International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I8P246

Volume 70 Issue 8, 453-462, August 2022

Original Article

Protection Policy Implementation using Web Ontology Language

Lingala Thirupathi[1], Venkata Nageswara Rao Padmanabhuni[2]

[1,2]*CSE Department, GIT, GITAM (Deemed to be University), Vizag, INDIA.*

[1]thiru1274@gmail.com

Received: 02 June 2022 Revised: 16 August 2022 Accepted: 24 August 2022 Published: 31 August 2022

Abstract **-** *This article is an experiment leveraging web ontology language to develop and evaluate Mandatory Access Control with Bell-La Padula (BLP) attributes for a Multi-Level Protection lattice model. The semantic web is built on top of the www to make data machine-readable so data processing and administration can be improved. The Web ontology language is a semantic web computational logic-based language for representing complex knowledge in a semantic format. Construct dominance relationships between variables within the lattice model and run different queries to see if the subject with security clearance can read or write to the object with security classification using the Multi-level protection (MLP) ontology. Furthermore, the ontology would only enable information to move from items with lower categorization to entities with higher classification by utilizing BLP characteristics.*

Keywords **-** *MLP, OWL, ontology, Security, Semantic Web.*

1. Introduction

Since the internet's inception in 1962, web development has never ceased. In the past, obtaining information via the internet required advanced understanding. Sir Tim Berners-Lee, the inventor of the World Wide Web, created it in the 1990s. Furthermore, with the invention of search engines, today's digital world was born, allowing ordinary people to access information on the internet without needing specialized knowledge. The rapid evolution of web technology has elevated the web to a data-centered processing age, in which users have become the primary source of data generation via broadcasting and social networking during the last 20 years.

Artificial intelligence and semantic web technologies have been utilized in the healthcare industry to model knowledge. Information security, on the other hand, is constantly a hot topic. Cyber security professionals have long been aware of the risks posed by emerging online technologies such as cloud computing, big data, the Internet of Things, and so on. The internet isn't the only source of security threats; the internal environment is also a source. Case studies like the Marriott Data Breach [1] and the US Office of Personnel Management have shown that designing and maintaining the security of information systems is a top responsibility for both private and public sector organizations. A total of 20 million persons were affected by this breach [2]. Organizations must collect, process, store, and share sensitive data securely. For example, patients' medical information, top-secret military resources, and personal identity information should all be safeguarded because data breaches can result in significant financial loss for individuals and organizations and raise national security concerns. MLP is widely used in military systems and is imposed even more stringently on their contractors and partners. To boost their security profile, several businesses have adopted the MLP in response to increased security risks from both internal and external contexts. According to the classification of the data, each utilizes access control to require pre-authorized user credentials to gain access to the designated information.

In [3], the authors use a security ontology to drive the administrator from high-level policy specification down to system configuration, mainly at the IP level. In [4], the authors discuss the necessity to implement the cyber security policy and reflect on studies presently being carried out using an ontology. In [5], the framework is developed with conceptual modeling and validated using three different datasets. But in none of the articles, the security policies are not implemented correctly. To overcome this existing problem, develop the policies using web ontology language.

The rest of the paper is laid out as follows. Section 2 covers previous MLP research and gives a brief overview of the semantic web. Section 3 shows how to utilize Protégé to build the MLP lattice model, and Section 4 explores how to apply dominance rules in the ontology using semantic web rule language. Section 5 concludes by summarizing the work done in this study and outlining opportunities for future research.

2. Literature Survey

Mandatory Access Control (MAC) is non-discretionary access control that assigns a uniform level of security to all individuals and objects in an information system. A person must be authorized to access an item (with security clearance) to block the flow of information (with security classification). MLP and MAC have

previously been related. MLP was first proposed by the armed community as a technique to strengthen the security of sensitive and secret data. It's widely used in the military-industrial complex, especially in military and government systems that demand higher levels of security than private organizations. MLP uses the BLP paradigm with the need-to-know requirement to prevent secret information from migrating from the upper to the lower levels [6].

To establish MLP security labels or levels, the BLP model adds additional information known as a compartment. A pair of sensitivity levels and a set of compartments make up an MLP security level or label. When designing a security level or label in an idea, utilize a colon to separate a sensitivity level and a group of compartments in this article.

2.1. Semantic Web Technologies Layers

The W3C has standardized the Semantic Web as an expansion of the current World Wide Web. Its purpose is to make data's implicit meaning explicit so that it may be machine-readable, allowing for better information retrieval and more useful work. The layers are described below.

2.1.1. RDF

The Resource Description Framework (RDF) is a fundamental building component of the semantic web that expresses the semantic meaning of knowledge using HTML, HTTP, and XML. Anything can be a resource, but it must be uniquely identified and referenced using an Internalized Resource Identifier (IRI). Knowledge is expressed as a triple, which consists of three components: subject, property, and object, and follows a simple pattern. The subject and property of an RDF triple must be IRIs, while the triple's object can be either an IRI or a literal (data type).

2.1.2. OWL

The W3C Web Ontology Language (OWL) is a Semantic Web language designed to represent rich and complicated data using description concepts to describe classes, people, and attributes. The study of the nature of existence, creatures, and their relationships is known as ontology. Ontology is a tool used in information science to develop unambiguous knowledge. A formal statement of entities' concepts, types, attributes, and interrelationships inside a real-world domain is known as "ontology." Formal ontology provides a precise context or meaning for humans and machines to grasp. Conceptual frameworks ensure everyone understands that information. Methodologies are used to describe and link disparate and complex facts in reality.

2.1.3. Semantic Rule Language (SWRL)

The Semantic Web Rule Language (SWRL) is a suggested language for the Semantic Web that combines OWL DL or OWL Lite with a portion of the Rule Markup Language to express rules and logic. The National Research Council of Canada, Network Inference (now bought by web Methods), and Stanford University submitted the definition to the W3C in May 2004 in collaboration with the Joint US/EU ad hoc Agent Markup Language Committee. The standard was developed based on the previous OWL rules language proposal.

According to [7], the authors suggested a hybrid technique for labeling and specifying business processes, including modular ontology design, consistent ontology design for each module, and a unified control flow for the process and its sub-processes. SWRL is the sole tool that collects ontologies to model information and makes decisions for industrial applications. The authors propose that SWRL be used to augment OWL models to create a learnable approach to production management. In [8], the authors propose a Multi-Level Protection lattice model architecture based on the Neo4j graph database.

Protégé is an open-source ontology editor developed at Stanford University School of Medicine's Stanford Center for Biomedical Informatics Research. This gadget is widely used by academic, government, and business organizations. It complies with W3C standards, has a graphical aid, and ample built-in equipment to assist in the creation of ontologies. Protégé comes with a slew of tools to assist developers in constructing, revising, and managing ontologies.

1. 3. Building Multi-Level Security in OWL

The authors [9] implemented a random walk and word embedding-based ontology embedding method. Others suggested adding rules for transforming UML class diagrams to ontologies [10. The authors [11] developed an OWL-based ontology model to annotate personal, physiological, behavioral, and contextual data from heterogeneous sources. In [12], the authors investigated the role of formal ontologies in information systems development, i.e., how these graphs-based structures can be beneficial during the analysis and design of the information systems. In [13], the authors provided an overview of the methods that use ontologies to compute similarity and incorporate them into machine learning methods. In [14], the authors proposed a model that provides a basis for pattern recognition, analysis, and identification of news articles on social media as fake. In [15], the authors developed a prototype for a tool that stores OWL ontology in a Cassandra database and finally introduced a reasoning strategy to compute the ontology closure using this Cassandra database.

The authors proposed a new life cycle for ontology training related to software technical prerequisites, explained a new strategy for constructing ontology from Relational database systems depending on the previously defined life cycle, added 3 original concepts that can be retrieved, and recommended an assessment method characterized by 2 groups of measurements: theoretical ontology evaluation measurements; and fact-based ontology methodologies in [16]. This section will show you how to create an MLP ontology in Protégé. It involves a 6 step technique. Classes [17], properties [18], and

people are the three major aspects of an OWL ontology. This article utilizes the following naming standards without spaces to identify each element:

Classes: upper cases (e.g., Member, Mammal, Groceries)
Properties: lower cases (e.g., isLessThan, hasChoice, goesTo)
Individuals: leading underscore (e.g., _LingalaThirupathi, _Tiger, _Pizza)

Step1. Creation of the classes

The first step is to create three classes, *Security Label*, *Sensitivity Level*, *Compartment* and their subclasses. In this, each node will be a subclass of the *Security Labels*. A *Security Label* has two components, sensitivity level and compartment. *TopSecret* and *Secret* are subclasses of Sensitivity Level, and *LingalaThirupathi*, *Lingala*, *Thirupathi*, and *Null (represents { })* are subclasses of the *compartment*.

Because OWL uses open global reasoning, classes that aren't specific to be extraordinary sorts of objects are unknown and hence allow intersections. To suggest that Security Label, Sensitivity Level, and Compartment do not have any common participants would be an understatement. No person can serve as an example for more than one of the three categories. Through the Establish Class Hierarchy tool, Protégé allows clients to create a list of classes and suggests disjointness. Pick a random class to view at the bottom of the Class Description to confirm the implementation. In the Disjoint With part, all sibling classes of the chosen class must be proven.

In addition, at the same class hierarchy level as Security *Label*, *Sensitivity Level* and *Compartment*, two more disjoint classes, *Subject* and *Object*, are created for implementation in the next section. Fig 3.1 shows the full list of classes with class hierarchy levels from the protégé tool.

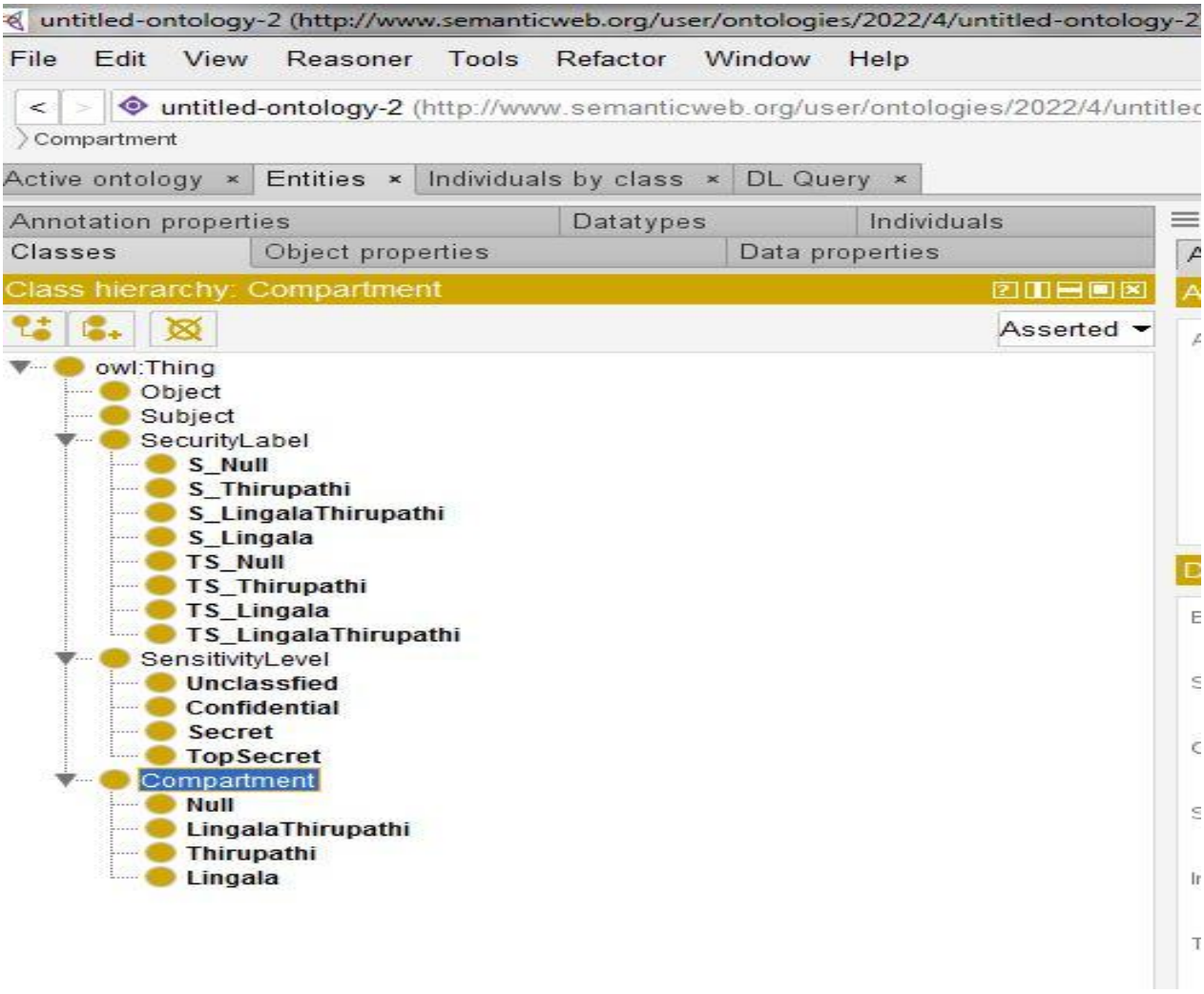

Fig. 3.1 classes with hierarchy levels

Step2. Creation of the Object Properties and its Inverse Properties

The second step is defining the entities' binary relationships (properties). The Fig. 3.2 shows the Object Properties created in the Protégé tool, and Fig. 3.3 shows the Creation of Domains and Ranges of the Object Properties.

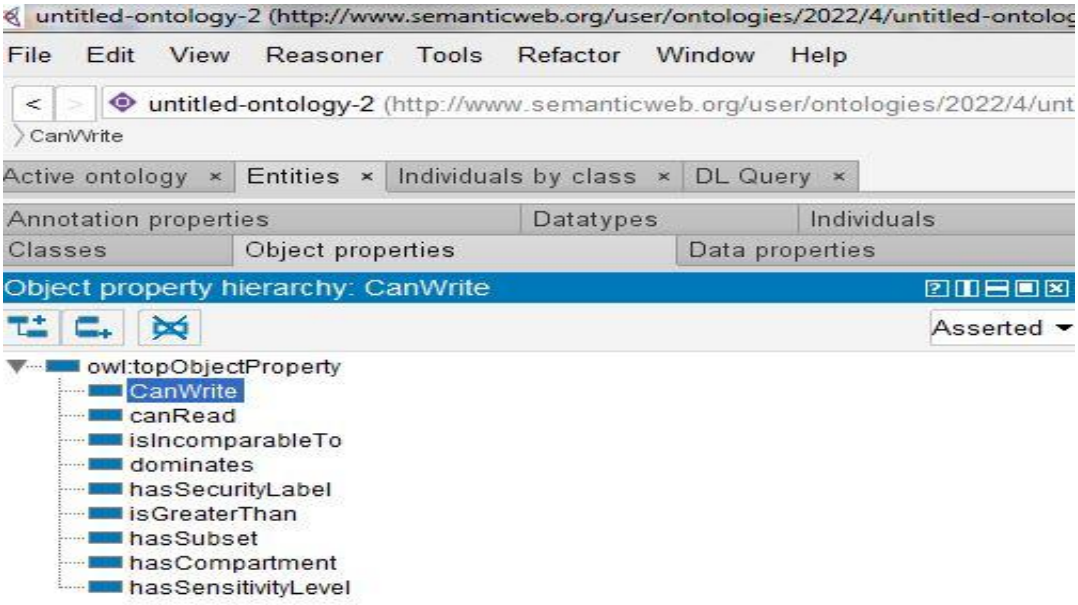

Fig. 3.2 Create Object Properties

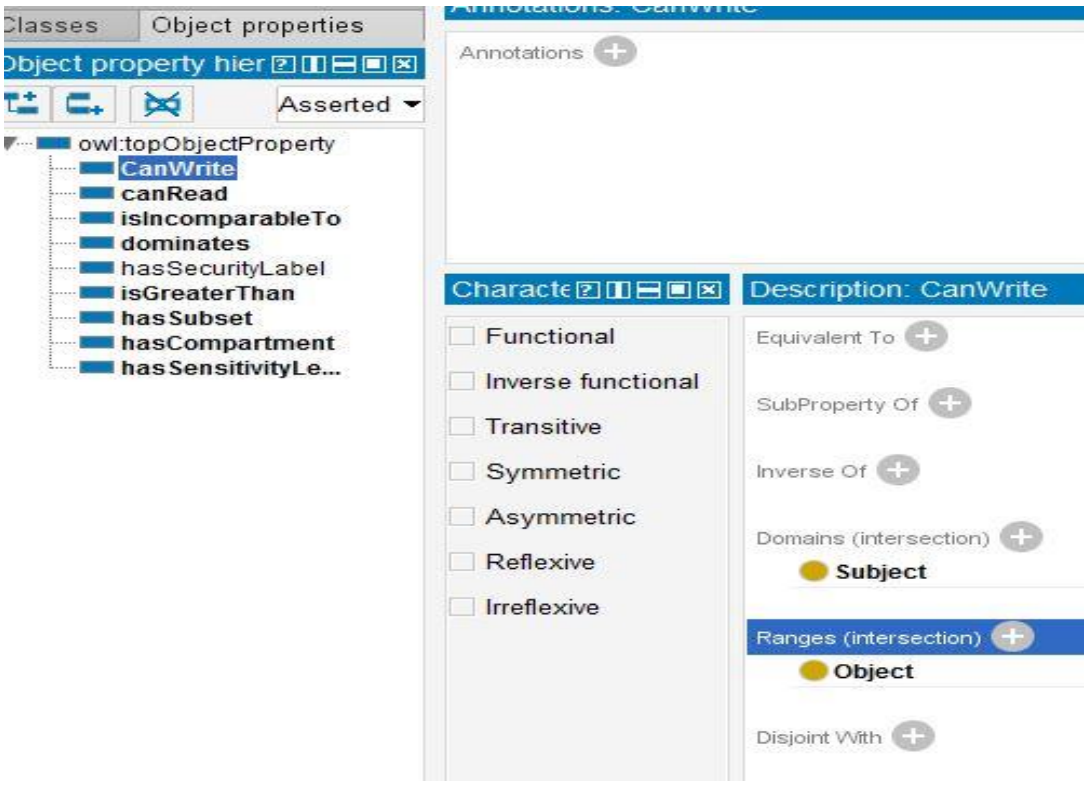

Fig. 3.3 Creation of Domains and Ranges of the Object Properties

Fig. 3.4 and 3.5 show the creation of Object Properties' characteristics and the Creation of Inverse Properties, respectively.

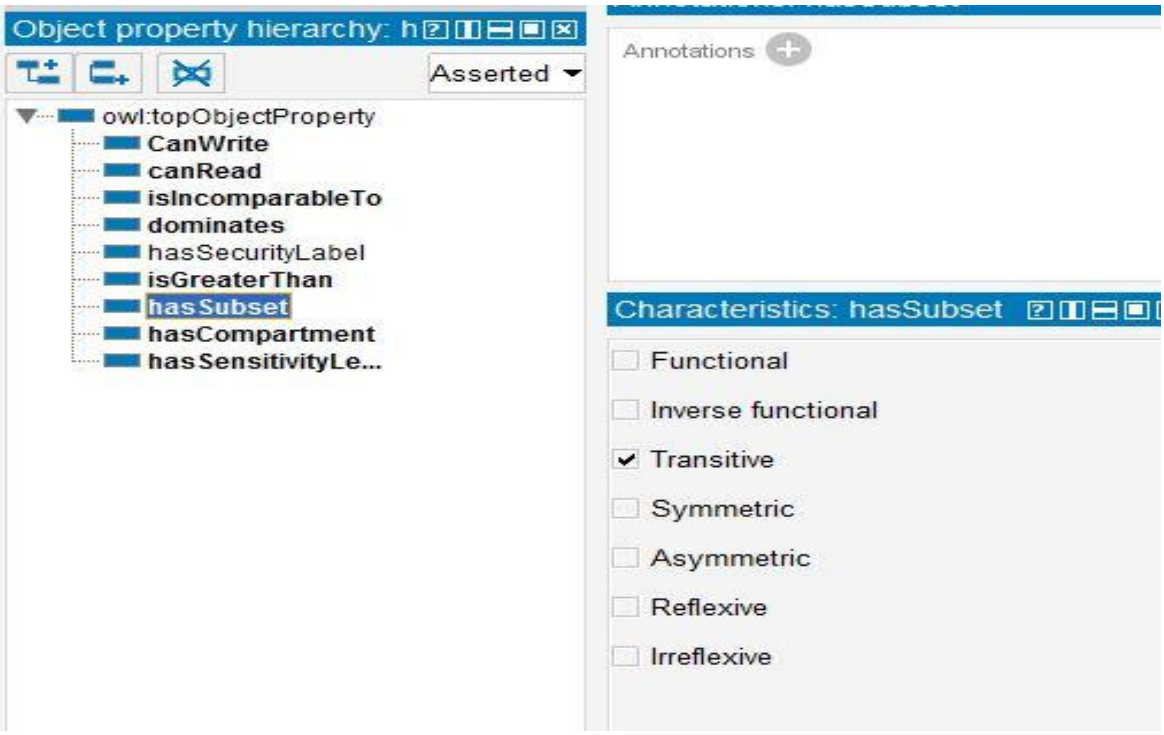

Fig. 3.4 Creation of characteristics of Object Properties

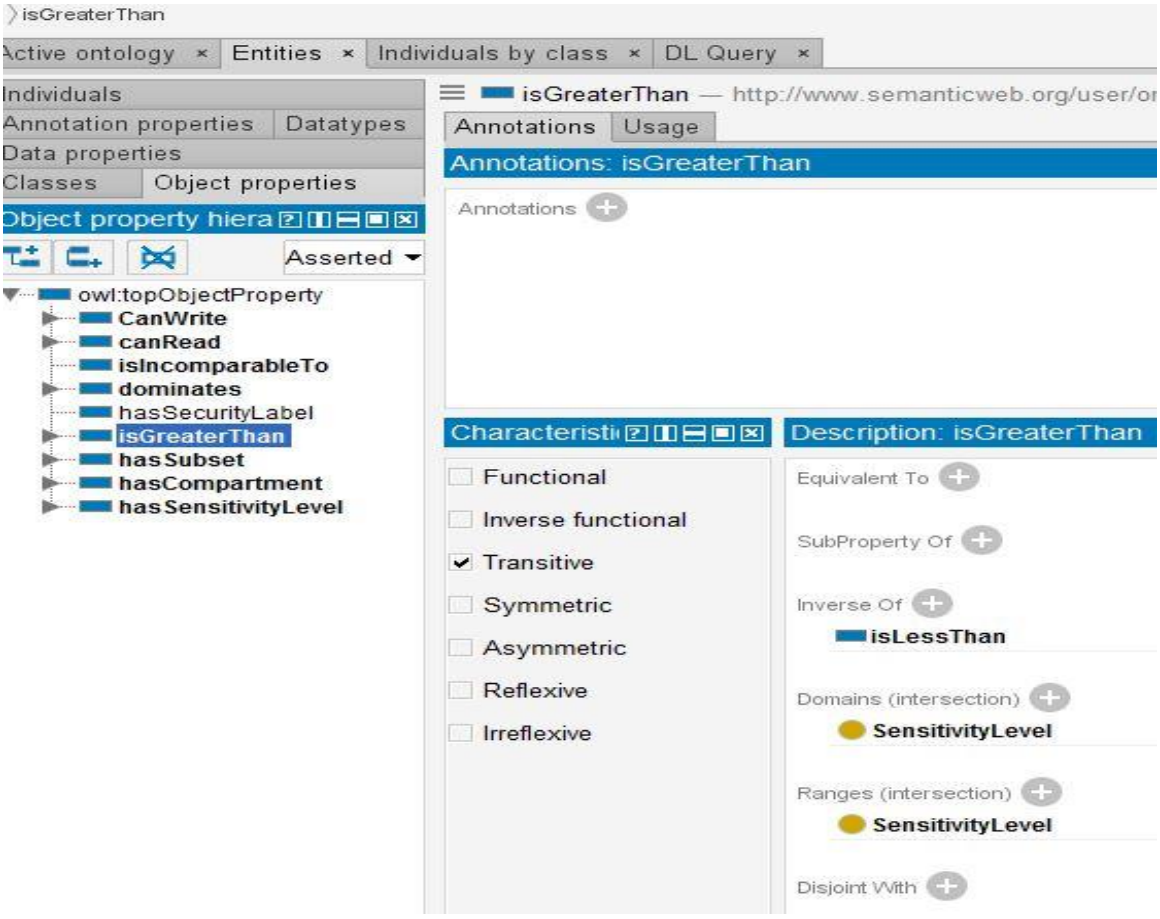

Fig. 3.5 Creation of Inverse Properties

Protégé also allows you to define the domain and range of attributes using mathematical equivalents. For example, the domain of hasSensitivityLevel is Security Label, and the scope is the Sensitivity Level. When hasSensitivityLevel is used in a triple assertion, the subject must be an instance of Security Label, and the object must be an instance of Sensitivity Level. Each object property may have inverse properties.

Step3. Modeling of the Classes Expression with the Property Restrictions [19]

The next stage is to represent class expression using property limitations. Properties describe individual connections. It can also be used as a unique type of class description to underline that the constraint must be met at all times in the class. The four types of property restrictions are existential, universal, cardinality, and value restrictions. Existential and universal limits could be utilized to outline Security Label and its subclasses to represent them.

The class must have a sensitivity label, and the security label must be TopSecret. (Existential & universal) and the class must have a compartment, and the compartment must be LingalaThirupathi (existential &universal)

According to the 2 conditions, 4 new property restrictions are applied: hasSensitivity Level some Top Secret, has Sensitivity Level only Top Secret, has Compartment some Lingala Thirupathi, has Compartment only Lingala Thirupathi.

Figs 3.6 and 3.7 show the property restrictions for TS_LingalaThirupathi before and after adding restrictions.

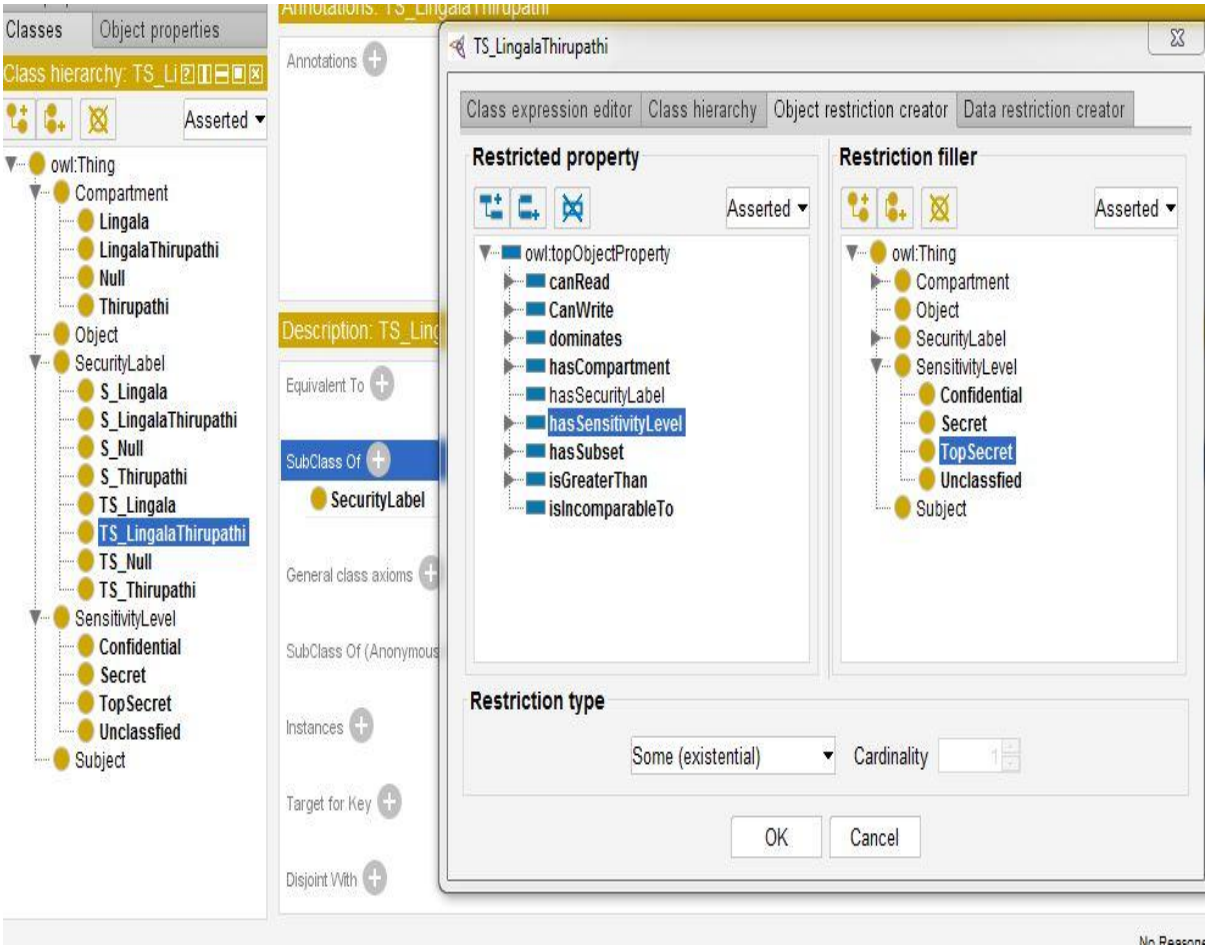

Fig. 3.6. Adding property restrictions for TS_LingalaThirupathi

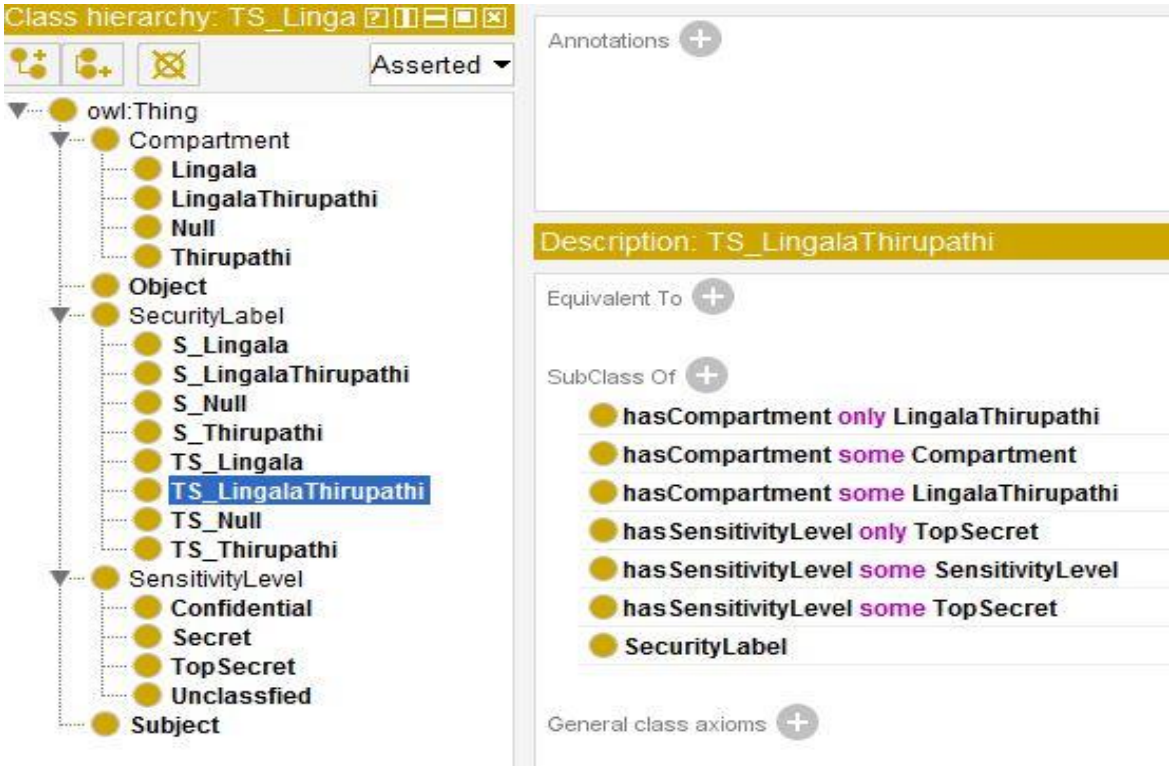

Fig. 3.7 After adding property restrictions for TS_LingalaThirupathi

Moreover, table 1 shows the list of the property restrictions applied to each class shown below.

Table 1. Property Restrictions of the classes

Class	Subclass	Property Restrictions
Compartment	LingalaThirupathi	hasSubsetsome(Lingala or Thirupathi)
	Lingala	hasSubsetsomeNull
	Thirupathi	hasSubsetsomeNull
Sensitivity Level	TopSecret	isGreaterThansomeSecret
	Secret	isGreaterThansomeConfidential
	Confidential	isGreaterThansomeUnclassified
Security Label	TS_ LingalaThirupathi	hasSensitivityLevel some SensitivityLevel hasCompartment someCompartment
		hasSensitivityLevel someTopSecret hasSensitivityLevel only TopSecret hasCompartment some LingalaThirupathi hasCompartmentonlyLingalaThirupathi
	TS_Lingala	hasSensitivityLevel someTopSecret hasSensitivityLevelonlyTopSecret
		hasCompartment some Lingala hasCompartmentonlyLingala
	TS_Thirupathi	hasSensitivityLevel some TopSecret hasSensitivityLevel only TopSecret hasCompartment some Thirupathi hasCompartmentonlyThirupathi
	TS_Null	hasSensitivityLevel some TopSecret hasSensitivityLevel only TopSecret hasCompartment some Null hasCompartmentonlyNull

	S_ LingalaThirupathi	hasSensitivityLevel some Secret hasSensitivityLevel only Secret hasCompartmentsome LingalaThirupathi hasCompartmentonly LingalaThirupathi
	S_Lingala	hasSensitivityLevelsome Secret hasSensitivityLevel only Secret hasCompartment some Lingala hasCompartmentonlyLingala
	S_Thirupathi	hasSensitivityLevelsome Secret hasSensitivityLevel only Secret hasCompartment someThirupathi hasCompartmentonlyThirupathi
	S_Null	hasSensitivityLevel some Secret hasSensitivityLevel onlySecret hasCompartment some Null hasCompartmentonlyNull
Subject		hasSecurityLabelsomeSecurityLabel
Object		hasSecurityLabelsomeSecurityLabel

Step4.Creation of the Individuals with their Property Assertions [20]

After modeling classes with property restrictions, then create instances with property assertions. Figs 3.8 and 3.9 show the Creation of Individuals with Property Assertions.

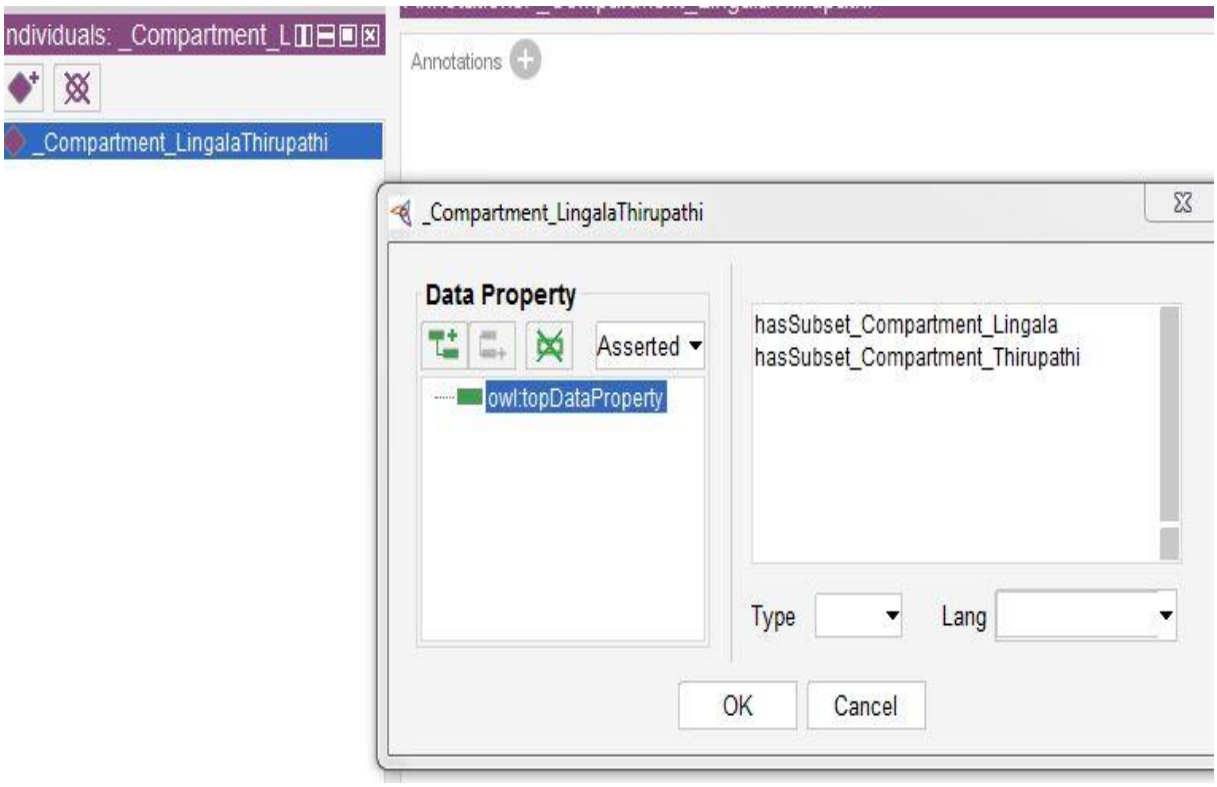

Fig. 3.8 Creation of one Individual with Property Assertion

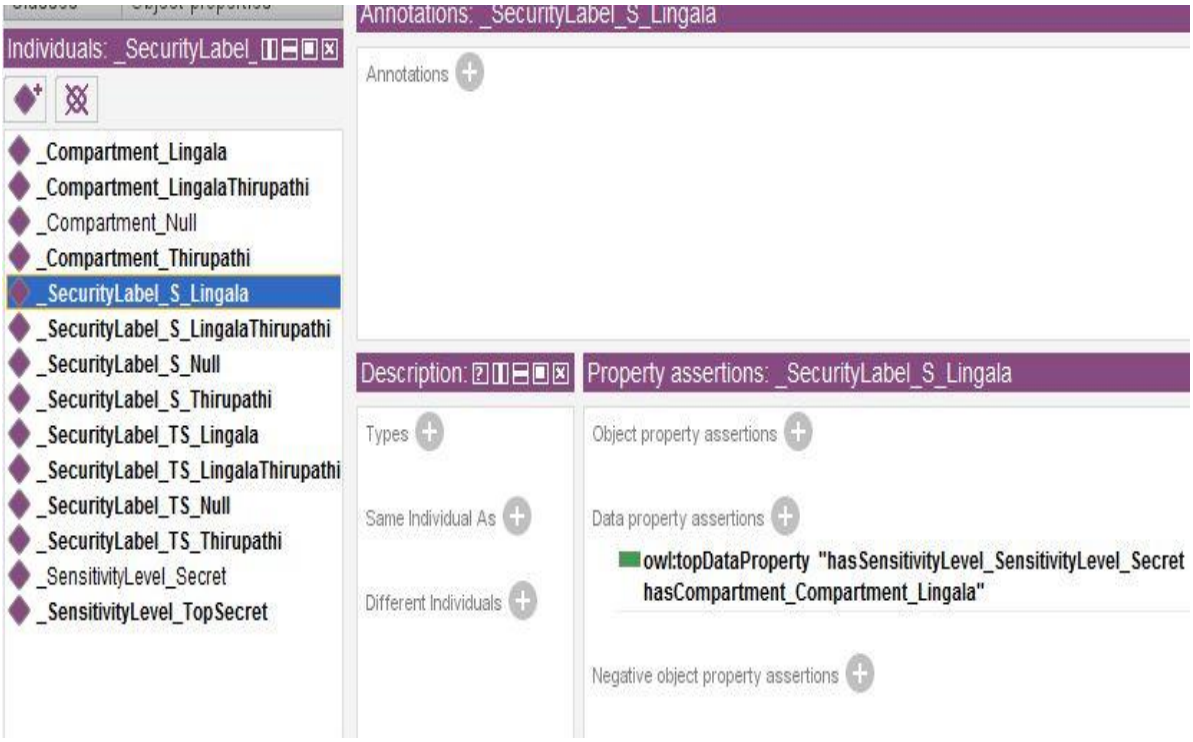

Fig. 3.9 Creation of Individuals with their Property Assertions for all

The ontology modeling constructs terminology assertions to instructions with asset restrictions. Individuals represent assertion information.

4. Conclusion

This article used meaningful internet as a platform and principles to create an experimental answer in protégé for MLP coverage in OWL. There are three stages to the proposed approach. The first stage, modeling safety, is based on MLP ideas. According to test queries, legal users are the most effective way to access tagged records. The findings indicate that the MLP policy can be implemented inside semantic internet infrastructure. According to the Semantic Scholar, this ontology is the principal MLP exercise in research investigations. Businesses may be able to use this security coverage to protect sensitive data.

References

[1] Sanger D.E, Perlroth N, Thrush G, & Rappeport A, 2018. [Online]. Available: https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html

[2] Thomas, Jason, "A Case Study Analysis of the US Office of Personnel Management Data Breech," 2019. 10.13140/RG.2.2.36670.23360.

[3] Basile, Cataldo & Lioy, Antonio & Scozzi, Salvatore & Vallini, Marco, "Ontology-Based Policy Translation," vol. 63, pp. 117-126, 2009. 10.1007/978-3-642-04091-7_15.

[4] Talib, A., Alomary, F., Alwadi, H. and Albusayli, R, "Ontology-Based Cyber Security Policy Implementation in Saudi Arabia," *Journal of Information Security*, vol. 9, pp. 315-333, 2018. Doi: 10.4236/jis.2018.94021.

[5] Välja, M., Heiding, F., Franke, U. et al., "Automating Threat Modeling using an Ontology Framework. Cybersecur," vol. 3, pp. 19, 2020. https://doi.org/10.1186/s42400-020-00060-8.

[6] Panossian, Garo, "*Multi-Level Secure Data Dissemination*," Electronic Theses, Projects, and Dissertations, vol. 946, https://scholarworks.lib.csusb.edu/etd/946.

[7] Roy, S., Dayan, G.S., Devaraja Holla, V, "*Modeling Industrial Business Processes for Querying and Retrieving Using OWL+SWRL*," In: Panetto, H., Debruyne, C., Proper, H., Ardagna, C., Roman, D., Meersman R. Eds., On the Move to Meaningful Internet Systems. OTM 2018 Conferences, OTM 2018. Lecture Notes in Computer Science, vol. 11230, 2018. Springer, Cham. https://doi.org/10.1007/978-3-030-02671-4_31.

[8] Lingala Thirupathi and Venkata Nageswara Rao Padmanabhuni, "Multi-level Protection (Mlp) Policy Implementation using Graph Database," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, no. 3, 2021. http://dx.doi.org/10.14569/IJACSA.2021.0120350.

[9] Chen, J., Hu, P., Jimenez-Ruiz, E. et al., "OWL2Vec*: Embedding of OWL Ontologies," *Mach Learn*, vol. 110, pp. 1813–1845, 2021. https://doi.org/10.1007/s10994-021-05997-6.

[10] Minh Hoang Lien Vo & Quang Hoang, "Transformation of UML Class Diagram into OWL Ontology*," Journal of Information and Telecommunication*, vol. 4, no. 1, pp. 1-16, 2020. DOI: 10.1080/24751839.2019.1686681.

[11] Chatterjee A, Prinz A, Gerdes M, Martinez S, "An Automatic Ontology-Based Approach to Support Logical Representation of Observable and Measurable Data for Healthy Lifestyle Management: Proof-of-Concept Study," *J Med Internet Res*, vol. 23, no. 4, pp. e24656, 2021. [Online]. Available: https://www.jmir.org/2021/4/e24656, DOI: 10.2196/24656.

[12] Husáková, Martina, and Vladimír Bureš, "Formal Ontologies in Information Systems Development: A Systematic Review," *Information* vol. 11, no. 2, pp. 66, 2020. https://doi.org/10.3390/info11020066.
[13] Maxat Kulmanov, Fatima Zohra Smaili, Xin Gao, "Robert Hoehndorf, Semantic Similarity and Machine Learning with Ontologies," *Briefings in Bioinformatics*, vol. 22, no. 4, 2021. https://doi.org/10.1093/bib/bbaa199.
[14] Bani-Hani, Anoud; Adedugbe, Oluwasegun; Benkhelifa, Elhadj; and Majdalawieh, Munir, "Fandet Semantic Model: An OWL Ontology for Context-Based Fake News Detection on Social Media," *All Works*, 4756, 2021. https://zuscholars.zu.ac.ae/works/4756.
[15] Faezeh Mostajabi, Ali Asghar Safaei, Amir Sahafi, "A Systematic Review of Data Models for the Big Data Problem," *IEEE Access*, vol. 9, pp. 128889-128904, 2021. 10.1109/ACCESS.2021.3112880.
[16] Ben Mahria, B., Chaker, I. & Zahi A, "A Novel Approach for Learning Ontology from Relational Database: From the Construction to the Evaluation, *J Big Data*, vol. 8, pp. 25, 2021. https://doi.org/10.1186/s40537-021-00412-2
[17] [Online]. Available: https://documentation.mindsphere.io/MindSphere/howto/howto-create-ontology-owl.html
[18] [Online]. Available: https://go-protege-tutorial.readthedocs.io/en/latest/ObjectProperties.html
[19] [Online]. Available: https://ontology101tutorial.readthedocs.io/en/latest/OWL_ClassRestrictions.html
[20] [Online]. Available: https://docs.oracle.com/cd/E24693_01/appdev.11203/e11828/owl_concepts.htm