Internet of Things 11 (2020) 100206

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Semantic Web Technologies for the Internet of Things: Systematic Literature Review

Ahlem Rhayem*, Mohamed Ben Ahmed Mhiri, Faiez Gargouri

Miracl-laboratory, Sfax University, Tunisia

ARTICLE INFO

Article history:
Received 5 February 2020
Revised 27 March 2020
Accepted 28 April 2020
Available online 6 May 2020

Keywords:
Internet of Things
Web of Things
Semantic Web Technologies
Ontology
Interoperability
Standards

ABSTRACT

Nowadays, the use of the Internet of Things (IoT) in diverse applications becomes very popular. Accordingly, a proliferation of objects with remote sensing, actuation, analysis, and sharing capabilities will be interconnected on top of heterogeneous communication networks. Their deployment contexts are continuously changed, which imply a change in their descriptions and characteristics. In addition, they are a fundamental source of a huge quantity of gathered data with different encoding formats. Accordingly, this data is badly expressed, understood and exploited by other systems and devices. From this regard, several challenges associated with standardization, interoperability, discovery, security, and description of IoT resources and their corresponding data have emerged. In this context, Semantic Web Technologies (SWT) seem a suitable and an efficient solution to relieve these challenges. Therefore, a Systematic Literature Review (SLR) methodology is performed to investiagte and analyze a set of the most recent and relevant approaches that deal with SWT in the IoT domain. These approaches are discussed and evaluated based on seven different research questions. Finally, future insights and research opportunities are suggested.

1. Introduction

1.1. Context

In order to ensure a comfortable life, a myriad of stakeholders become interested in integrating daily life objects into the network in the field of information technologies. Sensors, actuators, and RFID tags are widely exploited to enable this integration. From this perspective, users have the ability to access real-time information gathered by connected objects any time and anywhere. The evolution of using internet with real-world objects has led to the rise of the Internet of Things (IoT). The International Telecommunication Union defines the IoT as a global infrastructure for the Information Society, which enables advanced services to connect (physical and virtual) things based on existing and evolving interoperable information and communication technologies [1]. In addition, Perera et al. [2] affirmed that "The IoT allows people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service". In fact, billions of devices and node sensors, become connected to each other with potential capabilities to sense, communicate and share data and information about their surrounding environment.

* Corresponding author.
E-mail addresses: ahlemrhayem@gmail.com (A. Rhayem), med.mhiri@gmail.com (M.B.A. Mhiri), faiez.gargouri@isims.usf.tn (F. Gargouri).

https://doi.org/10.1016/j.iot.2020.100206
2542-6605/© 2020 Elsevier B.V. All rights reserved.

IoT is mainly based on the Wireless Sensor Networks field (WSN) that has emerged as one of the most promising technology. Thanks to the intelligent deployed sensors, WSN is greatly employed in many application domains that ensure efficient supervision.

IoT has recognized a regular evolution by exploiting its services from the web; known as the Web of Things (WoT).

For a better explanation of the fundamental concepts of these technologies, a special focus is put on their semantics.

1.2. Problem statement

Despite its importance, the continuous evolution of the IoT has led to a complexity level due to the huge amount of heterogeneous deployed objects, sensing data, and suggested services. On the one hand, the connected objects are designed by different manufacturers (Google, IBM, Nokia, etc). Accordingly, the generated data has different coding formats leading to a complex data exchange task. Moreover, this amout of data, including semantic heterogeneity (synonymy, antonymy, polysemy, etc), keeps growing. In this respect, the obtained measure can be expressed in different terms. For instance, temperature can be measured with the Celsius, Fahrenheit or kelvin degree. On the other hand, the variety of these objects and their continuously changing requirements and deployment contexts further complicate their management and configuration tasks. These challenges are raised due to the absence of a unified and standard model of IoT devices along with their data and services. Thereby, the notion of semantics plays a key role in the Internet of Things due to its efficiency in solving the problems of heterogeneity, interoperability, and data interpretation. Furthermore, semantic interoperability means the ability of different parties to access and interpret unambiguous data since the connected objects are able to exchange data with each other and with other users online. SWT exploitation in the IoT field provides an explicit, easy and comprehensible description in order to express semantic objects and their data. In addition, semantics subscribes to define consensus that facilitates dataset sharing, reuse, integration, and interrogation. This data, extracted from different connected objects and domains, ensures cooperation between the connected objects by facilitating the communication between them in order to highlight their intelligence aspects. Moreover, it ensures data analysis and reasoning that explain the need for data alignment with different vocabularies and frameworks.

For this purpose, applying SWT in IoT domain is considered as a suitable and reasonable solution. This aim was confirmed by Barnaghi et al. [3] who claimed that applying semantic technologies to IoT promotes interoperability among its resources, information models, data providers and consumers. It also facilitates effective data access and integration, resource discovery, semantic reasoning and knowledge extraction.

In fact, the synergy between SWT and IoT or WoT domains gives rise to the birth of a new appellation; known as the semantic web of things (SWoT). According to [4], [5] SWoT is an emerging vision, that brings together the semantic web and the Internet of Things.

1.3. Motivation and contribution

To ensure a reliable semantic modeling, ontologies are widely used for IoT devices and data annotation. According to Studer et al. [6], an ontology is a formal and explicit specification of a shared conceptualization. It is used to represent knowledge in the set of related concept fields.

It mainly consist of:

- Defining standard vocabularies that will be shared and reused between objects as well as between humans.
- Facilitating the discovery, integration, manipulation and configuration of IoT resources and their data.
- Supporting reasoning mechanisms for inferring intelligent decisions.

According to Ye et al. [7], ontologies can be classified on the grounds of their expressiveness (light-weight or heavy-weight) or generality (generic, domain-specific, or application-specific). In this work, our focus is restricted to the IoT/WoT domain in general without taking into account its applications.

We detail, classify, compare and discuss the most recent realized semantic modeling approaches in the IoT/WoT domain through a taxonomy of the previous approaches. We believe that this survey will help both researchers and developers to focus on the amalgamation between SWT and the IoT/WoT domain that will guide them towards future research directions.

We believe that this survey will help both researchers and developers to focus on the amalgamation between SWT and these domains as it will guide them towards new future research areas.

The primary contributions of our work are listed as follows:

- We provide an extensive review of the up-to date research progress about the role of SWoT.
- We propose an exhaustive classification which contributes to representing a deep analysis of a comprehensive literature review.
- We provide in-depth comparisons and discussions of various approaches, whose major role is to ensure semantic interoperability in the context of IoT, WoT, and sensors.
- We establish significant future trends for semantics in the IoT domain.

1.4. Paper organization

The organization of this paper is as follows: In Section 2, we provide a description of related survey papers for semantics IoT. Section 3 highlights the methodology of our survey. In Section 4, we intend to provide a breakdown of the reviewed papers for semantics representation in this field. In Section 5, an extensive discussion of the objectives of the studied research is provided. Section 6 extensively describes possible future research opportunities based on the systematic review in the previous sections. Finally, conclusions will be drawn in Section 7.

2. Related survey papers

Our survey is related to the state-of-the-art dealing with semantics in the IoT, WoT and WSN domains leading to the evaluation of some research survey papers. Thereby, in this section, we state the recent proposed survey papers on these topics.

The first investigation in this research area was revealed in 2012 by Barnaghi et al. [3] who have explained the importance of defining and presenting IoT semantics in order to resolve the heterogeneity and ambiguity of the huge collected data through connected objects and to ensure the interoperability between IoT systems. From this perspective, they proposed an overview of some existing ontologies that aim at representing sensors and their data, such as O&M and SSN ontologies.

In 2016, the survey work, realized by Szilaggi et al. in [8], highlighted an overview of SWT used at different IoT system layers and the well-important ontologies that were used to develop applications and services in IoT, namely SSN [9], IoT ontology [10], and the IoT-O [11]

In 2017, Bajaja et al. [12] studied, discussed and analyzed various ontologies that will be reused in the IoT domain by taking into account sensors, time, location and context-awareness. The aforementioned approaches were classified into generic and domain specific ontologies. In addition, the authors in [13], outlined the existing IoT ontologies to ensure semantic interoperability between heterogeneous IoT systems. They mainly focused on generic ontology that was applied in IoT platforms and domain-specific application ontologies (health care and logistic domains). De et al. [14] set forth a survey of the current state-of-the-art on the use of ontologies in the Web of Things (WoT), which ranged them in two layered-approaches. The cross-domain framework represents the concepts of WoT elements (devices, services, data, etc.) while the domain layer states some developed ontologies that are grouped into environment (smart home, agriculture, and so on.) and user-oriented (health care, e-learning, and others) domains.

In 2018, Androec et al. [15] collected and classified diverse works to ensure semantic interoperability in IoT. They conducted a systematic literature review methodology in their survey. The aforementioned studies are arranged according to their year of publication, country, and main contribution. This study covers different IoT application domains, namely healthcare, smart city, etc. In this work, the authors lightly introduce the selected approaches. Therefore, several recent and important studies are not considered in this survey.

Tables 1 and 2 recapitulate and discuss the surveys and overviews related to SWoT by highlighting their principal assets and drawbacks.

Despite their encouraging and neat outcomes, the aforementioned efforts showed remarkable shortcomings in the complementarity and the breadth of understanding semantics in WSN, IoT and WoT domains.

Our work is distinguished by:

- The primary goal of this survey is to consider and explain more recent and cited works than those mentioned in previous surveys.
- We cover diverse IoT semantic levels (resource, data, service, security). To the best of our knowledge, none of the proposed surveys have covered these aspects.
- We propose an in depth-analysis of the highlighted approaches in which we classify them into several categories describing their main features. Then we suggest a comparison and a discussion of the outlined approaches. In addition, we suggest several open research questions for readers.
- This survey paper consists of a new classification of related works.
- We offer a set of research questions to evaluate and compare related works in order to understand their shortfalls, strengths, and challenges.
- We discuss future directions of IoT domain, which are sketchely addressed within the IoT domain in the existing surveys.

3. Survey methodology

In this paper, we concentrated on a systematic literature review (SLR) [16,17] to analyze and evaluate relevant contributions related to SWoT. As elucidated by [16], SLR is composed of three main phases: planning the review, performing the review, and reporting the review. These phases will be described below. Fig. 1 shows the adopted procedure.

3.1. Planning review: Goals and research questions

This phase consists in developing a protocol review in order to draw the main objectives of this systematic review, outline the adopted research questions and propose the research strategy.

Table 1
Summary of IoT related surveys.

Items	Year	Assets	Drawbacks	Application Domain	Adopted Methodology
[3]	2012	-This work defined the semantic levels that should be considered in the IoT domain (resource level, data level, service level, security level and application level) to ensure interoperability between IoT systems. -It gave an overview of important works that were previously suggested in order to define IoT semantics, such as SSN and O& M ontologies	-Initial work has focused only on approaches that were suggested before and during 2012, like such as SSN and O&M. -This work has not made a comparison to its related works in terms of their main contributions, methodologies, features, etc.	IoT	×
[8]	2016	- The authors in this work explained the importance of using SWTs (OWL, RDF, DL) at different levels of IoT systems to guarantee semantic interoperability between these heterogeneous systems. - It gave an overview of the most cited ontologies that were proposed for IoT knowledge representation, such as SSN, SAN, and IoT-O.	- -Diverse relevant approaches were not included in this survey. The latter highlights only the works that were conducted before and during 2016. - The authors did not follow a methodology to select the cited approaches. Hence, there is neither a comparison nor a classification in this work.	IoT	×
[12]	2017	- This paper provided an overview of the most important ontologies that should be considered in the IoT domain such as sensor ontologies, time ontologies, location ontologies and so on. - It classified the existing approaches into generic and domain-specific categories.	- A weak comparison of the previous research works that did not consider semantic features to build their ontologies; including semantic language, and deployment method (modular, monolithic, from scratch, etc). - Limited semantic IoT approaches are presented in this paper. Approaches related to security aspects and WoT are not mentioned. - Absence of a notable discussion concerning the drawbacks of the studied works.	IoT	×
[13]	2017	- This work described related studies whose major role consists in defining ontologies not only in the IoT domain but also in healthcare and logistic applications in order to achieve semantic interoperability between IoT systems.	- The studied approaches in the IoT domain emphasized only domain-specific aspects of sensors and sensor networks. Approaches about IoT services, security and WoT are missing. - This work's approaches are just mentioned without comparing their semantic features (main scope, methodology, ontology reuse, semantic web language, etc) or discussing their drawbacks	IoT, Health care, Transportation and Logistics	×

Table 2
Summary of IoT related surveys (continued) Table 1.

Items	Year	Assets	Drawbacks	Application Domain	Adopted Methodology
[14]	2017	This work presented an overview of the proposed ontologies in the IoT/WoT domain and classified these approaches into generic and domain levels. - The studied approaches are sensor ontologies, location ontologies, service ontologies, data ontologies and other ontologies for a specific application (home, healthcare, etc).	- This paper focused more on the existing ontologies that can be reused in WoT (sensor ontologies, data ontologies, service ontologies, etc) without taking into consideration other domain-specific aspects, such as IoT-lite and IoT-O. - Various IoT aspects including security and WoT are not addressed.	WoT	×
[15]	2018	This work proposed a systematic literature review of SWT application in the IoT domain. The cited works are discussed and classified according to their publication dates, publication types (conference, journal, thesis, etc.), semantic usages,and citations in others works.	They do not compare the semantic features (semantic languages, methodologies, evaluations, modularizations, etc) of the cited approaches. Diverse IoT aspects are not highlighted in this survey, such as security, IoT service description, discovery, and WoT.	IoT	Systematic Literature Review

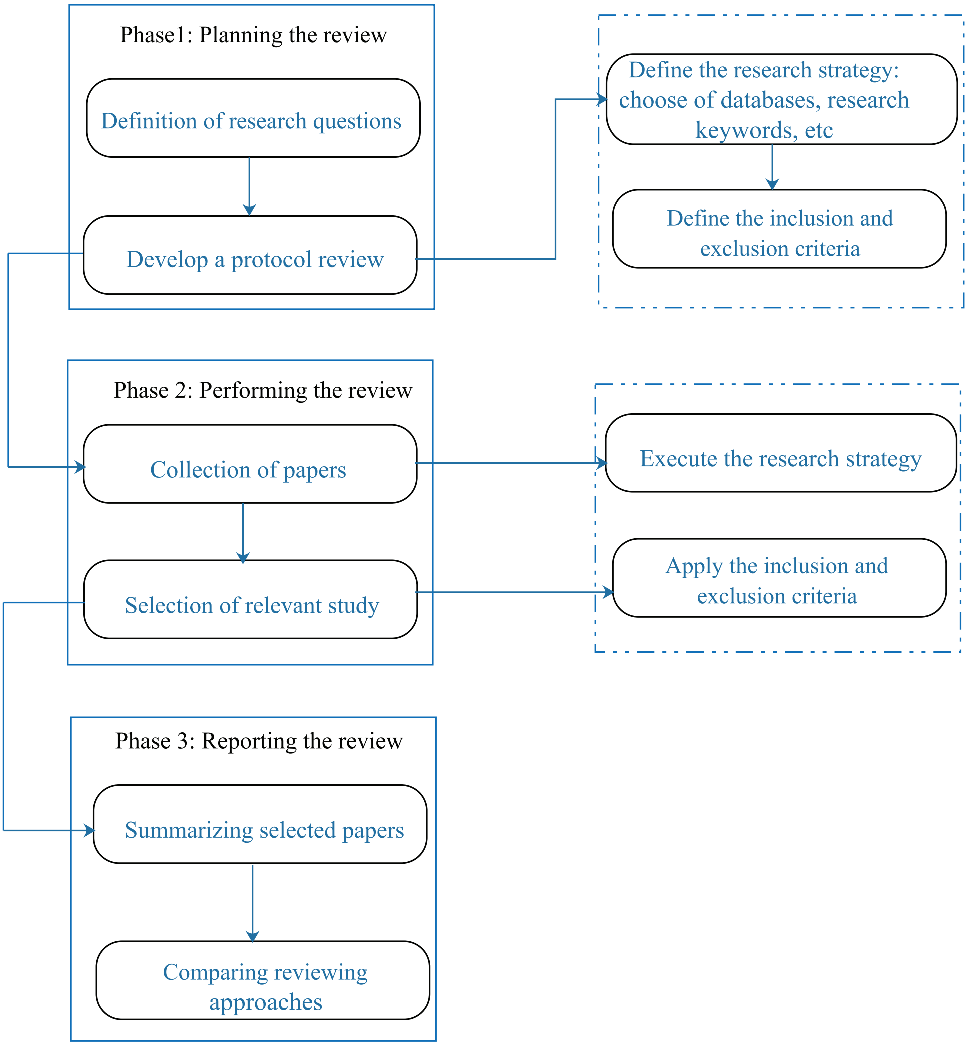
Phase1: Planning the review
Definition of research questions
Develop a protocol review
Define the research strategy: choose of databases, research keywords, etc
Define the inclusion and exclusion criteria
Phase 2: Performing the review
Collection of papers
Selection of relevant study
Execute the research strategy
Apply the inclusion and exclusion criteria
Phase 3: Reporting the review
Summarizing selected papers
Comparing reviewing approaches

Fig. 1. Systematic literature review applied steps adapted from [16] .

The present survey paper focuses on investigating and exploring the amalgamation of SWT and IoT. Section 2 summarizes the previous proposed surveys and highlights the contributions of our work compared to the previous ones. Thereby, in our paper, we analyze and discuss the recent reviewed works through a set of accurate research questions. We mainly focus on:

- How can the semantic interoperability between smart objects, data, services, and applications in the IoT domain be assessed?

Guided by this main research question, a special heed is paid to the following research questions:

- RQ1: What are the main objectives of applying SWT in the IoT domain?
- RQ2: Which aspects of the SWT stack are used?
- RQ3: Are the proposed ontologies based on other existing ontologies or are they built from scratch?
- RQ4: Did the proposed approach present a modularized representation?
- RQ5: Which contexts concerning deployment devices are considered in the proposed models?
- RQ6: Which methodology do the authors follow to build their models?
- RQ7: How do the authors evaluate their models?

3.2. Conducting the review

This phase focuses on identifying and selecting relevant papers that can provide a response to our research questions. This step is mainly made up of a research strategy and study selection steps.

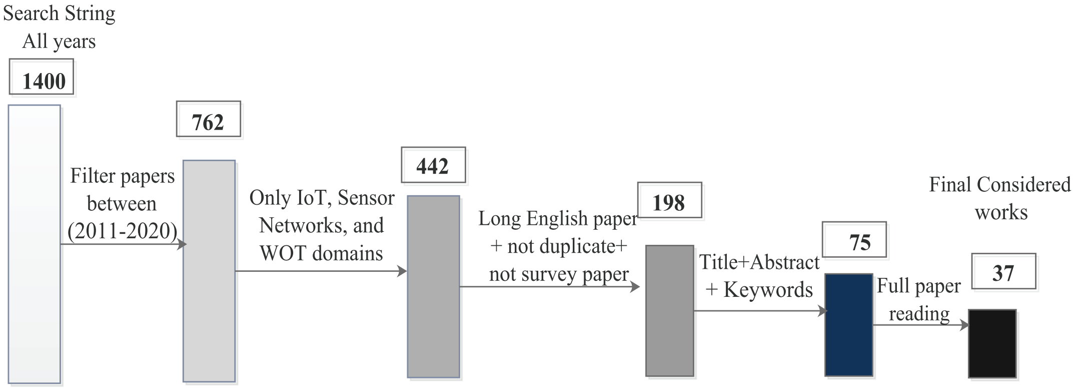
Search String
All years
1400
Filter papers between (2011-2020)
762
Only IoT, Sensor Networks, and WOT domains
442
Long English paper + not duplicate+ not survey paper
198
Title+Abstract + Keywords
75
Full paper reading
37
Final Considered works

Fig. 2. Iterative Papers selection results after applying inclusion and exclusion criteria.

3.2.1. Research strategy

In our survey, we use Web of Science, Google Scholar, IEEE Xplore Digital Library, Elsevier Scopus, ACM digital library, Citeseer library, Science Direct, and arXiv.org in order to search for relevant scientific contributions. In addition, we consider the linked open vocabularies for the IoT[1], IoT schema[2] and Web of Things Working Group[3] that are interested in interoperability issue in the IoT domain. In fact, we limit our keywords to Internet of things, Web of Things, Sensors, Ontologies and Semantics. Consequently, we use the following research string: ((Sensor OR WSN OR Internet of Things OR Web of Things) AND (Semantic Web Technologies OR Logics OR ontology)).

3.2.2. Study selection

After searching publications in online databases and filtering and screening the returned papers, an initial set of 1400 studies was found. The latter contains not only studies that do not focus on the specified research problem (e.g. survey papers about IoT) but also duplicate papers (e.g. appeared in different databases, PhD theses and related papers, duplicate languages etc.) that are proposed for different application domains along with others. Wherefore, a selection step of the relevant papers becomes necessary based on several inclusion and exclusion criteria.

The latter are defined during this phase to select the most recent and relevant works. First, we only considered the contributions that were published in peer-reviewed journals, conferences, and book chapters from 2011 to 2020. So, the number of papers was reduced from 1400 to 762. Second, we examined works whose major focus was on IoT, sensor networks and WoT in general without taking into consideration IoT domain applications, like Healthcare, logistics, industries, and so on. Consequently, we obtained 442 papers. Third, the number of papers was reduced to just 198 after removing duplicate papers, Ph.D. theses, survey papers, short papers, and non-English papers. After that, we have investigated the importance of these papers based on their titles, abstracts, and keywords. Accordingly, from a set of 75 selected papers that were fully read, we finally focused on 37 relevant studies in this work. Each contribution is analyzed to extract pertinent information about the proposed research questions. Fig. 2 shows the process.

3.3. Reporting the review

This phase is mainly comprises three main steps, such as summarizing, comparing, and discussing the selected papers. These steps are described below.

3.3.1. Summarizing selected papers

IoT semantics can be defined in a layered architecture [3] as described in Fig. 3. The first layer represents the IoT resource that aims to define semantic real-world objects and networks. The second one is, however, for data representation in order to describe IoT resources and their semantic data and explain the way SWT exploits this representation for management and interpretation goals. The service application, at the third layer, reveals how SWT helps develop IoT applications and recommend adequate services for users.The security layer shows the capabilities of these technologies to represent vulnerabilities and security mechanisms in the IoT domain. Inspired by this architecture and in order to answer the first research question, ”What are the main objectives of applying SWT in the IoT?”, we classify the studied approaches into five IoT related aspects, according to their main contribution namely IoT data, IoT data and service, IoT service, IoT security and WoT. In fact, Fig. 4 illustrates this classification where the IoT resources are already considered by other IoT aspects as follows:

[1] LOV4IoT: https://sensormeasurement.appspot.com/
[2] iot.schema.org
[3] https://www.w3.org/WoT/WG/

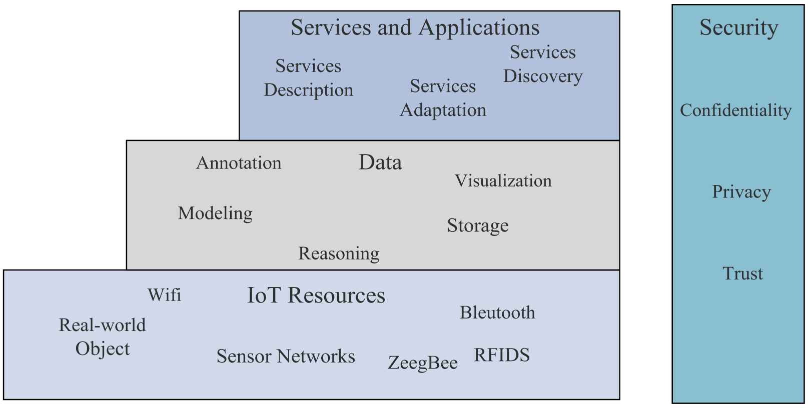

Fig. 3. Semantic layer in Internet of Things, adapted from [3].

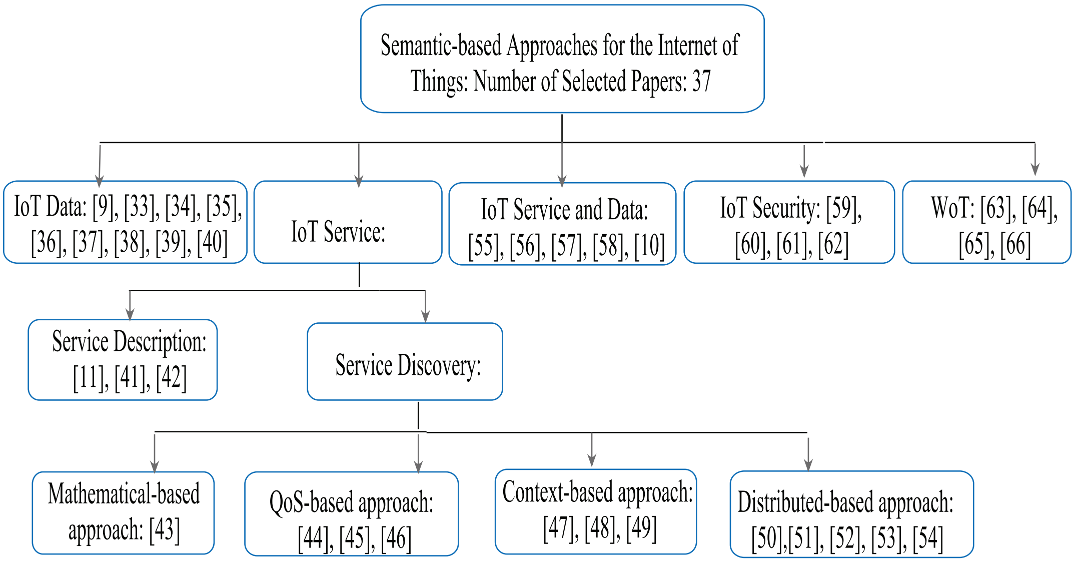
Semantic-based Approaches for the Internet of Things: Number of Selected Papers: 37
IoT Data: [9], [33], [34], [35], [36], [37], [38], [39], [40]
IoT Service:
IoT Service and Data: [55], [56], [57], [58], [10]
IoT Security: [59], [60], [61], [62]
WoT: [63], [64], [65], [66]
Service Description: [11], [41], [42]
Service Discovery:
Mathematical-based approach: [43]
QoS-based approach: [44], [45], [46]
Context-based approach: [47], [48], [49]
Distributed-based approach: [50],[51], [52], [53], [54]

Fig. 4. Classification of IoT-based Semantic Approaches.

- IoT data: This category summarizes the research works that proposed a semantic model of IoT resources and their detected data.
- IoT services: At this level, the proposed works emphasize the services given by IoT resources.
- IoT data & services: This category describes the suggested works that define a semantic model for both data and services generated by IoT resources.
- IoT security dimension: identifies approaches that are offered to ensure IoT security.
- WoT dimension: at this level, a seamless interconnection between the World Wide Web (WWW) and IoT resources is established in order to define the Web of Things. Consequently, heterogeneous devices can be easily used and configured through a web application. Thus, this can ensure efficient communication (monitoring, integration, deployment, deletion, etc.) between users and devices by using web standards (HTTP/WebSockets). From this respect, recent research works have deeply focused on SWT deployment in WoT, which will be at the heart of our work.

3.3.2. Comparing reviewed approaches

After reviewing each approach, we propose a comparative study according to several criteria. These criteria are explained as follows:

- ***Semantic Technologies:*** They are proposed to give an answer to this question ”Which aspects of the SWT stack are used”. This dimension specifies the modeling, reasoning and interrogating language (OWL, RDF, SWRL, SPARQL, etc.). In fact, ontologies are developed based on semantic web languages that offer formal semantics and a precise syntactic structure of the domain knowledge. In what follows, we will pay special attention to the most known languages.

The Resource Description Framework (RDF): According to the W3C[4], RDF is a graph that defines a standard model for data interchange on the web. It is also called an RDF triple as it comprises a subject, object, and predicate. The subject defines the semantic entity of interest, the object refers to the value of this entity and the predicate represents the relation between the entity and its value. RDF Schema (RDFS) is an extension of RDF that provides a structured data-modeling vocabulary for RDF data. It defines generalization relations (rdfs;Class, rdfs:subPropertyOf, etc) and constraints (rdfs;domain, rdfs:range) of RDF triples.

The Ontology Web Language (OWL): is an ontology language that is standardized by the W3C for the semantic web. It allows the representation of concepts and their relationship with logical reasoning and information systemsin an appropriate manner. It is easier and more expressive compared to the RDFS language. In 2009, the W3C OWL working group has proposed an extension of OWL, known as OWL2[5]. OWL2 has three different profiles, namely OWL 2 EL, OWL 2 QL, and OWL2 RL. The first profile is employed for ontologies that contain a large number of classes and properties. The second profile is very useful for a large ontology that includes a massive quantity of instances. The third profile is applicable to applications that require scalable reasoning, in time that is polynomial with respect to the size of the ontology.

The Semantic Web Rule Language (SWRL): is a rule language for the semantic web. It allows users to define rules based on OWL concepts and their relationships in order to infer hidden knowledge. It can be extended by using functions; named built-ins that can be mathematical operations, string operations, dates, and so on. Furthermore, it permits users to define their own built-ins that respond to their requirements. The SWRL language is composed of two main parts. The antecedent part refers to a set of conditions that should be verified while the consequence part describes results and actions that will be executed.

The Shape Constraint Language (SHACL)[6]: is a W3C specifications that focused on the validation of RDF graph via a set of conditions and constraints. These conditions are provided as shapes.

The SPARQL Query Language: According to the W3C, SPARQL is a query language for the RDF graph. It helps search, add, remove, and update RDF data. It also supports extensible value testing and constraining. The result of a SPARQL query is a set of RDF graphs.

- ***Reuse of ontologies:*** This criterion specifies if the authors taking into account the previous existing ontologies to represent the IoT domain knowledge, or rather define their ontology from scratch. This criterion gives an answer to the question ”Are the proposed ontologies based on other existing ontologies or are they built from scratch?”. In fact, during the ontology development process, it’s very important to reuse existing ontologies rather than build it from scratch for many reasons. Meanwhile, according to Lonsdale et al. [18], reusing an existing ontology guarantees the quality of the new ontology because the reused concepts have already been tested and validated. In addition, building an ontology from scratch is costly and needs great human efforts that will be reduced by reusing existing ones. Moreover, mapping between two ontologies, that share components through ontology reuse, is easier.
- ***Modularity:*** It verifies if the proposed models are presented by modules or not. This criterion gives an answer to the question ”Did the proposed approach present a modularized representation?”. In fact, a monolithic ontology is very difficult to be handled and reused [19], [20], [21]. In addition, a scalability problem can be revealed by monolithic ontology-based applications. This is justified by the amount of data that must be analyzed by semantic web technologies (SWRL, SPARQL, RDF,). In this regard, modular ontology is a promising solution as it can facilitate knowledge reuse across heterogeneous domains. It is easier to maintain, reuse, and manage distributed engineering of ontology modules in different locations and areas of expertise [22]. Accordingly, modularity is an important choice in IoT for ontology development, as a set of interlinked modules, in order to improve scalability, reasoning performance and reusable domain concepts based on necessary modules.
- ***Context:*** This criterion answers the research question RQ5: ”Which context concerning deployment devices are considered in the proposed models?”. In fact, with its swift growth, the networked deployment of objects become more complicated and difficult to be handled than ever. It refers to IoT resource contexts that should be taken into consideration to ensure an efficient and permanent configuration and management of these resources.

  Dey in [23] has defined context as *”any information that can be used to characterize the situation of an entity. An entity is a user, a place, or a physical or computational object that is considered relevant to the interaction between a user and an application, including the user and application themselves”.*

  The connected object constitutes the main entity of the IoT field. Therefore, we elucidate five contexts that are relative to object deployment, namely interconnectivity context (CoI), time context (CoT), location context (CoL), trajectory context (CoTr), and object’s requirement context (CoR).

  Time context (CoT): With the continuous progress of networked objects, temporal issues have been more powerful than before. Time context is employed to explain the temporal modeling and reasoning features of connected things. Accordingly, it improves the quality of services provided by these objects.

  Location context (CoL): Location awareness is inextricably linked to connected objects. It is strongly important to obtain and represent information about their position in the physical environment.

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

[5] https://www.w3.org/TR/owl2-overview/

[6] https://www.w3.org/TR/shacl/

Trajectory context (CoTr): Context-aware trajectory represents the mobility characteristics of connected objects. It is based on the two above-mentioned contexts (time and location). Thereby, it refers to a location list that is crossed by an object during a predefined period of time. Nonetheless, there is a lack of applying SWT to represent the trajectory behaviors of connected objects.

Inter-connectivity context (CoI): It is the fact of having knowledge about the used technologies to interconnect real-world objects to Internet. In fact, large amounts of shared data that consume a lot of network bandwidth are generated. Therefore, the network has to be effectively managed for efficient utilization.

Object's requirement context (CoR): this context focuses on the object's specifications, such as the battery level, memory capacity, coverage range, lifetime, and so on. These information are extremely salient during their state configuration.

- ***Methodology:*** This criterion helps us identify which methodology is followed to build ontologies in IoT. It is related to the research question ”RQ6: Which methodology do the authors follow to build their models?”.In fact, an ontology is a promising solution to ensure semantic interoperability between heterogeneous systems. Building an IoT ontology is not a straightforward task due to the complexity of the IoT domain in terms of the exponential growth of deployed devices, continuous deployment contexts, heterogeneous data, etc. This needs collaboration between the IoT domain and software engineering experts. In this regard, they should adopt a well-defined methodology during the ontology development process in order to define a reliable and efficient model that builds knowledge of the target domain. Four well-known methodologies can be selected from a diverse range of methods that were offered for ontology construction, namely methontology methodology [24], 101 method [25], Neon methodology [26] and agile methodology [27].
- ***Evaluation Techniques:*** This criterion refers to the suggested methods and techniques used for evaluating these works. It is suggested to address this question ”How do the authors evaluate their models?”.

  In fact, it is a primordial task to evaluate the quality, performance and usefulness of the proposed ontology. Therefore, four well-known techniques can be used for ontology assessment, namely gold standard assessment, human evaluation, data-driven evaluation and application-based evaluation [28]. Gold standard evaluation aims to compare the proposed ontology to either a high-level model or defined standards in the concerned domain. Human evaluation method is based on several predefined comparison criteria that are proposed to evaluate the ontology design, such as its clarity level, completeness, consistency, Gruber [29] and Gómez-Pérez [30]. Application-based evaluation consists in using an ontology in a specific application in order to evaluate its results. This ontology can be compared to a predefined data source, such as a corpus of documents in a particular domain, called data-driven evaluation.

4. Semantic-based approaches for IoT

Several projects are focusing on addressing the semantics IoT like IoT-A [31], SOFIA[7], SemSorGrid4Env[1], Linksmart[8], IoT.est[9], openIoT[3], FED4FIRE[10], Vital ontology[11]and CityPulse[2].

Gyrard et al [32], have developed a linked open vocabulary project (LOV4IoT[12]) that collects and regroups numerous relevant ontologies for the IoT domain such as, SAREF[13] standardized by ETSI with the name SmartM2M, spitfire[14] and the OneM2M base ontology[15].

In the following sub-sections, we propose an overview of the realized researches in this topic (the 37 selected papers as it was clarified in the previous section) that were classified according to their main contributions. We also compare the proposed works in each sub-section based on our research questions. However, Tables 3 and 4 highlights the main features and drawbacks of these studies.

4.1. IoT Data representation

The studies in this category focus on the use of SWT in representing the semantics of **IoT resources** and their **data**.

In 2012, the Semantic Sensor Network Incubator Group, belonging to the World Wide Web Consortium (W3C), developed an ontology called Semantic Sensor Network (SSN)[9]. This ontology is developed through the review of different proposed ontologies, namely SemSOS ontology [67], Ontonym-Sensor [68] and CESN ontology [69]. The SSN ontology describes sensors in terms of capabilities, measurement processes, observations and deployments in order to define the semantic interoperability of physical sensor networks. Its core concepts are sensors and their features and properties, observations, systems, measuring capabilities, operating and survival restrictions, and deployments.

[7] http://sofia2.com/

[8] https://linksmart.eu/redmine/projects

[9] http://ics-iot.weebly.com/iotest.html

[10] http://www.fed4fire.eu/

[11] http://vital-iot.eu/

[12] https://lov4iot.appspot.com/

[13] https://sites.google.com/site/smartappliancesproject/ontologies

[14] http://sensormeasurement.appspot.com/ont/sensor/spitfire.owl

[15] http://www.onem2m.org/ontology/Base

Table 3
Comparison between Semantic-IoT related works.

Items	Assets	Drawbacks
[9]	- This work, proposed an ontology for sensor networks and their observations (SSN ontology). - It was based on other ontologies, like O&M and SemSoS. - It is available online. It was used in diverse projects, such as IoT.est, open IoT,FED4FIRE, etc.	- The work was proposed for only sensors - It didn't consider the modeling phase of sensors services. - Evaluating the semantic quality (consistency, clarity, coverage, etc.) of the SSN ontology was not addressed. - Privacy and security issues were not presented and interpreted. - It did not support reasoning mechanisms for sensor configuration and data management.
[33,34]	The SSN ontology was extended to wireless and cloud sensor networks respectively.	- They focused only on sensors - They are not available online. - They did not define sensors and data management techniques. - Lack of privacy and security issues.
[35]	- This work expanded the SSN ontology to cover actuator devices and came up with SOSA ontology. - It is available online	- Both sensor and actuator services were not modeled. - It did not support reasoning mechanisms - Semantic quality was not assessed. - Privacy and security issues were not addressed.
[36–40]	These works have modeled IoT devices (sensors, actuators, RFIDs) and their data - They were based on the SSN ontology, except [39] and [40] which were built from scratch. - They were tested based on specific applications (smart city, smart home, healthcare). - They are available online, except [40]	They were interested only in IoT devices and their data stream without focusing on their services. - They did not support reasoning. - The evaluation step did not emphasize semantic quality. - Privacy and security aspects were not considered.
[11,41,42]	- These works introduced ontologies that describe connected devices (sensors, actuators) and their services. - They were linked to other SSN and OWL-S ontologies, except [42]. They were tested based on real objects.	- IoT data was not considered in these works. - They did not concentrate on IoT service selection. - They did not support reasoning mechanisms. - The ontology proposed in [11] is the only available online.
[43]	-This work proposed a modular ontology for IoT and their services - Despite that, it is one of the first attempts in IoT, the proposed ontology cover concept about the sensor, actuator, physical object and so on. - Defined mathematical rules modeled in the ontology for IoT services selection	-The evaluation was missing -The ontology not available online - Rules for IoT data and resource management were not defined
[44–46]	- These works put forward a semantic representation of IoT resources and their services. They proposed an IoT service selection method based on QoS. - The developed ontologies were built by reusing SSN and OWL-S ontologies, except [46] which was built from scratch. The suggested ontologies were tested based on a real use case (weather monitoring).	- These ontologies did not consider IoT resource data. Diverse characteristics of IoT resources were not considered in these works such as connectivity, virtualization, mobility, energy, and life cycle. - They are not accessible online. - Rules for inference and reasoning purposes were not presented. - The semantic quality of the suggested ontologies was not evaluated. - Security aspects were not taken into account.

It is then used by several projects like SemsorGrid4Env[16], CityPulse[17] and openIoT[18]. This ontology is then extended by Bendabbouche et al. [33], for wireless sensor network (wireless sensor network ontology), and by Muller for sensor cloud (sensor cloud ontology)[34].

The above-mentioned works have mainly focused on the semantic representation of sensors and their observations.

The MELODY projects introduced a semantic actuator network (SAN)[19] to represent the semantics of actuators and their capabilities and roles. Besides, the SOSA ontology [35], proposed by the joint group World Wide Web Consortium (W3C) and the Open Geospatial Consortium (OGC), represents the interaction between sensors, observations, actuators and sample concepts.

Recently, the SSN ontology has been simplified by removing some concepts including stimulus, systems, measurement and system capabilities, and by extending the SOSA ontology to represent knowledge about actuators [35].

Nonetheless, the IoT is not only composed by sensors and actuators. From this regard, Gyrard et al. [36] proposed an M3 ontology that is extended from the SSN ontology that includes various concepts, such as *transducer, RFIDS tag*, and *controller*. The *measurement* concept was proposed in this model in order to represent data streams obtained from IoT resources. This

[16] http://mayor2.dia.fi.upm.es/oeg-upm/index.php/en/activeprojects/
[17] http://www.ict-citypulse.eu/page/
[18] http://openiot.eu/
[19] https://www.irit.fr/recherches/MELODI/ontologies/SAN.html

Table 4
Comparison between Semantic-IoT related works (continued).

Items	Assets	Drawbacks
[47–49]	- These works proposed a context-awareness IoT service descriptions and selection approaches. - They reused existing ontologies, such as SSN and OWL-S. - They suggested context-awareness IoT service selection and discovery (temporal selection, geographic selection, uncertain selection, etc.).	- They did not present IoT data in their ontologies. - Management of IoT devices and their services through reasoning rules was not defined. - The evaluation was either missing or poorly described. - The proposed ontologies were not accessible online. - Security issues were not considered.
[50–54]	- These works proposed a distributed-based solution for describing and selecting IoT resources and services based on SWT. - The suggested method was evaluated based on specific applications.	- Semantic modeling and utilisation of IoT resource information were not addressed. - The evaluation focused only on the application-based method without addressing the criteria-based method to check the coverage, clarity, consistency, and completeness of these ontologies. - Reasoning and interpreting IoT resources and their services were not defined. - The proposed ontologies are not available online. - Security domain knowledge was not presented in these ontologies.
[10,55–58]	- These works proposed monolothic ontologies for the semantic representation of IoT resources, information and services. - Most of these works followed the application-based method as an evaluation tool. - Most of works were linked to other ontologies.	They addressed only modelling and annotation issues and ignored the interpretation and reasoning phases. - Only ontologies in [57], [58] are accessible online. - Evaluating the semantic quality of the suggested ontologies was missing in all approaches. - Security domain knowledge was not presented in these ontologies.
[59–62]	- These works set forth security ontologies for IoT applications. - The proposed ontologies were linked to the previous ones that were specific to sensors, networks, web, etc. - Only [59] and [60] are available online. - Reasoning mechanism to manage the occurred attacks was only defined by [61] and [62].	- Evaluation concentrated on implementing ontologies in applications without taking into account the quality of these ontologies, such as their correctness, completeness, clarity, and consistency levels. - The reuse of IoT ontologies, such as IoT-O, IoT-lite, and so on was treated only by [61].
[63], [64–66]	- These works introduced new concepts to define WoT semantics, such as WoT resources, Identifier (IRE), application protocols (COAP, HTTP), etc. - The majority of these works evaluated their ontologies within a web application. - These ontologies are available online.	- Evaluating the quality of the developed ontologies was not highlighted. - Reusing IoT domain knowledge (IoT devices,data, services) in these ontologies was absent. - Security aspects were not considered in these ontologies.

ontology was then simplified in the context of FIESTA-IOT H2020 EU project and it was called M3 lite[20]. It was integrated in a framework to facilitate the development of IoT applications.

To deal with the real-time sensor data, the authors in [37] suggested a framework for real-time semantic annotation of streaming IoT data to support dynamic integration into the Web. This framework (called CityPulse framework) was proposed in the context of the CityPulse[2] project. It is based on a Stream Annotation Ontology (SAO). The main concepts of this ontology are stream data, stream analysis and stream event. This ontology was extended by Elsalah et al. in [38] by adding other concepts to represent IoT devices, time, location, data units, and values. The extended version was called the IoT data streams ontology.

To ensure interoperability between two or more IoT data hubs, Tachmazidis et al. [39], presented a semantic enrichment of the BT Hypercat Data Hub. The latter gathers data from different sources to be brought onto a common platform and presented to users and developers in a consistent way. Therefore, the main concepts of the BT Hypercat ontology are sensor stream, event stream, sensor feed, event feed, etc. The access to the HB Hypercat ontology is ensured through the SPARQL language, based on the mapping between SPARQL and SQL queries.

In addition, the authors in [40] have proposed an ontology-driven approach to enable automatic generation of firmware for the IoT devices and middleware for the applications through human-machine interfaces. This ontology is composed of six modules. The first one is called the programming languages I/O structure ontology is used to make the source codes of the developed firmware and applications understandable by the users through the input/output data structures description. The data types ontology represents all data types supported by the system. The visual objects ontology is proposed for describing and monitoring the available visual objects and visualizing the graphical scenes of the result of IoT devices. The semantic filters ontology is interested in raw data filtering and pre-processing (e.g. denoising sensor data, and fusing data). The electronic components and middleware ontology defines a description of different programmable devices (sensor, actuator, transducer, etc.) and a description of different programming interfaces of the developed system.

Table 5, shows that these approaches utilize SWT to formalize their ontologies. In addition, we notice that almost of these approaches take the advantage of reusing the existing ontologies instead of building their ones from scratch. Therefore, only

[20] http://lov.okfn.org/dataset/lov/vocabs/m3lite

Table 5
Summary of semantic-based approaches for IoT resources and data description.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[9]	OWL2	SemSOS, Ontonym-Sensor, CESN, O&M	✓	✓	✓	×	×	×	×	application
[33]	×	SSN	✓	✓	✓	✓	×	✓	×	application
[34]	RDF, SPARQL	SSN	×	✓	✓	✓	×	×	×	application
[35]	OWL	SSN, DOLCE,	✓	✓	✓	×	×	×	×	application
[36]	OWL	SSN	×	✓	✓	✓	×	✓	Methondology	application
[37]	OWL	Dul and SSN	×	×	✓	×	×	×	×	application
[38]	RDF, SPARQL	SSN, SOSA, IoT-lite	×	✓	✓	×	×	×	101 methodology	application
[39]	RDF, OWL, SPARQL, JSON-DL	×	×	×	×	×	×	×	×	application
[40]	OWL	×	×	×	×	×	×	✓	×	application

two works [36,38] follow a methodology during the development process. Furthermore, only the works [9,33,35] present their ontologies in a modular models in order to facilitate their extension and reuse. The main modeled contexts in these works are the time and the location with less attention about the interconnectivty, the requirement and the trajectory contexts. Concerning the evaluation of their ontologies all the studied approaches in this category follow the application-based evaluation.

4.2. IoT Services representation & discovery

In this section, we review related works about describing and discovering IoT resources and their services. The suggested ontologies in this category define concepts only for **IoT resources** and their **services**.

De et al. [41] presented a semantic model for IoT components (entity, resource and service). They proposed an extension of the OWL-S ontology for IoT. Thereby, they added the concept of IoT service as a subclass of the OWL-S[21] ontology.

In the context of the ADREAM project, the authors of [11] proposed a modular ontology (IoT-O)[22] to ensure semantic interoperability between IoT components. IoT-O includes several modules, like sensing, actuating, life cycle, service and energy modules. The sensing module extends several concepts from the SSN ontology. The actuating module describes how the system interacts with the physical world and is modeled with the classes actuator, actuation, etc. The life cycle module models the state of machines and device usages. The service module, showing web service interfaces, consists of service, operation and message classes. The energy module provides classes for representing the power consumption of IoT devices.

The authors in [42] suggested a semantic service ontology to ensure heterogeneous IoT service descriptions in different contexts or platforms. The proposed ontology mainly comprises a *service-object* concept that is made up of three sub-classes: *property, capability*, and *server profile*. Property represents the static states of the connected objects. The capability concept represents the dynamically generated data by objects. The server profile determines a configuration of physical objects when it interacts with specific platforms.

Authors in the previous studies did not perform any mechanism for IoT service discovery. To overcome this issue, many proposed approaches are divided into four categories.

- Mathematical-based approach that is based on mathematical equations to retrieve IoT services.
- QoS-based approach concentrates on providing high quality services.
- Context-based approach aims to suggest services for users based on a predefined context.
- Distributed-based approach allows to discover heterogeneous and distributed IoT services in a scalable way

These categories are detailed in the following sub-sections.

4.2.1. Mathematical based approach

One of the first attempts, that proposed semantics IoT, is suggested by Hachem et al. [43], who introduced an IoT middleware based on the service-oriented paradigm that abstracts things as services. This middleware includes three major ontologies (device, physics and mathematics and estimation). The device ontology aims to describe "things". The physical ontology permits to model not only real world entities as physical concepts but also mathematical formulas and functions to facilitate the IoT service discovery. The estimation ontology describes models, which can be used when a service is unavailable.

4.2.2. QoS Based approach

This section displays approaches with the main goal of discovering and selecting IoT services based on the Quality of Service (QoS) values. The authors in [44] have proposed a common conceptual model, named "Physical Service Model (PMS)",

[21] https://www.w3.org/Submission/OWL-S/

[22] https://www.irit.fr/recherches/MELODI/ontologies/IoT-O/

for describing heterogeneous IoT services. The PMS is composed of three main concepts, namely *device, resource*, and *service*. The device class represents the employed hardware that is attached to a real-world entity. The resource concept defines a computational element, which is hosted on a device and exposed by a service through a common interface. The service concept represents the services of IoT devices, such as identifying, actuating and sensing. The PMS model contains spatio-temporal features that characterize the deployment of these three concepts. These features are then exploited as QoS attributes for IoT service rating. Other attributes are suggested, such as reliability, reputation, and execution cost. Finally, the service selection of this model is based on the user's preferences and requirements.

The authors in [45] have suggested a semantic-based framework for IoT transaction modeling and processing. This framework is composed of various layers: the entity link layer, the semantic annotation layer, the service registry center, the transaction construction layer, and the transaction execution control layer. This framework is based on the OWL-S ontology as it is the basis for logical reasoning. This ontology is extended by adding the *service-status* concept to represent dynamic services for IoT entities. This concept has not only refers to a location (current location) and the current status of IoT devices, but also a sequence of IoT transactions. In addition, Yachir et al. [46] proposed a semantic model for smart objects and users request resolution in the IoT domain using ontology and description logic techniques. This model facilitates the reasoning over services and devices. The selection of services is based on the QoS level. In fact, only services, providing higher quality than the required QoS level, are returned to the user.

4.2.3. Context based approach

In this section, we describe relevant works that mainly focused on how to provide IoT services according to a predefined context. Accordingly, a significant work has been proposed by Nambi et al. in [47], which suggest a unified semantic knowledge base for IoT that consists of several ontologies (resource, location, context and domain, policy and service ontologies). The resource ontology represents an entity in IoT (e.g., sensor, actuator, physical object and composite object). The location ontology describes semantic geospatial information for IoT. This ontology extends the GeoNames ontology[23]. The context and domain ontologies represent contextual information and domain-specific knowledge. The policy ontology is used to provide information on how to accomplish a service requested by an actor in dynamic environments. The service ontology describes, represents and models the IoT services. In [48], the authors have provided an ontology based context model to represent uncertain and temporal context. Therefore, Dynamic Bayesian Networks (DBN) are adopted to reason about these contexts for uncertain IoT services discovery. Besides, the work done by Li et al. in [49] developed a decentralized Location-preserving context-aware discovery framework, which is based on SWT. It uses ontology to encode context information and match queries with services to select the most appropriate ones.

4.2.4. Distributed based approach

The studied approaches in this section focused on applying the distributed-based solution for IoT services description and selection. The authors in [50] have developed a lightweight ontology for IoT services description, which contains seven main modules: IoT service, service test, Quality of service (QoS) and quality of information (QoI), deployment platform and networking, observation and measurement, IoT resource, entity of interest and physical locations. Scalable access to IoT services and resources is realized through a distributed, semantic storage design. In [51], authors set forth an integrated semantic service platform. The major purpose of this platform is to resolve three main problems in distributed IoT domains by applying semantic technologies to IoT, such as semantic discovery, dynamic semantic representation, and semantic data repository for IoT resources. This platform is based on the IoT-based service integration ontology. The latter contains three main concepts: *service* that represents one or more IoT-based services, *user* that describes information about end-users, and *reference* class indicates the way to refer to IoT resources located in external IoT service platforms.

The authors in [52] proposed ForwardDS-IoT a federated discovery service in the IoT context, which includes a semantic model. The latter is based on existing ontologies, such as SSN, SAN, and OWL-S ontologies. Additionally, Willner et al. [53] have put an open-multinet upper ontology (MON) to support the interoperability of federated infrastructures. It facilitates the management of heterogeneous resources through the amalgamation of different semantic ontologies. The MON ontology is composed of six sub-ontologies: omn-federation, omn-resource, omn-service, omn-lifecycle, omn-component, omn-policy, and omn-monitoring. By the same token, Zhu et al. [54] have suggested an SOA-based solution for IoT services discovery. In fact, they defined an ontology for cyber-physical systems and IoT domains to facilitate the service selection and composition. This semantic model is extended from the OWL-S ontology by applying the OWL-S constructs of the process-profile-grounding. The PT-SOA ontology includes four main concepts: the *physical profile* is used to describe the characteristics, components, and constituents of physical things; the *operation profile* is proposed to control physical things or operations when providing a service (maintenance, constraints, etc.); context is utilized to represent the dynamic state of IoT things and the scheduled services that describe the service delivery context (time, location, etc) by these things.

Tables 6–10 provide a comparative analysis of the studied works for representing and discovering IoT services. They show that these approaches use SWT to formalize their models. Only a few works [11,47,50] use modular representation for their models. The deployment contexts of IoT devices are partially addressed. Moreover, only the work achieved in [11] has adopted a methodology during the development of their models. The application-based method is frequently used for the evaluation purposes.

[23] http://www.geonames.org/ontology/documentation.html

Table 6
Summary of semantic-based approaches for IoT services representation.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[11]	OWL	SSN, DUL, PowerOnt, OWL-S	✓	✓	×	×	×	✓	NeON Methodology	application
[41]	OWL	SSN ontology, OWL-S	×	✓	✓	×	×	×	×	×
[42]	JSON-LD	×	×	×	×	×	×	×	×	application

Table 7
Summary of semantic-based approaches for IoT services discovery: mathematical-based approach.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[43]	OWL	×	×	×	×	×	×	×	×	×

Table 8
Summary of semantic-based approaches for IoT services discovery: QoS-based approach.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[44]	OWL, RDF, SPARQL	SSN, Geonames, FOAF, OWL-S	×	✓	✓	×	×	×	×	application
[45]	OWL	OWL-S	×	✓	✓	×	×	×	×	application
[46]	Description Logic	×	×	×	✓	×	×	×	×	application

Table 9
Summary of Semantic-based Approaches for IoT services discovery: context-based approach.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[47]	OWL	SSN, OWL-S	✓	×	✓	×	×	×	×	×
[48]	OWL	×	×	✓	×	×	×	×	×	×
[49]	OWL	contexts ontologies	×	✓	✓	×	×	×	×	application

Table 10
Summary of semantic-based approaches for IoT services discovery: distributed-based approach .

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[50]	OWL	OWL-S, SSN, Geonames, etc.	✓	×	✓	×	×	✓	×	×
[51]	Jena, OWL, RDF, Pellet, SWRL, SPARQL	×	×	×	✓	×	×	✓	×	application
[52]	OWL, SPARQL	OWL-S, SSN, SAN, Geonames	×	×	✓	×	×	×	×	application
[53]	OWL, SPARQL,	×	×	✓	✓	✓	×	×	×	application
[54]	OWL	OWL-S	×	✓	✓	×	×	×	×	application

4.3. IoT Data & services representation

This section states the relevant contributions, which focus on applying SWT to represent the semantics of heterogeneous IoT resources, their data and their services.

The authors in [55] suggested an IoT domain model that is composed of diverse concepts, such as augmented entity, user, device, resource, and service.

Kotis et al. [10], described an ontology that represents knowledge about the IoT devices in order to cooperate with each other in a large-scale, a federated and coordinated way. The main concepts of this ontology are device (sensing device, actuating device, attached device, computing device, etc.), IoT entity, and some concepts are extended from the SSN ontology, such as sensor, feature of interest, observation and property.

Ma et al. [56] set forth the a framework for a semantic information model for IoT applications. In fact, the proposed ontology describes (i) real word entities, namely the object being monitored, sensor devices and the network infrastructure, (ii) the spatial and temporal dimension, (iii) the captured (dynamic and static) data, (iv) services including applications (e.g., in the areas of healthcare or traffic), functions and interfaces.

Table 11
Summary of semantic-based approaches for IoT resources, data and services description.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[55]	×	×	×	×	×	×	×		×	×
[10]	OWL2 QL	DOLCE, SSN, FOAF, QUDT	×	✓	×	×	×	×	×	application
[56]	OWL2	×	×	✓	✓	×	×	×	×	application, data-driven
[57]	JSON-LD, RDF/XML, Turtle	SSN, Geonames, SAO	×	✓	✓	×	×	×	×	application
[58]	OWL	IoT-A, DUL, SSN, IoT-lite, Time, M3	×	✓	✓	×	×	×	101 Methodology	application

Table 12
Summary of Semantic-based Approaches for IoT Security.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[59]	OWL, SPARQL	existing security ontology	×	×	×	✓	×	×	×	×
[60]	OWL, SPARQL	STAC, SecurOntology, Security ontology, NRL security ontology	×	×	×	×	×	×	×	application
[61]	OWL, SWRL	SSN	✓	✓	✓	×	×	×	×	application
[62]	OWL, SPARQL, SWRL	×	×	×	×	×	×	×	×	application

In the context of both the EU FP7 FIWARE project[24] and the EU H2020 FIESTA-IoT project[25] the authors in [57] developed an IoT-lite ontology with the aim of describing IoT concepts in three classes: Objects, system or resources, and services. This ontology is a lightweight instantiation of the SSN ontology [9]. In the same context, Agarwal et al. [58] suggested a unified ontology for the IoT domain, which reuses a number of core concepts from several ontologies, such as SSN, M3-lite (a lite version of M3 and also an outcome of this study), WGS84, IoT-lite, Time, and DUL.

As described in Table 11, the majority of these contributions have formalized their ontologies with semantic languages and based on existing ones. Besides, it is pertinent to note that none of the approaches, except [58], follow a methodology during their models' development. Ensuring the interoperability beween IoT resources, its data and services are the main addressed challenge. Several methods are used for the evaluation step.

4.4. Semantics for IoT security

Instead of communicating with a centralized server, IoT objects communicate with each other which makes the insurance of a secure communication an important challenge that should be addressed. Unfortunately, we found only few works that focus on this challenge based on SWT.

Gyrard et al [59] proposed a STAC ontology to secure IoT applications. This work combined existing ontologies in different domains (sensor networks, mobile phone, network communications, and so on). The STAC ontology presents concepts concerning the security of devices, networks, data, and applications.

Mozzaquatro et al [60] offered a reference ontology for security in IoT, called "IoTSec" based on several existing ontologies for security. This work describes the vulnerability of IoT technologies, security properties (availability, confidentiality, integrity, etc.), and security mechanisms (contains cryptography algorithms).

The authors in [61] defined an ontology (LIoPY ontology) to protect privacy during the IoT data life cycle (collection-transmission-storage-process). The developed ontology is composed mainly of three modules. The IoT description module presents concepts related to the IoT environment. The IoT resource management module defines privacy requirements in terms of privacy attributes, privacy rules, and privacy permission setting classes before and during the collection phase. The IoT resource results sharing management module defines a set of privacy obligations (cryptography, data anonymization, and noise addition) in sharing the collected data.

Choi et al. [62] proposed an ontology-based security framework for IoT-cloud environment. The security ontology contains five main classes namely, customer, power grid, service, new regeneration, and transportation. Diverse rules are proposed in different contexts to verify the security of IoT-cloud environment at different levels (physical, network, system, and so on).

As specified in Table 12, all approaches have formalized their models within the OWL language. Furthermore, the authors reuse diverse concepts from other ontologies. Moreover, they do not propose or follow a methodology during the development process. Additionally, they evaluate their proposals by implementing different tools. The latter are not publicly available.

[24] https://www.fiware.org/
[25] http://fiesta-iot.eu/

Table 13
Summary of semantic-based approaches for WoT.

Reference	RQ2	RQ3	RQ4	RQ5					RQ6	RQ7
				CoT	CoL	CoI	CoTr	CoR		
[63]	OWL DL	WSMO-lite IoT-lite, OWL-S	×	×	×	×	×		×	×
[64]	OWL, SPARQL	×	✓	×	✓	✓	×	✓	×	application
[65]	OWL, SPARQL	SSN, SAO, SAN, QUDT	×	×	✓	×	×	×	×	application
[66]	OWL	Time, DOLCE, etc	✓	✓	✓	✓	×	✓	×	application

4.5. WoT ontologies

This section gives an overview of the use of SWT for the WoT.

The work, realized by Wu et al. [65], defined a semantic web of things framework for cyber-physical systems. This framework provides (i) uniform SWoT-O vocabularies by extending the SSN ontology, (ii) an entity-linking (EL) based methodology to annotate and extract semantics from a domain-specific representation of WoT resources, and (iii) rule-based semantic reasoning for WoT resource integration, anomaly diagnosis, and automatic control.

Charpenay et al. [63] have propounded an ontology for the WoT (WoT)[26] in the context of the Vicinity H2020 EU Project to integrate the concepts of existing IoT vocabularies (SSN, IoT-lite, IoT-O) in the semantic web. This ontology defines terms to describe Objects on the web and to present their interactions as specified by the thing description model. The key concepts of the WoT ontology are: **wot: ThingDescription** that represent IoT devices, **wot: InteractionPattern** describes how data can be exchanged between web client and the thing, **wot: Endpoint** defined the URI of web services that can be accessed by any application, and the **wot:dataschema**, which defines the input and the output data in the interaction model.

Mrissa et al. [64] suggested an avatar architecture to extend an object on the Web. They developed a set of ontologies (context ontology, functionality ontology, capability ontology, etc.) in order to infer and transform low-level data provided by the physical object into high-level functionalities.

Xu et al. [66] have focused in providing a common model for the WoT using an ontology-based approach to describe heterogeneous connected objects. This model can describe both static and dynamic information about WoT. The static model comprises nine classes (Semantic Virtual Object (SVO), Capability, Functionality, Parameters, State, Identification, Communication, Sense, and Information). The dynamic model aims to represent real time information that is composed of four main classes (CurrentStatus, RealTime-Information, RealTimeSVO and Context).

As described in Table 13, the proposed semantic models are usually formalized by both OWL and SPARQL languages. Moreover, none of them followed a methodology and only some of them are based on existing models. In addition, the main addressed issue is the interoperability between WoT resources. The authors evaluate their models using the application-based evaluation method. Therefore, the proposed applications are not available online. In the next section, we offer a discussion of the above-mentioned works in the previous sections.

5. Discussion

Special interest has been directed during the last years to the use of SWT in order to improve the adoption of sensors setworks, IoT and WoT. In fact, to address semantic interoperability in these areas, we need to understand how it is built-up. From the comparative tables previously cited and the description of each category, we can note the following insights.

- Domain of Interest: The domain of interest criterion helps us classify the realized approaches according to their perceived importance. In fact, we notice that none of the above-mentioned works has developed a complete model that addresses all the semantic layers (IoT resources, IoT data, IoT services, IoT security) in order to define a standard model that will be exploited with heterogeneous devices. In addition, representing the deployment context of employed devices is not well developed. Diverse concepts, such as trajectory, interconnectivity and object specification should be considered in addition to time and location. The trajectory context helps identify the crossed location at a given time in order to track the activity of the monitored element. The object specification and interconnectivity contexts are essential in configurating and managing the functioning state of the connected object.
- Semantic Technologies: With regard to RQ2, most of the proposed approaches have been concentrated on OWL, SWRL, and SPARQL languages. OWL has three varying levels of expressiveness: OWL Lite, OWL DL and OWL Full. It is not specified which OWL fragment is used to model the ontology in the majority of these approaches. In addition, only two works [10,56] used OWL2 in their models, without specifying which profile is used.

  In this paper, we determine that only a handful of approaches have used the description logic language. Furthermore, DL is characterized by its powerful expressiveness. Additionally, these approaches have ignored the rule interchange format (RIF) [70] capabilities to ease interoperability and portability between IoT systems, which use different rule languages. RIF is a W3C Recommendation,which is a promising solution for expressing rules and ensuring their exchange between rule

[26] http://w3c.github.io/wot/ire-extended.owl

systems. Moreover, it is important to consider the latest W3C standards, SHACL to validate the RDF graphs by defining a set of constraints.
Before implementing an ontology, several questions arised such as what is the most expressive language? Does the chosen language facilitate using and interpreting the ontology in applications? Is the language chosen compatible with other languages? What is the reasoning mechanism adopted by this language?

- Ontologies Reuse: We notice that the most reused ontologies in these approaches are SSN ontologies and generic ontologies, such as time ontology, location ontology, DOLCE, and so on.
Unfortunately, most of these approaches do not consider the previously proposed IoT ontologies. The latter define concepts related to IoT devices and their specifications rather than considering SSN which focuses just on sensors. In addition, some other approaches [39,40,42,46], have ignored the reusing task and built their ontologies from scratch.
- Modularity: IoT is a heterogeneous domain that generates a huge quantity of data. Therefore, a large and monolithic ontology containing this data is difficult to be used for both reasoning and reusing purposes.
In fact, despite the importance of building ontologies in a set of modules to solve these challenges, just few works [9,11,33,35,47,50] followed this methodological principle.
- Methodology: An ontology development methodology gives a set of practices and guidelines to help domain experts build an ontology.
Despite this fact, authors in this study do not specify which methodology to use to be able to build their ontologies. This was not the case of other approaches, such as the work of Gyrard et al.[36], which uses the methontology methodology, Elsalah et al. [38], and Agarwal et al. [58], who follow the 101 methodology and Seydoux et al. [11] who employ the NeOn methodology.
Nonetheless, the importance of agile methodologies in ontology building especially modular ontologies, as avowed by [71], was not taken into account.
- Evaluation: we notice that most proposed approaches choose the application-based evaluation technique to assess their ontologies. None of these approaches has proposed a complete evaluation of their models that take into consideration criteria-based, application-based, data driven-based and gold standard methods.
In fact, the reason for not choosing the gold standard method to evaluate their models can be due to the absence of a gold standard in the IoT field. Therefore, there are still significant shortfalls in the used methods and techniques to evaluate the proposed application. Indeed, we find that only a few approaches utilized precision, recall and F-measure metrics that can bring possible sophisticated solutions to improve reliability, performance and significance of applications. In addition, a comparison between the suggested application and the already existing ones is missing in the majority of works.

6. Open research questions

In addition to our research questions, we identify research opportunities, in the form of a roadmap toward mature and advanced semantic-based solutions. Future works should address diverse challenges such as the standardization (Section 6.1) the IoT resource management (Section 6.2), the scalability (Section 6.3), the uncertainty (Section 6.4), and the security issue (Section 6.5).

6.1. Standardization in heterogeneous connected environments

Thanks to IoT, real world objects become smart in the way that they can communicate under heterogeneous network, exchange data with their users as well as with each other, etc. There has been an exponential increase in the number of these objects during these few years, which brings various serious challenges. First, users need to control and monitor their devices regardless of their locations (e.g. person in his office can remotely control his connected devices in his home, he can send/receive notification to/from them) from only one application. These devices are designed by different manufacturers and often have a data exchange problem with each other. Consequently, there is a lack of consistency and interoperability, which demands a new industry alliance to set up unified standard models, protocols and programming language and to support interoperable IoT devices like the effort of the W3C/ETSI[27]. Standardization ensures the levels of interoperability, portability and manageability for various connected objects.

To build interoperable IoT devices in a very dynamic and heterogeneous environment, developers should focus more on ensuring standardization according to three aspects. The first aspect is to define a standard model from large amounts of data that will be exchanged between heterogeneous IoT devices. The second aspect is to build standard protocols (e.g. wireless standards) to make sure that devices can communicate with each other. The third aspect is to use a specific programming language to develop applications and to ensure reliable management and configuration of connected objects with different features. From this purpose, a standardized ontology becomes a vital need in such a complex domain. Defining standardized ontologies in the IoT domain will not be an easy task. Consequently, different versions will be released to deal with new devices and requirements. These new devices may not be usable at any time as their special features are

[27] https://www.etsi.org/

not considered in data structures, protocols and applications. For this reason, a new application is developed for a newer version that must take care of releasing only downwardly compatible versions, where the evolution of ontology and protocol approaches must be applied. Accordingly, a new research is necessary for the development of adequate evolutionary approaches for jointly evolving ontologies and protocols in SWoT.

6.2. IoT Resource management

A huge number of connected objects with limited resource devices appeared. These devices have scarce computing power and limited storage capacity, electrical power consumption,and definite lifetime, etc. In addition, most of these objects are dynamic and their behaviors change depending on their deployment time and location. Moreover, they are able to be moved from one system to another.

As a result,"managing IoT resources" from data acquisition to the suggestion of valuable services constitutes a major problem. IoT resource management includes modeling, resource allocation, discovery, and monitoring tasks. From this perspective, SWT is a promising choice to address these challenges.

During the modeling phase, SWoT researchers should focus on defining concepts to represent other specifications of IoT devices. For example, in order to express the dynamism and the portability of IoT devices, it is necessary to determine the basic concepts of the trajectory of connected objects. Therefore, the network has to be modeled and managed adequately for its efficient utilization.

However, it is required to guarantee the proper functioning of IoT resources and detect any kind of problem that prevents sudden breakdowns due to discharged battery, saturated memory, loss of connectivity, etc.

Therefore, rules must be proposed in order to analyze these situations and suggest suitable solutions. For instance, we can refer to an object (smartphone) located in a house and connected to the home gateway. Once the user is outside the house, the 3G connexion should be activated. In addition, if the connected object's battery is discharged, its allowed task will be directed to another one. Before assigning this task to the new object, it is important to verify its availability to be able allocate this task.

6.3. Scalability

The exponential growth of connected objects to the Internet produces a massive quantity of data called "Big data [72]". According to [73], the big data generated by IoT has different characteristics like large-scale data, heterogeneity, strong time and space correlation. Therefore, the main challenges encountered during the development of IoT applications/systems are the semantic IoT event processing, real-time processing of data streams and reasoning in a complex and dynamic context (spatiotemporal reasoning) in a scalable and secure way, etc. Consequently, these new requirements drive the need for the deployment of a scalable IoT system. Thereby, applying SWT (SWRL, SPARQL, DL safe rules, RIF, etc.) to the IoT domain faces a new challenge on how to manage and interpret such heterogeneous data during a limited period in a scalable way. This is justified by the fact that SWT needs a large storage memory, computing power and reasoning, and a powerful bandwidth to manage and transfer this massive data. However, IoT objects have limited resources in terms of their memory and processing capacity, which reflect their inability to process the obtained data with these technologies. Accordingly, developing a semantic-based scalable IoT system is a challenge that needs the alliance of SWT and the new emerging technologies (cloud computing, edge computing, fog computing, and big data) in SWoT infrastructure. In this perspective, as a good starting point for new research, it is crucial to mention the outcomes of the research conducted by Seydoux et al. in [74], in which the authors have proposed to apply fog-computing and cloud-computing to ensure a scalable IoT data processing with SWT. The main goal of this approach is to enhance semantic computing in Fog nodes that are closer to IoT devices, instead of sending this data to remote cloud nodes. The adopted a strategy called emergent distributed reasoning (EDR), which consists of distributing rules (expressed on SHACL) in a Cloud-Fog continuum. This strategy helps reduce response time, guarantee privacy and lower energy consumption.

In the context of big data, there exist the Neo4j[28] consists in constructing and managinghuge quantities of structured data that are presented in graph format. Large ontologies can be imported intoNeo4j that ensures efficient storage and interpretation of these ontologies. Therefore, implementing a new inference engine allows to manage big ontologies and big data technologies, like Hadoop and Spark, which seem to be reasonable solutions. Ron et al. [75] developed a hybrid adaptive distributed RDF stream processing engine Strider to ensure a real time processing of data streams in a scalable way. Strider contains two modules, namely data flow management module based on Apache Kafka, and computing core module based on Spark. In [76], the authors proposed a SANSA API to facilitate reasoning over RDF data stream in Spark.

We notice that the semantic-computing approaches that were based on big data technologies have focused on OWL-Horst and RDFS rule sets. Future researchers can focus on the management of SWRL rules with Spark and Hadoop.

In addition, much research should focus on complex IoT service discovery, integration, composition, etc, by taking into consideration the dynamic and spatio-temporal dependency of IoT resources.

Another open research question that should be considered in future works is the orchestration of IoT resources with the adoption of both SWT and the new emerging technologies.

[28] https://neo4j.com/

6.4. Uncertainty in IoT

IoT domain is characterized by the dynamic change of the connected objects' behaviors, which generate a massive amount of imprecise and vague data. Furthermore, classical ontologies cannot address this kind of knowledge. To deal with this issue, fuzzy and probabilistic ontologies are a powerful solution. Fuzzy ontology [77] is a quintuple OF= I, C, R, F, A where I is a set of individuals, C is a set of concepts, R represents a set of relations, F stands for a set of fuzzy relations and A symbolizes a set of axioms. The implementation of fuzzy ontology is based on a fuzzy description logic and OWL.

In addition, the probabilistic ontologies are widely used to present ambiguous, incomplete, and uncertain domain knowledge [78]. These ontologies are formalized via PR-OWL (probabilistic OWL).

In this perspective, future researchers can exploit these ontologies in order to handle the uncertain challenges in IoT.

6.5. Security issues in SWoT

IoT devices record and distribute sensible data of their owners. The absence of any applied security concept may make IoT devices transparent for others with the danger of misuses. It is the state-of-the-art to consider privacy as early as possible in software architecture design process (privacy-by-design [79]). To this end, semantic Internet of Things (SIoT) developers need to strive and integrate Separation-of-Duties (SoD), Separation-of-Concerns (SoC) and Separation-of-Information (SoI) into their system architectures. SoD [80] means that different tasks must be executed by different roles. Thus, SoD prevents fraud or misuse by isolating tasks from each other. SoC [81] refers to a programming concept that encapsulates functionality and data of different tasks in different software modules. Thus, SoC can be seen as realizing SoD into a software architecture. With SoI, we refer to a concept that organizes any personal data into separate entities that cannot be linked to an individual without his consent, e.g., by storing isolated data fragments that are indexed with encrypted identifiers [82]. Thus, researchers should transfer and present these principles (SoD, SoI, SoC) in IoT security ontologies via the definition of constraints and rules (e.g using SHACL language).

However, IoT environments generate large masses of data where it becomes much more difficult to avoid approaches and re-identification attacks, compared to other areas. Mishra et al [83] highlighted the main security challenges in IoT that need to be fixed and processed with the aim of developing secure and reliable SWoT applications. These challenges include confidentiality, integrity, availability, authentication, authorization, access control, and trustworthiness. These issues appear in three different levels during the development of IoT applications [84]. The first level, named *low level security* issues, focuses on the employed hardware and the obtained data. The second level corresponds to *intermediate level security* issues. The third level, dealing with security for IoT applications, is called *high-level security.*

Thereby, SWoT developers should focus on defining a standard security ontology in IoT. Thus, this can be achieved by attentively addressing these three levels. This ontology will contain different attacks as well as the suitable process that should be followed to avoid these challenges.

In another context, a new emerging technology, such as blockchain [85], [86], can be used by semantic web researchers to propose an ontology-based blockchain for IoT security. Blockchain is considered as a key solution for IoT, which stores and transmits the obtained data stream in a secure, transparent, distributed, auditable and efficient way. Thereby, the combination of blockchain and semantic technologies in the IoT field resolves several challenges, such as facilitating data sharing in a secure way, storing data in blockchain, etc.

7. Conclusion and outlook

With the emergence of IoT technology, an enormous quantity of real-world objects becomes more connected to the Internet than before and can communicate together and exchange data with each other. Accordingly, ensuring the interoperability between heterogeneous IoT systems is a difficult task that needs a lot of effort. In this regard, SWT is widely used to define a unified vocabulary that will be shared between IoT devices and systems. This study, detailed and analyzed the semantic-based approaches for IoT domain representation. For that, we have conducted a Systematic Literature Review to select the most relevant approaches based on different relevant academic articles.

The extracted studies in this review were categorized according to their main contribution using a classification scheme with five dimensions related to IoT data, IoT services, IoT data and services, IoT Security, and WoT.

The analysis of the existing works helped us to identify and describe open and new research questions and challenges in adopting SWT in IoT under many different aspects. Although there is a quick development of new SWoT approaches, many problems and issues are only rudimentary tackled so far (standardization, scalability, security, and so on) and various research studies still need to be undertaken.

To conclude, it is not reassuring to notice that all the proposed approaches have been based on partial models without taking into account several characteristics, like virtualization, context-awareness, and dynamism, and without addressing the principal components of the Internet of Things in the same model, like IoT resources (connected objects, devices and network technologies), IoT data and other related concepts, such as time and space, and IoT services.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] F. Wortmann, K. Flüchter, Internet of things, Bus. Inf. Syst. Eng. 57 (3) (2015) 221–224.
[2] C. Perera, C.H. Liu, S. Jayawardena, The emerging internet of things marketplace from an industrial perspective: a survey, IEEE Trans. Emerg. Top. Comput. 3 (4) (2015) 585–598.
[3] P. Barnaghi, W. Wang, C. Henson, K. Taylor, Semantics for the internet of things: early progress and back to the future, Int. J. Semant. Web Inf. Syst. (IJSWIS) 8 (1) (2012) 1–21.
[4] M. Ruta, F. Scioscia, E. Di Sciascio, D. Rotondi, Ubiquitous knowledge bases for the semantic web of things, First Internet of Things International Forum, 2011.
[5] A.J. Jara, A.C. Olivieri, Y. Bocchi, M. Jung, W. Kastner, A.F. Skarmeta, Semantic web of things: an analysis of the application semantics for the iot moving towards the iot convergence, Int. J. Web Grid Serv. 10 (2–3) (2014) 244–272.
[6] R. Studer, V.R. Benjamins, D. Fensel, Knowledge engineering: principles and methods, Data Know. Eng. 25 (1–2) (1998) 161–197.
[7] J. Ye, L. Coyle, S. Dobson, P. Nixon, Ontology-based models in pervasive computing systems, Knowl. Eng. Rev. 22 (4) (2007) 315–347.
[8] I. Szilagyi, P. Wira, Ontologies and semantic web for the internet of things-a survey, in: Industrial Electronics Society, IECON 2016-42nd Annual Conference of the IEEE, IEEE, 2016, pp. 6949–6954.
[9] M. Compton, P. Barnaghi, L. Bermudez, R. GarcíA-Castro, O. Corcho, S. Cox, J. Graybeal, M. Hauswirth, C. Henson, A. Herzog, et al., The ssn ontology of the w3c semantic sensor network incubator group, Web Semantic. 17 (2012) 25–32.
[10] K. Kotis, A. Katasonov, An iot-ontology for the representation of interconnected, clustered and aligned smart entities, Technical report, VTT Technical Research Center, Finland VTT Technical Research Center, Finland, 2012.
[11] N. Seydoux, K. Drira, N. Hernandez, T. Monteil, Iot-o, a core-domain iot ontology to represent connected devices networks, in: Knowledge Engineering and Knowledge Management: 20th International Conference, EKAW 2016, Springer, 2016, pp. 561–576.
[12] G. Bajaj, R. Agarwal, P. Singh, N. Georgantas, V. Issarny, A study of existing ontologies in the iot-domain, arXiv preprintarXiv:1707.00112(2017).
[13] M. Ganzha, M. Paprzycki, W. Pawłowski, P. Szmeja, K. Wasielewska, Semantic interoperability in the internet of things: an overview from the inter-iot perspective, J. Netw. Comput. Appl. 81 (2017) 111–124.
[14] S. De, Y. Zhou, K. Moessner, Ontologies and Context Modeling for the Web of Things, in: Managing the Web of Things, Elsevier, 2017, pp. 3–36.
[15] D. Andročec, M. Novak, D. Oreški, Using semantic web for internet of things interoperability: a systematic review, Int. J. Semant. Web Inf. Syst. (IJSWIS) 14 (4) (2018) 147–171.
[16] B. Kitchenham, Procedures for Performing Systematic Reviews, Keele, UK, Keele University 33 (2004) (2004) 1–26.
[17] D. Moher, A. Liberati, J. Tetzlaff, D.G. Altman, P. Group, et al., Preferred reporting items for systematic reviews and meta-analyses: the prisma statement, PLoS Med. 6 (7) (2009) e1000097.
[18] D. Lonsdale, D.W. Embley, Y. Ding, L. Xu, M. Hepp, Reusing ontologies and language components for ontology generation, Data Know. Eng. 69 (4) (2010) 318–330.
[19] S.B. Abbes, A. Scheuermann, T. Meilender, M. d'Aquin, Characterizing modular ontologies, in: 7th international Conference on Formal Ontologies in Information Systems- FOIS 2012, 2012, pp. 13–25.
[20] F. Ensan, W. Du, An interface-based ontology modularization framework for knowledge encapsulation, in: International Semantic Web Conference, Springer, 2008, pp. 517–532.
[21] Z.C. Khan, C.M. Keet, Toward a framework for ontology modularity, in: Proceedings of the 2015 Annual Research Conference on South African Institute of Computer Scientists and Information Technologists, 2015, pp. 1–10.
[22] M. Jarrar, Towards methodological principles for ontology engineering., Mustafa Jarrar: Towards methodological principles for ontology engineering. PhD Thesis. Vrije Universiteit Brussel.(May 2005) (2005).
[23] A.K. Dey, Understanding and using context, Pers Ubiquitous Comput. 5 (1) (2001) 4–7.
[24] M. Fernández-López, A. Gómez-Pérez, N. Juristo, Methontology: from ontological art towards ontological engineering, Spring Symposium Ser. (1997) 33–40.
[25] Ontology development 101: A guide to creating your first ontology. Ontology development 101: a guide to creating your first ontology. Technical report, Stanford knowledge systems laboratory KSL-01-05 and Stanford medical informatics technical report SMI-2001-0880, Stanford, CA, 2001.
[26] M.C. Suárez-Figueroa, A. Gómez-Pérez, M. Fernandez-Lopez, The neon methodology framework: a scenario-based methodology for ontology development, Appl. Ontol. 10 (2) (2015) 107–145.
[27] S. Peroni, A simplified agile methodology for ontology development, in: OWL: Experiences and Directions–Reasoner Evaluation, Springer, 2016, pp. 55–69.
[28] J. Brank, M. Grobelnik, D. Mladenic, A survey of ontology evaluation techniques, in: Proceedings of the Conference on Data Mining and Data Warehouses (SiKDD 2005), Citeseer Ljubljana, Slovenia, 2005, pp. 166–170.
[29] T.R. Gruber, Toward principles for the design of ontologies used for knowledge sharing? Int. J. Hum. Comput. Stud. 43 (5–6) (1995) 907–928.
[30] A. Gómez-Pérez, Evaluation of ontologies, Int. J. Intell. Syst. 16 (3) (2001) 391–409.
[31] D. Ref, A.S. Segura, N.V. SAG, Internet of things architecture iot-a project deliverable d6. 2–updated requirements list (2011).
[32] A. Gyrard, C. Bonnet, K. Boudaoud, M. Serrano, Lov4iot: a second life for ontology-based domain knowledge to build semantic web of things applications, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2016, pp. 254–261.
[33] R. Bendadouche, C. Roussey, G. De Sousa, J.-P. Chanet, K.M. Hou, Extension of the semantic sensor network ontology for wireless sensor networks: the stimulus-wsnnode-communication pattern, in: Proceedings of the 5th International Conference on Semantic Sensor Networks-Volume 904, CEUR-WS. org, 2012, pp. 49–64.
[34] H. Müller, L. Cabral, A. Morshed, Y. Shu, From restful to sparql: a case study on generating semantic sensor data, in: Proceedings of the 6th International Conference on Semantic Sensor Networks, Volume 1063, CEUR-WS. org, 2013, pp. 51–66.
[35] K. Janowicz, A. Haller, S.J. Cox, D. Le Phuoc, M. Lefrancois, Sosa: a lightweight ontology for sensors, observations, samples, and actuators, J. Web Semant. (2018).
[36] A. Gyrard, S.K. Datta, C. Bonnet, K. Boudaoud, Cross-domain internet of things application development: M3 framework and evaluation, in: 2015 3rd International Conference on Future Internet of Things and Cloud, IEEE, 2015, pp. 9–16.
[37] S. Kolozali, M. Bermudez-Edo, D. Puschmann, F. Ganz, P. Barnaghi, A knowledge-based approach for real-time IoT data stream annotation and processing, in: Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), IEEE, IEEE, 2014, pp. 215–222.
[38] T. Elsaleh, M. Bermudez-Edo, S. Enshaeifar, S. Acton, R. Rezvani, P. Barnaghi, Iot-stream: a lightweight ontology for internet of things data streams, in: 2019 Global IoT Summit (GIoTS), IEEE, 2019, pp. 1–6.
[39] I. Tachmazidis, S. Batsakis, J. Davies, A. Duke, M. Vallati, G. Antoniou, S.S. Clarke, A hypercat-enabled semantic internet of things data hub, in: European Semantic Web Conference, Springer, 2017, pp. 125–137.

[40] K. Ryabinin, S. Chuprina, K. Belousov, Ontology-driven automation of IoT-based human-machine interfaces development, in: International Conference on Computational Science, Springer, 2019, pp. 110–124.
[41] S. De, P. Barnaghi, M. Bauer, S. Meissner, Service modelling for the internet of things, in: Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on, IEEE, 2011, pp. 949–955.
[42] K. Hur, X. Jin, K.-H. Lee, Automated deployment of IoT services based on semantic description, in: Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on, IEEE, 2015, pp. 40–45.
[43] S. Hachem, T. Teixeira, V. Issarny, Ontologies for the internet of things, in: Proceedings of the 8th Middleware Doctoral Symposium, ACM, 2011, p. 3.
[44] X. Jin, S. Chun, J. Jung, K.-H. Lee, A fast and scalable approach for IoT service selection based on a physical service model, Inf. Syst. Front. 19 (6) (2017) 1357–1372.
[45] C. Qu, F. Liu, M. Tao, D. Deng, An owl-s based specification model of dynamic entity services for internet of things, J. Ambient Intell. Humaniz. Comput. 7 (1) (2016) 73–82.
[46] A. Yachir, B. Djamaa, A. Mecheti, Y. Amirat, M. Aissani, A comprehensive semantic model for smart object description and request resolution in the internet of things, Procedia Comput. Sci. 83 (2016) 147–154.
[47] S.A.U. Nambi, C. Sarkar, R.V. Prasad, A. Rahim, A unified semantic knowledge base for iot, in: Internet of Things (WF-IoT), 2014 IEEE World Forum on, IEEE, 2014, pp. 575–580.
[48] Q. Wei, Z. Jin, Service discovery for internet of things: a context-awareness perspective, in: Proceedings of the Fourth Asia-Pacific Symposium on Internetware, ACM, 2012, p. 25.
[49] J. Li, N. Zaman, H. Li, A decentralized locality-preserving context-aware service discovery framework for internet of things, in: Services Computing (SCC), 2015 IEEE International Conference on, IEEE, 2015, pp. 317–323.
[50] W. Wang, S. De, G. Cassar, K. Moessner, Knowledge representation in the internet of things: semantic modelling and its applications, automatika 54 (4) (2013) 388–400.
[51] M. Ryu, J. Kim, J. Yun, Integrated semantics service platform for the internet of things: a case study of a smart office, Sensors 15 (1) (2015) 2137–2160.
[52] P. Gomes, E. Cavalcante, T. Rodrigues, T. Batista, F.C. Delicato, P.F. Pires, A federated discovery service for the internet of things, in: Proceedings of the 2nd Workshop on Middleware for Context-Aware Applications in the IoT, ACM, 2015, pp. 25–30.
[53] A. Willner, C. Papagianni, M. Giatili, P. Grosso, M. Morsey, Y. Al-Hazmi, I. Baldin, The open-multinet upper ontology towards the semantic-based management of federated infrastructures, EAI Endors. Trans. Scalable Inf. Syst. 2 (7) (2015) 1–10.
[54] W. Zhu, G. Zhou, I.-L. Yen, F. Bastani, A pt-soa model for cps/IoT services, in: Web Services (ICWS), 2015 IEEE International Conference on, IEEE, 2015, pp. 647–654.
[55] S. Haller, A. Serbanati, M. Bauer, F. Carrez, A domain model for the internet of things, in: Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, IEEE, 2013, pp. 411–417.
[56] M. Ma, P. Wang, C.-H. Chu, Ontology-based semantic modeling and evaluation for internet of things applications, in: Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), IEEE, IEEE, 2014, pp. 24–30.
[57] M. Bermudez-Edo, T. Elsaleh, P. Barnaghi, K. Taylor, Iot-lite: a lightweight semantic model for the internet of things and its use with dynamic semantics, Pers. Ubiquitous Comput. (2017) 1–13.
[58] R. Agarwal, D.G. Fernandez, T. Elsaleh, A. Gyrard, J. Lanza, L. Sanchez, N. Georgantas, V. Issarny, Unified iot ontology to enable interoperability and federation of testbeds, 3rd IEEE World Forum on Internet of Things, 2016.
[59] A. Gyrard, C. Bonnet, K. Boudaoud, An ontology-based approach for helping to secure the ETSI machine-to-machine architecture, in: Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), IEEE, IEEE, 2014, pp. 109–116.
[60] B.A. Mozzaquatro, R. Jardim-Goncalves, C. Agostinho, Towards a reference ontology for security in the internet of things, in: Measurements & Networking (M&N), 2015 IEEE International Workshop on, IEEE, 2015, pp. 1–6.
[61] F. Loukil, C. Ghedira-Guegan, K. Boukadi, 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), IEEE, 2018, pp. 701–706.
[62] C. Choi, J. Choi, Ontology-based security context reasoning for power IoT-cloud security service, IEEE Access 7 (2019) 110510–110517.
[63] V. Charpenay, S. Käbisch, H. Kosch, Introducing thing descriptions and interactions: an ontology for the web of things., in: SR+ SWIT@ ISWC, 2016, pp. 55–66.
[64] M. Mrissa, L. Médini, J.-P. Jamont, N. Le Sommer, J. Laplace, An avatar architecture for the web of things, IEEE Internet Comput. 19 (2) (2015) 30–38.
[65] Z. Wu, Y. Xu, Y. Yang, C. Zhang, X. Zhu, Y. Ji, Towards a semantic web of things: a hybrid semantic annotation, extraction, and reasoning framework for cyber-physical system, Sensors 17 (2) (2017) 403.
[66] W. Xu, C. Marsala, B. Christophe, Matching objects to user's queries in web of things' applications, in: 2013 IEEE Symposium on Computational Intelligence for Communication Systems and Networks (CIComms), IEEE, 2013, pp. 31–38.
[67] C.A. Henson, J.K. Pschorr, A.P. Sheth, K. Thirunarayan, Semsos: Semantic sensor observation service, in: Collaborative Technologies and Systems, 2009. CTS'09. International Symposium on, IEEE, 2009, pp. 44–53.
[68] G. Stevenson, S. Knox, S. Dobson, P. Nixon, Ontonym: a collection of upper ontologies for developing pervasive systems, in: Proceedings of the 1st Workshop on Context, Information and Ontologies, ACM, 2009, p. 9.
[69] M. Calder, R.A. Morris, F. Peri, Machine reasoning about anomalous sensor data, Ecol. Inform. 5 (1) (2010) 9–18.
[70] M. Kifer, H. Boley, Rif overview, W3C working draft, W3C,(October 2009). http://www. w3. org/TR/rif-overview (2013).
[71] B.A. Gobin, An agile methodology for developing ontology modules which can be used to develop modular ontologies, in: 2013 IEEE International Conference on Computer Science and Automation Engineering (CSAE 2013), 2013.
[72] P. Barnaghi, A. Sheth, C. Henson, From data to actionable knowledge: big data challenges in the web of things, IEEE Intell. Syst. (2013).
[73] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proceedings of the first edition of the MCC workshop on Mobile cloud computing, ACM, 2012, pp. 13–16.
[74] N. Seydoux, K. Drira, N. Hernandez, T. Monteil, Towards cooperative semantic computing: a distributed reasoning approach for fog-enabled swot, in: OTM Confederated International Conferences" On the Move to Meaningful Internet Systems", Springer, 2018, pp. 407–425.
[75] X. Ren, O. Curé, Strider: A hybrid adaptive distributed RDF stream processing engine, in: International Semantic Web Conference, Springer, 2017, pp. 559–576.
[76] J. Lehmann, G. Sejdiu, L. Bühmann, P. Westphal, C. Stadler, I. Ermilov, S. Bin, N. Chakraborty, M. Saleem, A.-C.N. Ngomo, et al., Distributed semantic analytics using the sansa stack, in: International Semantic Web Conference, Springer, 2017, pp. 147–155.
[77] Q.T. Tho, S.C. Hui, A.C.M. Fong, T.H. Cao, Automatic fuzzy ontology generation for semantic web, IEEE Trans. Knowl. Data Eng. 18 (6) (2006) 842–856.
[78] P.C. Costa, K.B. Laskey, Pr-owl: a framework for probabilistic, in: Formal Ontology in Information Systems: Proceedings of the Fourth International Conference (FOIS 2006), 150, IOS Press, 2006, p. 237.
[79] OASIS, OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC, 2015.
[80] R.A. Botha, J.H.P. Eloff, Separation of duties for access control enforcement in workflow environments, IBM Syst. J. 40 (3) (2001) 666–682.
[81] W.L. Hürsch, C.V. Lopes, Separation of concerns, Technical Report, Technical report by the College of Computer Science, Northeastern University, 1995.
[82] C. Heidinger, E. Buchmann, M. Huber, K. Böhm, J. Müller-Quade, Privacy-aware folksonomies, in: Proceedings of the 14th European Conference on Research and Advanced Technology for Digital Libraries, in: ECDL'10, 2010.

[83] S. Mishra, S. Jain, C. Rai, N. Gandhi, Security challenges in semantic web of things, in: International Conference on Innovations in Bio-Inspired Computing and Applications, Springer, 2018, pp. 162–169.
[84] M.A. Khan, K. Salah, Iot security: review, blockchain solutions, and open challenges, Future Generat. Comput. Syst. 82 (2018) 395–411.
[85] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc., 2015.
[86] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, 2017, pp. 557–564.