Open Access

Open Journal of Cloud Computing (OJCC)
Volume 4, Issue 1, 2017

www.ronpub.com/ojcc
ISSN 2199-1987

Security and Compliance Ontology for Cloud Service Agreements

Ana Sofía Zalazar[A], Luciana Ballejos[B], Sebastian Rodriguez[A]

[A] GITIA, UTN-FRT, Rivadavia 1050, Tucumán, Argentina, {ana.zalazar, sebastian.rodriguez}@gitia.org
[B] CIDISI, UTN-FRSF, Lavaisse 610, Santa Fe, Argentina, lballejo@frsf.utn.edu.ar

ABSTRACT

Cloud computing is a business paradigm where two important roles must be defined: provider and consumer. Providers offer services (e.g. web application, web services, and databases) and consumers pay for using them. The goal of this research is to focus on security and compliance aspects of cloud service. An ontology is introduced, which is the conceptualization of cloud domain, for analyzing different compliance aspects of cloud agreements. The terms, properties and relations are shown in a diagram. The proposed ontology can help service consumers to extract relevant data from service level agreements, to interpret compliance regulations, and to compare different contractual terms. Finally, some recommendations are presented for cloud consumers to adopt services and evaluate security risks.

TYPE OF PAPER AND KEYWORDS

Short communication: *security, compliance, ontology, agreements, cloud service.*

1 INTRODUCTION

Cloud computing is a paradigm to optimize resource usage, and the cloud service provider can rapidly offer services and user accounts to a variable number of customers in the same physical server [4]. Providers offer computing resources and consumers pay for using them. Cloud techniques make possible to abstract software layers, scale up/down resources according to the requirements of users, and isolate the underlying infrastructure of services [24].

Due to different approaches and lack of standards [27] [31], each author presents his own definition of cloud computing. This work considers the definition of the *National Institute of Standards and Technology* (NIST), which addresses general aspects of cloud environments [21]: "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*".

The NIST considers that cloud computing has five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), five actors (consumer, provider, carrier, broker, and auditor), three service models (software as a service, platform as a service, infrastructure as a service), and four deployment models (private cloud, community cloud, public cloud, and hybrid cloud) [3].

Cloud services selection depends normally on the service level agreement (SLA) [4], which is a type of contract between providers and consumers, and it commonly identifies functional and quality parameters

(QoS). Generally, a SLA includes a description of the agreed service, service level parameters, guarantees, and procedures [33]. Cloud agreements are the basis for comparing different services, contracting providers, monitoring key indicators or parameters, and taking action when the expected service level is not achieved.

The agreement is usually composed of three basic parts: promises, limitations, and obligations [5]. Providers promise responsibilities: percent of service availability, data privacy policies, and data security mechanisms. In the limitation part, providers restrict their responsibilities in case of force majeure or events out of their control (i.e. accidents, security attacks, and restrictions imposed by public authorities, government, and regulations under the laws of the cloud services country) and they also reserve the right to change the contract or service any time [33]. The obligations part is referring to cloud consumers, which indicates that they assume the compromise of periodically checking the cloud agreement, paying the service on time, and having only legal content and correct software licenses in their contracted resources [33].

However, most of the cloud agreements are static and non-negotiable, sometimes ambiguous and unclear, and they are generally specified in the websites of the cloud provider [23]. Users have no way to specify requirements, obligations, and constraints about the service to big cloud providers. Thus, the agreements do not represent the individual needs and requirements of every service consumer [26]. Sometimes, the agreements are updated in a non-predictive manner and users should check periodically agreement changes [33]. These problems can be addressed having shared ontologies and common standards, which make possible automatic collaboration and information exchange between cloud providers and users.

Cloud consumers usually subscribe to a provider service by accepting the service agreement or terms of use. Cloud consumers agree to know and respect the jurisdiction laws and policy of the cloud service provider wherein the data is physically stored. Because there are many risks about data access, privacy and security (e.g. the provider can scan the user data and use the information for customize publicity), cloud consumers should carefully evaluate the agreements to decide which kind of information is uploaded to their cloud account and which cloud service satisfies the personal requirements [5].

To analyzing cloud agreements, several approaches have already been suggested [1][13]. Even so, they consider mainly functional parameters, while most legal and security aspects of cloud services (e.g. compliance, policy, and guaranty) are overlooked [5].

The goal of this exploratory research is to present a security and compliance ontology for cloud agreements for evaluating and analyzing cloud service characteristics. Cloud contractors should clearly share semantics and vocabulary between each involved party and give a clear definition of the formal agreements about service terms, so the ontology can be used for this purpose.

2 BACKGROUND AND RELATE WORK

An ontology is a conceptual artifact that represents the semantic in a specific domain and it comprises [12][15]: (a) *Terms*: words and group of words that represent domain entities (e.g. contract, provider, consumer); (b) *Properties*: characteristics of the entity that cannot be considered entities (e.g. legal name, start date of service contract); (c) *Relations*: elements that connect entities in the ontology (e.g. service provider "*is-A*" signatory part); (d) *Instances*: individual values of a domain entity or characteristic (e.g. “Google” *isInstanceOf* Service Provider); and (e) *Axioms*: representative sentences that are true over a domain and they are usually formalized in a logic language (e.g. "*ForAll*" Service Contract *hasProvider* Provider). Ontology is a formal specification of an explicit conceptualization used for knowledge sharing [12].

Taxonomy and ontology are two different terms. Taxonomy is a classification using class and subclass relations between entities, while ontology completely describes a domain [12]. A domain ontology provides a vocabulary of terms and relations in a specific domain, thus it is considered a semantic base for interconnection, communication and cooperation between parts. It also provides a conceptual context where is possible to infer knowledge, pursue common objectives, and interoperate [12].

Ontology is commonly applied to semantic web and knowledge management. It supports specific searching, matching and knowledge visualization [14]. An ontology is needed to consolidate views of cloud aspects, integrate definitions of similar service, combine automatic queries, translate different representations of the same entity (e.g. *“Product”* and *“Application”* can be referred to the entity named *“Service”*), and discover services that can replace others by interpreting their associated agreement [13].

Semantic Web exploits ontology benefits based on the idea of having linking data, so the data can easily be managed by machines and processed for more effective discovery and reuse [14]. Modeling a cloud domain using ontology facilitates the interoperability between different services and the automation of agreements negotiations, service compositions, and monitoring of service level.

Several contributions propose semantic models and ontologies for cloud computing, but none of them was

specifically defined for security and compliance aspects in cloud service agreements. This paper presents and describes an ontology for security and compliance issues in cloud service agreements, which have not been sufficiently addressed in existing works.

Youseff et al. [30] publish a small ontology for cloud computing in an attempt to establish knowledge domain in this area. The authors define a structure of five layers, their interrelationships and their interdependencies, to achieve a better understanding of this paradigm. However, this contribution does not give details for many relevant components.

Kang and Sim [19] present "*Cloudle*" which is a search engine for cloud systems. "*Cloudle*" is based on two ontologies that contain a set of concepts, individuals and relationships between them. The concepts are related to functional, technical and cost requirements. However, the authors do not consider security terms and service agreements.

Ma et al. [20] propose an ontology based on resource management systems to solve operative problems of cloud environments. This ontology is used to locate tasks and procedures in available resources, and it also defines concepts and describes relationships that are useful for understanding agreements.

Moscato et al. [22] propose an ontology definition in the mOSAIC project. This ontology is capable of describing services and interfaces between services to improve interoperability in cloud computing. The related concepts are extracted from the literature and existing standards.

Dastjerdi et al. [8] conclude that there exist a high need for semantic SLA that can be understood by all parties and services. Thus, they propose an ontology-based approach for SLA monitoring services in cloud computing. Their contribution is based on a discovery and ranking algorithm for monitoring, which analyzes few parameters (i.e. CPU, bandwidth, memory, availability, and throughput of the services). The proposed QoS properties for ranking of monitoring services are cost and reliability. Security attributes are ignored in this contribution.

Di Modica et al. [9] develop a set of taxonomies and ontologies to characterize semantically the features of resources offered by cloud providers and requirements specifications expressed by cloud consumers. Nevertheless, security and compliance characteristics are out of scope of these structures.

Hamadache and Rizou [16] introduce the concept of holistic SLA ontology to support fully feedback evaluation and reputation mechanism for cloud service selection. The authors evaluate feedback considering QoS parameters (i.e. agility, assurance, performance, usability and privacy), but they overlook legal regulations and security restrictions. However, in the proposal, cloud providers and cloud consumers are always limited by jurisdictions and security policies, which are important constraints during the service selection process.

Androcec et al. [2] present a literature review, wherein 24 primary studies of cloud ontology are identified. In these contributions, the main focuses are physical resources, services description, security interoperability, and provider selection. The biggest identified challenge is security in cloud computing and the major obstacles are referred to isolation and privacy of the information. However, the authors do not present any parameters and attributes in order to handle service requirements and agreements.

Proposed taxonomies and ontologies are generally developed to characterize respectively offers and requirements in cloud agreements [11] [29]. Security and compliance regulations are very complex to analyze, so existing ontologies overlook legal aspects and jurisdictional restrictions. Besides, theses ontologies can be enriched with these compliance terms and consolidated in a more sophisticated and integrative cloud ontology in the future.

3 SECURITY AND COMPLIANCE ONTOLOGY

The proposed ontology is based on academic references (standards, conferences and journals), some SLAs presented in cloud provider websites and the experience of practitioners (expert forums, blogs and social media). The ontology is offered as a tool for cloud providers and cloud consumers, which need common vocabulary and semantics to communicate requirements and capabilities. Thus, cloud agreements and requirements specification documents can be automatically matched using this ontology [29].

Figure 1 shows the ontology that helps to design and compare compliance regulations and SLAs. The aim of this view of cloud services is to present the key concepts for cloud adoption and some criteria for evaluating different offers by comparing security features from cloud agreements.

This ontology is a valuable tool that helps to security experts and service consumers to take decisions, consider risks, and choice the best service according to their compliance requirements and security policies. Before accepting an agreement, the service consumer can use the proposed ontology for mapping ambiguous and unclear security terms of contracts. Most of the legal issues involved in cloud domain should be resolved during the evaluation of contracts and agreements [33].

To understand the ontology, each concept is defined and the most important properties are explained.

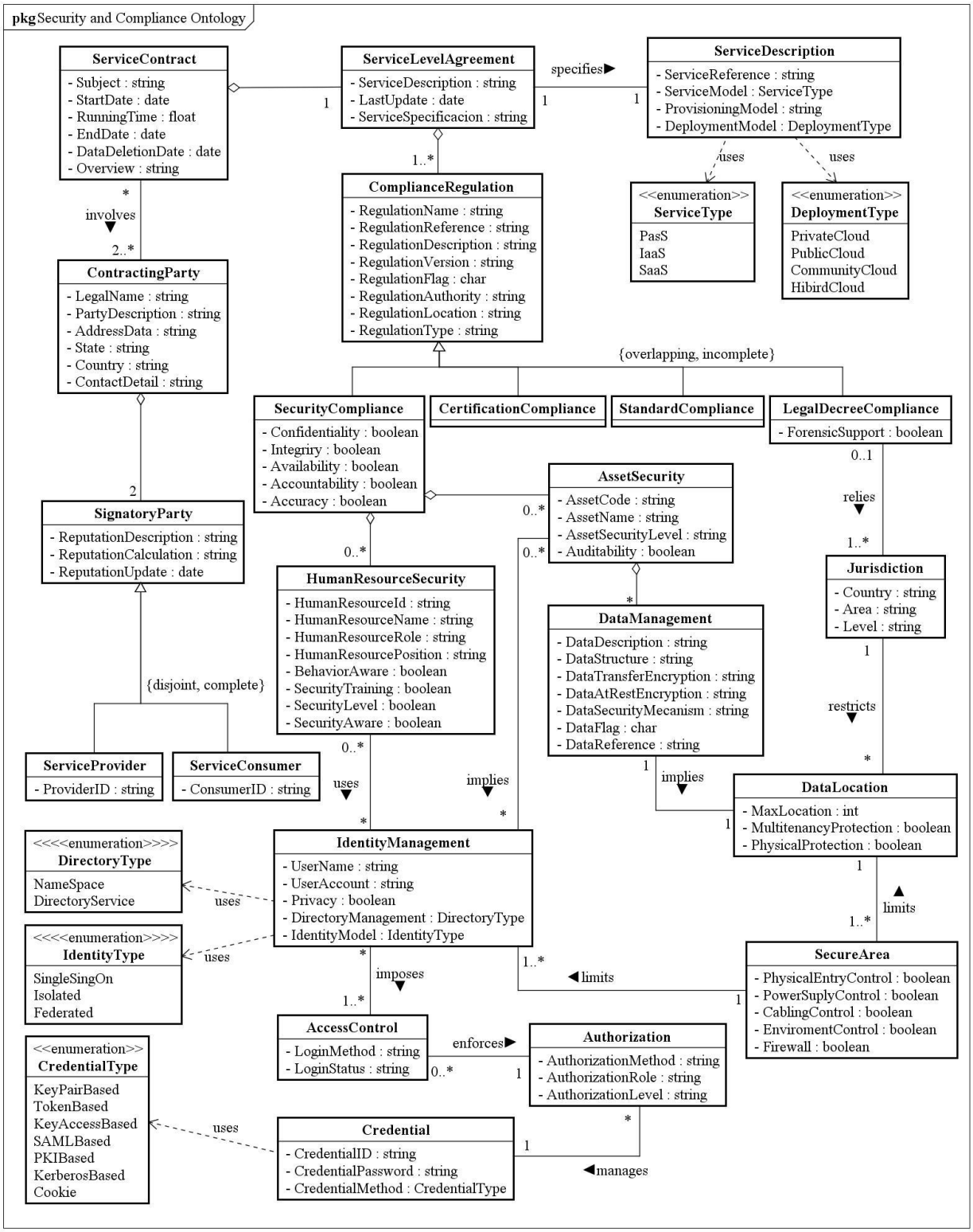

Figure 1: Security and Compliance Ontology

Service Contract: should have all the information for managing the contractual terms and agreements. The most important properties are "*Start Date*", "*End Date*" and "*Data Deletion Date*", because they indicate the beginning of the contract, the termination of the service supply and when the consumer data is going to be permanent eliminated in the provider infrastructure [32].

Contracting Party: should be a person, organization, entity or party that is involved in the service contract. The party should respect all contractual terms. This concept involves the "*Legal Name*", "*Contact Detail*", "*Address*", "State" and "*Country*" of the service stakeholders.

Signatory Party: should be a person, organization, entity or party that participates in the service contract as a service provider or a service consumer. "*Reputation Description*" implies the unambiguous definition of this attribute that refers to credibility and trust of the main actors.

Service Consumer: should be a person or organization that uses the service [21] and maintains a business relationship with a service provider.

Service Provider: should be a person, organization or entity that makes available a cloud service [21]. The service provider maintains the underlying physical infrastructure.

Service Level Agreement: should specify the service description, service specification and service level objectives. This document should be published by the provider and accepted by the consumers before contracting cloud services [10].

Service Description: should indicate all capabilities of the cloud service offered through the cloud contract. It includes the type of "*Deployment Model*" (i.e. Private Cloud, Public Cloud, Community Cloud and Hybrid Cloud) and the type of "*Service Model*" (i.e. Software as a Service, Platform as a Service and Infrastructure as a Service) [3]. "*Provisioning Model*" indicates the type of the provisioning (i.e. dynamic, static, increasing, on demand). "*Service Reference*" describes the scope and application of the cloud service.

Compliance Regulation: refers to the collection of regulations, norms and restrictions that are taken into account during the term of a service contract. Cloud consumer can infer from the proposed ontology that "*Compliance Regulation*" is generally considered in a cloud contract as a certification, standard, legal decree and security terms, regulated by a "*Regulation Authority*". The *"Regulation Type"* indicates the scope of the compliance restrictions and it can be directed to communication, virtualization, security, ecological commitment, federation or data interoperability.

Certification Compliance: implies formal certifications that service should comply with [10]. Some organizations have made significant investments to achieve certification (i.e. ISO 9000, ISO 27000) [6] in order to gain competitive advantage and to meet industry standards, and they want to ensure they will maintain their certifications [5].

Standard Compliance: is about all guidelines for data manipulation, security, and visualization of information. It should have the information of the regulations that service must meet to obtain quality levels.

Legal Decree Compliance: represents external regulations and constraints. Using this view of cloud services, legal experts and cloud consumers can infer that "*Legal Decree Compliance*" may belong to more than one "*Jurisdiction*" (cardinality is "1…* " which means "*one or many*"). Contractual agreements should be related to data protection aspects and law enforcement in cloud computing services, and these legal agreements are usually imposed by a governmental authority or jurisdiction. "*Forensic Support*" is the reserved right of the service provider to give evidences, user data and processes to external government and to collaborate with legal investigations.

Security Compliance: represents the pursued levels of confidentiality, integrity, availability and privacy. "*Accuracy*" indicates that the outputs match to the expected results. "*Availability*" indicates that the service is accessible and usable when is requested by an authorized entity [10]. "*Confidentiality*" indicates that such service is not available to unauthorized persons, entities or processes [18]. "*Integrity*" indicates services precision and completeness [18].

Human Resource Security: is about regulations regarding security of human resources that participate directly or indirectly in the administration of a cloud service. Security information about the staff should be evaluated periodically. "*Human Resource ID*", "*Human Resource Name*", "*Human Resource Position*" and "*Human Resource Role*" are the contact details of contractors, employees and users related to the cloud service. "*Behavior Aware*" indicates that employees have also accepted agreements and disclosures before receiving physical or logical access rights to facility, system, and data [6]. "Security Aware" indicates the acceptance of policy and procedures by the staff to maintain a safe environment and security area [6]. Human Resources departments usually implement "*Security Training*" programs for all contractors, third-

party, users and employees to keep appropriate level of security, so the property indicates the existence of this kind of programs.

Asset Security: describes the security programs for software, devices or any component related to cloud services, which should be protected against unauthorized access, destruction and data leaking.

Data Management: indicates the data policies for managing the data structure, data security, location and encryption [10].

Identity Management: manages the identity and correct access of an entity. It guarantees, with some degree of certainty that a given identity can be trusted [10].

Access Control: manages granted permissions and rights to authorized users, while preventing unauthorized users access to data and services.

Authentication: verifies the identity of an entity that wants to access a service [10].

Authorization: manages the permissions of a user to specify access to a resource. It involves role policies and security levels.

Credential: is a mechanism to implement secure accesses and password controls for applications, databases, server and network. Before granting any privilege, all security policies should be analyzed and evaluated [6].

3.1 Ontology Analysis

The ontology design is evaluated to consider the potential for richness knowledge representation [25].

Ontology metrics can be calculated according the *Width* and *Depth* of the structure [7]. The ontology has an acceptable level of quality and richness, so its semantic representation can help service consumers to extract data from service level agreements, interpret and compare different values and term agreements.

Width: number of terms visible at once is equivalent to the average number of subclasses (SC) in a parent class (PC) divided by the total terms of class (TC). In the proposed ontology, there are 23 classes, 2 parent classes ("*Signatory Party*" and "*Compliance Regulation*"), and 6 subclasses in total. Thus, *Width* is equal to 0.26 (on a scale of 0 to 1) [7].

Depth: number of levels of hierarchy is equivalent to the total relations from the roof term (RT) to the leaf term (LT) divided by the total terms of classes (TC). The roof term is "*Service Contract*" and the leaf term is "*Credential*" and there are 8 levels of relation. Thus, *Depth* is equal to 0.34 (on a scale of 0 to 1) [7].

Relationship Richness: number of terms needed is equivalent to the total number of no hierarchical relations divided by the total number of relations. The hierarchical relations represent inheritance. The *Relationship Richness* is equal to 0.76 (on a scale of 0 to 1) and this metric reflects the diversity of relations and placement of relations in the ontology. The ontology is richer than a taxonomy (value is equal to 0.5) [25].

Attribute Richness: average number of attributes or number of properties per class. The *Attribute Richness* is equal to 6.45 (on a scale of 0 to 10) and the ontology with high value indicates that much information is provided about each class [25].

3.2 Lessons Learned and Recommendations

Service consumers should consider the ontology terms and properties for deeply evaluating the risks of storing data and processes into external physical servers [3], because third parties may access the data and the processes may be used for unintended purposes.

Some lessons learned and recommendations about security and compliance aspects in cloud agreements are listed below [3][5][26]:

- After accepting cloud provider agreements, the service consumer should check periodically the current version of the agreement shown in the provider website (property "*Last Update*" of class "*Service Level Agreements*"). This is because the provider usually reserves the right to change and modify terms and conditions without noticing the service consumers.
- Cloud consumers should consider potential *"lack of service",* especially in cloud services that offer applications to edit and manage files. The stored files may only be accessible by using the cloud provider software, thus the cloud consumers are not free to reallocate resources in services of other cloud providers (property "*Data Structure*" of class "*Data Management*").
- Cloud consumers should notice the risk of *"loss of governance"*, when their data are replicated in multiple jurisdictions where diverse laws are implicated (class *"Jurisdiction",* class *"Legal Decree Compliance"* and attribute *"Max Location"* of class *"Data Location"*).
- Cloud consumers should accept agreements which present transparency in the allocation of data (class *"Data Location"*).
- The cloud service legal context may be different from the country of the consumers or the provider, so the cloud consumer should pay

attention to international agreements, obligations, and access of data by law enforcement entities of the service context (attribute *"Forensic Support"* of class *"Legal Decree Compliance"*).

- Cloud consumers are usually responsible of problems about their data security and privacy, thus they should use other internal mechanics (cryptography, passwords) to safe their data (attribute "*Data Security Mechanism*" of class "*Data Management*")

4 SUMMARY AND CONCLUSIONS

The goal of this exploratory research is to present a security and compliance ontology for cloud agreements to evaluate and analyze cloud service characteristics in service contracts. The proposed ontology is presented in a model and its terms are explained. To validate its design and richness, some metrics are considered and calculated. Finally, some recommendations and lessons learned about security and compliance aspects are presented for cloud negotiation.

A future work line should be an extensive evaluation on this ontology using inference and a discussion of its practicability and comprehension using different contexts and scenarios, like the one of cooperative hybrid cloud intermediaries [17].

Security and compliance aspects are often overlooked in cloud agreements, so the proposed ontology should be applied for sharing common understanding of these aspects. This ontology can be used as a basis for standards and matching applications, wherein security and compliance properties are considered high priority in cloud services selection. Cloud providers and cloud consumers should take into account the proposed ontology as a structure to provide clear information in service level agreements and in requirements specification documents. Then, the ontology can also be used to guide the process of information extraction from natural language [29]. Moreover, many knowledge-representation systems can import and export ontologies to extract data to different formats [12]. Future work in this area includes automatic matching and search engine based on this proposal.

Before acquiring cloud services, service consumer should be aware about jurisdictional policies and legal restrictions implied in the service contract, because the consumer may infringe upon the law and the data may be monitored by third-party. Service consumer should deeply evaluate compliance regulations, because these imply all information and characteristics about certification, standard, legal decree and security terms. The proposed ontology represents the integration of all aspects of security techniques, and it considers security policies for human resources and assets (facilities, physical servers, data bases, etc.). Mechanisms for authentication and authorization should be also evaluated before contracting service providers.

Finally, the proposed ontology can also be applied to new computing forms, such as dew computing and fog computing [24][28], which are closely related to cloud computing. This discussion is considered as future work. Accordingly, new terms and characteristics can be integrated to the ontology in the future. Moreover, semantic web tools can use this ontology to extract information and make decisions referring to the service adoption.

REFERENCES

[1] M. Alhamad, T. Dillon, and E. Chang, "*Conceptual SLA framework for cloud computing*", 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 606-610, IEEE, 2010.

[2] D. Androcec, N. Vrcek, and J. Seva, "*Cloud computing ontologies: A systematic review*", 3rd International Conference on Models and Ontology-based Design of Protocols, Architectures and Services, pp. 9-14, IARIA, 2012.

[3] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "*Cloud computing synopsis and recommendations*", NIST Special Publication 800-146, 2012.

[4] R, Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "*Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility*", Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, 2009.

[5] D. Catteddu and G. Hogben, "*Cloud computing: Benefits, risks and recommendations for information security*", ENISA, 2009.

[6] Cloud Security Alliance, "Cloud security alliance cloud controls matrix (CCM)", https://cloudsecurityalliance.org/research/ccm/, accessed 29th June 2017.

[7] R. M. Colomb, *"Quality of ontologies in interoperating information systems"*, Technical Report 18/02 ISIB-CNR, 2002.

[8] A. V. Dastjerdi, S. G. H. Tabatabaei, and R. Buyya, *"A dependency-aware ontology-based*

approach for deploying service level agreement monitoring services in cloud", Software: Practice and Experience, vol. 42, no. 4, pp. 501-518, 2012.

[9] G. Di Modica, G. Petralia, and O. Tomarchio, *"An SLA ontology to support service discovery in future cloud markets"*, 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 1161-1166, IEEE, 2013.

[10] European Commission, "Cloud service level agreement standardisation guidelines", Technical Report C-SIG SLA 2014, https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines, accessed 29th June 2017.

[11] K. Fakhfakh, T. Chaari, S. Tazi, M. Jmaiel, and K. Drira, *"ODACE SLA: Ontology driven approach for automatic establishment of service level agreements"*, International Journal of Systems and Service-Oriented Engineering (IJSSOE), vol. 1, no. 3, pp. 1-20, 2010.

[12] A. Gómez-Pérez, M. Fernández-López, and O. Corcho, "*Ontological engineering. advanced information and knowlege processing*", Springer, 2004.

[13] R. Greenwell, X. Liu, and K. Chalmers, "*Semantic description of cloud service agreements*", Science and Information Conference (SAI), pp. 823-83, IEEE, 2015.

[14] S. Groppe, "*Data management and query processing in semantic web databases*", Springer, 2011.

[15] T. Gruber, "*A translation approach to portable ontology specifications*", Knowledge Acquisition, Vol. 5, no. 2, pp. 199-220, 1993.

[16] K. Hamadache and S. Rizou, *"Holistic SLA ontology for cloud service evaluation"*, International Conference on Advanced Cloud and Big Data (CBD), pp. 32-39, IEEE, 2013.

[17] T. Haselmann, G. Vossen, and S. Dillon, *"Cooperative hybrid cloud intermediaries-making cloud sourcing feasible for small and medium-sized enterprises"*, Open Journal of Cloud Computing (OJCC), vol. 2, no. 2, pp. 4-20, 2015. [Online]: http://nbn-resolving.de/urn:nbn:de:101:1-201705194494

[18] ISO, "Information technology – cloud computing – reference architecture", ISO/IEC 17789:2014, https://www.iso.org/standard/60545.html, accessed 29th June 2017.

[19] J. Kang and K. M. Sim, "*Ontology and search engine for cloud computing system*", International Conference on System Science and Engineering, pp. 276-281, 2011.

[20] Y. B. Ma, S. H. Jang, and J. S. Lee, "*Ontology-based resource management for cloud computing*", Asian Conference on Intelligent Information and Database Systems, pp. 343-352, 2012.

[21] P. Mell and T. Grance, "*The NIST Definition of Cloud Computing. National Institute of Standards and Technology*", NIST Special Publication 800-145, 2011.

[22] F. Moscato, R. Aversa, B. Di Martino, T. F. Fortiș, and V. Munteanu, "*An analysis of mosaic ontology for cloud resources annotation*", Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 973-980, 2011.

[23] J. Repschlaeger, R. Zarnekow, S. Wind, and T. Klaus, "*Cloud requirement framework: Requirements and evaluation criteria to adopt cloud solutions*", 20th European Conference on Information Systems, 2012.

[24] K. Skala, D. Davidovic, E. Afgan, I. Sovic, and Z. Sojat, *"Scalable distributed computing hierarchy: Cloud, fog and dew computing",* Open Journal of Cloud Computing (OJCC), vol. 2, no. 1, pp. 16-24, 2015. [Online]: http://nbn-resolving.de/urn:nbn:de:101:1-201705194519

[25] S. Tartir, I. B. Arpinar, M. Moore, A. P. Sheth, and B. Aleman-Meza, "*OntoQA: Metric-based ontology quality analysis*", ICDM Workshop on Knowledge Acquisition from Distributed, Autonomous, Semantically Heterogeneous Data and Knowledge Sources, 2005.

[26] I. Todoran, N. Seyff, and M. Glinz, "*How cloud providers elicit consumer requirements: An exploratory study of nineteen companies*", 21st IEEE International Requirements Engineering Conference, pp. 105-114, 2013.

[27] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "*A break in the clouds: towards a cloud definition*", SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, 2008.

[28] Y. Wang, *"Definition and categorization of dew computing"*, Open Journal of Cloud Computing

(OJCC), vol. 3, no. 1, pp. 1-7, 2016. [Online]: http://nbn-resolving.de/urn:nbn:de:101:1-201705194546

[29] D. C. Wimalasuriya and D. Dejing, *"Ontology-based information extraction: An introduction and a survey of current approaches"*, Journal of Information Science, vol. 36, no. 3, pp. 306-323, 2010.

[30] L, Youseff, M. Butrico, and D. Da Silva, "*Toward a unified ontology of cloud computing*", Grid Computing Environments Workshop, pp. 1-10, 2008.

[31] A.S. Zalazar, L. Ballejos, and S. Rodriguez, "*Analyzing requirements engineering for cloud computing*", Requirements Engineering for Service and Cloud Computing, pp. 45-64, 2017.

[32] A. S. Zalazar, L. Ballejos, and S. Rodriguez, "*Cloud dimensions for requirements specification*", Requirements Engineering for Service and Cloud Computing, pp. 23-43, 2017.

[33] A. S. Zalazar, S. Rodriguez, and L. Ballejos, "*Handling dynamic requirements in cloud computing*", 16th Argentine Symposium on Software Engineering, pp. 220-233, 2016.

AUTHOR BIOGRAPHIES

Ana Sofia Zalazar is an Asistant Professor at Universidad Tecnológica Nacional (UTN) and Ministry of Education of Tucuman, Argentina. She is member of the Advanced Informatics Technology Research Group (GITIA). She worked as a Technology Consultant in several projects. Her main research interest are Cloud Computing, Requirements Engineering, and Systems Migrations.

Luciana Ballejos is a Full Professor at the Department of Systems Engineering at Facultad Regional Santa Fe, Universidad Tecnológica Nacional (UTN), Argentina. She is also member of the Information Systems Engineering Research & Development Center (CIDISI). She received Information Systems Engineer and Ph.D. degrees from Universidad Tecnológica Nacional, Facultad Regional Santa Fe.

Sebastian Rodriguez is a Full Professor at Universidad Tecnológica Nacional, Argentina. He is head of the Advanced Informatics Technology Research Group (GITIA) and an associate researcher at the University of Technology of Belfort-Montbéliard (UTBM), France. He received a Computer Engineer degree from Universidad Nacional de Tucumán (UNT), a M.Sc. degree in computer science from the University of Franche-Comté and a Ph.D. degree in computer science of the UTBM.