding author. This study is an extended version of the work published in [1]. We extend our previous work by performing an updated search of related works (Section 2). We also extended the IoTO++ creation process by following a methodology for ontology creation. This allows us to perform the validation from another perspective emphasizing the criteria of competence and quality. The results are discussed in Section 4 and included in the concluding remarks in Section 5.

1 Introduction

The advancement of technology has enabled communication between devices for continuous improvement in industrial processes, home activities, and others. The Internet of Things (IoT) appears as a technology with billions of devices exchanging data in real-time, for better efficiency, optimizing resources, and enhancing the quality of life [1, 2]. IoT ecosystems facilitate the creation of intelligent environments, where devices collaborate for a better resource utilization and support innovative solutions for society, such as energy efficiency and environmental sustainability. However, one of the main challenges in IoT environments is achieving interoperability, i.e., the ability of diverse systems, devices, and platforms to communicate and share data properly. Interoperability is crucial to perform the full potential of IoT, enabling systems to function correctly in domains such as smart cities, healthcare, and industrial automation. But IoT systems face significant limitations due to the heterogeneity of devices, operating systems, protocols, and data formats [3].

Semantic technologies have emerged as powerful tools to address these interoperability challenges. RDF (Resource Description Framework) and ontologies describe real objects on the Web. Particularly, ontologies allow us to define and categorize data, as well as their relationships. By enabling a shared understanding of concepts, ontologies ensure that IoT devices and systems can interpret and use data among different applications. Some ontologies have been developed to address specific aspects of IoT, such as data description, energy efficiency, and privacy management [4, 5, 6]. However, as more devices and applications are available, modeling key aspects of IoT systems, including data privacy, security, energy awareness, and ethical considerations, are essential for interoperability. Current ontologies often lack comprehensiveness and extensibility, making it difficult to address the evolving needs of IoT environments. For example, while privacy and security are critical in managing the huge quantity of data generated by IoT devices, existing solutions frequently fail to provide robust frameworks for handling sensitive information securely. Additionally, ethical concerns such as fairness, accountability, and human well-being have limited attention in the context of IoT, despite their growing importance as devices gain more autonomy [7, 8].

Building ontologies to address these challenges requires the application of methodologies that can ensure the design, construction, and evaluation in order to obtain reusable and extensible proposals. Ontology development methodologies guide the systematic creation of ontologies by defining phases including requirements, conceptualization, design, implementation, and evaluation. These methodologies emphasize the importance of capturing domain knowledge defining classes and properties and validating competency questions to ensure that the ontology meets its intended purpose. Some methodologies such as METHONTOLOGY [9] are well-structured but hard to manage documentation for large ontology systems [10]. Bravo et al. [10] has been designed to promote the reutilization of ontologies. This latter proposes a four-phase approach specifically designed for IoT ontology development, which includes ontology requirements, design, construction, and evaluation. Methodologies are essential for developing scalable ontologies that can model the complexity of IoT environments and domains while addressing critical aspects such as data privacy, security, environmental awareness, and ethics.

In this context, we propose an enhanced ontology, called IoTO++, designed to address the limitations of existing IoT ontologies. This integrates multiple key domains-interoperability, data privacy, security, energy efficiency, and ethics-into a unified framework, providing a comprehensive solution for semantic interoperability in IoT environments. By building on existing ontologies such as SOSA and SEAS, it extends their scope and incorporates novel elements to address critical gaps. The ontology is designed to support diverse IoT applications, enabling seamless data integration, efficient resource management, and ethically responsible decision-making.

The paper is organized as follows. Section 2 describes the related works in the field of semantic interoperability for IoT. Section 3 presents the design and development of our ontology, detailing the requirements, design, and construction. Section 4 validates the ontology using qualitative and quantitative metrics. Finally, in Section 5, the conclusions and future research directions are presented.

2 Related work

In this section, we describe works related to semantic interoperability. To do so, we browsed Google Scholar using keywords: "'Ontology"', "'Interoperability"', "'Semantic"', and "'IoT"'. We considered all types of publications (i.e., conferences, journals) from 2019 until now. The works focus on smart infrastructures, frameworks, applications, and reviews related to semantic interoperability were selected. While this review does not cover all existing literature, this highlights key aspects that significantly contribute to the understanding of semantic interoperability in smart infrastructures and related fields. Smart infrastructures include smart cities [2], smart homes [11] and smart building [12].

Pliatsios [2] proposes in his PhD thesis a semantic interoperability in Internet of Things (IoT)-enabled environments, with a particular emphasis on the creation, testing, and evaluation of the Semantic Social Network of Things Middleware (S2NeTM) and the associated ontology. S2NeTM supports the Social IoT (SIoT) paradigm, a strategy in which IoT devices establish network connections like interpersonal interactions in humans with the purpose of enhancing group functionality and redefining IoT interactions according to common objectives. Ryabinin et al. [11] integrate the brain-computer interface (BCI) into the IoT ecosystem using ontology-driven tools. Experiments are conducted to control IoT devices with imaginary motions detected by electroencephalography (EEG) devices. Ontology manages the interoperability of IoT devices making easy for the end-users. Lakka et al. [12] structure SEMIoTICS architecture in three layers. These layers are field, SND/NFV orchestration and application orchestration. At the field layer, there is components of semantic mapping between different data models and of binding different protocol and exposing a common semantic API. The end-to-end semantic interoperability is ensured with the development of data transformation techniques and validation mechanisms. Two Thing directories are the repositories of knowledge containing the necessary Thing models.

Frameworks are concerned with foundations or guidelines for the development of IoT systems [13] or infrastructures [14]. Cimmino et al. [13] use a methodology to built an ontology for interoperability. For this, they rely on a three-level framework syntactic, technical, and semantic interoperability. The authors propose to use several ontologies that interact with each other. The VICINITY ontologies reuse terms from well-known standardized ontologies, such as the SSN ontology, the SOSA ontology, or the SAREF4BLDG ontology. Teniente [14] uses the CMTS ontology (Connectivity Management Tool Semantic Ontology) to improve interoperability and management in the IoT domain. The ontological framework is specifically designed to manage and monitor IoT physical infrastructures. It provides a complete set of concepts and properties needed to ensure effective connectivity and management of IoT devices in various environments.

There are many fields of IoT applications, these include health [15], agriculture [16], industry in general [17]. Ahamed and Chishti [15] offers a mechanism based on ontologies to provide semantic interoperability in an Internet of Things-based healthcare system for the cardiovascular domain. Diverse patient data is collected using sensors and electronic gadgets where the patients are located e.g. hospitals, apartments, local dispensaries etc. In this work, the ontology-based model is limited to collect this data. Pliatsios et al. [16] advise a Semantic Social Network of Things (SSNT) framework. It specifies the integration of device-to-device collaborative services. Heterogeneous objects are semantically enabled to interact and participate in communities of smart objects. These communities can assist users to achieve their objectives establishing social relationships and taking collaborative actions. A proof-of-concept application in the smart agriculture domain is presented. Diamantini et al. [17] propose a semantic approach for the integration of data streams from the field in the context of the Industrial Internet of Things (IIoT), providing insights of systems and supporting analytical tasks. For this purpose, they have worked on the conceptualization of the ontology and the related Process Aware IIoT Knowledge Graph, which allows connecting raw sensor data and higher-level knowledge in a manufacturing industry. The ontology the authors call "bridge" between other ontologies Semantic Sensor Network (SSN); Sensor, Observation, Sample and Actuators (SOSA); DogOnt (Dog); KPIOnto (KPI); Event ontology (ONP); Business Process Ontology (BPO).

Some literature surveys have been reported. Hafizur and Hussain [18] offer an overview of several semantic interoperability solutions so that researchers can easily catch up without having to go into the specifics included in the standards specifications. The challenges reported are summarized as follows: a) Semantic models are too complicated and heavy to produce timely and scalable answers in heterogeneous IoT networks; b) The large delay in large-scale IoT is attributed by the centralized semantic models, which is unsuitable for critical applications; c) It should also be easier to exchange semantically enhanced heterogeneous data across the Internet in accordance with their semantic context; d) A general ontology that supports many IoT applications and concepts can lead to a more intelligent future. Pliatsios et al. [19] focus on semantic interoperability within smart cities enabled by the Internet of Everything (IoE). The paper presents a systematic literature review that evaluates the maturity of available solutions in this context using criteria such as modeling, scalability, and availability. Among the semantic technologies studied, linked data modeling, semantic mapping and query and reasoning are highlighted, highlighting their application in various smart urban contexts. The study recognizes significant challenges, such as the heterogeneity of data and models, the need to develop scalable and secure solutions, and the maintenance of standards and models in a constantly evolving environment. Nilsson and Sandin [20] address semantic interoperability in Industry 4.0 as a topic of increasing importance due to the complexity of cyber-physical systems and the diversity of standards, components, tools, and services. The paper presents a systematic literature review to identify and analyze different automation approaches. Applied models, methodologies and relevant research results in this field have been examined. Several applied models are presented in the study, such as the Framework for Architectural Reference for Industry 4.0 (RAMI 4.0) and the Industrial Internet Reference Architecture

(IIRA). These models provide structures for integrating physical assets with their cyber information, as well as for describing different viewpoints in terms of business, usage, functionality and implementation. Potena et al. [21] present an Special Issue with scientific contributions in the form of theoretical foundations, models, experimental research, and case studies for IoT ecosystems. These contributions provide insights on recent advances in semantic modeling for IoT in a variety of applications including sectors such as healthcare, smart work and smart cities. Aspects such as service interoperability, sensor data integration, security and resource scalability are also treated.

Table 1 summarizes the works described in this Section except the reviews.

Table 1: Related work

Work	**Ontology**	**Concepts**	**IoT**	**Context**
[2]	S2NeTM interoperability with FOAF, SSN, and IoT-lite.	Entity, User, Service, Service Property, Location and Platform	Sensors to collect data, Social relationships	Smart cities: Green Route and healthcare
[11]	EBNeuro EEG device ontology	BCI and EEG device, EEG channel,device specifications	EEG device EBNeuro Be Plus LTM	Smart home: Pager of Things
[12]	Thing directories	-	Sensors (temperature)	Smart building
[13]	VICINITY ontology network	WoT, adapters, wot-mappings, datatypes	Sensors	IoT ecosystems
[14]	CMTS	Site, Devices	Sensors, cameras	IoT physical infrastructures
[15]	Self-built	Demographic and Behavioral Risks, Medical and Physical Examination, Prediction and Patient	Sensors to collect data	Health
[16]	eChair, eDesk, eLamp, eBook Ontology	eObjects, positions, Sensors, Services	Sensors (temperature, humidity, and thermal cameras), web services, and actuators.)	Agriculture: Greenhouse automation, crop management, and Monitoring of climate conditions
[17]	Bridge (self-built)	Activity,resource, task, measures	Sensors	Industrial and non-industrial

3 An enhanced ontology for Interoperability in IoT: IoTO++

While looking for other ontologies that cover the IoT domain, we observed that each of the authors develops their ontologies without following a specific methodology; this can lead to some lack of standardization or readability.

For that reason, IoTO++ was created using the methodology proposed by Bravo et al. [10], which encourages the reuse of ontologies by incorporating ontology modules from the beginning of the ontology construction. In this way, the owners of resulting ontology modules can reuse them inside the enterprise for more applications. The methodology consists of four phases summarized as follows:

- Ontology requirement: This phase includes the specification of requirements i.e. the identification of the ontology scope, the definition of possible scenarios, users, the competence of the ontology, and the required quality characteristics.

- Ontology design: This phase consists of the term elicitation (A list of terms relevant for the particular domain of knowledge has to be produced), ontology modules identification (Individual ontologies conforming to the ontology system has to be selected), individual ontology design and formalization (Hierarchical relationships, data and object properties relationships, and axiomatization have to be defined).

- Ontology construction: This phase comprises the use of an ontology editor and a standard language to code all ontology modules, and to integrate them into an ontology system.

- Ontology evaluation: This phase covers aspects related to the competency and quality evaluation of the ontology. A given set of competency questions permits verification that a representational model is complete. And, the degree to which an ontology model conforms to specified design criteria can be utilized to assess its quality.

Figure 1 shows the main phases and activities of the methodology.

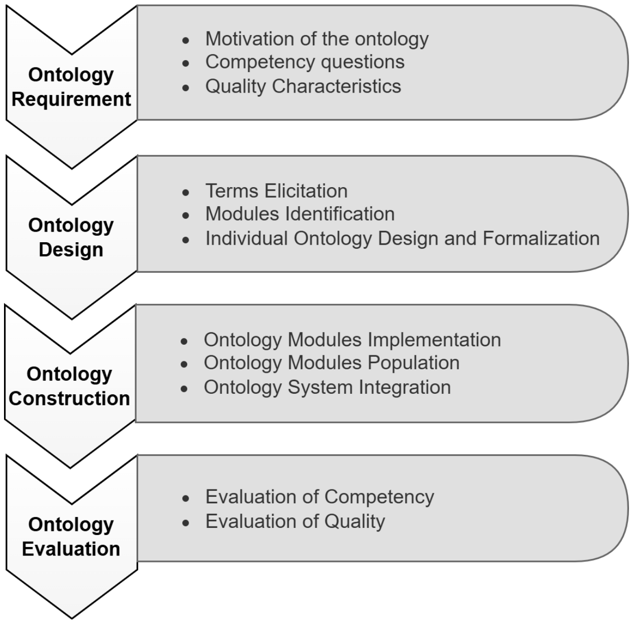

Figure 1: Phases and procedures for ontology construction [10]

3.1 Ontology Requirement

3.1.1 Motivation of the Ontology

In the related work section, we noticed that several ontologies cover the IoT domain to some extent. However, none of them model in detail the aspects of energy consumption, data security, privacy, or ethical issues. We believe that these are the main topics that an IoT ontology should include. Privacy and security facilitate the implementation of policies and mechanisms for safeguarding sensitive information. In addition, modeling environmental awareness by supporting context-aware systems allows resource usage optimization and minimizes ecological impacts. By embedding ethical principles, an ontology ensures that IoT systems act responsibly and prioritize human well-being and fairness in their operations.

3.1.2 Competency Questions

We constructed a gold standard in place of the competition questions. It contains a list of topics that an IoT ontology should consider to adequately model IoT environments and to provide a comprehensive solution. The list of topics, presented below, are the result of the research carried out in the related works, corresponding to the five modules that compose the proposed IotO++ ontology. The first four topics have been addressed in some way by previous works on semantic web and IoT environments. While the last, was considered since it is a topic of which there is a lack of knowledge to model IoT environments with a clear vision of ethics, accountability and transparency:

1. **Interoperability**:
   (a) IoT elements description
   (b) IoT data description
   (c) Spatio-temporal anchoring of data
   (d) Automated Orchestration
   (e) Standardized Protocols

2. **Data Privacy**:
   (a) Privacy Policies
   (b) Privacy Data Actors
   (c) Sensitive and non-sensitive data
   (d) Consent
   (e) Data Protection Principles

3. **Security**:
   (a) Secure Data
   (b) Categorizes Access Control
   (c) Regulations & Certifications
   (d) Data Security Actors
   (e) Data Protection Techniques

4. **Environmental Awareness**:
   (a) IoT elements Energy Consumption
   (b) Energy Types Categorization

5. **Ethics**:
   (a) Ethics Categories
   (b) Ethics Modes
   (c) Ethics Actors
   (d) Legislations

3.1.3 Quality Characteristics

IoTO++ is a domain ontology designed to model the knowledge generated by the IoT processes. As a general ontology, it can be adapted and applied to specific domains and IoT applications such as smart buildings, sensor predictions, and smart cities. Special emphasis is placed on ensuring clarity and extensibility throughout development to maintain consistency and quality.

3.2 Ontology Design

3.2.1 Terms Elicitation

An initial list of terms that are significant in the IoT knowledge domain must be generated. As a starting point, we took the gold standard previously defined and then identified the fundamental concepts (nouns) necessary to represent the ontology model. Table 2 lists the main nouns in each topic.

Table 2: Terms Elicitation

Interoperability	**Data Privacy**	**Security**	**Environmental Awareness**	**Ethics**
- Sensor -Actuator - Sample - Result - Evaluation -Observation - Measures - Feature of Interest	- Data - Privacy - Policies -Privacy Actors -Sensitive Information - Public Information -Consent - Disclosure - Contributor - Data control	- Access Control - Regulation - Certification - Security - Cripted Data - Crypto Manager - Hidden Data - Protected Data - Anonymous Data - Authentication	- Energy - Voltage - Battery - Energy Consumption	- Ethics Categories - Ethics Modes - Responsibility - Ethics Actors

3.2.2 Modules Identification

The IoTO++ modules were obtained from the gold standard explained in the previous phase. These include (i) interoperability, (ii) data privacy, (iii) security, (iv) environmental awareness, and (v) ethics. For each one of these categories, we looked for existing ontologies that model the topics we want to cover in IoTO++.

(i) Interoperability: With the ongoing advancements in sensor network technology, sensors worldwide are continuously generating data. However, integrating data from various sources is challenging owing to the lack of semantic consistency. The W3C Semantic Sensor Network Incubator group produced an OWL2 ontology to describe sensors and observations, the SSN ontology [4]. The SSN ontology provides a framework for describing the sensors based on their measurement processes, deployments, observations, and capabilities.

Based on the SSN ontology, there have been other efforts to improve interoperability in the IoT domain. Similar to Zhang et al. [22], they presented a solution for automatically mapping sensor data to the SSN ontology using a predefined XML-based document. Introducing a mapping language, SASML (Sensors Annotation, and Semantic Mapping Language), which provides a schema for annotating sensors and their sources, enabling the generation of an XML document for mapping purposes. In addition, the SDRM algorithm was created to automatically transform sensor data, described using SASML, into an RDF that conforms to the SSN ontology. Another example is the Sensor, Observation, Sample, and Actuator (SOSA) ontology [23] which provides a formal but lightweight general-purpose specification for modeling the interaction between the entities involved in the acts of observation, actuation, and sampling. This ontology emerges from a reevaluation of the SSN ontology. It stands independently without importing any other ontologies, ensuring freedom from vertical modules that enhance expressivity, or imposing additional ontological commitments on the lightweight semantics of the SOSA.

(ii) Data Privacy: Considering that IoT devices can communicate efficiently, it is possible to collect, process, and analyze data to offer insights into individual preferences and life patterns to provide personalized services. Nevertheless, the personal nature of these data and their associated risks have made privacy a critical concern. Even with growing legislative pressure, only a limited number of solutions have effectively addressed privacy requirements, including purpose specifications, consent, and limitations on data collection. We now explain the ontologies that solve this problem. Towards a new data-privacy-based approach for IoT, Loukil et al. [24] proposed a European legally compliant ontology to preserve privacy for IoT, called LIoPY. Using SSN ontology and incorporating privacy requirements from a legislative perspective.

Furthermore, OPIS IoT is an ontology-based privacy preservation approach for IoT [25]. In his thesis, Da Costa presented OPIS, which is an ontology that represents personal information on the sensor web. It is also based on an SSN ontology with two layers of semantic representations. The first is the semantic perception layer, which is used to build virtual sensors from the SSN sensor and observation classes. The second layer is the personal information layer, which defines a set of concepts used to represent the behavior of behavioral agents.

Another ontology related to data privacy is ColPri: IoT-collaborative privacy protection knowledge management ontology [6]. That is composed of the following modules:

- IoT System Description Module: This module builds upon the SSN framework to describe an IoT system. It also incorporates additional entities, such as edge services, gateways, and cloud infrastructure, to encompass all critical components of an IoT ecosystem.
- Data Module: Focused on characterizing the data produced by the IoT system, this module assigns the data to specific categories for better organization and management.
- Privacy Policy Description Module: ensures that every operation within the Data Lifecycle adheres to a privacy policy, which is governed by defined privacy attributes.
- Privacy Community Module: Designed to evaluate and recommend privacy policies, this module supports the activities of services and other key stakeholders within the privacy.

By analyzing work found in the literature, we noticed that even though there are ontologies used for privacy protection in the IoT. Those are not fully adaptive nor extensible ontologies.

(iii) Security Data security is another topic related to data privacy. Modern IT systems are characterized by their high complexity, growing number of subsystems, and the physical equipment required. This complexity creates challenges in maintaining the overall security of the architecture, as highlighted by numerous data breaches in recent years owing to inadequately secured systems. Therefore, an IoT environment requires proper storage, processing, and interpretation to obtain valuable insights. Research has been conducted on context-aware security in IoT environments and context-aware computing methods. In this section, we present some of these issues.

Denker et al. [26] conducted a research on security in the semantic web using OWL. They described the DARPA Agent Markup Language (DAML) family of ontologies, covering many security aspects such as access control, authentication, authorization, data integrity, key distribution, and policies.

The security toolbox (STAC) ontology [27] is a security ontology developed to assist non-security experts or software developers in recognizing and understanding key security concepts. These include attacks, security properties, security assets, and countermeasures, thereby enabling the design of secure software. This ontology defines essential security concepts including attacks, countermeasures, security properties, and their interrelationships. Countermeasures include cryptographic techniques (such as encryption algorithms, key management, digital signatures, and hash functions), security tools, and security protocols.

An Ontology-based Approach for Context-Aware Security in the IoT was developed using the STAC framework [28]. It was implemented in Protégé using pellet (incremental) reasoning to evaluate the ontology. This study values context-aware security in IoT environments and computing methods. This work models the concepts of authentication, access control, authorization, and privacy, employing a context-aware methodology to help non-expert users make informed security decisions. They collect data and transfer it between various healthcare devices to a knowledge base, ensuring the security of the context, such as patient data, by providing deeper insights and generating intelligent suggested solutions. Context-aware rules based on common experience for specific healthcare scenarios are incorporated to derive implicit insights among IoT nodes.

Pastuszuk et al. [29] present Dynamic Cybersecurity Ontology (DCO) for analysis of IT systems. This is the result of an analysis of existing cybersecurity ontologies, placing emphasis on being ready to support dynamic IT systems. Moreover, they presented a monitoring system based on the developed ontology, incorporating automatic data-mining mechanisms that aggregate results from dynamic knowledge sources such as Shodan or Censys. This enables the ontological examination of systems over time.

Gonzalez-Gil et al. [8] developed Lightweight Data-Security Ontology for IoT (ds4IoT) considering new regulations, such as General Data Protection Regulation (GDPR). It was done as a current demand for innovative approaches to data security, particularly regarding personal data. Their work represented data security concepts from the perspective of data. It incorporates new concepts like regulations, certifications, and provenance alongside traditional concepts such as access control methods and authentication mechanisms. This ontology distinguishes itself from previous works through its bottom-up approach and by addressing modern, relevant concepts in data security, emphasizing implicit knowledge over explicit knowledge representation.

(iv) Environmental Awareness: Environmental, economic, and sustainability challenges related to the ongoing rise in energy consumption are widespread globally. Recent changes in the electricity sector over the past few decades have significantly increased the complexity and unpredictability of power and energy systems (PES). To address this volatile environment, various software tools are available to simulate, analyze, test, and support decision-making for different entities in the sector. However, because these tools are developed for specific PES subdomains, they often lack interoperability, preventing the creation of more comprehensive simulations, management strategies, operations, and decision-support scenarios. That is why is important to work on interoperability but also environment aware ontology solutions.

The Smart Energy Aware Systems (SEAS) project tackles the issue of inefficient and unsustainable energy consumption [5]. This arises from the lack of adequate tools to control, monitor, estimate, and adapt the energy usage of systems in response to dynamic situations and conditions that impact them. This project presents a knowledge model that serves as a foundation for semantic interoperability within the SEAS ecosystem. The SEAS knowledge model is built on an innovative web ontology that has three main modules:

- seas:FeatureOfInterestOntology describes feature of interests and their properties;
- seas:EvaluationOntology details evaluations of these properties;
- seas:SystemOntology describes virtually isolated systems that share connections with other systems;

Additionally, the SEAS knowledge model provides the necessary expressivity for use cases while also being extensible to other use cases and domains, such as gas, water, air, and waste management.

An Intelligent Energy Systems Ontology (IESO) [30] was developed to support market and power system co-simulation interoperability within a society of multi-agent systems (MAS) in the context of PES. It provides agents with capabilities such as semantic reasoning, constraints validation, and data uniformization.

(v) Ethics: IoT environments offer significant societal benefits by enabling a wide range of user applications. However, the ethical implications of adopting such a pervasive technology on a large scale have not been adequately addressed. Smart devices equipped with artificial intelligence may make decisions that have ethical consequences. In our research, we did not find an ontology that fully modeled ethics in IoT environments. As a result, we decided to expand our research and found existing works that could help us model an initial version of this module.

The work of Siemers and Adamson [31] provides the ontological foundations for the Ethics of Technology. They proposed studying this matter through the lens of technology ontology. The concept of agency was used as an example to illustrate the connection between ontology and ethics. Initially, the relevance of the agency to various ethical discussions on technology was explored. The study then shows that any ethical stance on agency must be grounded in a position where agency resides. Ultimately, it is suggested that the question of where agency resides is (1) a factual question concerning specific entities (an 'ontic' question) and (2) a question regarding the nature of technology's being (an 'ontological' question).

Sholla et al. [7] considered the relevance in the design of ethics aware systems for the Internet of Things. They reaffirm the fact that it is often assumed that the functioning of IoT devices does not involve any ethical responsibility in relation to their context of application. This view can lead to situations that jeopardize core human values or cause physical or emotional harm. Therefore, it is crucial to integrate ethics into the design of intelligent systems to protect human interest. To address these issues, They propose a novel approach based on Boolean algebra, which allows machines to display varying ethical behavior through the use of *ethics categories* and *ethics modes*.

As a result of this knowledge acquirement phase, we selected two ontologies that are publicly available for Interoperability and Environmental Awareness (SOSA [23] and SEAS [5] respectively). Regarding the other modules, we did not find ontologies that were completely available, but their article descriptions allowed us to infer the main classes they introduced. This is the case for Data Privacy and Security module (ColPri [6] and ds4IoT [8]). Moreover, for the ethics module, we did not find an ontology that could be reused or extended. That is why based on the literature we will present an initial version of it in the next subsection.

Table 3 presents a summary of all ontologies considered to build IoTO++. We mark with a ✓if the ontology considers the elicited terms in each module (Table 2). Additionally, we evaluated the following:

- Availability: specifically whether it is hosted in a web repository that facilitates direct extension of the ontology.
- Reasoning: although most of the ontologies are enabled to work with a reasoner because they are developed in OWL-DL, not all of them have done experiments along a reasoner to validate this. We marked as Yes, publications that specify with which reasoner they work with.
- Specific Domain: the majority of the ontologies reviewed were designed for an specific domain or use case scenario. Only SSN and SOSA are domain ontologies. That is why they were imported and extended by [24] and [6].

Table 3: Already existing ontologies summary

Ontology Name	**Year**	**Interoperability**	**Data Privacy**	**Security**	**Environmental Awareness**	**Public Available**	**Includes Reasoner**	**Specific Domain**
SSN	2012	✓				Yes	No (OWL2 DL)	No
SOSA	2019	✓				Yes	No (OWL2 DL)	No
LIoPY	2018	✓	✓			No	Yes (OWL y SWRL)	Yes
OPIS IoT	2017	✓	✓			Yes	Yes (OWL DL)	Yes
Colpri	2020	✓		✓		No	No(OWL)	Yes
DAML	2005			✓		No	No(OWL)	Yes
STAC	2013			✓		Yes	Yes (OWL)	Yes
DCO	2021			✓		No	No (OWL)	Yes
ds4IoT	2020		✓	✓		Yes	No(OWL DL)	Yes
SEAS	2016				✓	Yes	No(OWL 2)	Yes
IESO	2023				✓	Yes	Yes (OWL 2 DL)	Yes

3.3 Ontology Construction

As we stated, IoTO++ is the result of integrating several pre-existing ontologies. To aid the visualization of the classes and relationships extended and/or added in IoTO++, figures extracted from the ontology editor are included. The yellow circular icons (Figure 3) represent classes and the blue rectangular icons (Figure 2) represent relations. In all Figures in this Section the nomenclature *prefix:ClassName* is respected. The classes or relations that do not have a prefix, i.e. that begin with the colon symbol, are all those included by IoTO++. The final version of IoTO++ is available in a public repository [1].

3.3.1 Ontology Module Implementation

While several ontology editors are available, this study utilized Protégé[2], as recommended by Bravo *et al.*. As an open-source editor, Protégé is regularly updated, thus providing the benefits of extensive support within the developer community. The main modules of the proposed ontology are described as follows:

(i) Interoperability The base ontology used for this module is **SOSA Ontology** [23]. That is a redesigned version of the W3C-XG Semantic Sensor Network (SSN) [32] ontology, influenced by changes in scope and intended users, technological advances, and knowledge gained over time. This ontology is under

[1] https://github.com/Alex23013/Ioto-Semantic-for-IoT-Environments
[2] https://protege.stanford.edu/

constant revision and extension and is supported by the W3C[3]. Furthermore, SSN has emerged as a de facto standard for semantic sensor annotation within the Sensor Web ecosystem [25].

This module considers concepts related to the description of both the IoT system elements and the data they generate. It is also important to add a spatio-temporal anchoring of the data. For which IoTO++ extends from SOSA classes such as: *sosa:phenomenonTime* and *sosa:resultTime*. As well as Colpri properties such as *colpri:hasDateTime*.

As IoT systems become increasingly complex, it is important to give IoT ontologies the capability of automated orchestration. SOSA and SEAS ontologies model the interconnection of the elements that make up IoT systems. Through relationships such as: *seas:connectedThrough*, *seas:connectedTo*, *seas:connectsSystem*, among others (see Figure 2).

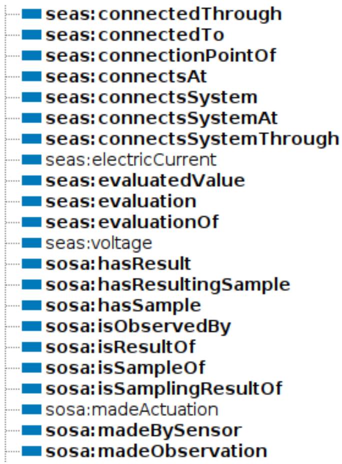

Figure 2: Some relationships for the Interoperability module.

This interoperability module also includes the necessary classes to facilitate the implementation of standardization protocols for IoT elements (*sosa:sensor*, *sosa:Sampler*, *sosa:Actuator*) and the data they model (*sosa:Observation*, *sosa:Result*, *sosa:Stimulus*) (see Figure 3).

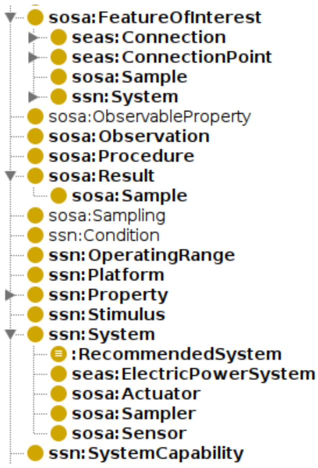

Figure 3: Classes associated with interoperability extracted from the SSN, SOSA and SEAS ontologies.

(ii) Data privacy The base ontology used in this module is **ColPri** Ontology, focused on the management of knowledge related to privacy protection [6]. The Privacy Attributes defined by the classes: (i) *colpri:Consent*; (ii) *colpri:Disclosure* and (iii) *colpri:Purpose*. Also the classes *colpri:DataLifeCycle* and *colpri:DataLifeCycleStep*, which define the data life cycle. This is important in order to model in which life cycle process the Privacy Community Members interact with the data.

The concept of *colpri:PrivacyCommunityMember*, where *colpri:Administrator* and *colpri:Contributor* give evaluations (*colpri:PrivacyPolicyEvaluation*) and recommendations (*colpri:Recommendation*) through evalu-

[3]https://www.w3.org/

ations to privacy policies (*colpri:PrivacyPolicy*). These policies regulate the use of sensitive or non-sensitive data (*colpri:SensitivePersonalData* or *colpri:NonSensitivePersonalData*).

Other categories that are modeled in this module correspond to the Data Protection Principles [33]. For example, for the principle of Specification we create the class *:DataController* that through the relationship *:definesPurpose* must define the purpose of the privacy attributes (*colpri:PrivacyAttribute*). For the data collection limitation principle, always with the consent of the subject involved, we have the Consent class (*colpri:Consent*) and its subclasses *colpri:GivenConsent* and *colpri:UngivenConsent*.

(iii) Security For this module we use **ds4IoT Ontology** [8]. This ontology covers the security representation of data, approaching it uniquely from the data point of view. It introduces concepts such as standards, certifications and provenance, in addition to traditional ideas such as access control methods and authentication mechanisms. ds4IoT defines actors involved in data security as *ds4iot:CapabilityManager*, *ds4iot:AuthenticationProvider* and *ds4iot:CryptoManager*. In IoTO++, the class *:SecurityCommunityMember* is created to include all these classes.

This module also includes the categorization of secure data. For data protection techniques [33], *ds4iot: CryptoManager* is included, which is responsible for masking the data (*ds4iot: EncryptedData*) or hiding it (*ds4iot: hiddenData*) if that is required. Techniques of pseudonymization or anonymization of data, are relate to *colpri: PseudoAnonymousData* and *colpri: AnonymousData*, respectively.

(iv) Environmental Awareness

The base ontology of this module is **SEAS Ontology** selected for its interest in building systems that are aware of energy consumption [5]. This module considers the classes *seas:ElectricEnergyProperty* and *seas:ElectricPowerEnergy*, among other classes that seek to describe the properties related to the types of Energy consumed by the IoT system elements. It also defines the types of Energy that could be used or produced by IoT systems such as *seas:ElectricEnergy*, *seas:HeatEnergy*, among others.

On the other hand, SSN has another strategy to address the problem of energy consumption, emphasizing the energy required for the correct operation of IoT elements. We select from it classes such as *ssn:OperatingPowerRange*, *ssn:BatteryLifetime* and *ssn:SystemLifetime*, among others.

(v) Ethics As we said in previous sections, we did not find an ontology that solved the problem of modeling Ethics for IoT systems. This is why IoTO++, proposes a general module that can serve as a basis for future extensions. This ethics module is based on the work of Sholla *et al.* [7] that presents a boolean algebra model.

In order to relate IoTO++ with its predecessors, relations and restrictions are added. For example, to express that "It is mandatory for the DataController to define the Purpose of the collected data", a *owl:Constraint* is used to specify that each *:DataController* must have at least one *:definesPurpose* relation. To link this requirement to the ethical category *:Mandatory*, the relationship *:hasEthicCategory* is added, with *:DataController* as the domain and *:EthicCategory* as the range.

In the case of Ethics Modes, to express that "It is recommended that IoT systems have a Mild ethical mode (*:Mild*), meaning a mode that allows all but forbidden scenarios", a relationship *:hasEthicMode* is created, with *ssn:System* as its domain and *:EthicMode* as its range. In the actors related to Ethics, *DataController* is added. The main role of this actor is to be responsible for everything related to security, privacy and ethics of IoT systems. To represent this role, the relationships *:takesResponsibilityForStep* and *:takesResponsibilityForThing* are added. As well as the classes:

- *:stepToTakeResponsibilityFor*: that includes the elements of the data life cycle (*colpri:DataArchiving*, *colpri:DataCollection*, etc.) and
- *:thingToTakeResponsibilityFor*: that comprises privacy attributes like *colpri:Disclosure*, *:PrivacyPolicyEvaluation* among others.

Additionally, this actor is in charge of defining purposes, as seen in a previous example. Finally, as a member of the class *colpri:PrivacyCommunityMember*, it can make Consents (*:makesConsent*) and Declarations (*:makesDisclosure*). These and more relations, included in the Ethics module are shown in Figure 4.

Finally, in the topic of Legislation, an example of use is added for the rights of protected data in Chile[4]. This work considers, the rights of: cancellation, access, rectification, opposition and portability. For them, IoTO++ includes the relationship *:isProtectedIn* that has *:LegalRight* as domain and *:Country* as range.

[4]https://www.bcn.cl/leychile/navegar?idNorma=141599

Figure 4: Relationships for the Ethics module.

3.3.2 Ontology Module Population

The ontology modules were populated and seamlessly integrated into the ontology system. The final ontology system comprises 1095 axioms, 155 classes, 65 object properties, 3 data properties, and 29 individuals. These metrics (Figure 5) were extracted using the Protégé tool.

Metrics

Axiom	1,095
Logical axiom count	353
Declaration axioms count	260
Class count	155
Object property count	65
Data property count	3
Individual count	29
Annotation Property count	24

Figure 5: Protege metrics

As part of the Ontology Module Population, we illustrated IoTO++ using graph visualization and Descriptive Logic (DL). Figure 6 shows a graph visualization and equation 1 its DL formalization for the `ioto:DataController` class.

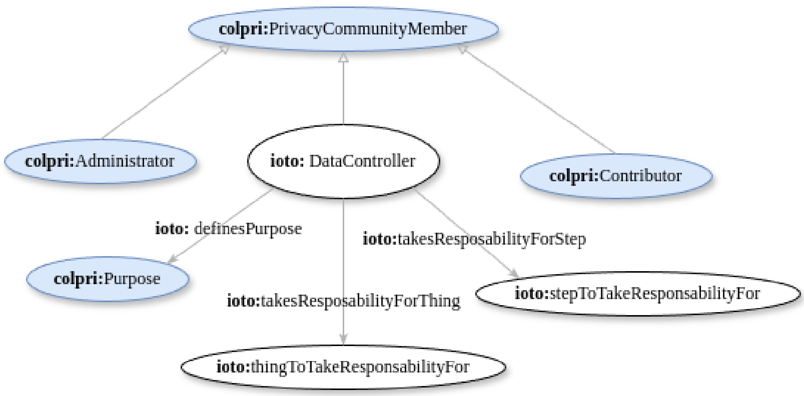

Figure 6: Graph visualization of formal definition of Data Controller class

$$Tbox = \left\{ \begin{array}{c} DataController \equiv \\ \exists definesPurpose.Purpose \sqcap \\ \exists takesResponsabilityForThing.thingToTakeResponsability \sqcap \\ \exists takesResponsabilityForStep.stepToTakeResponsability, \\ Administrator \subseteq PrivacyCommunityMember, \\ DataController \subseteq PrivacyCommunityMember, \\ Contributor \subseteq PrivacyCommunityMember, \end{array} \right\} \quad (1)$$

IoTO++ is an extension ontology built on the basis of its predecessors (SOSA, ColPri, ds4Iot and SEAS) which have been developed in OWL DL and OWL 2. They are therefore compatible with automatic reasoners giving the proposed ontology the ability to work with a reasoner if needed.

3.3.3 Ontology System Integration

Bravo et al. establish that the objective of performing an ontological evaluation is to demonstrate the conformity of a world model with a formally modeled world [10]. This is achieved focusing in Competence and Quality criteria. The next section explains the evaluation of IoTO++ using these criteria.

4 Validation of IoTO++

In a previous study, to validate IoTO++, we used the ontology comparison method proposed by Cardinale et al. [34]. This method proposes a methodological process to qualitatively and quantitatively compare ontologies at lexical, structural, and domain knowledge levels. We performed a level-by-level comparison in our previous study [1]. In the present work, we review the results obtained from a different perspective considering mainly the criteria of Competence and Quality, recommended by Bravo et al. [10].

4.1 Evaluation of Competency

Competence is achieved by ensuring that the ontology can answer an initial set of competence questions [10]. In our case the gold standard (Section 3.1.2).

Table 4 shows the result of the Knowledge Coverage evaluation. IoTO++ was evaluated, along with its predecessors, within the gold standard. When the ontology exhibits classes or properties that allow to model the subcategory evaluated it is marked with ✓. Also, in the last column of Table 4, the percentage (%) of categories modeled is presented. It is important to note that IoTO++ manages to cover all the categories proposed by the gold standard. Thus, becoming the most suitable ontology for modeling complex IoT systems.

Table 4: Knowledge Domain for IOT Ontologies

Ontologies	**Interoperablity**					**Data Privacy**					**Security**					**Environmental Awareness**		**Ethics**				**Categories modeled**
	(a)	(b)	(c)	(d)	(e)	(a)	(b)	(c)	(d)	(e)	(a)	(b)	(c)	(d)	(e)	(a)	(b)	(a)	(b)	(c)	(d)	%
SOSA	✓	✓	✓		✓											✓						23.81
SEAS		✓		✓	✓											✓	✓					23.81
ColPri			✓			✓	✓	✓	✓	✓					✓							19.05
ds4IoT											✓	✓	✓	✓	✓							23.81
IoTO++	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	100%

4.2 Evaluation of Quality

Regarding quality, the ontology must be [10]: clear and coherent. For that reason, definitions should be stated in formal axioms, like the ones presented in Eq. 1. Moreover, it is important that the ontology built is modular, allowing reuse, maintenance and evolution of the ontology. This requirement was achieved in IoTO++ by dividing the model into five independent ontologies. Each of these ontologies is independent and reusable.

In addition to the methods for testing the quality suggested in Bravo et al., we reviewed the results obtained using the Oquare methodology. This validates the quality of ontologies based on SQuaRE[5], which is a Software Engineering standard. These metrics propose a framework called OQuaRE[6], which considers two components: a Quality Model and Quality Metric. The OQuaRE Quality Metrics [35] are calculated **in Table 5**. Each metric was rated with a score ranging from 1 to 5.

In isolation, these metrics do not provide much value for analysing ontologies. This is why the OQuaRE Quality Model is necessary. It considers the following categories: Structural, Functional Adequacy, Reliability, Operability, Compatibility, Transferability and Maintainability. The results for the selected categories are detailed in the following:

- **Functional Adequacy**: this is the ability of ontologies to provide concrete functions. Sub-characteristics assessed: Knowledge acquisition-representation, Knowledge Reuse and Consistent search and query. Fig. 7 shows the result of the evaluation of this category, where it can be seen that the IoTO++ proposal is equal or superior to the other ontologies analyzed. It even excels in the sub feature of consistent search and queries.

- **Maintainability:** this is the ability of ontologies to be modified by changes in environments, requirements or functional specifications. Fig. 8 shows the result of the evaluation of the Maintainability

[5] SQuaRE: ISO/IEC 25000:2005 standard for Software product Quality Requirements and Evaluation
[6] http://miuras.inf.um.es/evaluation/oquare/

Table 5: OQuaRE Quality Metrics Score for IoT Ontologies

Metrics	SSN-SOSA		SEAS		ColPri		ds4IoT		IoTO++	
	Value	Score	Valor	Score	Value	Score	Value	Score	Value	Score
Lack of Cohesion in Methods (LCOMOnto)	3.778	4	2.417	4	3.971	4	1.600	5	2.531	4
Weigth method per class (WMCOnto)	6.000	4	1.061	5	2.755	5	1.330	5	2.183	5
Depth of subsumption hierarchy (DITOnto)	4.000	4	3.000	4	5.000	3	3.000	4	5.000	3
Number of Ancestor Concepts (NACOnto)	5.611	3	1.621	5	1.816	5	1.666	5	0.854	5
Number of Children Concepts (NOCOnto)	4.280	4	3.435	4	3.000	5	2.500	5	4.028	4
Coupling between Objects (CBOOnto)	0.651	5	0.804	5	0.897	5	1.923	5	1.000	5
Response for a concept (RFCOnto)	0.651	0	3.390	4	1.435	5	1.250	5	1.293	5
Number of properties (NOMOnto)	1.073	5	1.386	5	0.308	5	0.185	5	0.339	5
Relationship Richness (RROnto)	17%	1	51%	3	19%	1	11%	1	21%	2
Attribute Richness (AROnto)	129%	5	100%	5	275%	5	174%	5	418%	5
Relationships per concept (INROnto)	492%	5	131%	5	130%	5	148%	5	128%	5
Annotation Richness (ANOnto)	697%	5	733%	5	113%	5	7%	1	256%	5
Tangledness (TMOnto)	0.674	5	0.781	5	0.884	5	0.890	5	0.874	5

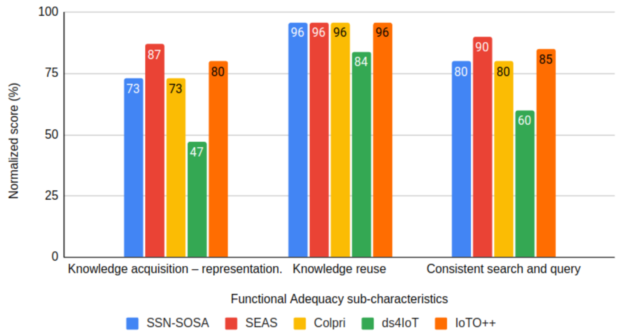

Figure 7: Quality Model: Functional Adequacy.

category of the OQuaRE Quality model. IoTO++ achieves 100% in modularity and testability. In the rest of the subcategories, it exceeds 89% showing a similar behavior to the other ontologies studied, which reveals that they are all maintainable ontologies.

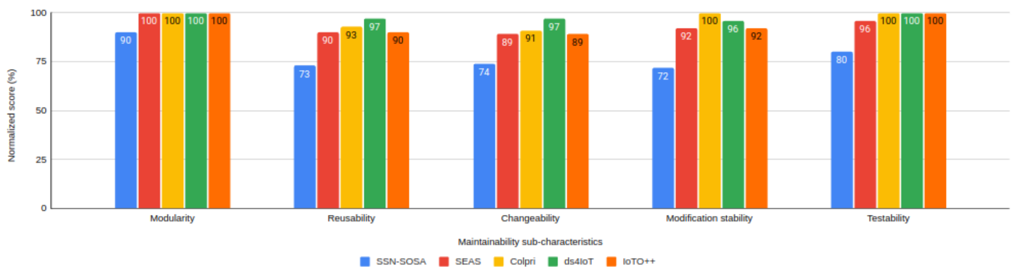

Figure 8: Quality Model: Maintainability.

- **Compatibility, Operability and Transferability** Fig. 9 shows the result of the evaluation of these categories of the OQuaRE Quality model. In all subcategories IoTO++ exceeds 85% which ensures that it can be easily learned by new users for future use in various applications, as well as its adaptability and usability in different contexts.

5 Conclusions

In conclusion, we have updated and revised the version of the IoTO++ ontology proposed above. The application of a methodology for the creation of ontologies that model complex environments, such as IoT environments, was presented. The use of more tools for ontology evaluation (such as the reasoner pellet) and the Protege framework itself were added. Each author can develop an ontology by defining requirements and

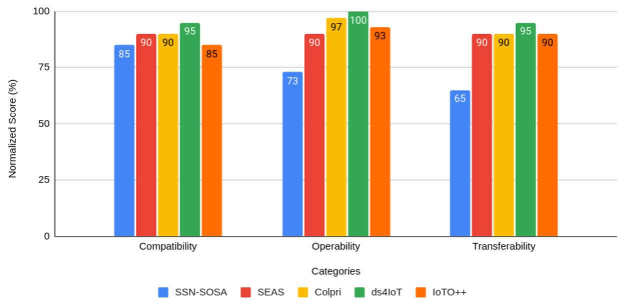

Figure 9: Other categories of oQuare model: Compatibility, Operability and Transferability.

implementing them according to the needs of the application. It is relevant to develop general ontologies that can be applied to multiple scenarios, for which it is important to follow methodological development.

As future work, IoTO++ can be instantiated in real-world scenarios such as smart homes, industrial IoT, or urban mobility systems, in order to demonstrate its versatility and practical applicability. Moreover, integration with established IoT standards (e.g., oneM2M, W3C SSN/SOSA) could enhance semantic interoperability across platforms. Additional performance evaluations-such as measuring reasoning times, system scalability, and integration responsiveness-would further validate the ontology's robustness and efficiency.

Acknowledgment

This study was funded by PROCIENCIA as executing entity of CONCYTEC under grant agreement no. PE501083407-2023-PROCIENCIA, project: Semantic and Distributed Repository for Low-resource Devices and fast Response in Urban Tourism.

References

[1] A. Aguilera, D. Garrido, I. Dongo, and M. Cornejo-Lupa, "IoTO++: an enhanced interoperability based on semantic for IoT environments," in *2024 L Latin American Computer Conference (CLEI)*, 2024, pp. 1–10.

[2] A. Pliatsios, "An ontology-based middleware for enhancing semantic interoperability in IoT-enabled smart city applications," Ph.D. dissertation, Department of Information and Communication Systems Engineering, 2024.

[3] K. Thakur, A.-S. K. Pathan, and S. Ismat, *Internet of Things (IoT)*. Springer Nature Switzerland, 2023, pp. 165–183.

[4] A. Haller, K. Janowicz, S. J. Cox, M. Lefrançois, K. Taylor, D. Le Phuoc, J. Lieberman, R. García-Castro, R. Atkinson, and C. Stadler, "The modular SSN ontology: A joint W3C and OGC standard specifying the semantics of sensors, observations, sampling, and actuation," *Semantic Web*, vol. 10, no. 1, pp. 9–32, 2019.

[5] M. Lefrançois, "The SEAS knowledge model," Ph.D. dissertation, ITEA2 12004 Smart Energy Aware Systems, 2017.

[6] A. Toumia, S. Szoniecky, and I. Saleh, "ColPri: Towards a Collaborative Privacy Knowledge Management Ontology for the Internet of Things," in *5th International Conference on Fog and Mobile Edge Computing (FMEC)*. IEEE, 2020, pp. 20–23.

[7] S. Sholla, R. N. Mir, and M. A. Chishti, "Towards the design of ethics aware systems for the internet of things," *China Communications*, vol. 17, no. 2, pp. 239–252, 2020.

[8] P. Gonzalez-Gil, J. A. Martinez, and A. F. Skarmeta, "Lightweight data-security ontology for IoT," *Sensors*, vol. 20, no. 3, p. 801, 2020.

[9] M. Fernández-López, A. Gómez-Pérez, and N. Juristo, "Methontology: from ontological art towards ontological engineerin," American Asociation for Artificial Intelligence, Spain, Technical Report SS-97-06, 1997.

[10] M. Bravo, L. F. Hoyos Reyes, and J. A. Reyes Ortiz, "Methodology for ontology design and construction," *Contaduría y administración*, vol. 64, no. 4, 2019.

[11] K. Ryabinin, S. Chuprina, and I. Labutin, "Tackling IoT interoperability problems with ontology-driven smart approach," in *Science and Global Challenges of the 21st Century - Science and Technology.* Cham, Switzerland: Springer, Oct. 2021, pp. 77–91.

[12] E. Lakka, N. E. Petroulakis, G. Hatzivasilis, O. Soultatos, M. Michalodimitrakis, and U. Rak, "End-to-end semantic interoperability mechanisms for IoT," in *24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD).* IEEE, 2019, pp. 11–13.

[13] A. Cimmino, A. Fernández-Izquierdo, M. Poveda-Villalón, and R. García-Castro, "Ontologies for IoT semantic interoperability," in *IoT Platforms, Use Cases, Privacy, and Business Models.* Cham, Switzerland: Springer, Jul. 2020, pp. 99–123.

[14] E. Teniente, "Iot semantic data integration through ontologies," in *International Conference on Services Computing (SCC).* IEEE, jul 2022.

[15] J. Ahamed and M. A. Chishti, "Ontology based semantic interoperability approach in the internet of things for healthcare domain," *Journal of Discrete Mathematical Sciences and Cryptography*, Aug. 2021.

[16] A. Pliatsios, C. Goumopoulos, and K. Kotis, "A review on IoT frameworks supporting multi level interoperability the semantic social network of things framework," *International Journal on Advances in Internet Technology*, vol. 13, no. 1-2, pp. 46–64, 2020.

[17] C. Diamantini, A. Mircoli, D. Potena, and E. Storti, "Process-aware IIoT knowledge graph: A semantic model for industrial iot integration and analytics," *Future Generation Computer Systems*, vol. 139, pp. 224–238, 2023.

[18] Hafizur and Md. I. Hussain, "A comprehensive survey on semantic interoperability for internet of things: State-of-the-art and research challenges," *Trans. Emerging Telecommun. Technol.*, vol. 31, no. 12, p. e3902, Dec. 2020.

[19] A. Pliatsios, K. Kotis, and C. Goumopoulos, "A systematic review on semantic interoperability in the IoE-enabled smart cities," *Internet of Things*, vol. 22, p. 100754, Jul. 2023.

[20] J. Nilsson and F. Sandin, "Semantic interoperability in industry 4.0: Survey of recent developments and outlook," in *IEEE 16th International Conference on Industrial Informatics (INDIN)*, 2018, pp. 127–132.

[21] D. Potena, A. Longo, A. Mircoli, and M. Zappatore, "Semantic modeling and design patterns for IoT ecosystems," *Future Generation Computer Systems*, vol. 142, pp. 1–3, May 2023.

[22] X. Zhang, Y. Zhao, and W. Liu, "A method for mapping sensor data to SSN ontology," *International Journal of u-and e-Service, Science and Technology*, vol. 8, no. 9, pp. 303–316, 2015.

[23] K. Janowicz, A. Haller, S. J. Cox, D. Le Phuoc, and M. Lefrançois, "SOSA: A lightweight ontology for sensors, observations, samples, and actuators," *J. of Web Semantics*, vol. 56, pp. 1–10, 2019.

[24] F. Loukil, C. Ghedira-Guegan, K. Boukadi, and A. N. Benharkat, "Liopy: A legal compliant ontology to preserve privacy for the internet of things," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2. IEEE, 2018, pp. 701–706.

[25] T. M. Da Costa, "OPP_IoT an ontology-based privacy preservation approach for the internet of things," Ph.D. dissertation, Université Grenoble Alpes, 2017.

[26] G. Denker, L. Kagal, and T. Finin, "Security in the semantic web using OWL," *Information Security Technical Report*, vol. 10, no. 1, pp. 51–58, 2005.

[27] A. Gyrard, C. Bonnet, and K. Boudaoud, "The STAC (security toolbox: attacks & countermeasures) ontology," in *Proceedings of the 22nd International Conference on World Wide Web*, 2013, pp. 165–166.

[28] A. Nazir, S. Sholla, and A. Bashir, "An ontology based approach for context-aware security in the internet of things (IoT)," *International Journal of Wireless and Microwave Technologies (IJWMT)*, vol. 11, no. 1, pp. 28–46, 2021.

[29] J. Pastuszuk, P. Burek, and B. xn Ksi-xnbżopolski, “Cybersecurity ontology for dynamic analysis of it systems,” *Procedia Computer Science*, vol. 192, pp. 1011–1020, 2021, knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 25th International Conference KES2021.

[30] G. Santos, H. Morais, T. Pinto, J. M. Corchado, and Z. Vale, “Intelligent energy systems ontology to support markets and power systems co-simulation interoperability,” *Energy Conversion and Management: X*, vol. 20, p. 100495, 2023.

[31] P. Siemers and G. Adamson, “Ontological foundations of the ethics of technology,” in *2021 IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS)*, 2021, pp. 1–7.

[32] M. Compton *et al.*, “The SSN ontology of the W3C semantic sensor network incubator group,” *J. of Web Semantics*, vol. 17, pp. 25–32, Dec. 2012.

[33] C. Vilches, “Biblioguias: Gestión de datos de investigación: Protección, derechos y acceso a los datos,” Jan. 2024, [Online; accessed 17. Apr. 2024].

[34] Y. Cardinale, M. A. Cornejo-Lupa, A. Pinto-De la Gala, and R. Ticona-Herrera, “Application of a methodological approach to compare ontologies,” *International J. of Web Information Systems*, vol. 17, no. 4, pp. 333–376, 2021.

[35] A. Duque-Ramos, J. Fernandez-Breis, R. Stevens, and N. Aussenac-Gilles, “Oquare: A square-based approach for evaluating the quality of ontologies,” *J. of Research and Practice in Information Technology*, vol. 43, pp. 159–176, 05 2011.