A Survey of Cloud Computing Taxonomies: Rationale and Overview

Fahad Polash, Abdullah Abuhussein, Sajjan Shiva
Computer Science Department
The University of Memphis
Memphis, USA
{mipolash, bhussein, sshiva}@memphis.edu

Abstract—**The Cloud Computing (CC) as a field is progressing by leaps and bounds. In order to organize the knowledge on this newly flourishing field, numerous taxonomies have been proposed over the last few years. A well-developed cloud taxonomy aims to support researchers and practitioners from academia and industry by organizing cloud computing-concepts and terminology. It provides researchers with a tool to focus on the aspects that eliminate research gaps. This paper presents a survey of the existing cloud computing taxonomies for various purposes. We aim to enable the readers to better understand the state-of-the-art of cloud computing and categorize the existing cloud computing related taxonomies into three classes: conceptual, performance and security taxonomies. This classification will help readers to find out different perspectives in cloud computing taxonomies. We infer that current endeavors in CC taxonomy have not yet extensively explored all aspects of the emerging field.**

Keywords-cloud computing, taxonomy, cloud services, cloud security, cloud performance.

I. INTRODUCTION

The cloud computing domain has evolved through several milestones since its inception. As the cloud computing concept expanded to include more than sharing a processor, a multitude of terms, concepts and technologies began to emerge on the scene. Many attempts to define and describe the evolving domain have produced solid ground for researchers from academia and industry. These attempts sought to connect the dots by defining the domain, its components, and the technologies used in it. Some other attempts went to define CC challenges (e.g. security, performance, and economics issues). However, the variety of stakeholders and technologies involved makes the overall picture confusing. Thus, researchers employed taxonomy in an attempt to classify and re-arrange the concepts of the emerging domain. Taxonomy is the science of categorization or classification of things based on a predefined system and contains a controlled vocabulary with a hierarchical tree-like structure [1]. The purpose of using a taxonomical approach to define a knowledge domain is to (1) simplify the terminology and show relatedness of its entities, (2) create an easy to grasp and memory-retainable terminology, (3) reveal the undiscovered potential branches that may comprise interesting problems and/or solution, (4) explore potential problems in the domain from different perspectives, and (5) benefit from the structurability feature in updating the terminology as the domain evolves.

A well accepted and comprehensive CC taxonomy would help alleviate many problems. It would assist in communicating cloud computing components and service offerings accurately. It can also be used to identify the similarities and differences among the cloud services and to identify the areas requiring further research. Researchers have proposed taxonomies for different goals. Some are accentuating concepts (conceptual), whereas others rummage for challenges (e.g. security, performance, etc.) and present solutions [1, 14].

The recent efforts in cloud computing taxonomy have succeeded arguably in articulating the cloud computing domain. This paper presents state-of-the-art cloud computing taxonomy research by showing a complete and thorough literature survey from different perspectives and contexts. We present a taxonomy of the prominent cloud taxonomy related efforts from research, standards and commercial domains.

Three major classes are identified through this literature survey: (1) conceptual taxonomies, (2) performance taxonomies and (3) security taxonomies. In the conceptual class we present the cloud taxonomies that are pertaining to architecture, definition, and certification of cloud services. The cloud taxonomies that are focused on performance and security issues are categorized in performance and security classes respectively.

The rest of the paper is organized as follows: Section II gives an overview of cloud computing; Section III introduces the classification of the current state of research in cloud taxonomies; Section IV shows some limitations of current efforts and the scope of potential future work; and Section V concludes.

II. OVERVIEW OF CLOUD COMPUTING

The National Institute of Standards and Technology (NIST) has a widely accepted definition of cloud computing [2]. NIST defines CC as "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". NIST has divided the cloud computing model into three service models and four deployment models [2]. A brief demonstration of service

models and deployment models is given in the following sub-sections.

A. Service Model

Three service models are available to describe cloud services:

- *Software as a Service (SaaS):* In SaaS model, consumers can access a cloud application that is hosted on provider's infrastructure through internet using different types of clients (i.e. thick or thin). Control over CC infrastructure (i.e. network, and operating systems) is the responsibility of the cloud service provider. Consumer's control is limited to application settings. Facebook and Twitter are some of examples of SaaS.

- *Platform as a Service (PaaS):* In this model, customers can develop and deploy application on the cloud. Customers are provided with the tools, programming environment and configuration management by the cloud service providers. Customers of PaaS include application designers, developers, testers or administrators. Google AppEngine is an example of PaaS.

- *Infrastructure as a Service (IaaS):* In this model, the customer has access to infrastructure provisioned by the cloud service provider. Customers can deploy development tools at their own accord and build application on top of IaaS. Customers of IaaS include system developers, system administrators, IT managers etc. Amazon EC2 is an example of IaaS.

B. Deployment Model

Cloud computing is composed of four deployment models. They are:

- *Private Cloud*: This deployment model is exclusively provisioned for a particular organization. The cloud infrastructure might be managed, owned and operated by that organization or by any third party company. The infrastructure can be located in the organization's premises or in a third party's premises.

- *Public Cloud*: This model is provisioned for general people. The cloud service provider is responsible for managing the infrastructure. The infrastructure is located in the provider's premises.

- *Community Cloud*: This model is applicable for a community of organizations who possess common interests, policies, objectives and missions. The infrastructure can be situated in one of the organizations' place or in a third party's place.

- *Hybrid Cloud*: It is a composition of two or more afore mentioned cloud infrastructures. The participating cloud infrastructures are bound together by standardized technologies which enable application portability among them.

III. Cloud Computing Taxonomy Classification

A well-established CC taxonomy can visibly and intelligibly shape a strong data management for all the concepts. It provides stakeholders with a better understanding of the global view of the potential problems. Directions for further research areas can also be highlighted when the domain is taxonomized appropriately. The key initial point is to create a taxonomy that can comprehensively break down the domain to be easily comprehended. As in reference [16], the characteristics of a good taxonomy are:

- *Mutually exclusive*: The classification should be done in such a way that no entity could be classified in more than one category.

- *Exhaustive*: The categories should include all the possibilities of classification.

- *Unambiguous*: The categories should be clear and precise so that it would not create any ambiguity in classification.

- *Repeatable*: Repeated entity should be always in the same category irrespective of the person classifying.

- *Accepted*: The categories should be logical and intuitive in order to be generally accepted.

- *Useful*: It should be useful to get insight into the field of study.

Through literature survey we noticed that efforts in CC taxonomy mainly belong to a specific purpose/objective class. Based on the objectives of taxonomies, we have classified them into three classes: conceptual, performance and security. Taxonomies that define the concepts, terminologies of cloud computing and propose architecture can be represented by the conceptual class. Performance taxonomies focus on the performance challenges and solutions of cloud computing. Finally security taxonomies deal with CC challenges and solutions of security and privacy issues. Each of the aforementioned classes represents a number of various perspectives as shown in Fig. 1. Table I maps the surveyed research efforts to our classification.

A. Conceptual Taxonomies

NIST Cloud Computing Taxonomy

NIST has proposed a CC taxonomy that mind maps stakeholder's roles. It describes the key concepts of cloud computing and their relations to different stakeholders. The taxonomy consists of four levels. The first level is the role, which is the behavior and obligations of different cloud

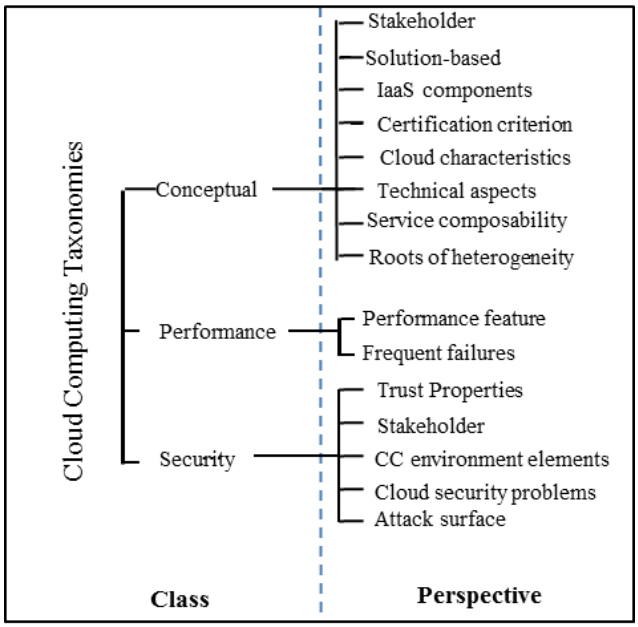

Figure 1. CC Taxonomy Research Classification

TABLE I. LITERATURE REVIEW OF TAXONOMIES

Ref.	Class	Perspective	# of citation	Year
[1]	Conceptual	Stakeholder	110	2011
[4]		Solution-based	12	2011
[6]		IaaS components	5	2013
[10]		Certification criterion	1	2014
[13]		Cloud characteristics	13	2012
[3]		Technical aspects	524	2009
[17]		Composability	676	2008
[19]		Roots of heterogeneity	35	2014
[5]	Performance	Performance feature	15	2012
[15]		Frequent failures	0	2014
[9]	Security	Trust Properties	2	2013
[11]		Stakeholder	0	2013
[12]		CC environment elements	95	2009
[14]		Cloud security problems	30	2012
[18]		Attack surface	61	2010

stakeholders. The second level represents the activities associated to a specific role. The third level is component and it is composed of tasks that need to be performed for the completion of an action. The fourth level is sub-component which is a modular part of the third level. Fig. 2 shows the NIST taxonomy with one role expanded [1].

OpenCrowd Cloud Solutions Taxonomy

The OpenCrowd Cloud Solutions Taxonomy [4] shown in Fig. 3 provides a reference of cloud computing products

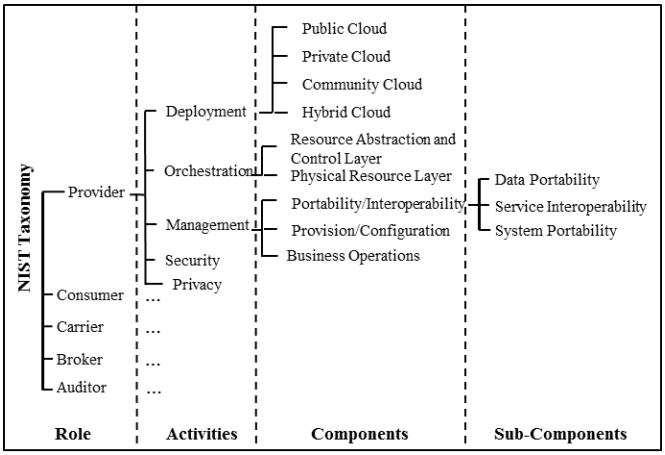

Figure 2. NIST Taxonomy

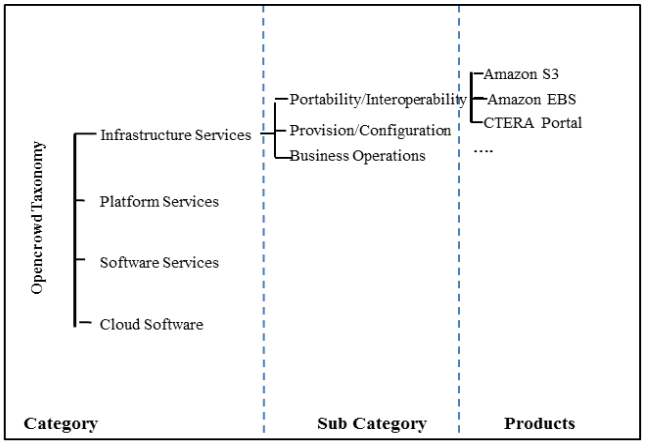

Figure 3. Opencrowd Taxonomy

available in the market. The products are categorized in four classes: Infrastructure services, Platform services, Software services and Cloud software. Developers and customers of cloud services can be up-to-date with the cloud products by viewing this taxonomy.

Dukaric et al. Taxonomy

Dukaric et al. [6] propose a unified taxonomy and architecture of cloud frameworks for IaaS which is shown in Fig. 4. Their taxonomy is composed of several layers: core service layer, support layer, value added services, control layer, management layer, security layer and resource abstraction. The goal of the taxonomy is to divide the components of IaaS into layers so that the taxonomy can be used to design the architectural framework of IaaS. For example, the components of security layers are: authorization, authentication, security groups, single- sign-on (SSO) and security monitoring. The components are identified by performing a literature review of the most important commercial and open-source IaaS products. The IaaS platforms are evaluated by mapping their capabilities into the components and layers of the proposed taxonomy.

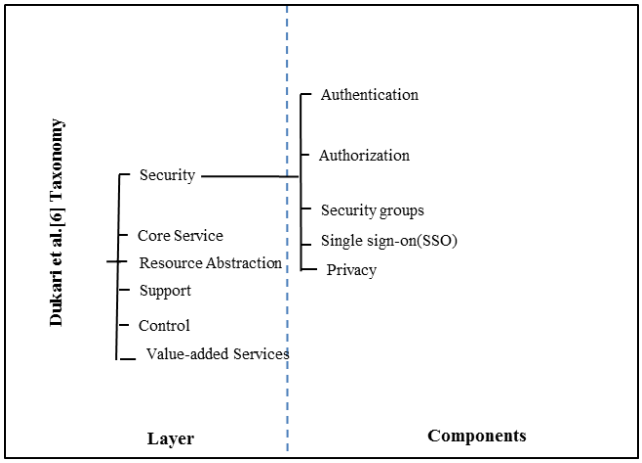

Figure 4. Dukaric et al. Taxonomy

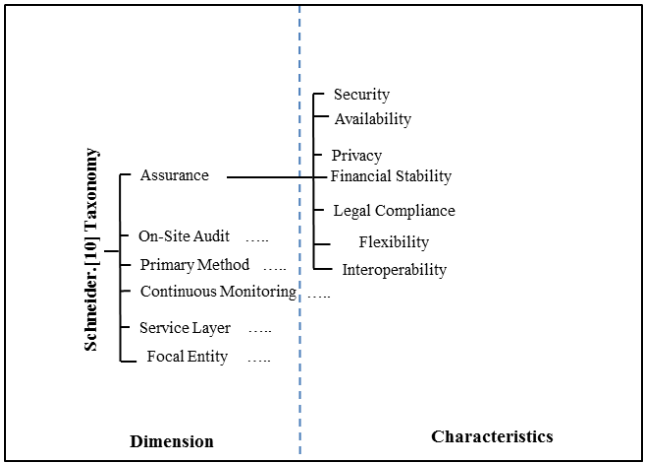

Figure 5. Schneider et al. Taxonomy

With the help of this taxonomy, we can make comparison among the available IaaS providers by observing whether a particular component is present or not in an IaaS platform. A similar taxonomy could be proposed to classify PaaS and SaaS components.

Schneider et al. Taxonomy

Schneider et al. [10] have proposed a taxonomy for cloud service certification (CSC) criteria as in Fig. 5. These certifications are provided by third party auditors to support potential cloud adopters in assessing cloud providers comprehensively. The authors have identified 328 criteria by interviewing the experts of cloud computing. They have proposed six classifiers (Assurance, On-Site Audit, Primary Method, Continuous Monitoring, Service Layer, and Focal Entity) to characterize the nature of a criterion. The Assurance classifier classifies a criterion among the characteristics of Security, Privacy, Legal Compliance, Flexibility, Interoperability, Availability, Financial Stability, Customer Support and Contract. The On-Site Audit classifier mentions whether the auditors need to be on-site or off-site to verify the criterion. For example, let us consider a certification criterion: 'Is the cloud provider equipped with the necessary tools to recover the cloud service in an event of damage or loss?' The Assurance classifier classifies the criterion into the characteristic of Availability, the On-Site Audit classifier puts the criterion into the characteristic of 'On-Site YES' as the criterion can be verified by the presence of the auditor on-site. This taxonomy will be useful to cloud certification auditors, cloud service providers and cloud consumers**.** However, the taxonomy is not evaluated yet against any practical project.

Repschlaeger et al. Taxonomy

Repschlaeger et al. [13] came up with a classification framework of cloud infrastructure services which is depicted in Fig. 6. Authors have identified six target dimensions based on interviews with experts. These dimensions provide the structure of cloud characteristics. The dimensions are: flexibility, costs, scope and performance, IT security and

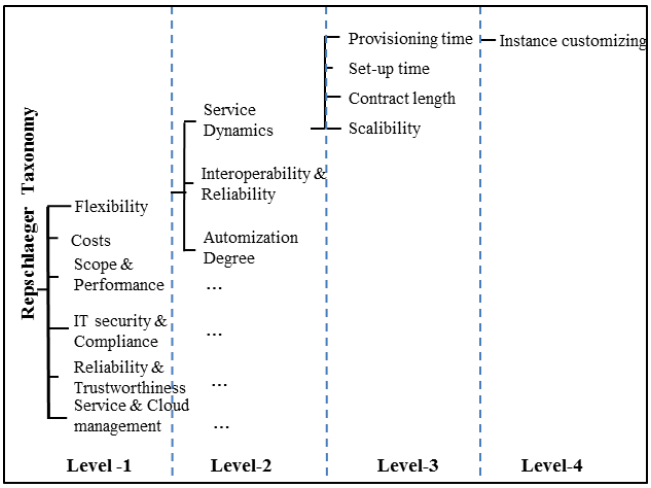

Figure 6. Repschlaeger et al. Taxonomy

compliance, reliability and trustworthiness, and service and cloud management. The target dimension is broken into different abstract classification criteria in the second level. Then operational classification criteria are there to measure the abstract criteria in the third level. Next, for each operational criterion, there are many requirements in the fourth level which are key performance indicators (KPIs).This framework helps consumers to classify IaaS providers in supporting their decision process of choosing cloud providers. The limitation of this work is that the framework is not tested against a real case study.

Rimal et al. Taxonomy

Rimal et al. [3] proposed a cloud computing taxonomy of the technical aspects. The taxonomy divides cloud computing into areas like: Cloud Architecture, Cloud Services, Virtualization Management, Fault Tolerance, Security and other cloud specific characteristics like Interoperability, Scalability etc. The architecture provided by NIST, Cloud Security Alliance (CSA), is inspired by the work of this paper.

Youseff et al. Taxonomy

Youseff et al. [17] proposed an ontology earlier when CC emerged. The classification in that ontology was based on the famous composability principle of SOA. Authors have considered cloud computing as a stack of five layers: cloud application, cloud software environment, cloud software infrastructure, software kernel and firmware/hardware. Each layer consists of one or more cloud services. For example, Computational Resources (IaaS), Storage (DaaS), and Communications (CaaS) are the services provided by the cloud software infrastructure layer. Cloud services of upper layers can be composed of the services from the lower layers. However, though the authors claim that their proposed ontology is unified, security aspect was not considered here.

Sanaei et al. Taxonomy

Sanaei et al. [19] made a rigorous attempt in studying heterogeneity in Mobile Cloud Computing (MCC). Heterogeneity in MCC is the presence of different hardware, architectures, infrastructure and technologies in MCC. The authors have investigated the roots of heterogeneity in MCC and devised a taxonomy of those roots. Three classes are observed as the roots of heterogeneity: Mobile, Cloud and Networks. In mobile and cloud classes, they have further classified the heterogeneity sources into hardware, platform, feature and API. Again, each class is categorized into vertical and horizontal classes. A vertical class is related to single hardware, single service or single operating system, whereas horizontal class is related to more than one hardware, multiple services and multiple operating systems. This paper also describes some of the major challenges of MCC.

Toosi et al. Taxonomy

Toosi et al. [7] have illustrated the motivation for the inter-connectivity of cloud computing among different service providers. They have described the challenges of interconnecting cloud services and proposed a taxonomy for the challenges. The challenges are composed of the following categories: Provisioning, Portability, Service Level Agreement, Security, Monitoring, Economy, Network, and Autonomics. Each category is divided into several sub-categories. For example, the challenges involved in portability category are divided into: Virtual Machine mobility, Virtual Machine portability and Data portability. People who are involved with interconnecting multiple services can use this taxonomy as a start-up reference to know expected challenges. The limitation of the paper is that challenges of different deployment models (SaaS, PaaS, IaaS) are not duly considered.

Kachele et al. Taxonomy

Kachele et al. [8] have proposed a taxonomy which is more fine-grained in terms of service offerings from the providers. For example, they have divided the PaaS into Runtime Environment as a Service (RaaS) and Framework as a Service (FaaS). IaaS is divided into Operating System as a Service (OSaaS) and Hardware as a Service (HWaaS). They have utilized the abstraction of different types of currently existing services (SaaS, PaaS, and IaaS) to make them specified in more granular terms. Storages and Networks are also considered as services (StaaS and NaaS). As such, the resources are viewed from three different domains: Compute, Storage and Network. This taxonomy will help system administrators, software developers and system architects in specifying requirements for cloud services. However, security issue is not considered by the authors in this paper.

B. Performance Taxonomies

Performance taxonomies focus on the performance feature of cloud computing.

Li et al. Taxonomy

Li et al. [5] proposed a taxonomy to evaluate the performance of commercial cloud services. The proposed taxonomy identifies the atomic elements of cloud-related performance evaluation and arranged them in two-dimensional spaces. This taxonomy can be used for the existing evaluation practices by decomposing them into elements. It can also be used to design new experiments through composing the elements. The motivation of their works is that they have found non-standardized terminology, correct but imprecise analysis, and incorrect analysis of cloud computing which could obstruct understanding CC. The two dimensions of taxonomy are: Performance feature and Experiment. Performance feature is further divided into two parts: physical & capacity part and experiment part. Experiment part is divided into environmental scene and operational scene. However, the authors did not present any case study of evaluation commercial cloud providers in this paper.

Barbar et al. Taxonomy

Barbar et al. [15] proposed a classification of frequent failures found in cloud computing. The failures are categorized as: Overflow, Timeout, Network failure, Hardware failure, Software failure, Database failures and others. This classification intends to help consumers to be more cautious and decisive while signing contract with the providers. But the classification provided in this paper is not that detailed.

C. Security Taxonomies

Habib et al. Taxonomies

Habib et al. [9] have proposed a framework for assessing the trust-worthiness of the cloud providers' claim of satisfying the controls of Consensus Assessments Initiative Questionnaire (CAIQ) in this paper. They have mapped the controls of CAIQ into trusted properties and stated who is going to validate the properties. The framework aims to resort the hybrid model of trust validation which is a

mixture of soft and hard trust validation procedures. This framework takes the input of users' trust thresholds which are somewhat difficult for the users.

Abuhussein et al. Taxonomy

Abuhussein et al. [11] have proposed a taxonomical approach to find out the security attributes the cloud consumers should be concerned with. The taxonomy consists of several levels: level-0 includes different types of stakeholders, level-1 comprises cloud computing deployment methods, level-2 includes different types of service models, level-3 defines corresponding issues and level-4 determines the attributes. With the help of this taxonomy, the consumers can compare different cloud providers based on security issues. This work can also help cloud providers to improve their security levels to compete in the market and ensure better customer satisfaction. This approach considers the well accepted standards of cloud computing provided by NIST.

Prodan et al. Taxonomy

Prodan et al. [12] proposed a taxonomy that identifies a common terminology and architectural and functional similarities among the cloud providers. It consists of eight elements: service type, resource deployment, hardware, runtime tuning, security, business model, middleware and performance. The security element is composed of three categories: Authentication, Static IP address and Firewalls. Authentication is provided by simple login and password mechanism. Static IP address helps configure specific security policy for a specific user. Firewall prevents unauthorized access to cloud resource. However, the authors did not consider the whole range of security risks and vulnerabilities of cloud computing.

Gonzalez et al. Taxonomy

Gonzalez et al. [14] have identified the major cloud security issues and grouped them into seven categories: Network Security, Interfaces, Data security, Virtualization, Governance, Compliance and Legal issues. Based on this, they have proposed a taxonomy of cloud security. It is divided into three main dimensions: Architecture, Compliance and Privacy. All the dimensions include sub categories that cover the identified problems of cloud security. The proposed taxonomy helps to identify how much research efforts have already been made in those dimensions and which area needs to be focused on. The authors have taken into consideration of all efforts made by the European Union Agency for Network and Information Security (ENISA), CSA and NIST.

Gruschka et al. Taxonomy

Gruschka et al. [18] proposed a taxonomy of cloud computing attacks and classified them into three entities: service users, service instances and cloud providers. Any attack in the cloud can take place by interactions within these three entities. The attacks are classified based on which entity has attacked which entity. For example, if a cloud provider is the attacker and service user is the victim, then it is a cloud-to-user attack. The six categories of attacks among the three entities are: service-to-user, user-to-service, cloud-to-service, service-to-cloud, cloud-to-user and user-to-cloud. So, with the help of this taxonomy, any entity can be aware of the risks and security threats from other entities.

IV. Limitations And Future Work

Taxonomies provide means to exhaustively detail the cloud computing domain by breaking it down to fine grained sub-components. The efforts in CC taxonomy presented in this paper have paved the way to solve many problems. Some intended to define cloud computing components and their relations whereas others tried to provide means to compare or rank entities like: services, providers, certifications, etc. These efforts were used by researchers and technology manufacturers to further explore the domain and produce solutions in many areas like green computing, performance, security, etc. Digital forensics investigators have also used these classifications to trace digital crimes [20]. However, most of the efforts focuses on a specific service (SaaS, PaaS, or IaaS), a particular stakeholder (e.g. provider, consumer, broker, etc.), or a specific purpose (e.g. energy/cost efficiency).

In this paper we presented various taxonomies from literature. We classified them objective-wise into three classes (conceptual, security, performance, etc.). Yet, taxonomies can also be classified from different perspectives rather than objective-wise. For instance, NIST and Abuhussein et al. [1, 11] presented two taxonomies of different purposes (i.e. conceptual, security respectively) as though both taxonomies are stakeholder oriented. Taxonomies can also be classified methodology-wise (e.g. standards-based, and hardware/software-based.).

There is an apparent lack of consensus on a unified CC taxonomy that serves all research purposes. So, we aim to combine existing taxonomies and propose a unified taxonomy in future.

V. Conclusion

A well-organized cloud taxonomy leads to consensus on standards and terminologies for cloud computing. In this paper, we have classified the existing efforts in cloud computing taxonomy research so that readers can get a glimpse of CC taxonomy state-of-research. We highlighted the important efforts in cloud taxonomy and shed light on their capabilities and conformance to standards.

In spite of the fair amount of taxonomy research, there are CC aspects that are yet to be fully explored. Moreover, some aspects might not be explored at all due to the evolving nature of the cloud. So, it is not possible at this point to determine whether any of the presented taxonomies is more appropriate than the others for all purposes. As new CC

taxonomy efforts are proposed in the future, it is obvious that new classes may need to be introduced in our classification of taxonomies.

REFERENCES

[1] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication, 500, 292.

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[3] Rimal, B. P., Choi, E., & Lumb, I. (2009, August).A taxonomy and survey of cloud computing systems. In INC, IMS and IDC, 2009.NCM'09. Fifth International Joint Conference on (pp. 44-51). Ieee.

[4] Alliance, C. (2011). Security guidance for critical areas of focus in cloud computing v3. 0. Cloud Security Alliance.

[5] Li, Z., O'Brien, L., Cai, R., & Zhang, H. (2012, June).Towards a taxonomy of performance evaluation of commercial Cloud services. In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on (pp. 344-351).IEEE.

[6] Dukaric, R., &Juric, M. B. (2013). Towards a unified taxonomy and architecture of cloud frameworks. Future Generation Computer Systems, 29(5), 1196-1210.

[7] Toosi, A. N., Calheiros, R. N., & Buyya, R. (2014).Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey. *ACM Computing Surveys (CSUR)*, *47*(1), 7.

[8] Kächele, S., Spann, C., Hauck, F. J., & Domaschka, J. (2013, December). Beyond IaaS and PaaS: An extended cloud taxonomy for computation, storage and networking. In *Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing* (pp. 75-82). IEEE Computer Society.

[9] Habib, S. M., Varadharajan, V., &Muhlhauser, M. (2013, July). A Trust-aware Framework for Evaluating Security Controls of Service Providers in Cloud Marketplaces. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 459-468). IEEE.

[10] Schneider, S., Lansing, J., Gao, F., &Sunyaev, A. (2014, January). A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on* (pp. 4998-5007).IEEE.

[11] Abuhussein, A., Bedi, H., & Shiva, S. (2013, June). Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing. In *Proceedings of the 2013 IEEE Sixth International Conference on Cloud Computing* (pp. 958-959).IEEE Computer Society.

[12] Prodan, R., & Ostermann, S. (2009, October). A survey and taxonomy of infrastructure as a service and web hosting cloud providers. In *Grid Computing, 2009 10th IEEE/ACM International Conference on* (pp. 17-25).IEEE.

[13] Repschlaeger, J., Wind, S., Zarnekow, R., &Turowski, K. (2012, January). A reference guide to Cloud Computing dimensions: Infrastructure as a service classification framework. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 2178-2188).IEEE.

[14] Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., &Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing*, *1*(1), 1-18.

[15] Barbar, J. S., Lima, G. D. O., &Nogueira, A. (2014, March). A Model for the Classification of Failures Presented in Cloud Computing in Accordance with the SLA.In Computational Science and Computational Intelligence (CSCI), 2014 International Conference on (Vol. 1, pp. 263-267).IEEE.

[16] Howard, J. D., & Longstaff, T. A. (2013). A common language for computer security incidents. Sandia National Laboratories (1998). *Forschungsbericht. SAND98-8667*.

[17] Youseff, L., Butrico, M., & Da Silva, D. (2008, November). Toward a unified ontology of cloud computing. In Grid Computing Environments Workshop, 2008. GCE'08 (pp. 1-10). IEEE.

[18] Gruschka, N., & Jensen, M. (2010, July). Attack surfaces: A taxonomy for attacks on cloud services. In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on (pp. 276-279).IEEE.

[19] Sanaei, Z., Abolfazli, S., Gani, A., &Buyya, R. (2014). Heterogeneity in mobile cloud computing: taxonomy and open challenges. Communications Surveys & Tutorials, IEEE, 16(1), 369-392.

[20] Marty, R. (2011, March). Cloud application logging for forensics.In Proceedings of the 2011 ACM Symposium on Applied Computing (pp. 178-184).ACM.