




# An OWL Multi-Dimensional Information Security Ontology

Ines Meriah<sup>1</sup><sup>a</sup>, Latifa Ben Arfa Rabai<sup>1</sup><sup>b</sup> and Ridha khedri<sup>2</sup><sup>c</sup>

<sup>1</sup> *Université de Tunis, Institut Supérieur de Gestion de Tunis, SMART Laboratory, Tunis, Tunisia*

<sup>2</sup> *Department of Computing and Software, McMaster University, Hamilton, Ontario, Canada*

**Keywords:** Information Security, Security Dimension, OWL Security Ontology, Multi-Dimensional Security Ontology, Dimensional View.


**Abstract:** To deal with problems related to Information Security (IS) and to support requirements activities and architectural design, a full conceptualisation of the IS domain is essential. Several works proposed IS ontologies capturing partial views of the IS domain. These ontologies suffer from incompleteness of concepts, lack of readability, portability, and dependability to a specific IS sub-domain. Following a rigorous and repeatable process, we systematically developed a comprehensive IS ontology. This process includes four steps: concept extraction, XML generation, OWL generation and dimensional view extraction. The obtained ontology is multidimensional, portable and supports ontology modularization. It is presented under XML format and OWL format. It comprises 2660 security concepts and 331 security dimensions.


## 1 INTRODUCTION AND MOTIVATION


The need for an ontology that outlines the domain knowledge related to information security is essential for several stages of software development. It can be used to support the requirements stage to improve traceability of non-functional requirements and elicitation and documentation of requirements. At the architecture design stage, it helps the designer put the necessary mechanisms to support non-function requirements. Particularly, when the non-function requirements that we are considering are those related to security, any supporting tool is extremely valuable. In this paper, we are concerned with the elicitation of an information security ontology that is modular and that support securing information systems in general.

The system' security aspect has a major effect in modern distributed software systems. For requirements management activities it is essential to answer questions about the dependencies among non-function requirements and particularly about security requirements. One also would wonder whether it is necessary to revise security in connection with changes in the functional requirements and wonder

about which project artefacts are affected by the change (Murtazina and Avdeenko, 2019). It is a traceability issue and ontologies could be of great help for requirements analysts in tackling this issue. Moreover, in IS domain, ontology presents security concepts and provides details about their relationships. An IS ontology is considered as a required container for the security of systems and their applications. According to (Sanagavarapu et al., 2021), an IS ontology facilitate threat intelligence, reasoning of attacks and anomaly detection. The ontological representation of IS domain helps in contextual readiness and awareness to defend a malicious attack and protect IT assets. Another perspective on the need for a security ontology at the requirements level is related to having a precise terminology to articulate security requirements. In a business environment, security and software stakeholders use existing IS ontologies to determine security risks and articulated the appropriate requirements for the countermeasures (Meriah et al., 2021). The security terminology should be efficiently organized in an IS ontology. Security concepts are extremely large in number, dynamic and evolving over the time. However, it is necessary to obtain comprehensible IS ontology to help resolve security problems and write the correct security requirements. Although there are several existing security machine learning models to identify security requirements and issues, most security stakeholders suffer from the lack

<sup>a</sup>  <https://orcid.org/0000-0002-8713-0216>

<sup>b</sup>  <https://orcid.org/0000-0002-5657-4682>

<sup>c</sup>  <https://orcid.org/0000-0003-2499-1040>

of readable view of IS domain (Meriah et al., 2021). This problem arises from the complexity of the field on the one hand, and the lack of effective communication and collaboration between stakeholders on the other hand. What aggravates further the issue is that security decision makers interpret IS terminology differently, which leads to misunderstanding among them when they assess threats or evaluate security risk scenarios (Pereira and Santos, 2012), (Martins et al., 2020). For example, the security terms of *attack*, *threat* and *risk* are confused and used as synonyms (Li and Chen, 2020). The challenge for requirements analysts is to remove ambiguities of IS concepts and become familiar with security terminology that is increasing and changing over the time (Elnagar et al., 2020).

Security concepts can be observed and regrouped regarding several dimensions (Jouini et al., 2021). Each dimension takes a specific manageable perspective on IS, where one can have a better understanding of the characteristics of concepts by accurately defining concepts with their features or attributes. For example, the security dimension of confidentiality represents the concept of *confidentiality* with its attributes such as *confidentiality impact*, *confidentially key* and *confidentiality mode*, and the security dimension of network represents the concept of *network* with its details like *network access*, *network file*, *network traffic* and *network defense*. In general, an ontological dimension is a component of the ontology that has a high level of cohesion between its concepts. The concepts of such component present a level of connectivity (through the relationships between them), which makes the component presents a sub-domain of the domain under consideration. Another way to consider the dimension in an ontology is to take as possible dimensions the concepts that are immediately connected to the root. For instance, in our case, the concepts *attack*, *threat*, or *risk* related to the root concept "Thing" (as shown in Figure 5) are possible dimensions that can give perspectives on the domain of IS. According to the design principle of low coupling and high cohesion, an ontology that exhibits high cohesion between its elements and low coupling with other components is deemed to be well designed. Decomposing ontologies into modules (i.e., sub-ontologies) using dimensions could be considered as an approach to ontology modularisation (LeClair et al., 2019; LeClair et al., 2022; LeClair et al., 2020). These dimensions help focus the attention of the requirement analyst to one aspect of the system security by eliciting the requirement from one aspect at the time. This paper proposes an IS ontology that has several dimensions and modules.

In this paper, we propose a multi-dimensional ontology of IS domain. The ontology is presented under an OWL format, in which several dimensional views can be extracted according to the user's security requirements and needs. The proposed ontology would support security stakeholders to use only the views that are relevant to their concerns, which reduces the burns of partially using a large ontology. Several software programs are used to support the generation of multi-dimensional IS ontology in OWL format. We used python for writing view extraction programs and *protégé* editor to visualise the obtained ontology in the form of dimensional views.

The paper is structured as follows: Section 2 presents related works. In this section, we describe existing IS ontologies, detail their structure in term of security concepts, and provide a critical analysis of them regarding security dimensions. Section 3 presents an overview of the systematic process of the multi-dimensional IS ontology generation. Section 4 gives an illustrative example of OWL ontology generation process and the dimensional views obtained. Section 5 compares the proposed ontology with three OWL IS ontologies. Section 6 presents the highlights of the proposed IS ontology and point to related future works.

## 2 RELATED WORK

Several IS ontologies have been presented in the literature. This section discusses the organization of security concepts under existing IS ontologies.

Herzog et al. (Herzog et al., 2007) propose the first OWL-based IS ontology for security researchers and professionals. The ontology models the basic concepts of security risk analysis namely *Asset*, *Threat*, *Countermeasure*, *Vulnerability*, *Security goal*, and *Defence strategy*. Each basic concept is hierarchically classified into specific sub concepts. In (Ramanuskaitė et al., 2013), a generic ontology based IS standards is developed to optimize the use of several standards in organization. The proposed ontology includes five classes: *Organization*, *Asset*, *Threat*, *Vulnerability* and *Countermeasure* (Meriah and Rabai, 2019). The standard mapping and the hierarchy structure of each class enable to provide details relevant to the high level IS cited concepts. In these ontologies, the authors consider only the organizational and risk assessment perspectives for modeling IS domain. We should consider other security aspects to provide a complete view of IS domain.

Other IS ontologies provide specific security aspects for modeling security knowledge. For example,

the OWL security ontology in (Solic et al., 2015) is used to estimate the level of system’s security. Thus, by considering the IS elements of *Network security*, *Software and hardware issues*, *Human influence*, *Security policy*, and *Disaster recovery plan*. These concepts model involved security issues in information systems. In addition, the ontology proposed in (Li and Chen, 2020) organizes the security requirement aspects of IS to four concepts *Asset*, *Security property*, *Countermeasure*, and *Security requirements*. The authors provide details of each security requirement concept using key words extracted from IS documents and standards. In fact, concepts in these ontologies are dependent to IS sub-domains as they are used to support IS models and frameworks.

In the literature, another category of IS ontologies are presented in the form of modules. Fenz and Ekelhart in (Fenz and Ekelhart, 2009) present a unified IS ontology to support security risk management in information systems. The proposed ontology is divided in three subontologies: Security, Enterprise, and Location. Security subontology includes four classes *Threat*, *Vulnerability*, *Attribute*, and *Rating*. Enterprise subontology includes three classes *Asset*, *Enterprise* and *Person* while the location subontology includes only the *Location* class. Souag et al. (Souag et al., 2015) present a core security ontology which model security requirement concepts with their relationships. The structure of the ontology is based on three dimensions: Organization, Risk, and Treatment. In (de Franco Rosa et al., 2018), an OWL ontology called Security Assessment Ontology (SecAOnto) is developed to describe security assessment aspects in organizations. The concepts are organized in three dimensions: System assessment, Information security, and Security assessment.

All the cited ontologies in this section provide an intuitive description of security dimensions and concepts without providing how the dimensional decomposition of their ontologies is established. In addition, we find that a clear ontological view of these dimensions is missed, which might affect the interpretation of the IS domain.

To the best of our knowledge, we lack a well defined systematic and/or automatic methodology to classify the ontology concepts into several IS specific aspects to generate multiple views regarding the final ontology user needs. Then, developing and proposing a multidimensional ontology to present dimensional views for most ontology concepts is undoubtedly needed by the IS ontology community.

### 3 THE PROPOSED OWL ONTOLOGY GENERATION PROCESS

To overcome the lack of a systematically generated multiple views of an IS ontology, we propose in this section a multi-dimensional ontology that contains domain concepts with their hierarchical relationships. The generation process of this ontology starts with online IS dictionary and leads to dimensional views generated from OWL ontology concepts. The dimensional views obtained provide an overview of the IS domain and help organizations to have details about particular IS concepts and identify their security needs and requirements. For example, from the OWL multi-dimensional ontology generated, ontology users can extract dimensional views such as *control*, *privacy*, and *authentication* dimensions. The generation process of OWL multi-dimensional IS ontology is fully automatic. As presented in Figure 1, it includes four steps:

1. Concept extraction: It is for the extraction of domain concepts from web dictionary.
2. XML generation: It leads to a hierarchical representation between concepts in the form of XML document.
3. OWL generation: It transforms the XML structure of the ontology into its corresponding OWL representation.
4. Dimensional view extraction: It supports the extraction of dimensional views relevant to a given concepts in OWL ontology.

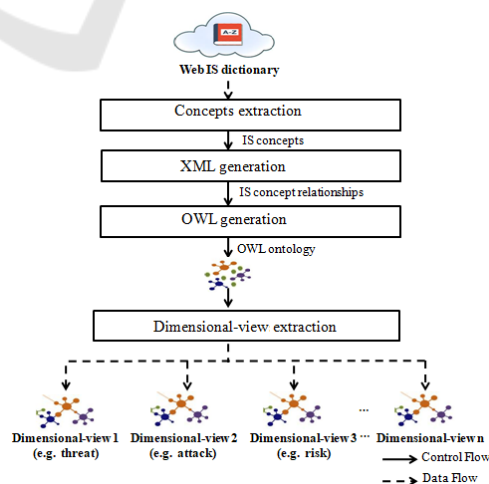


Figure 1: The proposed generation process of OWL Multi-dimensional IS ontology.

### 3.1 Concept Extraction

We have focused on online dictionaries presenting a large number of concepts in IS domain. Domain dictionaries provide to their users a well-defined vocabulary for searching and indexing. For constructing domain ontologies, dictionaries are often used to recognize domain concepts and identify such similarity between them (Harjito et al., 2018).

Domain concepts in dictionary are particularly noisy including an amount of useless information. Pre-processing tasks are necessary to exclude worthless symbols and obtain a cleaned space of concepts. To extract domain concepts, the classical tasks of pre-processing adapted in this stage consist of:

- Filtering useful domain concepts while excluding punctuation characters, special characters, numbers, abbreviations, and stop words.
- Removing some domain concepts that include adjectives or adverbs.
- Removing words with less than three characters.
- Converting the string-labels of the obtained concepts to lowercase.

In this first step that of concept extraction, we have used different Python libraries to identify required concepts. *BeautifulSoup* library is used to gather concepts from HTML pages while the *re* library is used to identify abbreviations. In other hand, we use NLP techniques like tokenization, POS and stop word removal to identify concept patterns. In fact, tokenization splits compound terms into a list of words called tokens. Then, POS is used to assign the corresponding POS tagging to each token. It consists of identifying the grammatical category of words such as noun (NN), verb (VB), adjective (JJ). Stop words removal is another method, which manages textual data and removes compound words including stop words (CC) (e.g., after, before, and, or).

### 3.2 XML Generation

A structural representation of domain concepts is required to capture concept relationships. In fact, XML is a simple and flexible data source which provides to their intended users a common syntax (Nguyen, 2011). In general, the structure of XML represents information in the form of tags to relieve the low semantics of HTML. Tags in XML can be represented as a structured tree giving a hierarchical representation of concepts (BRAY, 2000), (Nguyen, 2011). To generate an XML document in this second stage, two essential tasks are performed. The first is to map all extracted

concepts to XML Tags. The second is to provide concept hierarchies. As a result, we obtain concept relationships as structured tree regarding hierarchical levels. Table 1 shows concept patterns identified from the generated XML document and illustrates examples of IS concepts with their hierarchical levels. Concepts in level one present unique terms while concepts in level two and three present compound terms. We note that concepts in the second level of hierarchy include only two terms while concepts at the third level include at least three terms. We follow this structure to obtain concept relationships in the form of XML document.

Table 1: Identification of concept patterns from XML document.

Concept patterns	IS Concept examples	Depth
NN	computer	1
NN NN	computer security	2
NN NN NN	computer security incident	3
NN NN NN NN	access security log management	3

### 3.3 OWL Generation

To obtain the graphical representation of the ontology, it is needed to consider the XML document. Then, we generate the OWL file as XML structure. The obtained structure can be used for semantics and for reasoning. With only the XML format of concepts, it is difficult to do operations like classification, check consistency, selection, and comparison. Furthermore, to ensure the interoperability of concepts, after converting the XML to OWL ontology, we use the python library of *MinDom* for parsing XML as a tree and mapping its elements to OWL classes (dimensions) and OWL sub-classes (attributes). Hierarchical relationships in OWL ontology are the required components that reveal different security dimensions. In fact, RDF and RDFS support the understanding of the extracted information on the web. In our obtained OWL ontology, RDF operates the graphical representation of web resources using URI, while RDFS provides vocabulary specifying classes (i.e., *rdf: class*) on the hierarchical relationship between classes (i.e., *rdfs: subclassof*) (Bikakis et al., 2013), (Nguyen, 2011).

Figure 2 shows the corresponding OWL encoding of the class *computer* and the subclass *computer.abuse*. The OWL format of the complete IS ontology generated is available in (Meriah et al., 2023a).

### 3.4 Multi-Dimensional View Extraction

A view is a fragment of a target ontology, which is captured by ontology users (Lozano et al., 2014). A

```

<owl:Class
  rdf:about="http://www.semanticweb.org/user/ontologies/2021/5/
  untitled-ontology-45#computer"/>
<owl:Class
  rdf:about="http://www.semanticweb.org/user/ontologies/2021/5/
  untitled-ontology-45#computer_abuse">
  <rdfs:subClassOf
  rdf:resource="http://www.semanticweb.org/user/ontologies/2021/
  5/untitled-ontology-45#computer"/>
  </owl:Class>

```

Figure 2: Fragment of the OWL file generated showing the security dimension of *computer* with its attribute *computer\_abuse*.

dimensional view is considered as a portion of an existing domain ontology, which presents details related to a root ontology concept. The purpose of this stage consists of offering a well defined terminology regarding user security needs. As mentioned previously, the ontological representation helps ontology users easily querying and searching for particular concepts and details. Therefore, to extract dimensional view, three main tasks are performed:

1. Search the root concept by browsing OWL ontology.
2. Select the root concept, if it exists in the OWL ontology.
3. Visualize the dimensional view in which, all concepts that are reachable from the selected concept are involved.

In this final stage of our ontology generation process, we use the ontology implementation tool of *protégé* editor (Protégé, 2020). This tool provides an interactive graphical representation for a given OWL ontology and offers an API access to user knowledge bases.

The automatic generation of a sub-ontology based on words occurring after each other make security concepts related to each dimension readable, clear and precise. The proposed OWL multi-dimensional ontology is a means that help security stakeholders efficiently interpret security concepts. It is useful to define security dimensions and precise the relations among them.

## 4 A USAGE SCENARIO OF THE OWL ONTOLOGY GENERATION PROCESS

The following example illustrates the generation process of OWL multi-dimensional IS ontology and illustrates how users can exploit the obtained ontology to precisely decompose the three IS concepts *threat*, *attack*, and *risk*. Decision makers are often using these three terms for identifying, analysing, and evaluating their IS situation within the organization. The challenge for them is to remove ambiguities among these

terms in order to efficiently conduct risk assessment and make suitable IS decisions.

Attackers exploit system vulnerabilities to launch attack programs or multihost attacks that target computer resources in a progressive way (Meriah and Rabai, 2018). In organizations, the popular forms of attacks like phishing, malware and DoS/DDoS attacks make unauthorized access of information assets in order to use, steal or destroy sensitive data (Singhal and Ou, 2017; ISO Central Secretary, 2018). For example, DoS attack deactivates servers by gaining access to particular services from internet and making computer resources like disk space, processor and bandwidth unavailable. In addition, malicious attackers pose potential threats in information systems. In (Stoneburner et al., 2002), a threat refers to "a circumstance that cause damage to information system's assets". It can be an undertaken action performed by attacker or adversary to makes business losses. Significant threats that are commonly known include destruction, fraud, penetration, theft, disclosure, extortion, vandalism, and espionage.

In general, IS attacks and potential threats affect security objectives and make business prone to risk. According to (Jones and Ashenden, 2005), risk is an unexpected event that makes us at least losing one of the security requirements. As an initiative to address such risk, it is relevant to outline security threats in business environment and identify attacker's traces in a security context. In ISMS, a risk is defined as the effect of uncertainty on IS objectives (Alanen et al., 2022). It is considered as the potential of security threats to cause security breakdowns in an enterprise. The risk is measured by the likelihood and impact caused by attackers and IS threats. Therefore, modeling *threat*, *attack* and *risk* concepts as IS dimensions helps to improve their perceptions in IS domain and organizations.

We apply the OWL ontology generation process to *INFOSEC* dictionary (Center, 2022). This dictionary includes terminology changing in a continuous way and varying based on the IS sub-fields being considered. Related terms and definitions are mainly captured from IS security standards and guidelines like NIST Special Publications (SPs) and Federal Information Processing Standards (FIPS). We have considered IS concepts under the above dictionary (i.e., dictionary of (Center, 2022)) as it respects most of the requirements and hypothesis regarding the proposed ontology generation process.

In the first stage, we extract IS concepts regarding several tasks of pre-processing. In the second stage, we have offered a hierarchical representation between these IS concepts using XML document. The XML identifies the security dimensions as a root concepts

```

- <risk>
  <risk_analysis/>
  <risk_appetite/>
  + <risk_assessment/>
  <risk_assessor/>
  <risk_criteria/>
  <risk_evaluation/>
  <risk_factor/>
  <risk_framing/>
  <risk_identification/>
  + <risk_management/>
  <risk_mitigation/>
  <risk_model/>
  <risk_monitoring/>
  <risk_register/>
  + <risk_response/>
  <risk_tolerance/>
  <risk_treatment/>
</risk>

- <threat>
  <threat_actor/>
  <threat_analysis/>
  <threat_event/>
  <threat_information/>
  - <threat_intelligence>
    <threat_intelligence_report/>
  </threat_intelligence>
  <threat_monitoring/>
  <threat_scenario/>
  <threat_shifting/>
  <threat_source/>
</threat>

- <attack>
  <attack_signature/>
  <attack_surface/>
  <attack_tree/>
</attack>

```

Figure 3: Screenshot of *attack*, *threat* and *risk* dimensions in XML file.

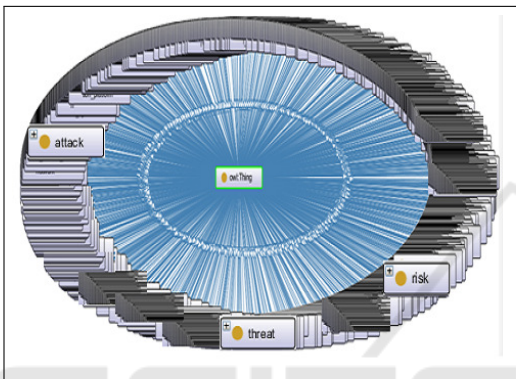


Figure 4: OWL IS Ontology generated.

organized with their features called attributes. In Figure 3, we present screenshots from XML document generated. The screenshots show the risk dimension with 17 attributes, the threat dimension with 7 attributes and the attack dimension with 3 attributes. To visualize the ontology, the XML structure of IS concepts is mapped to OWL ontology. As shown in Figure 4, ontology dimensions are fuzzy, ambiguous and unreadable due to the huge amounts of the stored concepts. Therefore, IS dimensions still difficult to read and interpret. To solve this problem, it is required to present *attack*, *threat*, and *risk* concepts as a dimensional views in order to perceive them correctly within information systems.

At the end of the ontology generation process, we have specified and visualized security concepts view by view. First, we have searched the required dimension by browsing the ontology itself. Second, we have selected the dimension in OWL ontology and finally we have displayed the view using OntoGraph plugin from *protégé* editor. Figure 5 shows *attack*, *threat*, and *risk* dimensional views. Attack view is represented with red box. Threat view is represented with blue box and risk view is represented by orange box. The low number of attributes of attack dimension is an indication about its limited perception in the IS

domain. In other hand, the high number of attributes of threat and risk dimensions is an indication of their wide scope in the domain. We note that all the concepts that are reachable from threat dimension are involved in threat dimensional view.

## 5 EVALUATION OF THE PROPOSED ONTOLOGY

In this section, we evaluate the proposed multi-dimensional ontology by comparing it with the most known and available OWL IS ontologies for the related community. We have focused on the importance of the multi-dimensional ontology obtained in terms of concepts, attributes and dimensions using a qualitative analysis. In fact, three OWL IS ontologies were selected for the ontological analysis: Herzog et al. ontology (Herzog et al., 2007), Fenz et al. ontology (Fenz and Ekelhart, 2009) and De Franco et al. ontology (de Franco Rosa et al., 2018). In Herzog et al. ontology (Herzog et al., 2007), concepts are derived from security databases and cryptographic models related to IS risk analysis and access control sub-domains. In other hand, the structure of Fenz et al ontology (Fenz and Ekelhart, 2009) highlights the relationships among top-level security concepts to ensure security compliance and IS risk management in organization. Most relevant concepts in Fenz et al. ontology are obtained from IT Grundschatz Manual, the french EBIOS and ISO/IEC 27001 standards. For modeling IS assessment sub-domain, SecAOnto ontology in (de Franco Rosa et al., 2018) presents terms from existing security taxonomies, ontologies and guidelines. Although the presented ontologies define an extensive list of security concepts, they still fragile as they highly dependent on specific IS sub-fields like access control, risk assessment and risk management. None of them covers a large number of IS sub-domains. It can be noticed that the ontology generated provides a major coverage of IS area because it incorporates concepts extracted from security dictionary (CSRC dictionary). Following the proposed process of ontology generation, the multi-dimensional ontology can update and interrelate their security terms in a continuous way. Thus, it enables ontology users to generate specific ontologies relevant to IS sub-fields. For instance, we can derive the security dimensions of threat, asset, vulnerability and control and then represent relevant details to IS risk management sub-domain. The main ontology elements considered for comparing ontologies are: the number of concepts, the number of attributes and the total number of security dimensions providing hierarchical

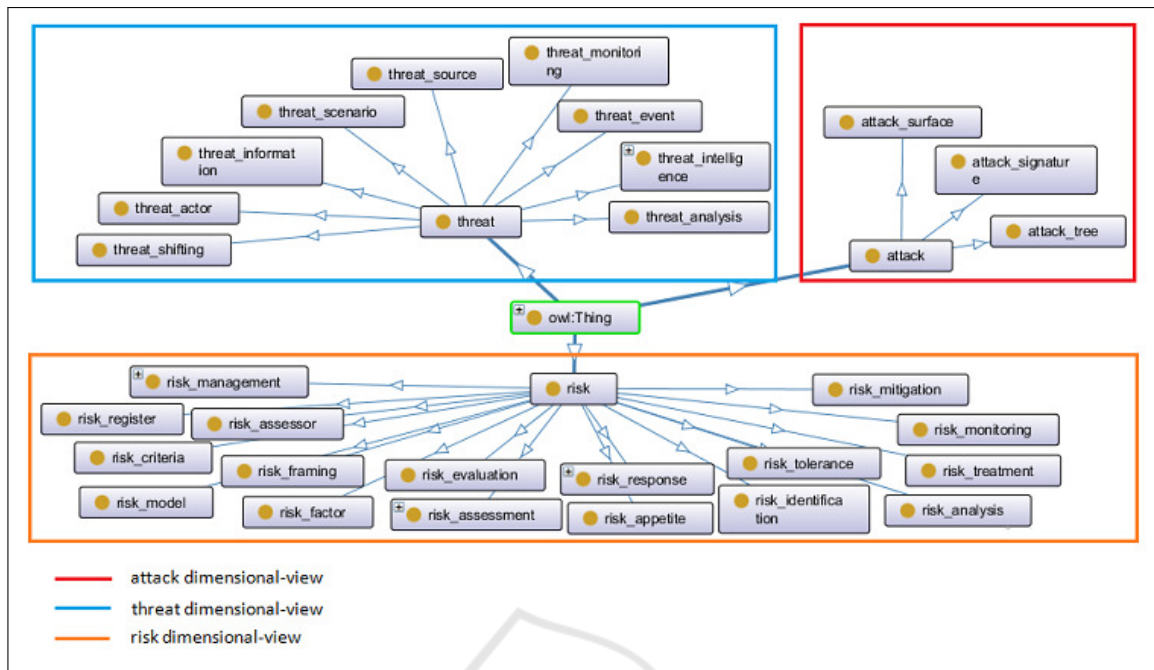


Figure 5: The dimensional views of *attack*, *threat*, and *risk*.

relationships. *protégé* editor metrics have been used to obtain quantitative data of these ontology elements.

Table 2: Data of comparison results of OWL IS ontologies.

OWL IS ontology elements			
References	Concepts	Attributes	Dimensions
(Herzog et al., 2007)	460	752	-
(Fenz and Ekelhart, 2009)	641	1051	3
(de Franco Rosa et al., 2018)	157	167	3
Proposed ontology	2660	1613	331

Table 2 compares the number of concepts, attributes and dimensions for each cited ontology and the proposed one. As results, De Franco et al. ontology has the least number of concepts, while the proposed multi-dimensional ontology has the largest number of security concepts and attributes. Regarding the dimensional aspect in these ontologies, the security dimensions are very low in Fenz et al. and De Franco et al. ontologies, while the proposed OWL ontology provides 331 security dimensions as sub-ontologies. Each security dimension precises generic security concept with its attributes. In fact, the dimensional aspect in ontology helps interpreting terminologies and domain concepts. In general, security dimensions make readable, shared and reusable the generic concepts like *threat*, *risk* and *control*.

Furthermore, dimensions in the proposed OWL IS ontology are used to remove ambiguities of security concepts. Their main purpose is to specify security concepts in an organized and detailed way.

## 6 CONCLUSIONS AND FUTURE WORKS

This paper proposes an OWL multi-dimensional IS ontology. The proposed ontology is comprehensive and extendable as it can be further enriched with concepts from IS corpuses. The overall ontology shows the ontological links between the dimensions of IS, which gives IS stakeholders an idea about the dependencies among the dimensions and their criticality on the security.

Following a rigorous and repeatable process that is discussed in Section 3, we developed an ontology covering the IS domain. This ontology is easily decomposable into modules each presenting a security dimension and providing a security perspective. The ontology is available at (Meriah et al., 2023b) under an XML format and at (Meriah et al., 2023a) under an OWL format. The process used in obtaining the proposed ontology can be applied to get ontologies in other natural languages. For instance, for an ontology in French one starts from a French dictionary for security and uses similar Python scripts as the ones we used (after adapting them to the specifics of the language) to extract the concepts and their relationships. Using the notion of ontology dimensions, we can decompose the proposed IS ontology into several modules. This modularization is essential when we want to focus on specific security concerns such

as management, risk, or threats. In (LeClair et al., 2019; LeClair et al., 2020), we find several ontology modularization techniques. The dimensionalities introduced in this paper could play a significant role in support of methods such as the view traversal modularization technique. ontology metrics of *protégé* editor are considered. Our future work aims at exploring further enrichment of the current ontologies with concepts and relationship extracted from other sources such as ISO standards, wiki-data, and several other corpuses. Our objective is to have the most current and complete IS ontology.

We plan to use other ontology evaluation metrics like precision, recall and f-measure to more evaluate the performance of our ontology generation approach. Furthermore, we aim to use the proposed ontology combined with DIS formalism (Marinache et al., 2021) in analysing security-log data to learn about the security situation surrounding the system under consideration.

## ACKNOWLEDGMENT

This study was funded by Natural Sciences and Engineering Research Council of Canada –NSERC– (CA) (RGPIN-2020-06859).

## REFERENCES

- Alanen, J., Linnoosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., and Tiusanen, R. (2022). Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (sta) method for industrial control systems. *Reliability Engineering & System Safety*, 220:108270.
- Bikakis, N., Tsinaraki, C., Gioldasis, N., Stavrakantonakis, I., and Christodoulakis, S. (2013). The xml and semantic web worlds: technologies, interoperability and integration: a survey of the state of the art. In *Semantic hyper/multimedia adaptation*, pages 319–360. Springer.
- BRAY, T. (2000). Extensible markup language (xml) 1.0 , w3c rec-xml. <http://www.w3.org/TR/REC-xml/>.
- Center, C. S. R. (2022). Glossary. <https://csrc.nist.gov/glossary/>.
- de Franco Rosa, F., Jino, M., and Bonacin, R. (2018). Towards an ontology of security assessment: A core model proposal. In *Information Technology-New Generations*, pages 75–80. Springer.
- Elnagar, S., Yoon, V., and Thomas, M. (2020). An automatic ontology generation framework with an organizational perspective. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.
- Fenz, S. and Ekelhart, A. (2009). Formalizing information security knowledge. In *Proceedings of the 4th international Symposium on information, Computer, and Communications Security*, pages 183–194.
- Harjito, B., Cahyani, D. E., and Doewes, A. (2018). An automatic approach for bilingual tuberculosis ontology based on ontology design patterns (odps). *TELKOMNIKA Telecommunication Computing Electronics and Control*, 16(1):282–289.
- Herzog, A., Shahmehri, N., and Duma, C. (2007). An ontology of information security. *International Journal of Information Security and Privacy (IJISP)*, 1(4):1–23.
- ISO Central Secretary (2018). Information technology — security techniques — information security management systems — overview and vocabulary. Standard ISO/IEC 27000:2018, ISO, Geneva, CH.
- Jones, A. and Ashenden, D. (2005). *Risk management for computer security: Protecting your network and information assets*. Elsevier.
- Jouini, M., Ben Arfa Rabai, L., and Khedri, R. (2021). A quantitative assessment of security risks based on a multifaceted classification approach. *International Journal of Information Security*, 20(4):493–510.
- LeClair, A., Khedri, R., and Marinache, A. (2019). Toward measuring knowledge loss due to ontology modularization. In Dietz, J., Aveiro, D., and Filipe, J., editors, *In Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2019)*, volume 2 of *IC3K*, pages 174–184, Vienna, Austria. SCITEPRESS Science and Technology Publications, Lda.
- LeClair, A., Khedri, R., and Marinache, A. (2020). Formalizing graphical modularization approaches for ontologies and the knowledge loss. In *Knowledge Discovery, Knowledge Engineering and Knowledge Management*, volume 1297 of *Communications in Computer and Information Science series*, chapter 18, pages 1–25. Springer.
- LeClair, A., Marinache, A., Ghalayini, H. E., MacCaull, W., and Khedri, R. (2022). A review on ontology modularization techniques - a multi-dimensional perspective. *Transactions on Knowledge and Data Engineering*, pages 1–28.
- Li, T. and Chen, Z. (2020). An ontology-based learning approach for automatically classifying security requirements. *Journal of Systems and Software*, page 110566.
- Lozano, J., Carbonera, J., Abel, M., and Pimenta, M. (2014). Ontology view extraction: an approach based on ontological meta-properties. In *26th International Conference on Tools with Artificial Intelligence*, pages 122–129. IEEE.
- Marinache, A., Khedri, R., Leclair, A., and MacCaull, W. (2021). DIS: A data-centred knowledge representation formalism. In *IEEE International Conference on Reconciling Data Analytics, Automation, Privacy, and Security (RDAAPS)*, pages 1–8, Hamilton, Ontario, Canada. IEEE Computer Society.
- Martins, B. F., Serrano, L., Reyes, J. F., Panach, J. I., Pastor, O., and Rochwerger, B. (2020). Conceptual characterization of cybersecurity ontologies. In *IFIP Working*



- Conference on The Practice of Enterprise Modeling*, pages 323–338. Springer.
- Meriah, I. and Rabai, L. B. A. (2018). A survey of quantitative security risk analysis models for computer systems. In *Proceedings of the 2nd International Conference on Advances in Artificial Intelligence*, pages 36–40.
- Meriah, I. and Rabai, L. B. A. (2019). Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science*, 160:85–92.
- Meriah, I., Rabai, L. B. A., and Khedri, R. (2021). Towards an automatic approach to the design of a generic ontology for information security. In *2021 Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS)*, pages 1–8. IEEE.
- Meriah, I., Rabai, L. B. A., and Khedri, R. (2023a). Multi-dimensional Information Security Ontology. [https://github.com/inesmeriah/Multi-dimensional-Information-Security-Ontology/blob/main/owl\\_Ontology.owl](https://github.com/inesmeriah/Multi-dimensional-Information-Security-Ontology/blob/main/owl_Ontology.owl).
- Meriah, I., Rabai, L. B. A., and Khedri, R. (2023b). Multi-dimensional Information Security Ontology. [https://github.com/inesmeriah/Multi-dimensional-Information-Security-Ontology/blob/main/xml\\_Ontology.xml](https://github.com/inesmeriah/Multi-dimensional-Information-Security-Ontology/blob/main/xml_Ontology.xml).
- Murtazina, M. and Avdeenko, T. (2019). An ontology-based approach to support for requirements traceability in agile development. *Procedia Computer Science*, 150:628–635. Proceedings of the 13th International Symposium “Intelligent Systems 2018” (INTELS’18), 22-24 October, 2018, St. Petersburg, Russia.
- Nguyen, V. (2011). Ontologies and information systems: a literature survey.
- Pereira, T. and Santos, H. (2012). An ontological approach to information security management. In *7th International Conference on Information Warfare and Security*. Seattle. University Washington, pages 368–375.
- Protégé (2016 (accessed January 5, 2020)). *A free, open-source ontology editor and framework for building intelligent systems*. <https://protege.stanford.edu/>.
- Ramauskaitė, S., Olifer, D., Goranin, N., and Čenys, A. (2013). Security ontology for adaptive mapping of security standards. *International Journal of Computers, Communications & Control (IJCCC)*, 8(6):813–825.
- Sanagavarapu, L. M., Iyer, V., and Reddy, Y. R. (2021). Ontoenricher: a deep learning approach for ontology enrichment from unstructured text. *arXiv preprint arXiv:2102.04081*.
- Singhal, A. and Ou, X. (2017). Security risk analysis of enterprise networks using probabilistic attack graphs. In *Network Security Metrics*, pages 53–73. Springer.
- Solic, K., Ocevcic, H., and Golub, M. (2015). The information systems’ security level assessment model based on an ontology and evidential reasoning approach. *Computers & security*, 55:100–112.
- Souag, A., Salinesi, C., Mazo, R., and Comyn-Wattiau, I. (2015). A security ontology for security requirements elicitation. In *International symposium on engineering secure software and systems*, pages 157–177. Springer.
- Stoneburner, G., Goguen, A., Feringa, A., et al. (2002). Risk management guide for information technology systems. *Nist special publication*, 800(30):800–30.