CONTRIBUTIONS TO THE DEVELOPMENT AND STANDARDIZATION OF THE SEMANTIC WEB

Phd thesis – Survey

for achieving of the scientific title of 'Doctor' at

Politehnica University Timișoara

in the doctorate domain: Computer Science and Information Technology

author: ing. Zamfira Constantin Andrei

phd supervisor: prof.univ.dr.ing. Horia Ciocarlie

month **02**, year **2022**

1. Actuality of the Theme

As its very name says, this thesis was emphasized on making contributions to the development of the new generation of the most important and currently used service in the Internet, the World Wide Web, which is known under the name Web 3.0, or Semantic Web

This version appeared in the early 2000s, being invented by none other than the father of the Internet and the World Wide Web, the English scientist sir. Timothy Berners-Lee. Its main purpose was to bring a structure into the clutter that currently exists on the Web, which is dominated by unstructured (plain text) and semi-structured (XML, HTML) documents, extending these documents to data that have a semantic structure. Another objective of this new generation of World Wide Web is the possibility of automatic data processing by machines, which will replace human labor related to searching, finding, processing, combining information from web pages; in other words, it was intended to automate the processes. This can be achieved by annotating web resources with the help of annotations that keep information about their content and that can be understood by automatic agents on the Web, called semantic bookmarks. To ensure that different agents have a common understanding of the terms in these descriptions, ontologies are used where both the terms and the relationships existing between them are defined. Ontologies are the 'cornerstone' of the Semantic Web, supporting the realization of automated processes, providing vocabulary with their terms and relationships. Due to the fact that the Semantic Web is in its infancy, there is currently a great need for these vocabularies with semantically structured data, as well as for intelligent agents who have to execute the necessary operations on resources on the Web, the most important being those of reasoning.

In order to achieve the design objectives, a project architecture was created consisting of a stack of levels that were proposed ad-hoc to support the functionality of the Semantic Web. For most of these stack levels, languages and technologies have been created, but there are others that have not yet been standardized due to the many problems and dissociations that exist in those areas; these are the levels of Logic, Trust, and Evidence of the SW architecture, for which standards have not (yet) been developed.

Having said the above, I considered that the field of the Semantic Web is a favorable one to carry out my research, with many areas that require problem solving and to which I could also contribute with the knowledge gathered so far in the field of Tracing Science.

2. Content of the thesis

Chapter 1 – What is the Semantic Web?

Chapter 1 of this thesis, as is normally the case, is meant as an introduction to the field in which the research is carried out, in my case the Semantic Web. This chapter aims to present, explain to the reader the notions underlying the application domain considered. To this end the chapter started with the definition of the terms 'Internet' and 'World Wide Web', the presentation of the architectures and the explanation of their functionalities, what were the phases of evolution from iys inception and until present day. Then I went forward and presented the field on which I conducted my research, that of the Semantic Web. I put the emphasis from my discussions on its architecture with its levels each mapped to one (or more) technologies created and standardized by the group in charge of the realization of the complete project, the W3C. Here were presented the triad of fundamental technologies of sw, which are the URIs, the universal RDF data model and the language of ontologies representation, the OWL. Each of these will be picked up and discussed in more detail in the following chapters (especially in Chapter 2).

The next main point of the chapter was with the Application Domains, where I presented and explained in which branches of industry the project finds its greatest uses. Like any scientific review paper, because it cannot cover the entire field discussed, I presented 5 application areas that I considered to be the most important of those studied in the literature and I offered the reader references where he can find further knowledge that are discussed in other works in the domain.

Since from a scientific review paper couldn't miss a study about the current state of research in literature (state-of-art), I have made one also here, which is an important section of the chapter (the last one before the final conclusions). Here I presented and listed the most important achievements that have been made to support the development of the Semantic Web domain, being so many that we considered it better to put them in categories; thus I have talked about development environments for SW applications, systems for performing inferences (reasoning), deposits of triple RDF, transformers between data models (traditional-semantic, and vice versa), vocabularies of public ontologies in different fields. At the end of the section were made a series of comparisons, presented in tabular form, and analyses in textual form in relation to the capabilities that can be provided by the technologies of the two versions of the Web: the traditional and the Semantic one, the results of the analyses clearly showing the superiority of semantic technologies. During this review section, as normally, in addition to the issues discussed I have provided references in the literature where the reader can enrich his knowledge in that field.

Chapter 1, as happens with each chapter of the thesis, closes with a section of conclusions that very briefly presents the content of the chapter and the contributions made into it.

Chapter 2 – Logics as Support for the Semantic Web

This chapter aims to discuss the crucial role that logical formalisms play in the realization of processes on the Semantic Web, especially that of creating languages for the representation of ontologies. Web pages are annotated with some bookmarks that describe their content that can be understood by agents on the Web. These terms, along with their relationships, are defined in ontologies that are accessed by heterogeneous agents to establish a common and shared terminology, allowing agents to interpret the data correctly and unambiguously.

The first section of this chapter discusses the field of ontologies, which, as was said above, is the foundation of the Semantic Web. An ontology is defined as a formal specification of the conceptualization of a desired application domain, trying to capture important concepts along with the relationships between them. It is a technology for the representation of knowledge that is used especially in areas that require storing large volumes of data and performing inference operations on them, such as deflection, consistency checking, querying, etc. At the end of the section were briefly presented the most important languages that have been created for the representation of ontologies, from the beginnings of the field to the present.

The second (and most important) section of the chapter deals with the field of Descriptive Logics. These are logically based formalisms for the representation of knowledge in an application domain derived from The Logic of Order 1. First Order Logic - FOL) having as objective to keep the reasoning processes on the data indefinite (unlike FOL). Each language that is a member of the DL family is obtained from an already existing one by adding new builders of concepts and/or roles in order to represent new types of information, the most primitive being AL (Attributive Language), which contains only 3 constructors, namely that of intersection, value restrictions and existentiality. Here I have presented a table with 12 of the most important DL languages created in literature by the great scholars of the field. At the end of section 2 was presented what are the most important application areas of DL, with the emphasis of course on the most important, ontology languages. Quality Ontologies have a fundamental role on the Semantic Web, and their construction, integration and evolution depend on the existence of good semantics and powerful reasoning tools. Because DL's own both makes them ideal candidates for creating ontology languages. Here were presented 3 of the most important such languages existing today: DAML+OIL, OWL and OWL2, their syntaxes and semantics, the DL languages over which they were created, as well as a series of analyses and comparisons between the capabilities offered.

After section 2 in which was talked about DL and logical knowledge bases, in section number 3 I went ahead and discussed the next important feature of SW, namely the processes of performing reasoning and inference. There are two types of inference tasks in DL knowledge bases: standard and non-standard. The most common are satisfiability and subsumption, and they belong to the category of standard ones.

After presenting the tasks it also makes sense to talk about the algorithms created that perform these tasks and the industrial scale systems developed for the purpose of reasoning on the DL knowledge bases. The focus was on tableaux algorithms, which are the most important technique for performing reasoning tasks in DL. In order to demonstrate how a Tableaux algorithm works, I have provided an example for calculating the satisfiability of a concept in the ALCN language, to explain to the reader the functionality of this technique. The other two methods of reasoning, namely the one based on structural inclusion and the one based on automatics, not being as important (and older) than the tableaux technique, were discussed more briefly. The end of the section contains a list of reasoning results from standard tasks for some of the DL languages, collected from the resources in literature read by me in the realization of this chapter.

The last section of this important chapter (which is also the most extensive of the thesis) is, as expected, a literary study in which I recounted the most important resources I read from the literature on the field of Descriptive Logics.

The chapter ends with the final conclusions section, which summarizes its content.

Chapter 3 – Object-Oriented Reasoner for the Saturation of Logical Knowledge Bases

In this chapter is proposed a system of performing reasoning on a logical basis of knowledge represented in the syntax of logic of order 1 (FOL). The knowledge base, in addition to the usual ones (facts and rules of deduction) also contains a special type, constraints, which express the conditions that the data must meet in order to be put into the base. This is what sets our system apart from the currently existing ones.

The chapter begins with a section in which the general issues of the logical bases of knowledge and of all the processes that will be used along the way to build the proposed reasoning system, such as those of substitution, homomorphism, derivation, saturation, etc. are presented.

Section 2 does a study from the literature about existing projects, and the only systems with a functionality as close as possible to my needs are the business rule frameworks developed in the OO programming languages, among which: Drools, EasyRules, RuleBook, Jrules (I considered the ones from Java because I also created my system in this language).

Section 3 discusses the design and 4 the implementation of the proper system in which I built models of processes in the form of UML diagrams (classes, activity, objects), was explained how to represent the entities and the knowledge base in the object-oriented environment (its logical representation being in FOL) and detailed the functioning of the system where was explained how the calculations on the knowledge base were done (inference of new facts by applying the rules, verification of constraints in the ontological level). The techniques used in the implementation were Backtracking and Forward Chaining. I provided the reader with concrete examples of the realization of the inference process in the OO environment (application of the collection of objects of the type rules on the facts) in order to better consider the processes of performing calculations in the system.

The chapter concludes, as normal, with a section of experiments carried out with the system and comparisons with other similar techniques, the results taking into account the superiority of the proposed system in terms of the number of reduced calculations performed due to the use of search optimization techniques in the space of possible solutions, such as Backtracking, as well as optimization methods used in the logical inference process, such as Forward Chaining, all these are explained broadly into the chapter from the thesis and also provide reader with references in literature where he can enrich its knowledge.

Chapter 4 – Intrusion Detection and Prevention Systems

This chapter represents the beginning of the second part of my thesis which is about cybersecurity and the latest technologies used in building attack detection and prevention (IDPS) systems, among which of course are those of the Semantic Web, which is the core domain of my research.

The chapter commenced with an introductory section in which were presented the most important areas that require defense against cyber attacks, was stated what IDPS systems are and

I listed what technologies they use in the process of detecting attacks, what are the phases they have gone through in their evolution, etc.

Section 2 discusses the typical components in the composition of an IDPS system, which are the roles of each in the detection process. For this I created models in the form of figures for a better presentation of the issues discussed, in order to be better understood by the reader.

In section 3 of the chapter were discussed the security capabilities of IDPS systems, their 4 main responsibilities are: data collection from networks, logging, detection and (sometimes) prevention.

In section 4 I went to discuss the type of detection systems that are most important and that I will also consider further in this thesis, that of IDPS for networks. I resumed what was discussed in the previous 2 sections for their concrete case, namely the components (architectures) and security capabilities, all mapped to the case of detecting attacks from computer networks. Then were then presented what are the IDPS management capabilities for networks, which are under the task of security administrators. Administrators have the most important tasks to perform when deploying a security solution, as stated in all sources in the literature. They have 3 major responsibilities: implementation, operation and maintenance. The first phase says that after a network IDPS product has been chosen, administrators must create an architecture, test the components in isolation, secure the components, and finally deploy the IDPS. Each of these phases was discussed widely in the chapter, along with concrete examples and graphic models (figures) that better expose the procedures visually. The next stage concerns the possibility of operating IDPS by administrators through its visual console. Some systems also have command-line controls – CLI which, unlike user interfaces (GUI) that are normally used for remote control of sensors and servers, those are usually used in a local context. The console allows administrators to configure and update IDPS components (sensors and management servers and databases), as well as monitor the states they go through. The vast majority of IDPs allow administrators to create accounts for each type of user (admin or simple user) and provide only the necessary privileges for the role of each. The degree of control offered may differ from one product to another, depending on the degree of their performance and implementation. The last phase is the maintenance phase, in which administrators must perform tasks such as: checking at well-established intervals the operation of the system, applying software updates to the components received from sellers, receiving news from suppliers about security problems of IDPS, etc. Software updates can affect only part of the components or even the entire system, including sensors, management servers and consoles. Administrators must validate the integrity of updates before applying them because there is a possibility that they may be unintentionally modified or replaced.

Chapter 4 ends with the usual conclusions section in which the content is summarized and the contributions made by my research are presented to the reader.

Chapter 5 – Artificial Intelligence and Semantic Web Technologies used in Cybersecurity

This chapter is intended as a review one in which a series of discussions and analyses are made regarding the new and innovative technologies used in the construction of cybersecurity systems. These technologies are borrowed mainly from the field of Artificial Intelligence, where the most capable methods and algorithms for making different types of calculations from various fields are found, and more recently and again the emerging domain of the Semantic Web whic, as it has been showed previously, it is not too different from AI. The chapter consists of 2 parts. The first deals with the use of AI methods in intrusion detection and the second with Web Semantic.

Section 1 discusses the 5 technologies in AI that are most useful in the field of attack detection and prevention, namely:

- Evolutionary Algorithms, whose class includes Genetic Algorithms, Genetic Programming, Grammatical Evolution
- Fuzzy LOgic
- Clustering and Outliers
- Artificial Neuronal Networks
- Data Mining

For each of these 5 technologies in AI, the role they can play in the process of detecting attacks have been considered. Thus, Genetic algorithms are used in automatic model design, data classification and optimization, feature selection, etc. Fuzzy logic is a technique that is especially useful in analyzing and reasoning over incomplete or uncertain datasets, making them some important tools in analyzing and evaluating the risks of attacks. Cluster and orphan point analysis technology finds its most use in detecting anomaly-based attacks, where the former represent normal data and the latter are attack data. They detect intrusions from raw audit data (previously unprocessed), which makes the effort required to adjust the IDS less. The technique of NRAs is the core of machine learning science and, as can be easily realized, it can find applications in numerous and varied fields due to the many capabilities it has, such as making the right decisions, recognizing forms and patterns, etc. In the field of intrusion detection, neural networks are used in abnormality-based detection when creating and learning benign activity profiles from raw traffic data and perform detection by classifying new events based on created profiles. The last technique discussed in the first section, that of Data Mining, is useful in the field of attack detection especially in analysis, more precisely it is focused on reducing dimensionalities, classification and clustering, resulting, in the opinion of renowned researchers of the field, in increasing the speed and accuracy of detection, as well as strengthening the system's own security. This first section, in addition to the extensive discussions and analyses made in this area, also proposed some models of the detection processes based on the AI technologies discussed, models that were created in the form of graphic figures, as block diagrams of processes, UML diagrams of activity, in order to put into account and make the reader understand much better how things are going, as opposed to simple textual description.

Section 2 of the chapter talked about the newly emerging technologies of the Semantic Web that find their use in the field of IDS, of which the most important are those of 'content', 'ontology' or 'multi-agents'. Every security method that is based on the notion of content can use SW technologies, and intrusion detection systems are a good example of them. Some renowned scientists of Computer Science have opened a new branch in the field of information security, that of using ontologies along with their advantages. They stated that: "ontologies are an extremely promising new paradigm in the area of information security through which we have an unlimited event classification tool". The section proposed two tables in which are presented some of the most

important commercial and research IDS systems collected by me from the literature read, which use in the detection processes techniques from AI and SW.

The chapter, as expected, being one for review, also has a state-of-art section in which I presented the most important works read by me in its realization. It ended with the related conclusions section.

Chapter 6 – Ontology for Cybersecurity in Networks of Computers

In this chapter I proposed a model of the field of cybersecurity in the form of an ontology that can be used by IDS systems to detect the nature of potentially dangerous events. Ontology aims to describe the field of computer attacks capturing the most important concepts and the relationships between them. For its construction and evaluation were used state-of-art methodologies of literature, such as the ontology languages of the Semantic Web created by W3C (OWL2), or standard rule language (SWRL).

Section 1 is meant as an introduction that presents and defines the important notions used in the chapter, such as the types of IDs, the phases they went through in evolution, as specified in the field literature, what are the ontologies and what is their role in the construction of cybersecurity systems. Section 2 is a state-of-art with the most important works in literature read by me in the realization of this chapter.

Section 3 describes the construction of the ontological model. For this, of the many methodologies created in the literature, I have the ontology development 101 methodology, which is a process of building a 7-step field ontology, which I also followed for my model.

Section 4 presents the assessment of the proposed model. To test the ontology was taken an application-level firewall where the ontological model is kept in the knowledge base from where it is accessed by the firewall through inferences to detect the nature of the newly occurring events. The fact that it is based on semantic rules makes the model more efficient in terms of execution times by providing a substantial reduction in the search station and achieving lower rates of false positives. For the evaluation I used the OntoClean methodology, which has a total of 15 evaluation criteria, as stated in the literature, but I chose 8 that I considered to be the most important for my case.

In section 5 I showed and explained how ontology is incorporated into the IDS firewall and how it is accessed by it in the process of detecting the nature of newly emerging situations. I worked on an example of a Cross Site Scripting attack and showed every phase that this time goes through the IDS system, from the input to its journaling as both known. Section 6 presents the experiments done with our detection system. For testing the Kyoto2006+ attack dataset was used, which is the best set for this purpose. My system based on semantic technologies I compared them with the two systems in the literature, namely Snort and ModSecurity, the results obtained after 3 metrics, namely Precision, Recall and F-metric showed a slight superiority of my system regarding the efficiency of detection and false alarm rate.

Chapter 7 – Intrusion Detection System based on Semantic Web and Artificial Intelligence Technologies

In this chapter was proposed a distributed IDS system for networks that uses the latest and most innovative technologies borrowed from the fields of Artificial Intelligence and the Semantic Web with the aim of increasing the efficiency of detecting real attacks and decreasing that of errors. The main objective of this distributed IDS is to solve the problems of the centralized ones involving a multi-agent architecture in which each agent has certain tasks to perform. The knowledge base is represented in the form of an ontology that captures the terms in the field of intrusions and their relationships, and is used by agents to detect the nature of the events received (normal data or attacks). One of the most important functions of the system is the possibility of detecting previously unknown attacks (Day-0), which is implemented by the agent performing anomaly-based detection.

Section 1 is an introduction in which was presented the important notions that will be used throughout the chapter. Also, the disadvantages of the centralized IDS were considered, such as that of the single point of fall (represented by the central node), namely if this node is attacked then the entire IDS falls, or the problem of overloading the network due to the transfer of information from all the sensors placed in various places on the network and up to the central node; this is called the scalability problem of systems.

In section 3 I presented the component architecture of my system, and I detailed each agent what function it has. In 4 I talked about the functions of ontology for attacks, having the role of a more optimized knowledge base and containing more intelligence in content analysis. It contains mirrors that allow a semantic representation that favors the processes of inference and reasoning. The rules are extracted from ontology using the standard language of the Semantic SWRL Web, which expands ontology and enriches its semantics through deductive reasoning capabilities. Then I gave an example of the SWRL rule of ontology, what structure and syntax it has. and how it is railed by the system to produce consequences. Section 5 discusses the clustering algorithm used in the detection of anomalies, which is one based on the well-known K-means in Data Mining.

This chapter concludes, as is normal, with a section where I tested my system. I evaluated the performance of the IDS according to 2 metrics: scalability and detection. Network attacks were simulated using Metasploit 3.5.1 tool, which generated the following attacks: Smurf, Backdoor, Spyware Put Hijacker, Nmap TCP Scan, Finger User, RPC Linux Statd Overflow, DNS Zone Transfer, HTTP IIS Unicode. During the evaluation process I compared the results of my system with those of the centralized IDS Snort and the one distributed to MONI, which show the superiority of the proposed architecture.

3. Conclusions, Personal Contributions, Research Capitalization through Publications

The research carried out in this thesis, as it has been affirmed since its title and numerous times along the way, has had as objectives to contribute and help the development of the new generation of web, published in the early 2000s, which is intended to be one of universal structured data and automatic execution of processes, which, as we can also tell from everyday life, represents the future in the industry. Everywhere we see cars and devices that have taken the place of people in carrying out tasks, such as those for the issuance of travel tickets from train stations, bus stations, electronic systems for payment of travel in means of transport by card, without requiring tickets, automation payment systems in supermarkets / hypermarkets that in

the last 2-3 years have stormed these stores, and the examples can continue. This also happens with the World Wide Web, the most important and used service in the Internet.

The issues that have been created in this thesis aimed at contributing to the development of the field under research are of two kinds:

- reviews of different areas in the Semantic Web field in which were presented, defined the notions underlying that area, made analyses, comparisons, stated personal opinions about them and offered the reader, for each notion / definition, references in the literature where he can find more information about the issues discussed in the chapter
- building new and innovative systems by combining technologies taken from other fields of Computer Science in order to solve existing problems in a certain field

The first class of contributions includes chapters 1, 2, 4, and 5, where I focused my attention on the following areas: Logical formalisms of knowledge representation, Cyber defense systems, Innovative technologies used to build IDS systems, and, of course, presentation of the main field of the present research, namely the Semantic Web.

The other category includes Chapters 3, 6 and 7, where I have built new systems and methods for solving open problems in certain areas. In the first I created a reasoning system to make inference on a special type of knowledge bases composed of three types of knowledge (facts, rules, constraints). In the second I have created a model of the field of computer security proposed in the form of an ontology that aims to capture as much domain information as possible together with the relationships between the concepts, thus leading to the increase of the detection capacity of the IDS system and to the decrease of its error rate. In the last chapter I wanted to continue the work done in the previous 2, which are all about the field of cybersecurity. Here I have built an attack detection system in computer networks that uses new and highly efficient technologies in the fields of Artificial Intelligence and Semantic Web in order to create the problems faced by today's IDS, in particular, the low detection rate of real attacks, the mistakes of detection, the impossibility of detecting attacks never seen before (Day-0), as well as the strengthening of the system's own security.

My personal conclusion at the end of this thesis is that I have met the objectives that I have initially set for my present research, I have made contributions to the researched field (those listed above), which is also proven by the 15 international publications that I have achieved during my PhD studies. It is true that out of all 15 most of them are review papers of some component areas of the main studied field, the Semantic Web, but they also contain the results of my work, those of presenting the field in question, the realization of literary studies in which they discuss what has been achieved in the literature by others, analyzes are made, comparisons, etc. Three of the review papers are about Descriptive Logics, which were discussed in chapter 2 of the thesis, one is about the field of my research, the Semantic Web, and another one about another field, related to the Semantic Web and which has experienced a relatively similar evolution to it in recent decades, namely the Internet of Things. Two other works deal with the field of Artificial Intelligence, in which I analyzed the most important human cognitive function that distinguishes us from the most evolved other primates: communication (verbal or written). Among the works that proposed new systems and/or techniques are the creation of a cybersecurity ontology, a reasoning system for a special type of knowledge base, and a distributed IDS system based on technologies taken from the fields of Artificial Intelligence and Web Semantics. The full list of my scientific publications can be found in the thesis in the reference section, for more details.

BIBLIOGRAPHY

[1] F.Abdoli, M.Kahani; *Ontology-based Distributed Intrusion Detection System*, Proceedings of 14th International Computer Conference (CSICC), Teheran, Iran (2009)

[2] N.Agarwal, Z.Hussain; *A Closer Look at Intrusion Detection Systems for Web Applications*, Hindawi Journal on Security and Communication Networks, vol.2018

[3] G.Antoniou, P.Groth, F.v.Harmelen, R.Hoekstra; *A Semantic Web Primer*, MIT Press (2012)

[4] M.d'Aquin, E.Motta, M.Sabou, S.Angeletou; *Toward a New Generation of Semantic Web Applications*, IEEE Intelligent Systems, vol.23,no.3, pp.20-28 (2008)

[5] A.Aviad, K.Wecel, W.Abramowicz; *The Semantic Approach to Cybersecurity – Towards Ontology-based Body of Knowledge*, Proceedings of the 14th European Conference on Cyber Warfare and Security (ECCWS,2015)

[6] F.Baader, D.McGuiness, D.Nardi, P.Schneider; *The Description Logic Handbook: Theory, Applications and Implementations*, Cambridge University Press, New York, USA (2003)

[7] T.Berners-Lee; *WWW: Past, Present and Future*, IEEE Computer Magazine, vol.29 no.10 (1996)

[8] T.Berners-Lee, R.Cailliau, J.Groff; *The World Wide Web*, Communications of the ACM (1994)

[9] T.Berners-Lee, M.Fischetti; *Weaving the Web*, Ed. Harper-Collins, San Francisco (1999)

[10] T.Berners-Lee, J.Hendler, O.Lasilla; *The Semantic Web*, Feature Article, Scientific American (2001)

[11] T.Berners-Lee, R.Swick; *Semantic Web Development,* Technical Report AFRL-IF-RS-TR-2006-294, New York (2006)

[12] T.Berners-Lee, J.Hendler, *From the Semantic Web to Social Machines: A research challenge for AI on the World Wide Web*, Journal of Artificial Intelligence, vol.174 no.2 (2010)

[13] I.Brahmi, S.Yahia, H.Aouadi, P.Poncelet; *Towards a Multi-agent based Intrusion Detection System using Data Mining Approaches*, Proceedings of 7th International Workshop on Agents and Data Mining Interaction (ADMI), pp.173-194, Taipei,Taiwan (2011)

[14] N.Dalwadi, B.Nagar, A.Makwana; *Semantic Web and Comparative Analysis of Inference Engines*, International Journal of Computer Science and Information Technologies, vol.3, pp.3843-3847 (2012)

[15] F.Donini, F.Massacci; *Exp-Time Tableaux for ALC,* Artificial Intelligence, vol.124, no.1, pp.87-138 (2000)

[16] D.Fensel, J.Hendler, H.Lieberman, W.Wahlster; *Spinning the Semantic Web: Bringing the Web to its Full Potential*, MIT Press (2003)

[17] F.v. Harmelen, V.Lifschitz, B.Porter; *Handbook of Knowledge Representation*, Foundations of Artificial Intelligence, Elsevier (2008)

[18] I.Horrocks, P.Schneider; *Knowledge Representation and Reasoning on the Semantic Web: OWL*, Handbook of Semantic Web Technologies, pp.365-398, Springer (2011)

[19] J.Pan; *Desciption Logics: Reasoning Support for the Semantic Web*, PhD thesis, Univ. of Manchester (2004)

[20] A.Razzaq, Z.Anwar, F.Ahmad, K.Latif, F.Munir; *Ontology for Attack Detection: An Intelligent Approach to Web Application Security*, Computers&Security, vol.45, pp.124-146, Elsevier (2014)

[21] K.Scarfone, P.Mell; *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Recommendations of the National Institute of Standards and Technology (NIST), Special Publication (2007)

[22] M.Schmidt-Schaus, G.Smolka; *Attributive Concept Descriptions with Complements*, Journal of Artificial Intelligence, pp.1-27 (1991)

[23] N.Shadbolt, T.Berners-Lee, W.Hall; *The Semantic Web Revisited*, IEEE Intelligent Systems, vol.21, pp.96-101 (2006)

[24]J.Song, H.Takakura, Y.Okabe; *Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation*, Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, pag.29-36, Salzburg, Austria (2011)

[25]Y.Zhu; *Attack Pattern Ontology: A Common Language for Cyber-Security Information Sharing*, TU Delft Publication, Master Thesis (2015)