Use of Foundational Ontology for mapping of Vulnerabilities: A Perspective for IaaS Service in the Public Cloud

Rita de Cássia C. Castro[1], Hedwio Carvalho e Silva[2], Anilton Sales Gracia[3], Marcos José Negreiros Gomes[4]
[1]Federal Institute of Education
Science and Technology of Ceará (IFCE)
[2]Professional Master in Applied Computing
University State of Ceará (UECE)
[3]Lab Tel – Telecommunications Research Laboratory
Federal University of Espírito Santo (UFES)
[4]University State of Ceará (UECE)
ritacastro@ifce.edu.br, hedwio@gmail.com, Anilton@inf.ufes.br, Negreiros@graphvs.com.br

ABSTRACT: *In the present days, business applications are still designed for human consumption, which does not allow machines to understand the information contained in them, particularly preventing the correlation between concepts from different fields, in the generation and submission of new information for the handling of large data sets. The increasing complexity of applications, increases the attention in the construction of knowledgeable systems that can be understood and shared by all (application / machines / people). Using the concept of Ontology as a tool for knowledge representation has been effective, in order to develop applications with these said characteristics, since the semantic models have the ability to map and integrate different concepts from the same domain or different domains of knowledge, related to each other, therefore providing conditions for understanding the information contained herewith. Presently, there are different proposals for the aforesaid mapping, considering the semantics and ontological integrations, as well as interoperability of the information systems. This study presents a conceptual modeling in domain knowledge, about the potential vulnerabilities in environments, IaaS, in the public cloud, as a scenario using ontology reasoning. The purpose this modeling, is to provide an effective mechanism, capable of handling two major security issues, such as: providing a common vocabulary to describe vulnerabilities unambiguously and resolving the issue of semantic interoperability between the databases of vulnerabilities maintained by various entities.*

Keywords: Cloud Computing, Public Cloud, Vulnerabilities, Ontologies, Conceptual Models, OntoUML

Received: 2 June 2012, Revised 21 July 2012, Accepted 26 July 2012

1. Introduction

Understanding the importance of cloud computing, in order to learn to deal with this trend, is now a major challenge that presents itself to the corporate world. The technology that makes up the cloud, is the result of evolution and the meeting of technical fundamentals in areas such as the Server Virtualization, Grid Computing, Software-Oriented Services, Management of large facilities (Data Centers), among others. It is an efficient technology, regarding to the use of software access, storage and

data process, across different devices and web technologies. In practice, it would be the transformation of physical computer systems in a virtual base, with the ability to provide computational resources with features that differentiates them from other technologies.

With reference to the adoption of the Cloud Services process business procedures, it is necessary to take into account the security and the privacy of the information that will be in the cloud. Hence, it is necessary to have adequate in the security of the information, in order to assist the establishment of guidelines for the usage of services having a Cloud with acceptable safety levels, in accordance with the nature of the transactions.

Several studies [1], [2] and [3], showed the use of ontologies as a tool for achieving semantic interoperability through the formal structure for terms in a particular domain of knowledge. However, it is understood that an approach involving the use of ontology for the mapping of vulnerabilities in contrasting environments, IaaS (Infrastructure as a Service), the model of the Public Cloud is able to represent a contribution in the search for mechanisms that promote the standardization of aspects related to safety in this particular scenario. Therefore, the goal is to catalog information about vulnerabilities in these stated environments, in order to allow automated tools making the correlation in various sources of information.

The primary motivation in this proposed ontological model, is to outline an initiative towards the interoperability of storage and disclosure of the new vulnerabilities in the computer environments, such as bases maintained by the Research Institutes CERT (Computer Emergency Response Team / Coordination Center) and the CVE (Common Vulnerabilities and Exposures), which will enable organizations to reduce the uncertainties associated with the active information service models, in the adoption of the IaaS public cloud.

These ideas lead to the identification of potential users in ontology, since this will serve as coping mechanisms for IT managers in decision making, when planning for adoption of the Cloud Computing. Based on its essential purpose, the ontology modeled herewith, which can also be used by specific applications, as oriented semantic models, duly developed by manufacturers of solutions for the identification and monitoring of vulnerabilities in computer environments.

The main objective of this study is to present the description of a stage terminology for the conceptual modeling in an ontology mapping, focused on the possible vulnerabilities of a scenario in the Public Cloud delivery model (IaaS) services, in order to assist the definition of guidelines for the consumption of Cloud Services, having an acceptable level of safety in accordance with the policies for the security of the organization's information.

This particular study, is structured as follows: the introduction is presented briefly on the general aspects of Cloud Computing; Section 2 presents the main works that contributed to the development of this article; Section 3 presents the relevant aspects of the ontology construction; Section 4 deals with aspects related to vulnerabilities in the IaaS environments; Section 5, proposes a model and in Section 6, it deals with the completion of this study.

2. Related Works

In the context of Vulnerability Management Services in the adoption of a deployment template Cloud duly observed, the research settings comprises differently, even though the work which is rare, if not nonexistent, however in its ratings, defines an ontological model for the application in this context, providing adequate support for decision making at the time of contracting a Cloud.

Grobauer [4], is a well-founded assessment of an impact on security in Cloud Computing, through the analysis of important factors, for instance, the new vulnerabilities associated with this model. This said paper defines four indicators of vulnerabilities in the Cloud and proposes a security architecture for this specific environment. The study also provides examples of specific vulnerabilities for each component in the architecture of the Cloud.

In the study entitled "*Cloud Computing and Information Policy: Computing in a Policy Cloud ?*" [5], shows the absence of information policies as the main problem in hiring a Cloud, listing issues such as privacy, security, reliability, access and regulation, as being critical natures. The work explores the nature in the vulnerable Cloud Computing and its technological evolution without identifying possible vulnerabilities in a specific model.

Rimal [6] presented a comprehensive taxonomy for describing the architecture of Cloud Computing. The authors arrived in a taxonomic model of multiple Cloud Services by mapping existing design features, such as Google, Amazon and force.com. The taxonomy presented in this study, was used to identify similar features in different architectural approaches of Cloud Computing and its identifying areas, which requires further investigation.

The contributions of the work from Youssef [7], represents one of the first attempts to establish a detailed ontology of the cloud, proposing an ontology of Cloud Computing that allows the community to have a better understanding of the technology in question. This author proposed a detailed ontology for the Cloud in an attempt to establish the domain knowledge of the Cloud and its relevant components, along with the method of composition for the construction of an ontology, which allowed the capture of relations between its different components.

Brandão [8], proposed the use of ontology to classify known vulnerabilities, introducing basic concepts of ontology, advantages of computer security and a methodology for creating an ontology, which presented vulnerability implemented, using the OWL language.

As a result of an extensive study, ENISA (European Network and Information Security Agency), published in late 2009 [9], a document on various models of consumption with Cloud Computing, listing its benefits, risks and especially their vulnerabilities. This document has become a reference guide to the hiring of services to the Cloud. The ontological model proposed in this particular study, was populated mainly with information about the vulnerabilities and the affected assets described in the study duly published by ENISA. This study indicated that some characteristics, such as the mass concentration of resources and data in the Cloud, is an attractive target for attackers.

Almeida [10], highlights the importance of classifying information in a corporate environment for security purposes. The study shows the use of ontologies as an alternative and introduces the terminology of a domain for ontology information security. The study also presents a classification of vulnerabilities in computing environments, where most of the concepts originate in glossaries and taxonomies for information security and vulnerability databases, as maintained by NIST, called NVD (National Vulnerability Database) and CVE (Common Vulnerabilities and Exposures Project).

3. Ontology Engineering - Theoretical Basis

Several studies have proposed methodologies for developing ontologies for use in computing systems, as observed [11], [12] and [13]. An ontology defines a specific vocabulary used to describe a certain reality, plus a set of explicit decisions, setting accurately the intended meaning to the vocabulary.

An ontology involves a vocabulary of representation, which captures the concepts, relationships and their properties in any area, and a set of axioms that constrain its interpretation. However, [11] observes that there is fully mature methodology for the purpose of ontology construction.

In each approach there are activities that are no longer understood. According to the authors, a combination of methodologies is interested in the process of ontology construction. In [14], the development of ontologies is a complex activity and, therefore, to build high quality ontologies, it is necessary to adopt an engineering approach. Thus, the construction of ontologies to appropriate methods and tools used.

The methodology for building ontologies called SABiO (Systematic Approach for Building Ontologies), proposed by [12] scheme is based on methodology proposed by [15] and is enhanced by features such as presenting a graphical language for expressing ontologies, a classification of axioms, also addressing the issues of skills addressed by [16], which refers to questions that the ontology should be able to answer. They define the scope and purpose of the conceptualization of the field, and support the evaluation activity of the ontology. The main activities that the methodology includes SABiO are: (i) identification of purpose and specification requirements, (ii) capture of the ontology, (iii) formalization of the ontology where the concept is captured explicitly represented by means of a formal language, such as definitions of formal axioms using First-Order Logic, (iv) integration with existing ontologies, and (v) evaluation and documentation of the ontology.

The characteristics listed above provide a set of procedures that allow the capture of knowledge for the modeling of the domain under study, trying to maintain compatibility (integration) with pre-existing ontologies.

The strategy for development of ontologies used in this work do not fully follow the steps laid down by the SABiO method, although some steps to save the procedures set forth herein.

Each step in the development of an ontology has its specific objectives and therefore requires different types of methods and tools to meet their specific characteristics. In a phase of conceptual modeling ontology should strive for expressiveness, clarity and accuracy in representing the concept of the field [2]. The product description of a domain, obtained using a representation language, is called Conceptual Model. The virtue of a conceptual model is to be open to interpretation by a human being, that even not knowing the area (but knowing Ontology Grounds used), could interpret the model information and share knowledge described here [3]. The stage of modeling of an ontology language requires the use of specialized able to approach as much as possible the ideal field of the ontology. The same conceptual model can give rise to many different implementations, in different languages [2].

3.1 Foundational Ontology

A Foundational Ontology (also known as the High Level Ontology) promotes the concept of the most basic and potentially present in any domain (e.g., The relationship any part existential dependencies and categorization) [17]. Representation languages derived from ontologies and reasoning have developed the ability to adequately describe a wide range of areas. The Ontology of Reasons together results in a system of Formal Ontology categories independent domain (e.g. Concepts as part of the whole paper, and event), used to articulate concepts of various fields.

The Unified Foundational Ontology (UFO) proposed by [18], has been developed based on a number of theories in the areas of Formal Ontology, Philosophical Logic, Philosophy of Language, Linguistics and Cognitive Psychology [19]. The UFO tries to address the limitations in the ability to capture the basics of conceptual modeling languages and ontologies for other reasons, such as DOLCE (*Descriptive Ontology for Linguistic and Cognitive Engineering*) and GFO (*General Formal Ontology*). UFO's proposal is precisely to unify these ontologies, taking advantage of their positive characteristics and remedying the limitations detected [18]. This paper particularly interested in a part called UFO-A, which defines terms related to structural aspects such as general concepts of objects, their intrinsic properties and relational types they instantiate the roles they play, etc.. The specifications built using the concepts of UFO are more expressive and accurate than a specification represented by UML (Unified Modeling Language), for example. In [20], the advantage of having more precise specifications and expressive is the sharing, reuse, understanding and learning the appropriate domain knowledge and the ability to operate semantically with other systems. However, all these advantages are achieved by sacrificing the decidability (answer in finite time) and computational efficiency. These characteristics are very important when you want to use these specifications in processing machines [20]. Generally speaking, the UFO has been applied successfully to evaluate, (re) design and integrate models of conceptual modeling languages, as well as to provide real-world semantics of their model elements [18].

Not part of the scope of this work to deepen the study of all the layers of reasoning ontology UFO. Further details on key aspects of the UFO can be found in [18] and [19].

In order to allow a general understanding of the ontology presented and the models constructed, only a few relevant concepts of UFO-A will be described. The UFO-A is an ontology Endurants, covers the concepts of objects, properties of objects and relationships between objects, Figure 1 illustrates one of its fragments. What characterizes the Endurants is that they do not have temporal parts and persists over time while maintaining their identity.

Endurance is present, all its temporal parts are present. The basis of this ontology is the pairs of categories-Substantial Substantial Universal (Object-Object Univeral) and Moment-Moment Universal.

All elements of the UFO specializes the fundamental concept of UFO-A named Entity. The main distinction of the UFO is among the categories of individuals (private) and Universal. The former are entities that exist in reality and have a unique identity (e.g. the car of Joseph, brother of Mary, I used the keyboard to write this work). The latter, in turn, are entities that are independent space-time patterns of features (e.g. A person, a car, a keyboard, a house). The Universals can be instantiated in various Particulars. Each is thus a universal instance. With regard to subjects (private), there are specific individuals (Concrete Private) and abstract (Abstract private). Individuals lasting (Endurant) are specific types of individuals that can be categorized into: Substantial, ways and Situation.

3.2 Conceptual Modeling with OntoUML

OntoUML (Ontological Unified Modeling Language) is the name given to the version ontologically well-founded (Class diagram)

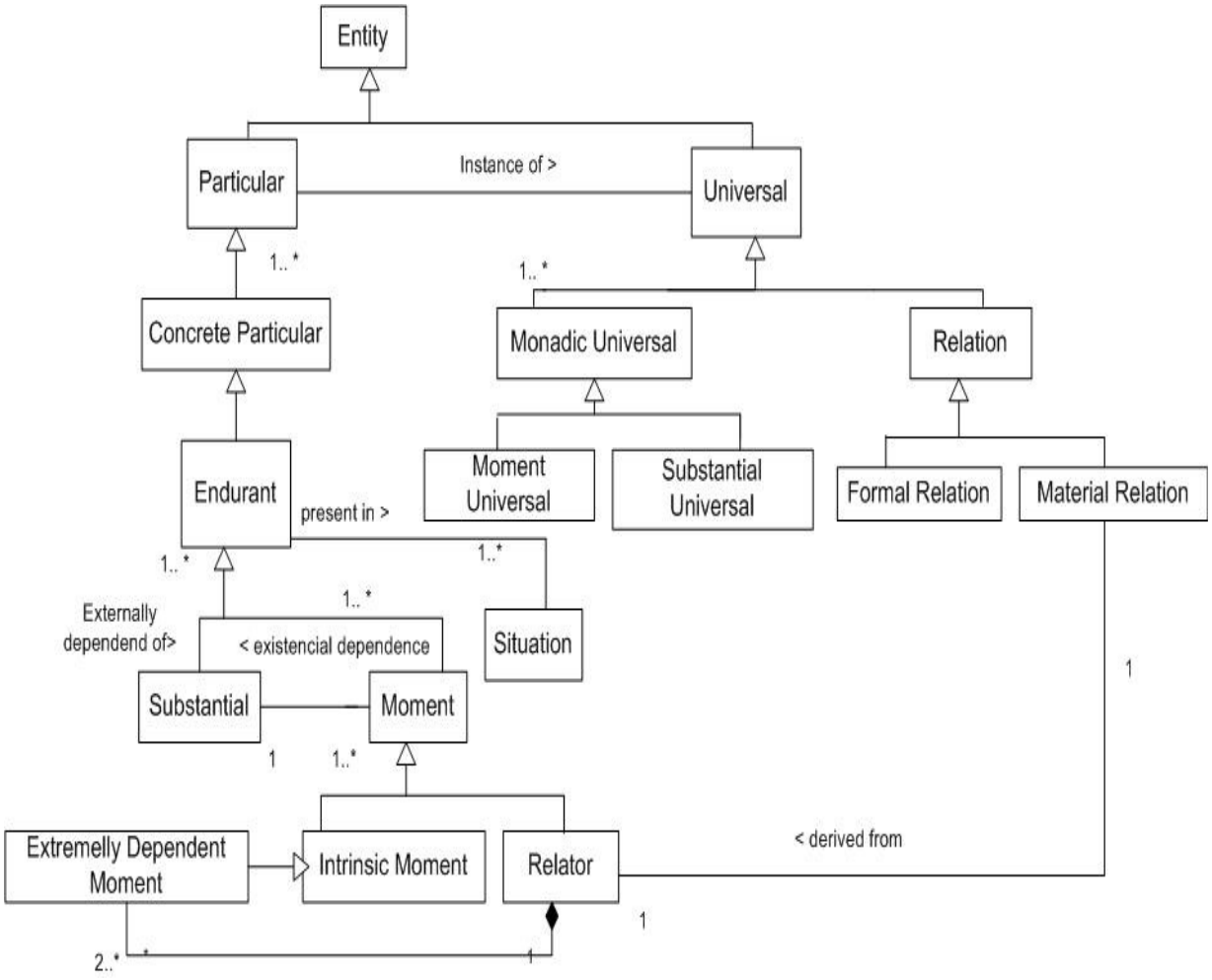

Figure 1. A fragment of the ontology UFO-A [18]

UML 2.0 (Unified Modeling Language), proposed by [18]. The author shows that lack a precise definition of formal semantics of UML, and this extends the metamodel to be isomorphic to the UFO-A, making it ontologically consistent. The UML has extension mechanisms which affect the language elements such that a coherent set of these extensions is a UML profile. The OntoUML is therefore a UML profile comprises a set of stereotypes ontological categories that represent the type of the proposed universal UFO-A, as well as constraints reflecting the formal axiomatization of UFO such that it restricts the set of OntoUML grammatically valid models in those situations that represent eligible according to the UFO theory [3]. Thus, the explanation of the application of stereotypes is identical to the universal application of the corresponding types of UFO.

To understand the security vulnerabilities presented in Cloud Computing, it is important to understand the relationships and dependencies between the models and their implementation services. The IaaS service is the foundation of all cloud services and other service models, built into its base. Figure 2 illustrates this feature through the diagram of the Reference Cloud, drawn up by the Cloud Security Alliance. As the capabilities are inherited, the integration between the layers are also inherited in the issues of information security and its vulnerabilities.

The IaaS service includes all the features in the infrastructure stack from the premises until the hardware platforms that reside in them. It incorporates the ability of abstract resources (or not) to provide physical and logical connectivity to these said resources. This service also provides a set of APIs (Applications Programming Interface), allowing management and other forms of interaction in the infrastructure for the consumers.

The aforesaid architectural model level (IaaS), is the basis for all other models providing a service (PaaS and SaaS), and the lack

of security at this level will certainly affect the models built on it. The usage of Virtualization, for example, allows providers to Cloud Computing, maximizing hardware utilization, switching multiple VMs (Virtual Machine) of consumers in the same physical infrastructure. Another important point is that IaaS providers, offer services sharing the same physical infrastructure.

4. Modeling Proposal

The ontology of possible vulnerabilities in environments (IaaS), is modeled for the purpose of representing knowledge about failures (technical failures and administrative and/or governance), in the infrastructure provided by the Public Cloud, in order to obtain the advantages of a model using ontologies, for instance, common vocabulary, taxonomy, sharing and reuse. Another purpose for the creation of possibilities in ontology is the interoperability of data storage and dissemination of vulnerability, using semantic models.

Figure 3 illustrates the steps followed for the construction and modeling of the ontology presented. The procedures followed in the steps of the Domain Identification, Requirements Specification and Domain Conceptualization, following the methodology SABiO, discussed above.

The Competency Questions (CQ), set the stage for Requirements Specification, defined a lead to a scenario that correlates concepts related to vulnerability management and the inherent concepts in the IaaS environment, specifying requirements. After jurisdiction, there is an effective mean of defining what is relevant to ontology and what is not.

Furthermore, specifying a relationship between the issues of competence and motivation scenarios, is giving a justification for ontology, particularly providing a mechanism for evaluation [18], hence, the proposed ontology established the following questions of competence:

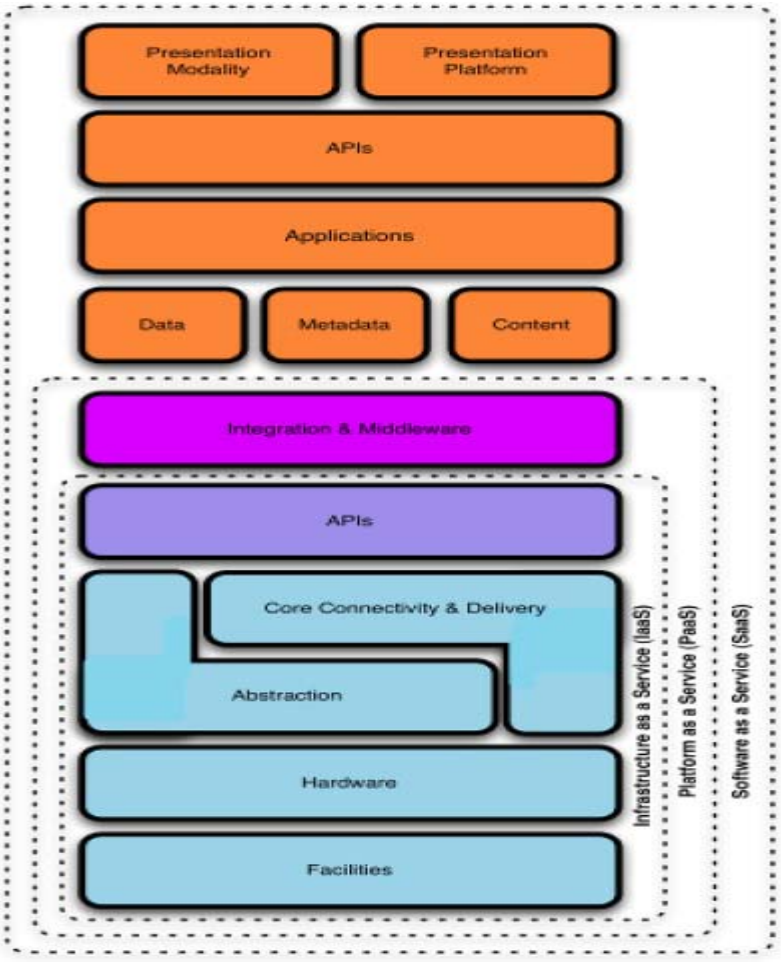

Figure 2. The diagram of the Reference Cloud

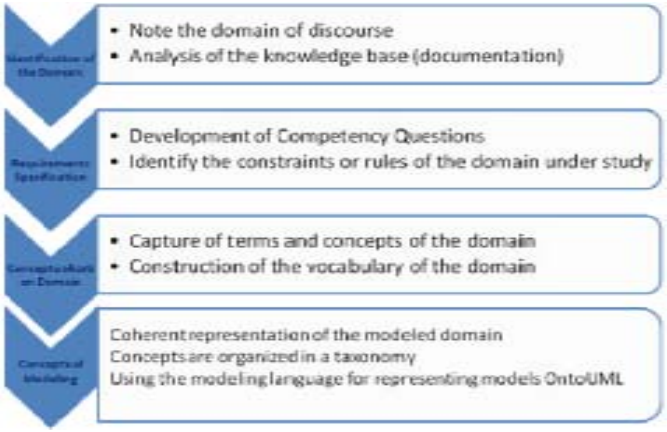

Figure 3. The steps followed for the construction and modeling of the ontology

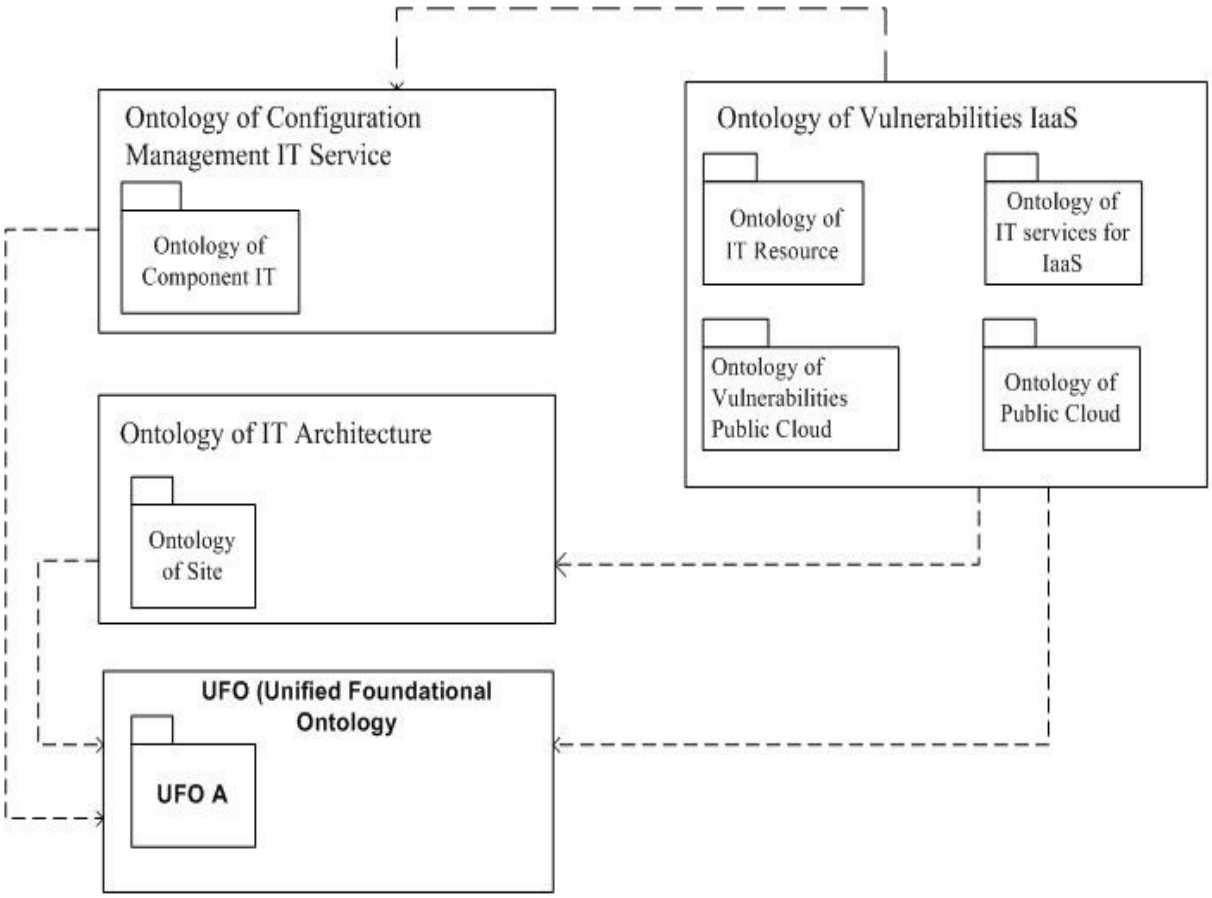

Figure 4. The ontology of Vulnerabilities IaaS and its dependencies with the ontologies used

QC01: What kind of services does the IaaS environment provide?

QC02: What are the basic characteristics of the IaaS environment?

QC03: What types of vulnerabilities exist in the environment of an IaaS public cloud scenario?

QC04: What assets are involved in the provision of an IaaS environment and how threats could exploit vulnerabilities in this said environment?

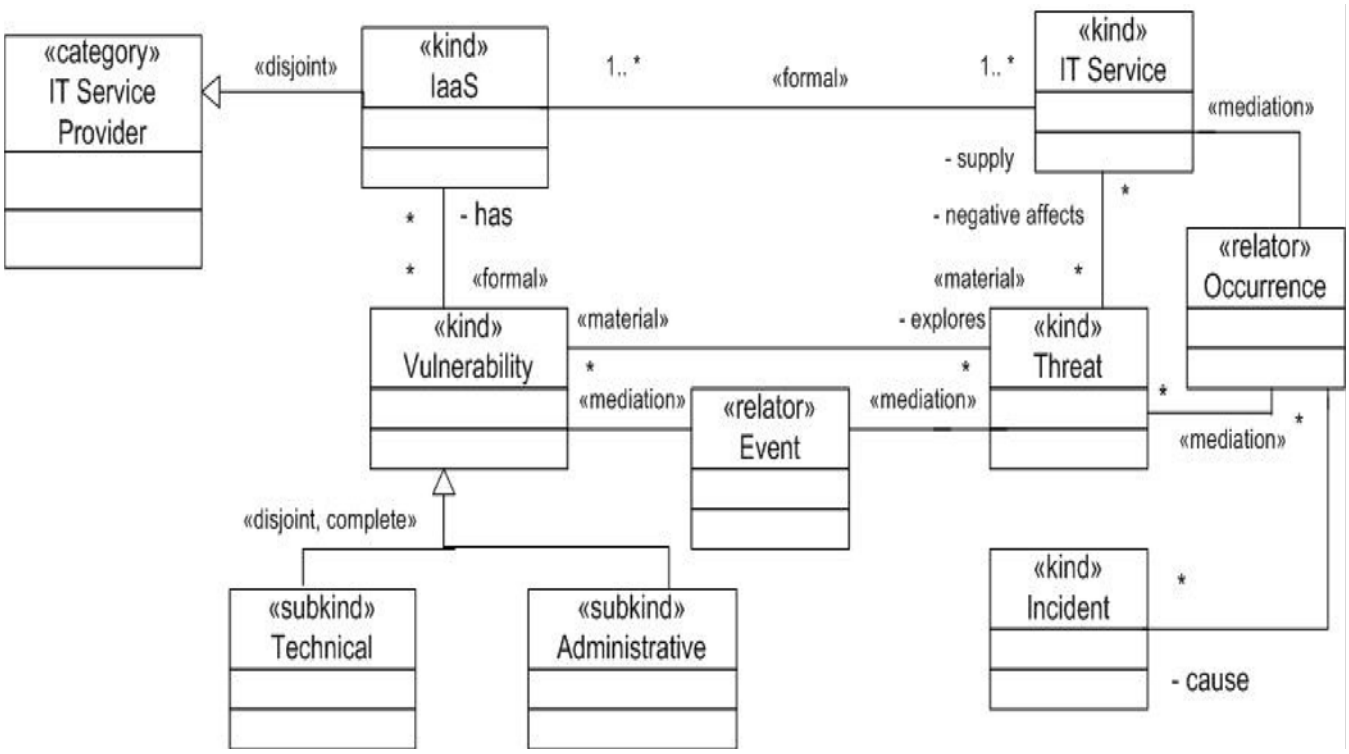

Figure 5. Ontology of Vulnerabilities in the Public Cloud

Class - Vulnerability
Subclass – Administrative
Incorrect modeling of environmental
Lack of a process for vulnerability assessment
SLA clauses conflicting with poorly defined
Audit not available to customers
Certification systems not suitable for cloud
infrastructure
Policies on use of resources poorly scaled
Storing data in multiple jurisdictions and lack of
transparency on this
Lack of transparency in terms of use

Table 1. Hierarchy of the Classes - Ontology of Vulnerabilities in the Public Cloud

QC05: What type of event may jeopardize the safety of the IaaS environment?

The responses generated by jurisdictional issues, relate to the following sub-ontologies: (i) Sub-ontology of IT services to in IaaS; (ii) Sub-ontology of IT resources and (iii) Sub-ontology Vulnerabilities in Public Cloud. These stated subontologies complement each other in relation to the formation of ontology vulnerabilities in the environment of an IaaS Public Cloud. However, since IaaS environments are directly related to the provision of IT services, other ontologies in this area, were

Class - Vulnerability
Subclass - Technical
Mechanisms for authentication and authorization disabled
Unsafe storage of credentials
Credentials stored in a machine transient
The customer cannot control the process of supply
Credentials are still valid canceled due to delays in implementation of the repeal
Remote access to management interface
Faults in hypervisor
Lack of resource isolation
Fault isolation reputation
Lack of encryption for data in transit
Processing of data is not encrypted
Lack of technological solutions and standards

Table 2. Hierarchy of the Classes - Ontology of Vulnerabilities in the Public Cloud

examined in order to check the reusability of concepts. Thus, the following ontologies were investigated:

a. Ontology of Configuration Management / IT Service: [2], proposes an ontology of the domain service management in IT governance. This ontology will be reused the concepts of IT component, specifically the concepts related to hardware and software.

b. Ontology of IT Architecture: proposal [21], presents a vision of the IT architecture from the continuity of IT services, based on standard PAS77. This ontology will be reused the concept of IT component. Figure 4 shows the relationship between these ontologies. Moreover, since the ontology of vulnerabilities in IaaS is based on ontology UFO, Figure 4 also shows the interaction between these two ontologies.

The following section presents the resulting process of analyzing the answers of Questions of Competence. This step is called Conceptualization of the Domain, where the relevant terms and concepts are captured, using a knowledge base of pre-established. The ontology is proposed here consists of various models, as described in Figure 4, therefore, for reasons of space, will be represented in this article only model the Ontology of Vulnerabilities in the Public Cloud (Figure 5).

The definition of classes and class hierarchy of the Ontology Vulnerabilities in the Public Cloud, are presented in Tables 01 and 02. The terms are placed into hierarchies so that the more general are specialized in more specific terms. Therefore, it is a combination of strategies used top-down and bottom-up, according to the presented in [13]. That is, the main concepts are defined first and were refined and / or generalized to the definition of other classes.

5. Conclusion

This study presents a conceptual model of the domain vulnerabilities in an IaaS environment. It was developed based on an engineering approach in ontology. The methods and techniques used the methodology of the Wise (Systematic Approach Building Ontologies). This approach used an ontology philosophically well-founded, namely the ontology UFO (Unified Foundation Ontology).

The purpose of this conceptual model is to allow a common understanding in the shared conceptualization of a modeled domain among different stakeholders, such as business, people, processes, tools and technologies. A formal specification in the domain vulnerabilities for IaaS environments, allows the modeled concepts to be understood clearly and explicitly, in order to avoid ambiguity and inconsistent interpretations. It is important to emphasize that the ontology UFO, played an important role in the development of the conceptual model presented in this study. It is helpful building a conceptual model committed to maximizing expressiveness, clarity and truthfulness concerning a modeled domain. These characteristics are key qualities attributing to a conceptual model, being responsible for theeffectiveness in a model as a framework of reference to the tasks of semantic interoperability and the reusage [3].

The domain ontology that results from this study, may support the efforts of experts in bettering design security issues for Cloud Computing environments. Among the forms of contribution, the following is quoted:

i) The creation of conceptual models that enable the adoption of Cloud Services safely;

ii) The identification of solutions in a scenario of a security incident in the Cloud;

iii) To promote semantic interoperability between different databases, storage and disclosure of vulnerabilities;

iv) The creation of a standard for structuring data on vulnerabilities in computing environments, allowing different terms mapped in the ontology;

v) Reuse of safety data by importing and exporting ontologies;

vi) Support for managers in decisions about adherence to Cloud Services.

It is hereby wished that the results of this study, might contribute significantly to the work groups involved in the development of safety standards for Cloud Computing, helping organizations in key issues regarding the management of vulnerabilities in the Cloud, with the purpose of ensuring information security throughout the supply chain of information, involving suppliers and customers in the Cloud Services.

References

[1] Almeida, Mauricio, B., Bax, Marcello, P. (2003). An overview about ontologies: survey about definitions, types, applications, evaluation methods and construction. *Information Science*, Brasília, 32 (3) 7-20. Sept. /Dec.

[2] Baioco, G. (2009). Service Management and IT Governance - Concept and Process Modeling a Configuration Management Approach using a foundational ontology, Dissertation (Master in Computer Science) – Federal University of Espírito Santo - UFES, Vitória – Brazil.

[3] Guizzardi, G. (2007). On Ontology, ontologies, Conceptualizations, Modeling Languages, and (Meta) Models. *Frontiers in Artificial Intelligence and Applications*, Databases and Information Systems IV, Olegas Vasilecas, Johan Edler, Albertas Caplinskas (editors). Amsterdam: IOS Press.

[4] Grobauer, B., Wallaschek, T., Stocker, E. (2010). *Understanding Cloud-Computing Vulnerabilities* – IEEE Security & Privacy-*Special Issue on Cloud Computing*. Available <www.ieee.org>.

[5] Jaeger, P. T., Lin, J., Grimes, J. M. (2009). Cloud Computing and Information Policy: Computing in a Policy Cloud? - University of Maryland, MA – USA.

[6] Rimal, B. P., Choi, E., Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing System – *Fifth International Joint Conference on IC*, IMS and IDC - Computing and Network Services – York University, Ontario, Canada. <www.ieee.org>.

[7] Youseff, L., Butrico, M., Silva, D. (2010). Towards a Unified Ontology of Cloud Computing, University of California, Santa Barbara, CA, USA.

[8] Brandao, A. J. S., Martimano, L. A. F., Moreira, E. S. (2008). Use of Ontology in Vulnerability Alerts, *Institute of Mathematics and Computer Science* - University of São Paulo (ICMC-USP), São Carlos, SP - Brazil.

[9] ENISA - The European Network and Information Security Agency, *Cloud Computing Benefits, risks and recommendation for information* – November 2009. <http://www.enisa.europa.eu/ >.

[10] Almeida, M. B., Souza, R. R., Coelho, K. C. (2010). A Proposal for Domain Ontology for Information Security in Organizations: Description of Stage terminology. Department of Theory and Information Management, School of Information Science, Federal University of Minas Gerais. *Information & Society* , João Pessoa, 20 (1) 155-168, Jan./April.

[11] Gomez-Perez, A., Fernendez, M., Cocho, O. (2004). *Ontological Engineering* (2ª Ed.)- Springer.

[12] Falbo, R. A., (2004). Experiences in Using a Method for Building Domain Ontologies, *In*: Proceedings of the 16th Conference on *Software Engineering and Knowledge Engineering* (SEKE), p. 474-477, Banff, Alberta, Canada.

[13] Noy, Natalya, F., Mcguinness, Deborah, L. (2001). *Ontology Development 101: A Guide to Creating Your First Ontology*. Stanford University, CA, USA.

[14] Falbo, R. A. (1998). Knowledge Integration in a Software Development Environment, PhD Thesis, COPPE/UFRJ, Rio de Janeiro, December.

[15] Uschold, M., King, M. (1995). Towards a Methodology for Building Ontologies, *Workshop on Basic Ontological Issues in Knowledge Sharing*, IJCAI'95.

[16] Gruninger, M., Fox, M. S. (1995). Methodology for the Design and Evaluation of Ontologies, *Technical Report*, University of Toronto.

[17] Monteiro, M. E. (2010). A Proposal for a Semantic Service-Related Self-Management in Optical Transport Networks. Doctoral Thesis – Federal University of Espírito Santo, UFES, Vitória, Brazil – ES.

[18] Guizzardi, G. (2005). Ontological Foundations for Structural Conceptual Models, Ph.D. Thesis, University of Twente, The Netherlands.

[19] Guizzardi, G., Almeida, J. P. A., Guizzardi, R.S.S., Falbo, R. (2009). Foundational Ontology and Conceptual Modeling - *Center for Research on Conceptual Modeling and Ontology* (NEMO), Federal University of Espírito Santo (UFES) - Vitória-ES, Brazil.

[20] Costa, A. C. M. (2008). Modeling the Domain Processing Service Level Management ITIL Standard: An approach using Foundational ontology reasoning and its application in Platform Infraware, Dissertation (Master in Computer Science). Federal University of Espírito Santo, UFES, Vitória, Brazil.

[21] Carvalho, H., Castro, R., Gomes, M. J. N., Garcia, A. S. (2012). Well-Founded IT Architecture Ontology: an Approach from a Service Continuity Perspective - *Fourth International Conference on Networked Digital Technologies*. Canadian University of Dubai – Dubai.