Towards an Ontology for IoT Context-Based Security Evaluation

Pedro Gonzalez-Gil, Antonio F. Skarmeta
DIIC
Universidad de Murcia
Murcia, Spain
Email: pedrog@um.es, skarmeta@um.es

Juan Antonio Martinez
Odin Solutions
Murcia, Spain
Email: jamartinez@odins.es

***Abstract*—As a consequence of the massive adoption of IoT technologies in a wide spectrum of applications, from *Smart Cities* to *Smart Agriculture*, security has become a great concern. Many different technologies and devices, often constrained by energy consumption, size or price, make for a complex and difficult scene. Added to that, a broad range of data consumers and agents interacting with those systems have different requirements and expectations regarding security and privacy, while existing approaches at evaluating security do not account for that diversity of security and privacy expectations. Ontologies have proven to be a a good way to represent knowledge in a way that embraces the distributed nature of *IoT*, as well as the capability of being machine-friendly. On top of that, previous works have been already established a foundation on the representation of those security elements and traits in several scenarios, including *IoT*, establishing the grounds for this work. In this paper we present an *Ontology for IoT Context-Based Security Evaluation (IoTSecEv)*, developed following the *NeOn methodology*, performing a conceptual formalization of the observer's context on security preferences, and linking this knowledge to concepts of an existing ontology on *IoT* Security: *IoTSec*.**

***Keywords*-IoT; Semantic Web; Linked Data; WoT; Security Evaluation; Ontology**

I. Introduction

In the continuous advance and merging of society and technology, concepts such as *Smart Cities*, *IoT*, *M2M*, *WoT*, *Smart Home*s, reveal the pervasiveness of technology in all of the levels of our life as species, from the highest levels of society to our daily activities, and reaching more and more deep down into our personal life. The widespread and ever increasing presence of those technologies is now being lead by the continuous introduction of connected intelligent devices, that sense and interact with their environment, communicating and exchanging information in an autonomous way.

A. IoT

Some forecasts like the *CISCO Visual Networking Index: Forecast and Trends, 2017-2022* [1], state that "IoT connections will represent more than half (14.6 billion) of all global connected devices and connections (28.5 billion) by 2022", complemented by *Ericsson Mobility Report* [2] "The number of cellular IoT connections is expected to reach 3.5 billion in 2023 increasing with an annual growth rate of 30 percent", show the emancipation of those devices from local and controlled networks, out into the *wilderness* of internet. This new paradigm introduces a plethora of challenges and opportunities [1] that need be met, regarding, among others, the management and structuring of those vast amounts of data.

Scenarios like *Smart Cities*, that build upon the IoT technology, add a level of abstraction and complexity by promoting the integration of different technologies, data providers and agents, that must cooperate for the benefit of the whole, crossing the boundary of the scopes of their own domains. This poses new levels of difficulty for the exchange of data and the design of interfaces.

The same goes for *Smart Home*, *Industry 4.0*, and *eHealth* among others, where different device providers will have to cope with unknown environments and face the demands of users by cooperating in a highly dynamic, flexible and multi-domain structure, where *security* and *privacy* become a pressing concern.

B. WoT and Semantic Web

In the massive amounts of data in IoT, searching, accessing and exchanging information in an standardized way, are non-trivial tasks. In this context, the *Web* presented as the best existing approach at solving the problem. Web technologies are increasingly becoming the preferred technology for communication between connected devices, allowing and embracing diversity by setting a common safe ground for communication. Further on, new protocols and specifications are being developed on top of Web technologies, such as *Fiware*'s *NGSI* approach [2], setting new layers on top of web technologies, specifically aimed at addressing the IoT challenges, and giving birth to the concept of *Web of Things (WoT)*.

One of the solutions offered by Web technologies, initially aimed at the problem of finding the right information in

[1] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf

[2] https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf

the exponentially growing body of data, was *Semantic Technology*. Search engines where limited on their success to provide meaningful results, hindered by the inability of machines to understand the context of indexed elements. The most successful solution at that point, was to add semantic annotations, based on ontologies defining various domains of knowledge. Latter improved by new approaches for linking data, such as JSON-LD [3], this new scenario of *Smart Everything* became a great candidate for applying new *Ontologies*, adding structure and context in a *machine friendly* way. This last one is a key point, considering the aforementioned *CISCO* forecast: "M2M connections will be more than half of the global connected devices and connections by 2022 [...] There will be 14.6 billion M2M connections by 2022", implying that a big part of the data exchange is going to take place between intelligent devices.

C. Security

Even more concerning and pressing than the previous point, is security. As a pervasive characteristic to all scenarios of IoT, security and privacy are key points to address for the successful development and adoption of the technology into our society. In this regard, existing approaches into the definition of security and its evaluation, become lacking [4] when faced with the diversity of elements and decentralized nature of IoT. A broad range of devices, technologies, data consumers, agents and application scenarios make extremely difficult the characterization of security, and on top of that, there is no common security definition by which to evaluate it, among the different parties involved, falling to a default case-by-case basis. Even further on, the pressing concern for M2M scenarios calls for a machine-friendly solution, placing the problem of the security evaluation in a completely foreign landscape.

As a first attempt into the aforementioned problem, this work presents a *IoT Context Based Security Evaluation Ontology*, that addresses security evaluation in a machine friendly way attending the distinct expectations of security by different observers.

The rest of this work is structured as follows: in II a state of the art is summarized, relating to existing related works on security evaluation and security ontologies. In III we present a general overview of the problem and the methodology followed in creating the resulting ontology. In IV the *IoT Security Evaluation Ontology* is introduced. In V conclusions are presented and a discussion on next steps is laid out.

II. State of the Art

In this section we present a state of the art of the ontologies related with security with special attention to those aimed at IoT. Some of the mentioned ontologies, as well as many ad-hoc ones, have been already used in application scenarios similar to those considered relevant in this work, such as *Smart Home*, *Smart Cities* and *Industry 4.0*. Finally some papers on the most relevant alternative approach to security are presented, and a conclusion.

A. Security as dimension of QoI

In the search for related scenarios of use of a context-based metric of security, we found a potential use case in the *CityPulse* platform [5], where they use security as a dimension of *Quality of Information (QoI)*, designing a mechanisms to annotate data streams with such metric. That metric is defined as a numerical vector:

$$Q = \langle L, P, E, B, Ava, C, Acc, S \rangle$$

In which the different dimensions stand for *latency, price, energy consumption, bandwidth consumption, availability, completeness, accuracy* and *security*, although it doesn't provide a model for evaluating the security, nor any contextual framework or ontology for defining security, nor any user-based context in which define interesting treats of security from the perspective of the user, to be used as a base for evaluating the security.

B. Security Ontologies

Many security ontologies have already been developed for different contexts. Following this paragraph, some are briefly listed, as they are of interest to some of the application domains of IoT, are directly based on IoT or are used as base for other ontologies of interest for this paper.

Naval Research Laboratory (NRL) Security Ontology for annotating resources [6] aggregates a set of related ontologies, inprooving them and making them extensible by redefining concepts for addedd expresiveness. It is focused in specific military technologies and certifications, and there are no publicly accessible *OWL* files (to the extent of our efforts on finding them), nor available entry in *Linked Open Vocabularies (LOV)*[3].

In [7], something similar is done in the context of the *ETSI M2M model*; they build a security knowledge base (ontology, dataset, rule) to help designers secure *M2M* applications during the design phase. The model is published[4] as the *STAC* ontology and dataset, and is later used as a base for, or linked into other ontologies.

In [8] the *IoT Security Ontology (IoTSec)* is presented, gathering and harmonizing several related ontologies (one of which is *STAC*). This ontology represents knowledge about security in the form of *Assets, Threats* and *SecurityMechanisms* among others, providing an extensible and ample data-set (or catalog of knowledge), as well an expressive semantic to represent the security related traits considered in this work.

In [9], *SecAOnto* is presented, an ontology that formalizes knowledge on *security assessment*, focusing on its aspects

[3]https://lov.linkeddata.es/dataset/lov

[4]http://securitytoolbox.appspot.com/stac

and particularities, addressing the relationship between *Information Security* and *Software Assessment*, built on top of *STAC*. It does offer a data-set, but it contains far less elements than *IoTSec*'s, and it is not specifically focused on the *IoT* scenario, having many concepts out of the scope of the field of interest for this paper.

C. A Different Approach: Trust

During the research phase on context-based security evaluation for this work, we came upon other approaches regarding this matter, being *trust* the most relevant based on the number of articles and attention obtained.

In [10] the *Trust Ontology*[5] is defined, focused on formally modeling trust structures as information sources and information dependencies.

In [11] a computational trust model that considers semantic relations among entities, and different trust categories, is proposed. It is used to calculate trust values about other entities and make decisions regarding the granting or denial of interactions.

D. Conclusion

Many previous works have targeted security as their source of interest, many ontologies have been developed to represent knowledge on different scenarios, such as *Smart Home*, *IoT*, *e-Health* and industrial scenarios. Different objectives were pursued, such as helping in the design phase of new systems, assess the security of a system, and dynamically manage the security of systems.

To the extent of our effort while creating this work, though, we have not found previous literature on the evaluation of security that accounts for different observers with concerns of their own but we did find evidence that supports the need for it.

III. Description of the Problem

In this section, we will briefly describe the extent of the problem about evaluating security based not only on the description of the different security traits of the elements that compose an IoT system, but also on the observer's context. In this case, the observer could be a final user, a service consumer, another device (*M2M*), a cataloging service or search engine, to name but a few.

The approach selected has been:

1) Establish the extent of the problem by performing a bibliographical research, finding related works on security ontologies for the different application scenarios typical in *IoT* as well as establishing a proper definition of *security* in this context.
2) After confirming the lack of an existing solution to the problem, we choose a methodology to approach it: the *NeOn methodology* [12]. By following it, we harmonize the conceptual knowledge of the security expectations of an observer, to the security trait descriptions offered by other existing ontologies.

The bibliographical review performed showed *IoTSec* ontology as a great candidate for representing the different elements and security traits that where revealed for the different scenarios that we focused on. It harmonizes other existing ontologies on security, providing a verbose, flexible and rich semantics for describing the context of security in *IoT* scenarios. Furthermore, it can easily be extended to accommodate new concepts of interest in prospective future works.

A. Perceived Security

Our focus with this work is to define an ontology by which to describe the different security preferences of an observer, based on concerns and interests on different security elements, such as threats, vulnerabilities, security mechanisms or features. Such descriptions, considered as the context of the observer, can later be used to perform a security evaluation that can, in turn, be used as a metric for different applications. In order to do so, we start by establishing a baseline, or definition, on what security is in the context of IoT. The definition of *Cyber Security*, for this work, based on the one provided by [13], could be summed up as the protection of the different involved systems, from disruption or misdirection from their *expected* functioning.

It is obvious then, that there can not be an evaluation of security without a context from the observer, in which the expected behavior of the the system is stated. Formally expressed, the security of a system is a function of the context of the system and the context of the observer:

$$S = f(D_{ctx}, U_{ctx})$$

Where the context of the observer represents those security traits of interest or valuable, and the context of the system represents the different aspects or elements of security intrinsic to the system under evaluation.

This greatly contrasts with traditional approaches to security assessment, in that, for the later, there is only one view to what is considered secure, that is; U_{ctx} is fixed, having as a result a simplified form:

$$S = f(D_{ctx})$$

In which only the context of the device is evaluated, that is, only the characteristics of the system are considered when generating an evaluation of security, not accounting for the expectations of different observers. This work changes that perspective, accounting for the diversity of scenarios in IoT where many different applications call for various security traits, and where traditional approaches are lacking.

[5] http://ontology.eil.utoronto.ca/trust.owl

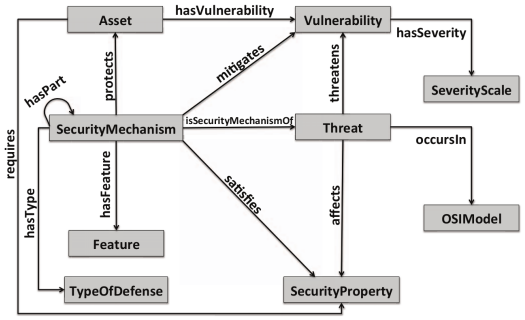

Figure 1. IoTSec diagram as depicted in [8]

B. Ontology for IoT Security (IoTSec)

In order to represent D_{ctx}, we will be using concepts represented in the *IoTSec* ontology, and U_{ctx} is, thus, going to refer to elements of it (see Figure:1) in the form of interests and concerns from an observer point of view, which are to be rated, bundled and associated to an evaluation algorithm or formula, according to the *IoT Security Evaluation Ontology* later described in IV.

IoTSec harmonizes concepts from other ontologies, defining itself as a Reference Ontology for IoT Security, and follows many of the common best practices for ontology sharing described in III-D.

C. NeOn Methodology

In order to develop our *IoT Security Evaluation Ontology*, we follow the guidelines offered by the *NeOn Methodology*, categorized in a set of scenarios. Among all of those described, the third scenario: *Reusing Ontological Resources*, best represented our case, establishing a process composed of 5 activities: *search, assessment, comparison, selection* and *integration* of ontologies, that guided our work.

D. Sharing

We have followed *Semantic Web* best practices [14] on ontology creation, metadata use [15] and sharing by referencing domain ontologies on the *LOV* and *LOV4IoT* [16] catalogue and semantic search engines. Our ontology was developed in *OWL DL* language, using the *Protègè* tool during design, validation and testing phases, facilitating it's sharing and later re-utilization in other ontologies and works.

IV. Context Based IoT Security Evaluation Ontology

In any of the frequent IoT scenarios present today in, security is a pervasive concern that must be addressed on a case by case basis. Expressing the interests and concerns of an observer regarding a set of IoT devices, offered in a way that is machine-readable, and decentralized-ready is of paramount importance for the successful application of IoT technology.

In this context, ontologies appear as a great resource for describing the knowledge about security, as well as the different preferences from an observer point of view, regarding the different characteristics, elements and traits of security, creating a common vocabulary and enhancing reuse and interoperability; both characteristics most relished in the IoT field.

Recent developments have been made on the integration of ontological metadata as a part of the information exchange, with the introduction of the *JSON-LD* extension to the popular JSON data format. Even further support to our work comes from the ETSI Industry Specification Group for Context Information Management (*ETSI ISG CIM*) that is taking efforts towards adding security as a property related to entities, information otherwise lacking in the original *NGSI-LD* standard, that itself uses *JSON-LD* as a data exchange format.

A. Modeling and integration process

The process of modeling the *Context Based IoT Security Evaluation Ontology* starts with the study on the previous work on security, security evaluation and ontologies related to both fields. From that study we extracted the best candidate for the representation of the security elements and traits for the IoT landscape. Following the *NeOn methodology* (see III-C) this represents the bulk of the 4 first steps of the *reusing scenario* guideline, followed in this work.

The next step was to explore the different keywords, terms and concepts used in the context of security evaluation from different observer's point of view, establishing a lexicon of the domain. This lead the design and building of the ontology, and it's later integration with the security ontology selected.

B. Ontology

From the thesaurus and glossary of terms built, we modeled the different concepts related to our ontology into 4 distinct classes: *Observer, Concern, Interest* and *Evaluator*, as well as a set of relations between those classes (*object properties* in OWL) and *data properties* describing data and values associated to the instances represented.

The result is the *Context Based Security Evaluation Ontology* represented in Figure: 2 in which classes from *IoTSec* ontology are represented in a light gray background.

1) Observer: An *Observer* could be anything from an end-user to an IoT device. It represents the entity which is interested in performing an evaluation of security for a system. As such, the observer has concerns about different threats and vulnerabilities that can impact it's intended interaction and use of the system. It can also have interests about certain security elements, that represent advantages or requirements specific to it's field. Finally, it has a preferred way of evaluating security, based on those interests and concerns, be it in the form of an algorithm, technique or

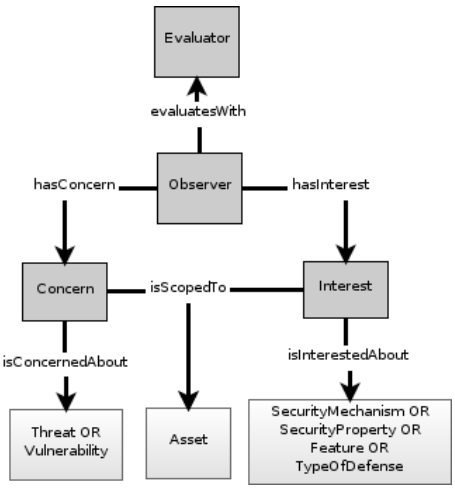

Figure 2. Context Based Security Evaluation Ontology

even a service. Distinct methods or algorithms for evaluating security could take into account lack of information, uncertainty or incorporate new information spontaneously.

2) Concern: Is an statement about a trait or element of security that represents a level of concern about vulnerabilities or threats, that can be limited to the scope of an specific *Asset* (or family of them) and has, as object of the concern, a *Vulnerability, Threat* or even an *OSIModel* layer.

Concerns can be valued according to the user preference, in a value range from 0 to 2, being 0 neutral, and 2 very concerned. Moreover, concerns can be linked to others in a "more than" relationship (and it's inverse: "less than") or in an equality relationship ("same as").

3) Interest: An *Interest* on some *SecurityMechanism, SecurityProperty, Feature* or *TypeOfDefense*. Again, just like concerns, interests can be scoped to an specific *Asset* (or family of them), although unlike them, the interest can have a positive or negative value. It represents the predisposition of an observer towards the usage of some technology or approach, regarding security, which could lean towards "like" or "dislike". This kind of statements serve the purpose to encapsulate higher level knowledge and concerns regarding concepts outside security, like power consumption, latency, technology alignment and so on.

In that sense, interest value is ranged in an scale from -2 to +2, conveying the meaning that a +2 means a strong interest on this *Security Mechanism*(s) and a -2 conveys a strong rejection, being 0 the neutral value.

4) Evaluator: An *Evaluator* represents the technology behind the actual evaluation computation. As such can be represented by an algorithm, methodology, process or service (to name but a few) that will actually carry the evaluation based on the Observer context. The motivation behind this concept is the representation of the different alternatives existent regarding how to compute the value

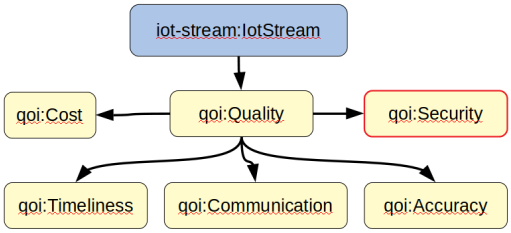

Figure 3. IoTCrawler ontology detail

representing the security level of the systems under test. This selection could impact how uncertainty or lack of information affect the computation, as well as how the final value is represented.

C. Groupings and Families

One difficulty we faced during the development of the ontology, was the representation of groups and families, e.g. all the assets of class *CloudTechnology*, or all of the threats categorized as *SensorAttack*s, to be used as values of object properties. Although *OWL FULL* allows the use of classes as values for object properties, *OWL DL* doesn't allow such expressions.

We followed the recommendations from the *W3C*, on their draft about "Representing Classes As Property Values on the Semantic Web"[6], for representing such element *families*. Among the options presented by the draft, we choose the second approach described, by creating special instances of the class, to be used as property values. One such example could be an instance called *CloudTechnologyFamily*, representing all of the assets belonging to the set of *CloudTechnology*.

D. Use Case: IoT Search Engine

One possible application of the ontology could be the evaluation of security as a parameter or dimension of *QoI* (quality of information). Such technology could be used, for instance, in the frame of the IoTCrawler project, where a context-based search engine for IoT is proposed. In this scenario, data consumers with different interests and concerns in security elements and traits, have a way to have their query results ranked by some combination of parameters on different aspects of quality of information, one of which is security, as can be seen in Figure 3.

In that regard, being able to evaluate security from a context-based standpoint in which the different interests and concerns of the observer are properly addressed, can be of great interest to the overall solution.

V. Conclusions and Future Work

In this paper we have presented an ontology for context based evaluation of security for IoT, that integrates knowledge on security of IoT devices represented according to

[6]https://www.w3.org/TR/2005/NOTE-swbp-classes-as-values-20050405/

concepts and information of the *IoTSec* ontology. It was developed following the *NeOn methodology* and some of the best practices recommended for sharing, referencing and re-using ontologies.

The evaluation of security based on the representation of the context of an observer, and described by *IoTSecEv* ontology, has proved to be an actual problem with immediate application in many fields of application of IoT, where security is a pervasive concern and the diversity of agents accessing information with varying expectations regarding security, makes traditional approaches unfeasible.

A use-case scenario of application of this technology has been presented, in the form of the evaluation of security as a dimension of quality of information, in the frame of the project *IoT Crawler*, that offers a IoT search engine capable of querying sources of information and to rank them according to several parameters, one of them the security. Our proposal is to evaluate that security based on the context of the observer (user or device performing the query) in contrast to traditional approaches based on a single definition of security.

Future work could include the extension of the IoTSec ontology by adding new devices (assets) as well as threats and vulnerabilites, representing (among others) physical threats to devices deployed in the field, as well as a pletora of IoT devices that are not already accounted for in the *IoTSec* ontology.

ACKNOWLEDGMENTS

This work has been sponsored by the European Commission through the *IoTCrawler* project (contract 779852), the *Torres Quevedo* program (grant TQ-15-08073). The authors would also like to thank colleagues from *University of Murcia* and *Odin Solutions* for their support during the development of this work.

REFERENCES

[1] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, 2012.

[2] FIWAREFoundationeV., "FIWARE Open Source Platform for the Smart Digital Future," 2018.

[3] M. Sporny, G. Kellogg, and M. Lanthaler, "JSON-LD 1.0 - A JSON-based Serialization for Linked Data," 2013.

[4] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of Security and Privacy Issues of Internet of Things," *International Journal of Advanced Networking Applications*, vol. 6, pp. 2372–2378, 2015.

[5] D. Puiu, P. Barnaghi, R. Tonjes, D. Kumper, M. I. Ali, A. Mileo, J. Xavier Parreira, M. Fischer, S. Kolozali, N. Farajidavar, F. Gao, T. Iggena, T. L. Pham, C. S. Nechifor, D. Puschmann, and J. Fernandes, "CityPulse: Large Scale Data Analytics Framework for Smart Cities," *IEEE Access*, 2016.

[6] A. Kim, J. Luo, and M. Kang, "Security Ontology for annotating resources," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3761 LNCS, pp. 1483–1499, 2005.

[7] A. Gyrard, C. Bonnet, and K. Boudaoud, "An Ontology-Based Approach for Helping to Secure the ETSI Machine-to-Machine Architecture," in *2014 IEEE International Conference on Internet of Things(iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom)*. IEEE, sep 2014, pp. 109–116. [Online]. Available: http://ieeexplore.ieee.org/document/7059650/

[8] B. A. Mozzaquatro, R. Jardim-Goncalves, and C. Agostinho, "Towards a reference ontology for security in the Internet of Things," *2015 IEEE International Workshop on Measurements and Networking, M and N 2015 - Proceedings*, pp. 117–122, 2015.

[9] F. de Franco Rosa, M. Jino, and R. Bonacin, "Towards an Ontology of Security Assessment: A Core Model Proposal," in *Advances in Intelligent Systems and Computing*, vol. 738, 2018, pp. 75–80.

[10] J. Huang and M. S. Fox, "An Ontology of Trust Formal Semantics and Transitivity," *8th International Conference on Electronic Commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, 2006.

[11] M. Taherian, R. Mili, and M. Amini, "PTO: A trust ontology for pervasive environments," *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, pp. 301–306, 2008.

[12] M. C. Suárez-Figueroa, A. Gómez-Pérez, and M. Fernández-López, "The neon methodology for ontology engineering," in *Ontology Engineering in a Networked World*, 2012.

[13] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security," *The Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, 2017. [Online]. Available: https://commons.erau.edu/jdfsl/vol12/iss2/8/

[14] A. Gyrard, M. Serrano, and G. A. Atemezing, "Semantic web methodologies, best practices and ontology engineering applied to Internet of Things," in *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, 2015.

[15] P.-Y. Vandenbussche and B. Vatant, "Metadata recommendations for linked open data vocabularies," *Version*, 2011.

[16] A. Gyrard, G. Atemezing, C. Bonnet, K. Boudaoud, and M. Serrano, "Reusing and unifying background knowledge for internet of things with LOV4IoT," in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 2016.