

Towards an Ontology for Enterprise Level Information Security Policy Analysis

Debashis Mandal¹^a and Chandan Mazumdar²^b

¹Centre for Distributed Computing, Department of CSE, Jadavpur University, Kolkata, India

²Department of CSE, Jadavpur University, Kolkata, India

Keywords: Information Security, Ontology, Security Policy, Policy Analysis.

Abstract: Securing the information and ICT assets in an enterprise is a vital as well as a challenging task because of the increase in cyber-attacks. Information Security policies are designed for an enterprise to prevent security breaches. An enterprise needs to adhere to and abide by the policies for its disciplined functioning. Analysis of the policies is necessary to find their applicability, conflict detection, revision and compliance checking for the enterprise. To analyze the policies, it is necessary to decompose them into its constituent parts. This decomposition is facilitated by ontologies. An in-depth analysis of the policy decomposition show that the published information security ontologies are grossly inadequate for any policy analysis application. In this paper we present an approach for development of an ontology specifically for information security policy analysis. The structure of the ontology and its implementation are presented and the importance of this ontology in information security policy analysis is established.


1 INTRODUCTION


Information security policies are important to any enterprise. These are designed to help enterprises protect their information and assets from unauthorized access or usage. These policies are expressed in sufficiently high level natural language. The enterprises mandate their stakeholders to abide by the policies to assure that information security is preserved. There may be changes in the security policies due to various reasons, e.g., introduction of “Work-from-Home”. The security policies designed for an enterprise needs to be analyzed to ensure their applicability to the enterprise. A policy can be decomposed into its constituent parts to satisfy different analysis goals. Goals of policy analysis include finding their applicability, conflict detection, revision and compliance checking for the enterprise. Ontologies facilitate this decomposition because of their capability to represent the knowledge of a domain by identifying various concepts and their relationships in that domain. An ontology to be used for enterprise information security policy analysis should represent knowledge in the domains of

enterprise assets, action, space, time and cyber space in addition to core information security.

The existing information security ontologies published in the literature (referred in Section 2) are developed for accomplishment of various tasks including information security management, security modelling, security requirements elicitation, network security attacks, cyber forensics etc. But none of them address the concerns of information security policy analysis tasks requiring the knowledge of the related domains as indicated above. In this paper, a methodology for development of Information Security Ontology for analyzing security policies has been discussed, which also considers and includes knowledge from the domains of enterprise assets, action, space, time and cyber space.

Rest of the paper is organized as follows: Section 2 contains the related work followed by details on information security policy analysis and its challenges in section 3. In section 4 we discuss about information security ontology. In section 5, we detail the structure of our proposed ontology. In section 6 we have discussed about the approach of our work and section 7 contains the implementation details. In

^a <https://orcid.org/0000-0003-3203-876X>

^b <https://orcid.org/0000-0002-4252-8861>

section 8 we present a number of applications of the proposed ontology and conclude in section 9 along with some discussions on the future direction of work.

2 RELATED WORK

The common goal for developing ontologies is sharing common understanding of the structure of information among people or software agents (Musen, 1992, Gruber, 1993). Analyzing domain knowledge, separating the domain knowledge from operational knowledge, re-use of an existing generic ontology are also some of the goals of defining or using an ontology (Noy & McGuinness, 2001).

There are surveys (Cristani & Cuel, 2005), where the authors compare different ontology development and learning methodologies. Single ontology approaches, multiple ontology approaches and hybrid ontology approaches are the three different ways of employing an ontology in integration of content explication, used for explicit description of the information source semantics as identified in (Wache et al., 2001). In (LeClair, Khedri and Marinache, 2019), the authors formalize the graphical modularization technique, View Traversal, address the issues related to an evolving domain enriched with data and numerous autonomous agents. The authors use Domain Information Systems (DIS) instead of the Description Logic (DL) to represent ontology based systems in their work.

In (Basile, Liroy, Scozzi&Vallini, 2010), the authors present an approach called Ontology-Based Policy Translator (OPoT) which uses the ontology-based reasoning to refine policies into configuration for the actual controls. In (Evesti, Savola, Ovaska & Kuusijärvi, 2011), the authors present an ontology for information security measurement by combining a measurement ontology and an Information security ontology. In (Souag, Salinesi, Mazo & Comyn-Wattiau, 2015), the authors developed a security ontology for elicitation of security requirements, where the main objective of the ontology was to provide a generic platform containing knowledge about the core concepts related to security. In (Uzbek et al., 2004) KAOs, the authors have used description logic and ontology for policy representation which differentiates between positive and negative authorizations and positive and negative obligations. In (Tsoumas & Gritzalis, 2006), the authors implemented a security ontology related to risk assessment and demonstrated that extraction of security information is feasible from high level statements. In (Oltamari, Cranor, Walls &

McDaniel, 2014), the authors build upon existing ontologies and outline the structure of "CRATELO", a three level ontology for the Cyber Security Research Alliance program funded by the Army Research Laboratory (ARL). CRATELO is an ontological framework composed of OSCO, DOLCE and SECCO ontologies and currently includes 223 classes and 131 relationships (161 object properties and 15 datatype properties) encoded in OWL-DL. In (Obrst, Chase & Markeloff, 2012), Obrst et al explain the process to be followed in developing a cybersecurity ontology and catalog the sources upon which it is based. They discuss the foundational ontologies for the cyber ontology which include utility ontologies of Persons, Time, Geospatial Ontologies, Events and situations ontologies and network operations ontologies.

In (Bermejo-Alonso, 2018), the authors classify the existing task and planning ontologies and describe the different stages followed in ontological engineering of a planning ontology. (Altarish, 2012) presents a comparison of five ontology editors namely Apollo, OntoStudio, Protégé, Swoop and TopBraid Composer. Ontology The three types of ontology reasoner attributes categorized by Dentlar et al in (Dentler, Cornet, ten Teije & de Keizer, 2011) are reasoning characteristics, Practical usability characteristics and Performance indicators. For developing an ontology, various ontology languages exist such as XML, RDF, RDFs, OWL, DAML etc. ("Policy Analysis", 2020).

From the above study of related works, it is found that there is no published ontology which also consists of the domain knowledge of enterprise assets, action, space, time and cyber space. High level information security policies have some specific constituents and encompass different aspects of space and time. As such policy analysis requires composition of various ontologies as well as special treatment of the action imperatives in the policies. Also, the identification of the non-taxonomic relations for security policy analysis pose challenges. In this paper this research gap has been addressed.

3 INFORMATION SECURITY POLICY ANALYSIS

The overall objective of information security is the preservation of the confidentiality, integrity and availability of information and information resources (Peltier, 2004). It is the responsibility of the information security professionals to implement

policies that reflect the business and mission needs of an enterprise.

3.1 Information Security Policies

A policy is a statement of intent, and is implemented as a procedure or protocol. A policy can be defined as (Peltier, n.d.):

“A high-level statement of enterprise beliefs, goals and objectives, and the general means for their attainment for a specified subject area. A policy should be brief (which is highly recommended) and set at a high level.”

Policies can be either a closed policy or an open policy. Policies can also be classified as Permission policies, Prohibition policies and Obligation policies (Von Wright, 1951). In (Alotaibi, Furnell & Clarke, 2016), the basic types of policy constraints specified are: subject/target state, action/event parameters and time constraints, which limit the applicability of a policy.

An information security policy is a definition of what it means to be secure for information or information resources. The ISO 27002:2013 standard defines the objective of an Information Security policy as:

“to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations”.

Example of an information security policy is:

All workstations must use organization approved antivirus and antimalware software which must be updated automatically at regular intervals.

Information security policies are designed to enable enterprises handle their information in an organized manner and prevent them from being leaked through security breaches that may take place due to various reasons. As such, the policies contain the meta actions like permit, prohibit or obligate; the action to be qualified by the meta actions; the agent, object, instruments, recipient, beneficiaries of the action (usually these are from the assets of the enterprise); the temporal constraints; the geospatial and cyberspace constraints. These are specified in sufficiently high level terminologies so that they can encompass the existing and upcoming entities in an enterprise.

3.2 Policy Analysis

Analysis is the process of breaking a complex topic into its constituent parts in order to gain a better understanding of it. Policy analysis is the process of determining which of various policies will achieve a

given set of goals in light of the relations between the policies and the goals. The areas of interest and the purpose of analysis determine what types of analysis are conducted.

In the points that follow, we have summarized the types of policy analysis:

1. **Applicability:** The policies must be analyzed to see if they are applicable to the enterprise ground situation.
2. **Conflict Detection & Removal:** Here, the goal of analysis is to look for and remove any conflict arising between two or more policies applicable to the same enterprise to ensure the correctness of their implementation.
3. **Revision Requirement:** Analysis is required for revision at regular intervals or due to changes in the enterprise and/or regulations.
4. **To formulate guidelines, controls and procedures:** Analysis of policies is also necessary while formulation of security guidelines, controls and procedures for an enterprise.
5. **Compliance checking:** Policy analysis aids in checking compliance of the events happening and actions taken in an enterprise.
6. **Determine time and location constraints:** Analyzing a policy is also necessary in order to determine the time constraints (e.g. during office hours) and proper physical and cyber location constraints (e.g. particular campus or IP address) which the policy should be complied with. This factor has a deep impact on the current scenario, when “work-from-home” practice is being adopted at huge scales and hence new physical and cyber constraints are emerging.

3.3 Challenges in Policy Analysis

The high level abstract nature of the policies lends themselves to remain unchanged for a reasonable period of time. In many cases, there are specific extensions of the policies for various groups of users, assets and sites. The same policy may use different terminologies for the same entity or action for different enterprises.

Though the language of a policy may be of a very high level, the analysis is to be done in the context of the enterprise. This means the analyst must take into account the various components of the actual enterprise: its assets, people, technology and processes. Thus each of the high level constituent parts of the policy has to be mapped with one or a

group of actual entities of the enterprise. For a large enterprise, this poses substantial challenge for manual analysis. For a small to medium enterprise, in order to execute automatic analysis, the challenge is to map the high level concepts in the policies to the ground level entities in the enterprise.

This is where an appropriate ontology will be of help. In the following section, Information Security Ontology is introduced.

4 INFORMATION SECURITY ONTOLOGY

Ontologies are structures particularly appropriate for representing both knowledge and information about a problem or domain in different abstraction levels thus allowing its reuse and easy extension (Gruber, 1995). Ontologies typically consists of two components: (a) Names for important concepts in the domain, and (b) Background knowledge or constraints on the domain. Ontologies can be represented using first order logic, description logic, deontic logic, etc.

Ontology is defined as tuple in (Girardi, 2010) as follows:

$$O = (C, H, R, P, I, A) \quad (1)$$

where,

- C is a set of entities of the ontology; and is the union of CC (set of classes or concepts) and CI (set of instances).
- H is a set of taxonomic relationships between concepts
- R is a set of non-taxonomic ontology relationships
- P is a set of properties of ontology entities
- I is a set of instance relationships related to CC, CI, P and R
- A is a set of axioms expressing various kinds of constraints on concepts.

According to (Guarino, 1998), ontologies are classified into a hierarchy according to their level of dependence on a particular task as follows:

Top Level Ontology: Describes general concepts like space, time, matter, event, action etc. that are independent of a particular domain.

Task Ontology & Domain Ontology: Specializes the terms introduced in top level ontology to describe the vocabulary related to a generic domain or a generic task.

Application Ontology: Specialization of both the domain and task ontologies and correspond to the roles played by the domain entities while carrying out an activity.

Non-taxonomic relationships are classified as domain dependent or domain independent. Domain independent relationships are of two types: ownership and aggregation. Domain dependent relationships are expressed by particular terms of an area of interest (Girardi, 2010).

An information security ontology can be defined as a model of information security domain knowledge representation including the relevant concepts and relations. In (Fenz & Ekelhart, 2009), the authors developed an information security ontology with an objective to provide a knowledge model of the information security domain consisting of the most relevant information security concepts of threats, vulnerabilities, assets and controls. They have concentrated on supporting the information security risk management domain where the concepts are linked by relations. In (Herzog, Shahmehri & Duma, 2007), the authors present an information security ontology that builds upon the classic components of risk analysis – assets, vulnerabilities, threats and countermeasures. It provides a generic overview of the information security domain, contains a detailed vocabulary and supports machine reasoning. In (Do Amaral, Bazilio, Hamazaki Da Silva, Rademaker & Haeusler, 2006), the authors use a natural language processing based approach to come up with an ontology for information security which provides a vocabulary for information security domain and stores logical forms of statements in the text and set of axioms used for inference in description logic.

5 STRUCTURE OF THE PROPOSED ONTOLOGY

In this paper our interest is to develop an ontology for Enterprise Information Security Policy Analysis, which determines the Application to support. Obviously, the target Ontology should express the concepts involved in Enterprise, Information Security and actions and meta actions in the policies. We have linked the below-mentioned ontologies to be used for our purpose of information security policy analysis. The need for doing this arises from the fact that we intend to come up with a single ontology satisfying all the pre-requisites of performing a policy analysis and thus aiding in addition, removal or modification of new or existing policies of the enterprise and their constraints and detecting any conflicts arising thereby.

Thus, the target ontology will be a combination of the following separate ontologies:

Enterprise Ontology: An ontology describing the concepts and relations of enterprise assets – hardware, software, network, personnel, site, and organizational structure.

Information Security Ontology: This describes the concepts of various information security terms, their properties and relations.

Policy Actions Ontology: Consists of the actions and meta actions along with their synonyms and relations used in the Information Security policies.

Geospatial & Cyberspace Ontology: Concepts related to the location, boundaries, sites, etc. and their interrelationships. (Ressler, Dean & Kolas, 2010) presents a survey of the available geospatial ontologies.

Time Ontology: Expresses the date, timestamps, time intervals and the relevant relationships. Various theories of the structures of time have been proposed (Hayes, 1996).

The information security ontology is a hierarchy of concepts relevant to information security and enterprise assets. We have used the already available taxonomic relations and the derived non-taxonomic relations (from the action ontology) to link all the ontologies mentioned above. The linked ontology is instantiated with the enterprise asset information of any particular enterprise. After complete instantiation, the ontology contains individuals at the lowest level.

6 OUR APPROACH

In our work, we have come up with an ontology which is a combination of the above-mentioned ontologies that are developed using new relevant concepts and sub-concepts, as well as reusing some existing concepts from other ontologies thus preserving the common goal of developing an ontology. All the ontologies are linked to one another in the sense that one concept of an ontology is related to a concept of another ontology. This is accomplished using a non-taxonomic relationship derived from the policy actions ontology. We have used our ontology to analyze the information security policies of an enterprise. We have observed that using our proposed ontology, a wide range of security policies can be analysed for a large enterprise with considerably huge number of assets, employees and network connections.

The information security ontology consists of information security related terms and concepts and the enterprise ontology consists of information about the assets of an enterprise including its employee

information as well as network connectivity information. They are arranged hierarchically in the form of concepts and sub-concepts. The time ontology is a similar hierarchical representation of concepts related to the time-domain. Similarly, the cyberspace ontology and the geospatial ontology are hierarchical representations of geo-locations and cyber-locations respectively, with respect to an enterprise. The Policy Actions Ontology contains a hierarchy of actions relevant to an enterprise. An action mentioned in a high level policy may be found either by following the taxonomic relations of actions or as a synonymous action in the Ontology. The concepts related to a policy action can be similarly obtained from the Ontology.

The ontology is instantiated with the information about a particular enterprise for which the policies are to be analysed. This results into the ontology containing the enterprise assets at its leaf level. As we delve down the ontology starting from one of the selected concepts or sub-concepts relevant to the policy statement, we arrive at a new sub-concept with each traversal and continue the traversal up to the leaf level.

Stated below are some information we need to obtain from the policy statements in order to analyse them using our ontology:

- Whether the policy statement expresses a permission, prohibition or an obligation?
- What is the action that is allowed or denied as a result of the policy?
- What are the instruments (e.g., software tools) necessary to carry out the task to comply with the policy?
- What are the time and location constraints (if any) applicable on the policy?
- Who is the agent (doer) and recipient or beneficiary of the policy?

Thus a policy imposes constraints on the instantiated ontology. Each policy when applied to the ontology imposes certain constraints or restrictions to the different concepts, elements or individuals thus binding them by certain rules and regulations. The constraints may be location constraints, time constraints, access constraints, action constraints etc. Identification of the existing constraints and their modification on addition, removal or change in the existing or new policies is well managed and properly handled in our approach. It is elucidated with the help of “work-from-home” scenario taken up in section 8. Answers to the above and similar questions can be found by navigating our ontology to search for the instance level answers to

these questions and subsequently analyse the policies and detect conflicts, if any.

7 IMPLEMENTATION

In our implementation, we have used the Protégé tool for developing and editing our ontology, the HerMiT reasoner for its conflict and overlap detection, and OWL-DL as the ontology language. Our selection was motivated by the work carried out by (Altarish, 2012) and (Dentler, Cornet, ten Teije & de Keizer, 2011) and (Bermejo-Alonso, 2018).

On complete instantiation of the ontology with the enterprise information, the specific individuals form the terminal nodes of the instantiated ontology. Next we move on to find the relevant object property or relationships which links the concepts identified in the ontology from the high-level policy statement. Once all the concepts in a policy are identified and all the concepts are linked with other concepts using relevant relationships or object properties, we traverse the ontology downwards starting from the identified concepts till we reach the last level of the ontology. With each level of traversal, the concepts and sub-concepts become more specific. This, in turn, helps us derive a more specific policy with each level of traversal, by combining the linked concepts of the same level. Finally, at the last level of the instantiated ontology we obtain values for the concepts which are enterprise-specific (since, the ontology is instantiated with enterprise information). Combining the concepts of the last level, using the relationships or object properties, we are able to form the rules corresponding to that enterprise for that particular policy whose analysis is being carried out. These low level rules, thus obtained, facilitate different kinds of policy analysis. Every participant of the enterprise under consideration should abide by these rules to enable secure and efficient functioning of the enterprise. So far about 257 concepts, the relevant relations and the object properties have been included in the proposed ontology.

8 APPLICATIONS

Besides helping in policy analysis, our ontology also serves as a hierarchical representation of any enterprise along with its assets. We have tested our ontology against a number of available high-level information security policies. We have been able to decompose the policies and convert them to rules

using the enterprise information to instantiate the ontology and following the procedure described in the previous section.

Analyzing the policies with our ontology would be helpful in detecting policy conflicts and thereby its removal using the reasoner. It also fulfils the requirement of revising or reviewing the existing policies while including new policies, without incurring much manual intervention and thus aids in formulation of guidelines and control procedures for the analysed policies. Determining the applicability of a policy for the enterprise is also possible because of the use of domain specific ontologies as a part of our combined ontology. It also comes handy in defining the appropriate time constraints and proper geo-spatial (physical) constraints and cyber location constraints for the enterprise policies. This is significant in the current scenario since the adoption of “work-from-home” policy by a wide range of enterprises. With the introduction of “work-from-home”, new constraints of time and space boundaries have been adopted by the organizations. The applicability of the policies is no more confined within the office campus and so are the policies that apply to them. The organizations now permit the users to access their resources remotely from their homes 24X7. Thus with the introduction of “work-from-home”, the time and location constraints of an existing policy needs to be updated. Changing the policies, updating their constraints and checking for conflicts in such cases can be time-taking and prone to errors, when carried out manually. Using our ontology, adaptability to such policy and policy-constraint changes, and proper detection of conflicts is facilitated, with increased speed and efficiency, thus saving a lot of time and labour of the organization. Our ontology is extendible and can be updated as and when necessary. We could save time required for the process of policy analysis, by automating the process. Advantages of using this is more prominent as the size of the enterprise under consideration increases. We claim that it is capable of handling large enterprise scenarios. It is also a unique approach towards serving the purpose we intend to accomplish.

Figure 1 is a partial representation of our ontology from which relationships can be determined. Some of them are:

1. A software runs on a host and the software has some vulnerability.
2. An attacker uses malware to exploit the vulnerability of a software.
3. Authorised users have an account using which they log into a host.

4. Authorised users can install, delete or update a software.
5. An attacker performs an attack which uses a malware.
6. Passwords must be changed at regular intervals (time constraints).
7. Authorised users can backup data daily from a machine located in the office premises (geo-location constraints) and has an IP address within the defined range (cyber-location constraints).
8. Antivirus software must be updated by authorised users at regular intervals (time constraints).
9. A remote device is located outside office premises and has a defined range of IP address. The users can register their device as a remote device and use it for accessing other devices in the office from a remote location, e.g. their homes. (work-from-home).

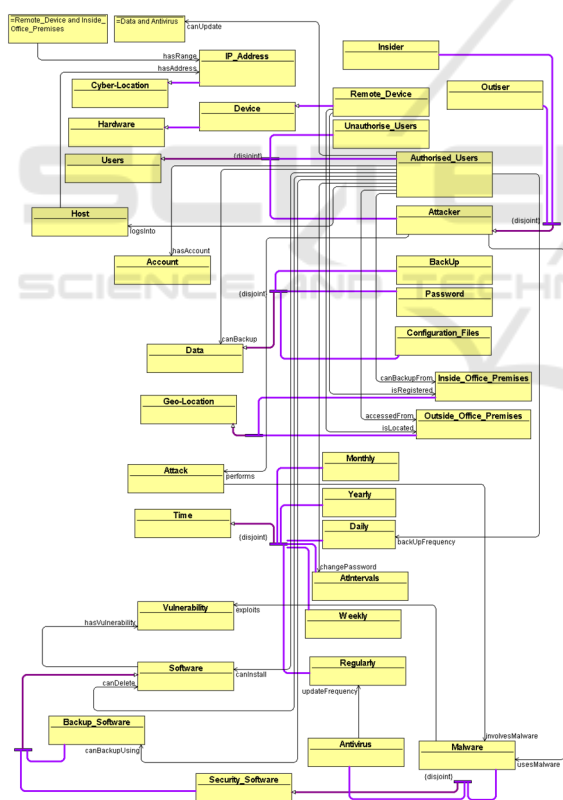


Figure 1: A partial representation of our Ontology.

9 CONCLUSION & FUTURE WORK

This paper discussed the importance of Ontology in Enterprise Information Security Policy Analysis. It has been brought out how the different disparate ontologies can be combined to develop an application specific ontology for Policy Analysis. It has also been shown how the different kinds of analyses can be performed easily using the proposed ontology developed using standard tools.

This work is an extension of the concepts discussed in the context of the paper (Mandal & Mazumdar, 2018) regarding a Policy Compliance checking tool from Log records. The authors intend to extend the work and make use of this ontology for high-level information security policy analysis including compliance checking. This would aid in saving time and reducing human errors involved in the process, which in turn would improve the efficiency of an enterprise by helping to assure its information security.

REFERENCES

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: a review of challenges and influencing factors. In The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016) Information (pp. 352-358). IEEE.

Altarish, E., 2012. Comparison of Ontology Editors. ERAF Journal on Computing, 4, pp.23-38.

Basile, C., Liyo, A., Scozzi, S. and Vallini, M., 2010. Ontology-based security policy translation. Journal of Information Assurance and Security, 5(1), pp.437-445.

Bermejo-Alonso, J., 2018. Reviewing Task and Planning Ontologies: An Ontology Engineering Process. In: Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2018) - Volume 2: KEOD. SCITEPRESS – Science and Technology Publications, Lda, pp.183-190. doi: 10.5220/0006922401830190

Cristani, M. and Cuel, R., 2005. A Survey on Ontology Creation Methodologies. International Journal on Semantic Web and Information Systems, 1(2), pp.49-69.

Dentler, K., Cornet, R., ten Teije, A. and de Keizer, N., 2011. Comparison of reasoners for large ontologies in the OWL 2 EL profile. Semantic Web, 2(2), pp.71-87.

Do Amaral, F., Bazilio, C., Hamazaki Da Silva, G., Rademaker, A., & Haeusler, E. (2006). An Ontology-based Approach to the Formalization of Information Security Policies. 2006 10Th IEEE International

- Enterprise Distributed Object Computing Conference Workshops (EDOCW'06). doi: 10.1109/edocw.2006.21
- Evesti, A., Savola, R., Ovaska, E. and Kuusijärvi, J., 2011. The design instantiation and usage of information security measuring ontology. In: MOPAS 2011 The Second International Conference on Models and Ontology-based Design of Protocols Architectures and Services. pp.1-9.
- Fenz, S., & Ekelhart, A. (2009). Formalizing Information Security Knowledge. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (pp. 183-194).
- Girardi, R. (2010). Guiding Ontology Learning and Population by Knowledge System Goals. In Proceedings of the International Conference on Knowledge Engineering and Ontology Development (pp. 480-484). KEOD.
- Gruber, T., 1993. A translation approach to portable ontology specifications. *Knowledge Acquisition*, 5(2), pp.199-220.
- Gruber, T. (1995). Toward principles for the design of ontologies used for knowledge sharing?. *International Journal Of Human-Computer Studies*, 43(5-6), 907-928. doi: 10.1006/ijhc.1995.1081
- Guarino, N. (1998). Formal Ontology and Information Systems. In 1st International Conference on Formal Ontology in Information Systems (pp. 3-15). Amsterdam: IOS Press.
- Hayes, P. (1996). A Catalog of Temporal Theories. University of Illinois at Urbana-Champaign.
- Herzog, A., Shahmehri, N., & Duma, C. (2007). An Ontology of Information Security. *International Journal Of Information Security And Privacy*, 1(4), 1-23. doi: 10.4018/jisp.2007100101
- Jain, V., & Singh, M. (2013). Ontology Development and Query Retrieval using Protégé Tool. *International Journal Of Intelligent Systems And Applications*, 5(9), 67-75. doi: 10.5815/ijisa.2013.09.08
- LeClair, A., Khedri, R. and Marinache, A., 2019. Toward Measuring Knowledge Loss due to Ontology Modularization. In: Proceedings of the 11th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2019). SCITEPRESS – Science and Technology Publications, Lda., pp.174-184. doi: 10.5220/0008169301740184
- Maedche, A., & Staab, S. (2001). Ontology learning for the Semantic Web. *IEEE Intelligent Systems*, 16(2), 72-79. doi: 10.1109/5254.920602
- Mandal, D., & Mazumdar, C. (2018). Automating Information Security Policy Compliance Checking. 2018 Fifth International Conference On Emerging Applications Of Information Technology (EAIT). doi: 10.1109/eait.2018.8470420
- Mishra, S., Malik, S., Jain, N., & Jain, S. (2015). A Realist Framework for Ontologies and the Semantic Web. *Procedia Computer Science*, 70, 483-490. doi: 10.1016/j.procs.2015.10.087
- Musen, M., 1992. Dimensions of knowledge sharing and reuse. *Computers and Biomedical Research*, 25(5), pp.435-467.
- Noy, N. and McGuinness, D., 2001. "Ontology Development 101: A Guide To Creating Your First Ontology. Stanford University, Stanford, CA, Tech. Rep.
- Obrst, L., Chase, P., & Markeloff, R. (2012). Developing an Ontology of the Cyber Security Domain. Da Costa, P.C.G. And Laskey, K.B. (Eds.) STIDS., 49–56.
- Oltramari, A., Cranor, L., Walls, R., & McDaniel, P. (2014). Building an Ontology of Cyber Security. *CEUR Workshop Proceedings*, 1304(1613-0073), 54-61.
- Peltier, T. (2004). Information security policies and procedures. Boca Raton, FL: Auerbach Publications.
- Peltier, T. Information security policies, procedures, and standards (p. 21).
- Policy Analysis. (2020). Retrieved 5 October 2020, from https://www.cdc.gov/policy/polaris/policyprocess/policy_analysis.html
- Ressler, J., Dean, M., & Kolas, D. (2010). Geospatial Ontology Trade Study. In T. Janssen & W. Leo Obrst, *Ontologies and Semantic Technologies for Intelligence* (pp. 179-212). Amsterdam, Berlin, Tokyo, Washington D.C.: IOOS Press.
- Souag, A., Salinesi, C., Mazo, R. and Comyn-Wattiau, I., 2015. A Security Ontology for Security Requirements Elicitation. *Lecture Notes in Computer Science*, pp.157-177.
- Von Wright, G. (1951). Deontic Logic. *Mind*, 60(237), 1-15. Retrieved from <http://www.jstor.org/stable/2251395>
- Tsoumas, B. and Gritzalis, D., 2006. Towards an ontology-based security management. In: 20th International Conference on Advanced Information Networking and Applications. pp.985-992.
- Uszok, A., Bradshaw, J., Johnson, M., Jeffers, R., Tate, A., Dalton, J. and Aitken, S., 2004. KAoS policy management for semantic Web services. *IEEE Intelligent Systems*, 19(4), pp.32-41.
- Wache, H., Vögele, T., Visser, U., Stuckenschmidt, H., Schuster, G., Neumann, H. and Hübner, S., 2001. Ontology-based Integration of Information - A Survey of Existing Approaches. In: Proceedings of IJCAI-01 Workshop: Ontologies and Information Sharing. pp.108 - 117.