Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing

Abdullah Abuhussein, Harkeerat Bedi, Sajjan Shiva
Computer Science Department
The University of Memphis
Memphis, USA
{bhussein, hsbedi, sshiva}@memphis.edu

Abstract— **The emerging paradigm of cloud computing (CC) arises security risks that adversely impact its different stakeholders. The widespread deployment and service models of CC in addition to the wide variety of stakeholders make it difficult to guarantee privacy and security. This work-in-progress paper proposes a stakeholder-oriented taxonomical approach that determines the security and privacy issues for various CC models from a stakeholder's perspective. It recommends a comprehensive list of security and privacy attributes that are related to these issues. The goal is to provide stakeholders with the security issues associated with their interaction with the cloud. This will assist every stakeholder of a CC model in identifying the security and privacy concerns that are pertinent to them, based on the service and deployment model they use. This will help promote security and privacy among the stakeholders and refute their fears from utilizing this emerging technology.**

Keywords: cloud computing, cloud computing security, taxonomy, cloud stakeholders, cloud privacy, service models

I. INTRODUCTION

With the significant advancement in cloud computing, among other issues, security is considered as highest priority. Researchers in academia and industry are striving to propose a security silver bullet. However, the pool of the cloud service providers is getting bigger, and the services offered through the cloud as a utility are increasing rapidly. Security and privacy issues are becoming harder to trace and control because of (1) the diversity in these issues (security breaches, disasters, etc.), (2) the number of service forms that CC enjoys (SaaS, PaaS, and IaaS), (3) and the kinds of deployment models of CC (Public, Private, Hybrid, Community).

Moreover, Cloud adopters are also capable of obtaining nested services from different service providers. This increases divergence of stakeholders' authority and control over the multiple service and deployment models. This lack of consensus among stakeholders on the authority of the security concerns broadens the scope of the problem [6]. Furthermore, laws and regulations diverge in some industries and different locations make it even harder to focus towards providing a unified process to secure the CC model.

In order to cope with these issues, we attempt to segregate the security and privacy issues of different CC deployments and services based on how the stakeholders interact with a CC model. We are presenting a stakeholder-oriented taxonomy that structurally enables the comprehension of all the various CC model components and their security aspects. It also recommends a list of security and privacy attributes associated with the way a stakeholder interacts with the cloud. This provides the opportunity to improve the security and privacy in their interaction.

II. MOTIVATION

The current CC taxonomies are primarily geared towards representing the attacks on different CC services [1], the infrastructure of the cloud, or the different components of the CC model [2]. Some other approaches investigated the security requirement of the CC models but were directed towards a single stakeholder's perspective or a single service that could be offered through the cloud [3]. These approaches and similar ones have been extensively presented in literature but we are yet to observe their benefits in the real world in terms of security and privacy improvement. In this work we propose a stakeholder-oriented taxonomy that determines the security and privacy issues for various CC models from a stakeholder's perspective. The novelty of this approach is to draw the line between the security concerns, responsibilities and needs of the different cloud stakeholders so they can address them.

III. OUR STAKEHOLDER-ORIENTED APPROACH

To address the above mentioned issues, in this paper we present a unique approach that is:

- Taxonomical: this methodological arrangement of features enforces a better understanding of the different use cases of a CC model and facilitates extensions and upgrades on the same in the future.
- Inspired from the NIST characteristics of cloud computing [4], to conform to the standards in the field.
- Stakeholder-oriented: Stakeholders are the most tangible aspect of the CC model and hence they represent a significant part of the taxonomy. Every stakeholder's interaction with the CC model will be classified in route that ends with a list of suggested security and privacy attributes.

Our taxonomy is shown in Figure 1 and is composed of five levels. Because of space constraints, we illustrate only two stakeholder scenarios in Figure 1. Level 0 of the taxonomy is the stakeholder's level with an extensive pool of

978-0-7695-5028-2/13 $26.00 © 2013 IEEE
DOI 10.1109/CLOUD.2013.132

nine possible stakeholders followed by the NIST deployment and service models in level-1 and level-2 [4]. In level-3 we provide a list of potential security and privacy issues [5]. The taxonomy proposes a list of attributes [6] that are associated with the corresponding issues in level-4.

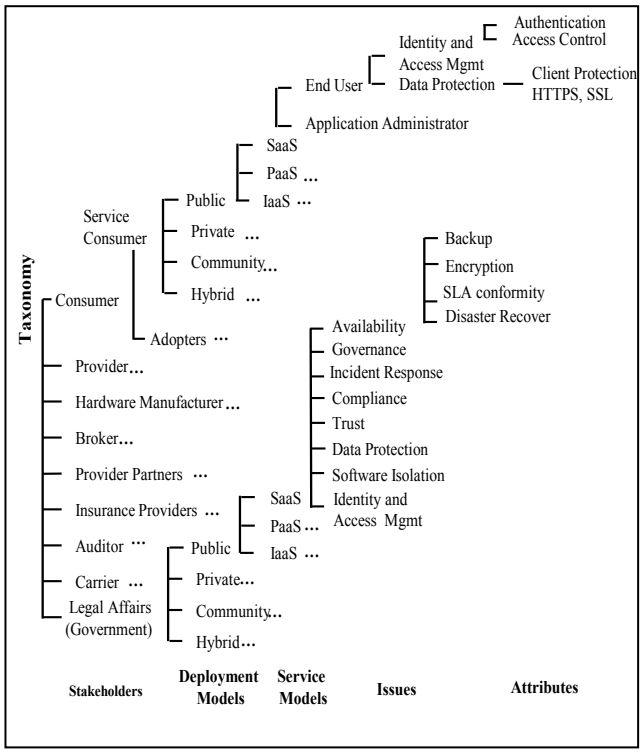

Figure 1. Our Stakeholder-Oriented Taxonomy.

The stakeholder level of the taxonomy tends to be the most important classifying factor. It states the scenario of the stakeholder who is interacting with the CC model. The taxonomy traversal in Figure 1 starts at first level (Stakeholders). By determining a choice in level-0 you decide the stakeholder of the scenario. Further to the right is level-1 (Deployment Models), and level-2 (Service Models) to determine the type of the CC. Based on the choices of the first three levels we setup the scenario of our interest and obtain a list of possible security and privacy issues in level-3 and a list of security attributes in level-4. For instance (Scenario A) in top part of Figure 1; a user who interacts with Google Docs to create or edit a text document would be traversed on the taxonomy as an end user consumer on a SaaS public cloud. Identity and access management and data protection are the possible security and privacy issues in level-3. Level-4 presents authentication and access control as two suggested security and privacy attributes associated to the issues the previous level. A representation of the taxonomy traversal for this scenario is shown in Table I.

Another interesting scenario is the Government that puts and enforces laws. This is shown in the lower half of the Figure 1. Our approach intends to see the Government as judicial and legislative authority and then provide them with the security and privacy issues and attributes for this mission. The issues that interest the Government as a stakeholder when devising and enforcing laws and regulations for the CC model are availability and governance. The security attributes associated with these issues such as backup, encryption, etc. are also suggested by the proposed taxonomy.

Another interesting utilization of this taxonomy is to enable stakeholders to learn the security concerns of other stakeholders by simply tracing their roles through this taxonomy. For examples, this can help the providers can in understanding the security requirements of their consumers.

TABLE I. A TAXONOMY BASED REPRESENTATION FOR SCENARIO A

Features	Scenario A	
Stakeholder	End User (Consumer)	
Deployment	Public	
Service	SaaS	
Security Issues	Identity and Access Mgmt	Data Protection
Sec. Attributes	Authentication, Access Control	Client Protection

IV. CONCLUSION AND FUTURE WORK

This paper presents a unique approach to define the security scope for the different stakeholders of a cloud computing model. We extensively examined the various cloud stakeholders, determined their ways of interacting with the cloud and investigated the security issues that can concern them based on their nature of interaction with a CC model. Our proposed taxonomy provides them with a comprehensive list of security and privacy attributes that are associated with their issues. The strength of this approach resides in its affinity to the stakeholders and its capability to comprehend different scenarios. It reduces the stakeholders' efforts to identify the issues in the different forms of CC services they use. As a work-in-progress, we aim to continue to collect the security and privacy issues and their related attributes. Moreover, we intend to examine our approach on popular and diverse stakeholders like commercial service auditors, brokers and cloud service providers.

REFERENCES

[1] G. Nils, M. Jensen,"Attack surfaces: A taxonomy for attacks on cloud services." Cloud Computing (CLOUD), 2010 IEEE 3rd Int'l Conf.

[2] R. Prodan, S. Ostermann. "A survey and taxonomy of infrastructure as a service and web hosting cloud providers." Grid Computing, 2009 10th IEEE/ACM Int'l Conference on.

[3] N. Bhensook, T. Senivongse. "An assessment of security requirements compliance of cloud providers." Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th Int'l conf.

[4] NIST,"http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf" , retrieved on Feb 20, 2013.

[5] NITS, "Guidelines on Security and Privacy in Public Cloud Computing",http://csrc.nist.gov/publications/nistpubs/800144/SP800-144.pdf, retrieved on Feb 20, 2013.

[6] Abuhussein A., Bedi H., Shiva S., "Evaluating Security and Privacy in Cloud Computing Services:A Stakeholder's Perspective", (ICITST-2012).