CSSR: Cloud Services Security Recommender

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

Frederick T. Sheldon
Computer Science Department
University of Idaho
Moscow, ID
sheldon@uidaho.edu

Abstract— **The emerging paradigm of cloud computing (CC) presents many security risks that can potentially and adversely impact any one of the plethora of stakeholders. The widespread deployment and service models of CC in addition to the wide variety of stakeholders make it difficult to comprehend security and privacy (S&P). In this paper, we present CSSR[1], a Cloud Services Security Recommender tool. CSSR codifies a stakeholder-oriented taxonomy. The goal for CSSR is to identify the various S&P risks for the kaleidoscope of different CC models from the stakeholder's perspective. CSSR will recommend a comprehensive list of S&P attributes that must be considered as controls necessary to minimize the CC attack surface. By identifying the S&P concerns that are unique to the particular usage scenarios (again from a stakeholder perspective), CSSR provides a comprehensive basis from which to choose alternative security solutions. This model then provides a structured and well-informed process of mitigating risk as envisioned by each and every stakeholder based on their needs.**

Keywords: cloud computing, cloud computing security, cloud taxonomy, cloud stakeholders, security and privacy, service computing, cloud economics.

I. INTRODUCTION

With the significant advancement in Cloud Computing (CC), among other issues, cloud security is considered as the highest priority. Researchers in academia and industry are striving to propose holistic security solutions for the cloud. However, the pool of the cloud service providers (CSPs) is getting bigger, and the services offered through the cloud as a utility are increasing rapidly.

Recent incidents on Amazon AWS [1], Adobe [2], Dropbox, Google Drive, and iCloud [3] indicate that the leaders in CC market are not immune to becoming victims of fatal security issues. These incidents and similar ones have caused significant damages to governments, private enterprises, and the general public in terms of financial loss, data confidentiality, and reputation.

Despite all the attempts of service providers in the market and the efforts by researchers and industry to protect cloud services, CC stakeholders are yet to put their hands on security approaches that maintain availability, elasticity, expandability and at the same time guarantees S&P. The practical reasoning for this is embodied in the next section.

II. MOTIVATING SCENARIOS

In this section, we introduce motivating scenarios. We illustrate the limitations of the current S&P solutions to handle security in these scenarios.

A. Cloud Computing Landscape

S&P problems are becoming harder to trace and control [6]. This is due primarily to the following three factors (1) sheer diversity and lack of stronger reporting regulations and policy (security breaches, disasters, reputation etc.), (2) number of service forms that CC enjoys (SaaS, PaaS, and IaaS) and, (3) kinds of deployment models of CC (Public, Private, Hybrid, and Community). Moreover, security of cloud services may fluctuate due to the dynamic Internet environment [7], which makes security inherently uncertain and consequently the need for an efficient CC security advising approach is becoming much more urgent. Finally, CSPs usually have different offerings for the same S&P feature (e.g. different disaster recovery plans with various volumes, backup and restore bandwidths, etc.), each of which adds complexity and has its own significance and cost. This raises the need for an approach that is *structured* and *expandable* to enable effective updating of emerging and obsolete solutions. Such an approach must draw the consumers' attention to the various facets in those complex and diversified S&P solutions that are available in market. Furthermore, the degree of protection that every solution offers carries its own inherent costs/risks. Thus, a *quantitative* approach is deemed valuable and desirable.

B. The Stakeholder Conundrum

CSPs must be able to alleviate adopters' S&P concerns. They provide cloud services with a variety of S&P attributes, yet many cloud adopters, in their haste to reduce costs and focus on performance at expense of security. Adopters typically do not know how to properly setup these services. Thus, they end up falling into additional costly contractual and operational measures while at the same time without fully understanding the architectural security risks. This is evidenced by the eighth top cloud security threat from CSA's (Cloud Security Alliance) notorious "Insufficient due diligence" [5]. Even experienced cloud consumers face a hidden potential

[1] This work is an expanded republication of the work first published as a WIP paper in IEEE CLOUD 2013 [4]

complexity when choosing S&P features. In March 2013, some customers of Amazon's S3 cloud storage left their data publicly exposed because they were not sure how to configure the privacy settings. That was discovered by a security testing firm who found more than 126 billion data files being publicly exposed [2].

Also, due to the variety of services and CSPs, in addition, to the elastic nature of clouds, cloud adopters are capable of obtaining nested services from different service providers. For example, a developer who is using an Oracle Cloud Platform – PaaS – that runs on top of Amazon EC2 instance(s) – IaaS. This scenario and many others increase the divergence of stakeholders' authority and control over the multiple service and deployment models. This raises the typically obfuscated question about who within the chain of providers is actually responsible (liable) for governing and maintaining security? The lack of consensus among stakeholders on this question of authority/responsibility of security concerns broadens the scope of the problem [6]. The issues described above become even worse due to stakeholders' apathy in CC security, stakeholders non-transparent interaction on the cloud, and laws and regulations divergence among industries based in different geographical locations.

Organizations have many different CC security objectives. This type of diversity involves different requirements, assets, exposure to public, and tolerances to security risks. An organization's ability to detect S&P weaknesses (i.e., issues) in CC, respond to them effectively depends on the organization's budget, and the criticality and sensitivity of such issues. Thus, the decision here is left to the organization to decide the degree of security that is needed based on how much they are willing to invest in safeguarding their cloud-based assets.

The matters above call for a solution that reduces the stakeholders' efforts to protect their cloud services, supports *consumer involvement* and promotes *accountability*, and *transparency* among stakeholders so that they can *make well-informed decisions*. Therefore, we introduce CSSR (Cloud Service Security Recommender) to boost these qualities.

We presented a brief overview concerning scenarios of insecurity in CC. In the remainder of this paper, we go over a brief literature review of the existing cloud S&P recommenders from research and industry in Section 3. In Section 4, we introduce our "cloud services security recommender" tool. Section 5 and 6 present tool integration and an empirical test of the proposed tool respectively. We evaluate the tool in Section 7. We explore CSSR limitations and future plans in 8 and conclude in Section 9.

III. RELATED WORK

Cloud security includes old and well-known issues (e.g. network, user access, authentication, and privacy) and also emerging concerns mainly Virtual Machine (VM) security issues (e.g. VM starvation, VM jumping, VM side channel attacks, etc. [8]). These issues are researched independently, and some are innovatively solved. However, a secure CC environment requires several countermeasures working harmoniously together to provide a fully resilient solution.

Some industry leaders demonstrate effective security as a service (SECasS) solutions combining technology and innovative business models to safeguard clouds. CloudPassage Halo [9], CipherCloud [10], and CloudLock [11] among others are popular commercial cloud security solutions. Their business is to secure computing services. Most of these solutions emerged with the cloud and had naturally advanced well since then. Thereby, customers who do not want to hassle can simply rely on a commercial cloud security solution. However, these solutions are not flawless. For instance, they offer cloud compliance support for standards like PCI DSS, HIPAA, SOC 2, ISO 27001, and COBIT5 yet, DISA (Defense Information Systems Agency) and the DoD (Department of Defense) have recently identified shortcomings within these standards, particularly in the areas of boundary defenses, privileged users, audits and incident response [12]. Therefore, cloud adopters should not take commercial security solutions for granted. They still must take due diligence with regard for the specifications of security features provisioned within the cloud service. The main difference between these commercial tools and our proposed recommender tool are that we focus on educating stakeholders about security issues and solutions in clouds, and guiding them throughout the security features selection process by supporting consumers' involvement and promoting accountability, and transparency.

Also, founders of standards in cloud security like CSA, NIST, and ENISA among others produced security controls to be used by cloud adopters to maintain security. For example, the CSA Cloud Control Matrix [13], NIST Federal Information Systems Security Controls [14], ENISA CC information assurance requirements [15] and others (e.g. FERPA [16], HIPPA [17], etc.). Although these controls aim to counteract or minimize security risks in cloud environments, novice cloud adopters and even experienced adopters still see that security is a major concern. A recent study shows that cloud adopters still find it less strenuous to rely on CSP or a third party (e.g. broker) to choose security features for their clouds [18]. The reason for this confusion is that the list of controls is colossal and overlapping among stakeholders. Consequently, monitoring and controlling these controls is a hard problem. This leads to more problems such as lack of knowledge and overlapping security features. Refer to the whitepaper in reference [19] for examples of some generic cloud use cases. We propose a tool that utilizes these security controls and enables CC consumers to better understand and wisely choose security attributes from a pool of various security attributes.

Besides standards and commercial solutions, cloud service recommenders (CSRs) have been the focus of study within the research community. Cloud service recommenders aim to enable simplified and intuitive cloud service selection. Past efforts in cloud service recommenders are either:

- Geared towards selecting a service based on its qualities [20-27] or its non-functional requirements with some focus on security, but no research has up to now, presented a cloud security recommender.
- Focused on a particular CC application like multimedia clouds, storage as a service clouds, etc. [22,26]
- Tailored to choose a service based on existing consumers' feedback or future consumer's' requirements. However, when choosing security features, we cannot rely on consumers' decision only [20- 27].
- Designed to treat all recommendation criteria equally in terms of their importance [20, 21, and 27]. However as stated before, different consumers might have different requirements, assets, exposure to public, and tolerances to security risk.

Finally, expert systems methods have much to offer to security practitioners. This work is inspired by important works that propose utilizing expert systems in the area of security [28, 29].

CSSR tool embraces three taxonomies to enable stakeholders to comprehend their CC model(s) and to identify its potential security issues based on possible attack surfaces. It also educates stakeholders about their security issues by listing each one's operational impact(s), informational impact(s), and thereby recommends a defensive action(s) for enabling a corresponding (set of) security attribute(s).

IV. CSSR: CLOUD SERVICES SECURITY RECOMMENDER

The proposed CSSR is enjoys following features:

- Scenario-based: provides hypothetical stories to help users work through a complex problem and evaluate usage patterns and operational scenarios. The process here is based on the principle that behavior occurs within specific contexts. Every stakeholder interacts with the cloud in a certain way. Thus, every stakeholder needs to focus on and comprehend the operating CC model, which facilitates better and more well-informed choices. In turn, this promotes cloud security accountability.
- Taxonomical: CSSR is a triage tool that provides a methodological arrangement of components. This, in turn, enforces a better understanding of the different use cases of a CC model and facilitates *extensions* and *upgrades* on the same in the future.
- NIST-Inspired characteristics of CC [33]: CSSR conforms to the standard practices in the field.
- Stakeholder-oriented: Stakeholders are the most tangible aspect of our CC model and hence they represent a significant part of the taxonomy. Every stakeholder's interaction with our CC model will be classified in a manner that resolves into a list of recommended S&P attributes. Due to the "lack-of-trust" dilemma that has emerged within the CC environment, we would argue that a shift from the data ownership approach to a stakeholder-oriented approach and a consumption scenario based approach can go a long way towards reducing the major weaknesses inherent in the data ownership approach to security.

With these characteristics we propose a unified process to secure CC environments by:

- Promoting Stakeholder involvement in the defining the security needs and responsibilities.
- Promoting stakeholders' transparency for trustworthy cloud services by considering both consumer and provider involvement. This also encourages healthy competitiveness among CSPs.
- Promotes stakeholder's accountability by defining the security responsibility of every stakeholder.

CSSR (Figure 1) has two main objectives. Given a scenario (i.e. a consumer, a service, and a deployment model), CSSR (1) identifies the potential S&P issues, and (2) recommends essential S&P attributes to stakeholders to assist stakeholders in selecting a service with the appropriate security features and the stakeholder goals – e.g. maximum gain, minimum cost.

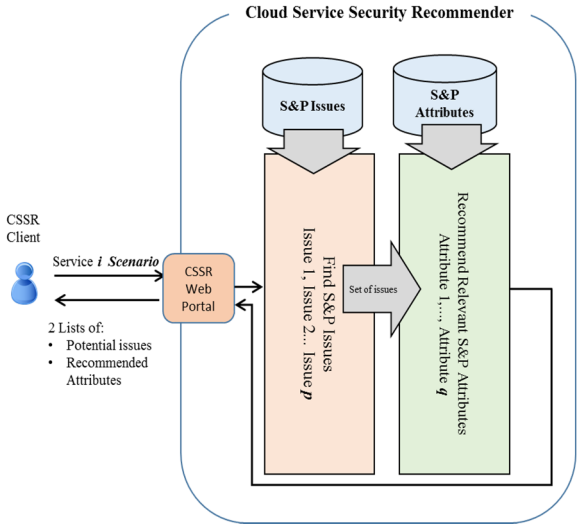

Figure 1. CSSR Components

We will first illustrate the framework and the methodology based on which the tool is built, and further elucidate in details architecture of the proposed tool. The following subsections present how CSSR functions:

A. Stakeholder-Oriented Taxonomy

One of the immutable features of electronic services, in general, is that services are actions performed by an entity (provider) on behalf of another (consumer) [30]. In other words, for it to be considered a service, it has to be demanded, discovered and more importantly consumed. Consequently, before the service requires protection, a consumer must start utilizing it. We call this the consumption scenario of the service.

In this context, the proposed solution takes a consumption scenario from set $SC = \{sc_1, sc_2, sc_3 \ldots sc_l\}$ as an input (Figure 1). This scenario builds the CC model. Each scenario consists of a consumer (i.e. application developer, tester, deployer, application administrator, end user, organization, software administrator, system

administrator, third party software provider/designer) [31] who interacts with a service model (i.e. SaaS, PaaS, or IaaS). This service interaction is utilized over a deployment model (i.e. public, private, hybrid, or community).

Every consumption scenario is vulnerable to potential S&P issues. CC services are usually offered with S&P attributes that are either default (e.g. Access Control, Authentication, etc.), or non-default where a consumer must request the attribute and a fee might be involved, like backup, encryption, etc. Additionally, cloud consumers demand and get S&P attributes directly from the service provider or through a service broker. However, different CSPs offer multiple options of every attribute. Each of which has different properties. For example, A CSP can offer two backup attributes with different restoration bandwidth. Also, it is worth noting that the same attribute might be used to secure the model from more than one S&P issue. Based on this, we propose taxonomy to effectively and clearly elicit the S&P issues threatening every consumption scenario and recommend corresponding safeguarding attributes.

To demonstrate how this taxonomy can be traced to secure CC, consider the following use case: An (Application Developer) consumer wants to develop a SaaS application and deploy it on top of a public cloud infrastructure for public to use. In this case, the developer consumes IaaS and PaaS. The developer is also a provider of SaaS that is consumed by the end users. Our taxonomy represents every scenario as:

Scenario= (Stakeholder, Service, Deployment)

Example 1: *Sc1 = (Application Developer, IaaS, Public)*

Example 2: *Sc2 = (End User, SaaS, Public)*

According to the consumption scenario, the taxonomy shows a pre-stored list of potential S&P issues and recommends, at least one, defensive security feature pertaining to each S&P issue. $R = \{ r_1, r_2, r_3, \ldots, r_n \}$ and $A = \{ f_1, f_2, f_3, \ldots, f_m \}$ are respectively, the set of all possible S&P issues and all possible safeguarding features in CC.

So a scenario can be described in terms of its S&P risks as D_i row vector $[d_1 \; d_2 \; \ldots \; d_n]$ that describes a scenario $sc_i \in SC$ where each element $d_j \in D_i$ represents vulnerability of the scenario sc_i from r_j of R.

Similarly, a scenario can be represented in terms of its safeguarding S&P attributes as A_i row vector $[a_1 \; a_2 \; \ldots \; a_m]$ that describes a scenario $sc_i \in SC$ where each element $a_j \in A_i$ represents a protecting S&P attribute of the scenario sc_i .The stored values of the two vectors are carefully identified by breaking up the scenario into smaller and analyzable portions using taxonomy B and C in the following subsections. Analyzing a consumption scenario enable us to prospect S&P issues that have the likelihood to occur in order to protect the cloud from them. Scenario analysis [32] is a process of analyzing possible events by considering possible alternatives. It has been widely used in finance and economic to forecast risks to allows improved decision-making by allowing consideration of outcomes and their implications.

B. Attack Surface Taxonomy

The attack surface taxonomy in reference [33] (See Figure 2) aims to anticipate the classes of vulnerabilities that arises from the CC paradigm. It helps in classifying S&P issues, thus making CC more concrete. We use this taxonomy to enable dividing every scenario into 6 tinier sub-scenarios (i.e. attack surfaces) based on how *user*, *cloud* and *service* interact.

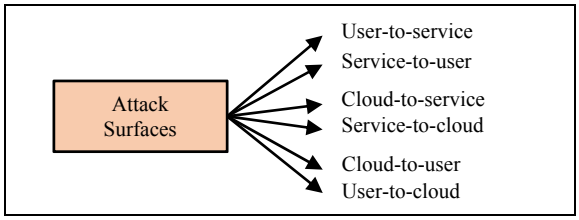

Figure 2. CC Attack Surface Taxonomy.

The attack surfaces (Figures 2) means the sum of security risk exposure and is divided to:

(a) *Service-to-user*: all kinds of attacks that are performed by the service against a user which are possible in ordinary client-server-architectures. The threat targets here are client, interface, network and data. For example, buffer overflow, SQL injection, etc.

(b) *Cloud-to-user:* all kinds of attacks that are performed by clouds against a user using the interface controlling the service (control panel) and insider attackers. The threat targets here are client and Interface (e.g. Amazon EC2 Control Panel). For example, acquire more instances, delete instances, etc.

(c) *User-to-service*: all kinds of common environment attacks a client program (interface) provides to a server. The threat targets here are client and Interface. For example SSL spoofing, phishing attacks.

(d) *User-to-cloud*: all kinds of attack that targets a user to originate attacks at the cloud system. The threat targets here are Virtualization, and Data. For example faked usage of cloud service and bill increase.

(e) *Cloud-to-service*: all kinds of attacks a cloud provider can perform against a service running on it. Threat targets here are Virtualization, Network, and Data. For example Availability reductions.

(f) *Service-to-cloud*: all attacks that a service instance can run against its hosting cloud system. Threat targets here are Virtualization, Network, and Data. For example, attacks against the cloud system hypervisor.

Although attack surfaces (c), (d), (e), and (f) represent a vulnerability to attacks on service or cloud, however, the consumer will indirectly be the eventual victim. For instance, attack surface (f) affects the customer by triggering the cloud provider to provide more resources that the consumer does not truly need.

By dividing consumption scenarios into smaller pieces, we aim to enhance its analyzability, comprehensibility, expandability and structurability. Every attack surface that corresponds to a scenario is then

analyzed to find its potential attack vector and the essential safeguarding attributes in Section C.

C. AVOIDIT: Attack Taxonomy

For every attack surface in a scenario, S&P issues and defense methods are identified using AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact, and Target) taxonomy [34]. AVOIDIT provides details to support comprehending each attack classification. It uses the cause, action, defense, analysis, and target (CADAT) process to classify attacks against a particular target that corresponds to an attack surface of a CC scenario. The CADAT process consists of the following:

- Identify target(s) to which the defense is sought. Targets are client, interface, network, virtualization, compliance, governance, and Legal issues.
- Identify the attack vector(s): which are the potential CC attacks for each target.
- Identify the operational impact: The type of action conducted resulting from the impact the attack vector enabled to take place. Possible values are; misuse of resources, client compromise, cloud compromise, and denial of service.
- Classify the Informational Impact: Providing an analysis for reporting purposes to what damages have or may take place once the attack is successful. Possible values are: distort, disrupt, destruct, disclose, and discover.
- Classify the Potential Defense: Understand how to defend properly using preventative and reactive methods to a potential attack. Possible classifications are mitigation and remediation.

Every scenario that is constructed early in taxonomy A is decomposed into six possible attack surfaces using taxonomy B. AVOIDIT taxonomy further breaks down every attack surface into targets and then identify every targets potential attacks, and recommends a defensive action(s). We extrapolated the past published S&P incidents and CC regulatory bodies reports (e.g. ENISA, CSA notorious nine, NIST S&P guidelines) to extract and identify *attack vectors*, their *operational* and *informational impact*, and *defensive methods* in the following level of the taxonomy as in Figure 3.

Since AVOIDIT is only concerned with cyber-attacks, we tweaked its content to have physical and virtual related targets (e.g. Virtualization) as well as physical and virtual attack vectors. An attack vector in this context is a path by which an adversary can gain unauthorized access to the CC model. This includes vulnerabilities, as it may require several vulnerabilities to launch a successful attack. Thus, in this work, we consider cyber, physical and virtualization attacks in addition to vulnerabilities as attacks. The defense methods recommended by this taxonomy are then mapped to real-world S&P attributes (see [35, 36] for our list of cloud S&P Attributes) to enable consumers to meet their S&P requirements.

Taxonomies A, B, and C are respectively used to analyze CC consumption scenarios, break up every scenario to derive the potential S&P issues and recommend defense actions then interpreted those defensive actions into security attributes.

V. Scenarios Acquisition And CSSR Integration

CSSR [37] is a (php/mysql) web-based tool that accepts a consumption scenario as an input and outputs a set of potential S&P issues that can compromise the scenario and a set of S&P attribute(s) that are required to safeguard the scenario from each issue. Figure 4 shows the landing page where the user of CSSR selects a service model (e.g. SaaS, Pass, or IaaS), a deployment model (e.g. public, private, community, or hybrid) and the consumer type (e.g. application developer, tester, deployers, application administrator, end user, organization, software administrator, system administrator, third party software provider/designer). Based on user input the tool retrieves list the S&P issues and their corresponding S&P attributes as in Figure 5.

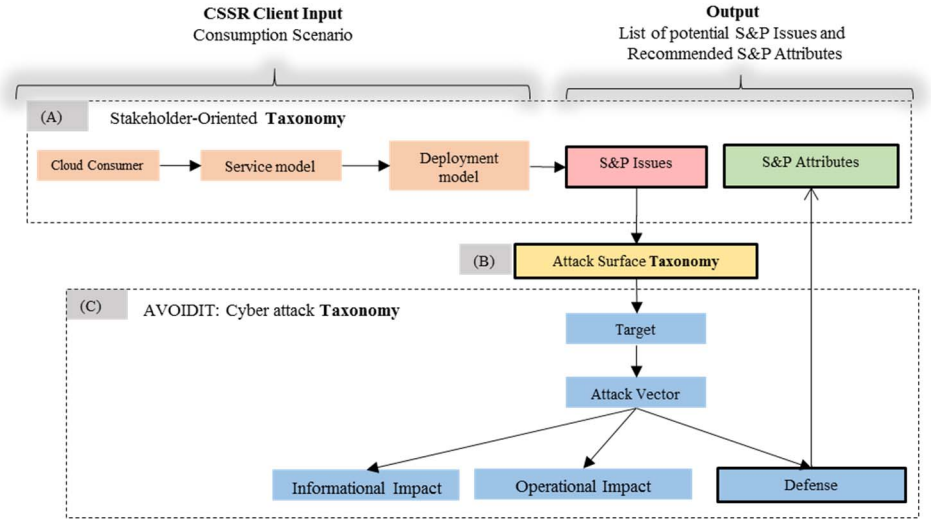

Figure 3. Operations flow in CSSR Framework of taxonomies.

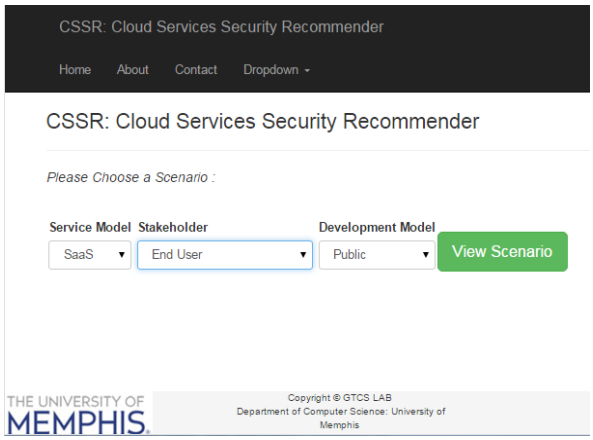

Figure 4. CSSR landing page shows client input

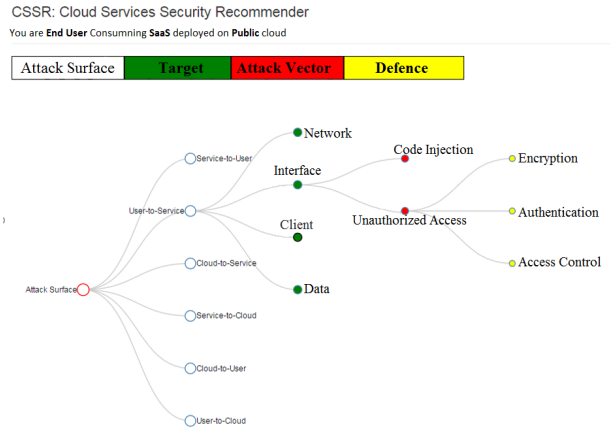

Figure 5. CSSR represents S&P issues (Attack Vector) and recommended Attributes (Defense)

VI. An Empirical Test Of A Taxonomy

The CSSR tool accepts a CC scenario as an input and identifies the possible S&P issues that can threaten that model. The system then recommends a set of S&P attributes that can be used to secure the model from each issue. Note that multiple Attributes can be used to secure the model for one issue. To do so, the recommendation system relies on the stakeholder-oriented taxonomy Figure 3 (A) that is composed of five levels. Level 0 of the taxonomy is the stakeholder's level followed by deployment and service models in level-1 and level-2. In level-3, Attack surface Taxonomy Figure 3 (B) and AVOIDIT taxonomy Figure 3 (C) to break a scenario for better analysis.

Based on the scenario analysis performed in level-3, the taxonomy recommends a list of attributes that are associated with the corresponding issues in level-4. These attributes include: backup, encryption, authentication and access control, dedicated hardware and data isolation, monitoring, data storage location, security standards and certifications, data sanitization, SLA guarantee and conformity, disaster recovery, performance and scalability, hypervisor security, and client-side protection. In addition to this list of tangible attributes we have a list of intangible attributes that are also necessary to consider for a CC scenario such as insider trust, new dimensions of security, customized security profiles, and self-healing.

For example, (Scenario X): 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. Unauthorized Access and Insider Attacks are the presented S&P issues in level-3. Level-4 presents (authentication, access control, encryption, and Insider trust) as recommended S&P attributes associated with the issues the previous level. A representation of the taxonomy traversal for this scenario is shown in Table I.

TABLE I. A TAXONOMY BASED REPRESENTATION FOR SCENARIO X

Features		**Scenario X**		
Stakeholder	L0	End User (Consumer)		
Deployment	L1	Public		
Service	L2	SaaS		
S&P. Issues	L3	-unauthorized access	Insider Attacks	…
S&P. Attributes	L4	-Authentication -Access Control -Encryption	-Insider Trust	…

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. The attributes in level-4 of the taxonomy were carefully identified, collected and categorized in [36]. They include a list of 19 different S&P attributes. Each of which is accompanied by a list of considerations that defines the quality of the attribute (i.e. how good is the attribute?). A sample attribute along with its considerations (i.e. yes/no questions) appears in Table II.

S&P attributes are simply features that are offered by CSPs or brokers as the provisioners of S&P in the cloud. These attributes and their considerations are then used to assess S&P and compare CC services so that consumers can make well-educated choices. CSPs also can use them to build and offer better cloud solutions.

TABLE II. A SAMPLE SECURITY ATTRIBUTE FOR CC.

	Consideration
Encryption	1. Is the data transferred to and from the cloud service encrypted by default? 2. Is the data that resides on cloud servers encrypted by default? 3. Does CSP have different offerings of encryption? 4. Is data encrypted while in process? 5. Do the CSP administrators know the keys used to decrypt consumers' data? 6. Does CSP support encryption that happens on consumers' computers (client-side)? 7. Is data encrypted in the backup facility? 8. Does CSP follow standards for encryption? 9. If (8) is yes, does encryption comply with standards in the countries where the service resides? 10. If (8) is yes, does encryption comply with standards in the countries where the service is consumed?

VII. Evaluation and Feedback

Given the increasing popularity of CC, much research has focused on security for different types of applications such as scientific computing, e-commerce, and web applications. Also, many organizations like NIST and

CSA have published S&P controls for cloud services [12 and 13]. Our work complements these standards by utilizing these security controls and enabling CC consumers to understand and choose among security attributes from a pool of security attributes. Now, the question becomes how does our proposed approach and CSSR tool impact CC security?

Herein we propose a systematic method for scenario analysis to guide CC stakeholders to choose (*effectively)* the most relevant (*correct*) S&P attributes. Naturally, we need to validate CSSR's correctness and effectiveness.

In the Fall of 2015, an offline version of CSSR was evaluated by 10 graduate students. Each of the students qualified on the basis of having recently completed at least one full semester of a graduate cloud computing cybersecurity course and/or similarly a software engineering graduate course. Each student completed a survey. Five participants played a consumer role, 3 played a CSP role, and 2 were considered security experts. We asked the consumers and security experts groups to give feedback on the tool in terms of its ability to recommend, educate, promoting transparency and accountability. The feedback was that the tool is easy to learn and understand, and the taxonomy helped them to comprehend the CC model. They all agreed that CSSR promotes transparency but not entirely convinced about accountability. The feedback from CSP group was that CSSR improves competitiveness. However, for security and business purposes, they were not totally confident to what extent CSPs can publicly share the description of their cloud security attributes.

To validate the correctness of CSSR output, we used a real-world example from recent publications. In late 2014, Code Spaces [38], a subversion and git (i.e. open source distributed version control system) hosting provider for software projects management and development was subjected a DDoS attack [39]. That DDoS attack turned out to be a smokescreen for another attack that was aimed at gaining access to the target's systems. Cyber security analysts described the incident as a textbook case and caused the company to shut down. Code Spaces was hosted on an Amazon web services (AWS) infrastructure where the backing up of data is left entirely to the end user. Several vendors offer solutions to ease backup efforts from Elastic Compute Cloud (EC2), but at a cost. According to the proposed CSSR, Code Space is a (System Admin) consumer of IaaS and should have obtained disaster recovery, backup attributes among others to maintain minimum S&P requirements which it did not.

CSSR is extensible and updatable. CSSR administrators keep track of any emerged and/or obsolete technology or S&P issues when CSSR lacks attribute(s) or over-recommends an attribute(s). Because CSSR ensures consistency, lack of redundancy (i.e., complementarity), and internal completeness of the generated scenarios, it can fully support user requirement variance toward fully meeting their CC needs.

VIII. CSSR Limitations And Future Work

A. Limitations

We believe that the contribution of CSSR lie, not only in its ability to assure a security tailoring for user's cloud environment needs but also in its capability to educate and prompt cloud consumers about potential S&P issues and other necessary security attributes (i.e. countermeasures) to enable effective decision making. The tool also seeks to promote transparency among providers to enable consumers to better understand the trade-off among competing providers who are then incentivized to provide more trustworthy and visible services. On the other hand, this tool can serve as a cloud service brokerage tool for service brokers. Also, an important feature of CSSR is the ability to continuously modify its internal taxonomy to track evolving technologies, issues, and S&P attributes. The inherent updatability of CSSR's internal taxonomy facilitates a formal and systematic approach to monitoring adapting/accounting for the natural migration of the threat/vulnerability space. Unfortunately, CSPs cannot be forced to cooperate in entering their offerings details into the tool, and we do not anticipate that they will voluntarily make their security attributes publicly available. However, they are motivated to cooperate with US-CERT and other entities that collect and disseminate the necessary (but possibly insufficient) information to keep our CSSR taxonomy current.

B. Future work

It is widely agreed that cloud security is more than just technical measures. There are different examples in which a cloud consumer's resources may be used by other parties in malicious ways that have negative economic impacts on consumers as well as CSPs [40]. This work is also closely related to cloud economics research area. At this stage, CSSR does not consider CSPs as users but there is nothing inherently adverse to such a use-case. CSSR enables S&P in clouds to become more quantifiable toward improving security awareness and thus supports: (1) S&P assessment of a service offered by a CSP against "other services offered by other CSPs". Given a consumption model and, at least, two CSPs, a score can be computed for every CSP individually to support selecting a particular service with the appropriate (e.g. maximum gain, minimum cost) security features. (2) Cloud S&P metrics against "a standard benchmark".

Acknowledgment

This work is partially supported by Cluster to Advance Cybersecurity & Testing (CAST), University of Memphis.

IX. Conclusion

We proposed (CSSR), a web-based CC recommender that offers stakeholders a holistic perspective for governing S&P of cloud service, minimizes risks and cultivates a cloud security culture amongst stakeholders. We demonstrated the rationale behind the stakeholder perspective to secure cloud environments and described

the tool framework. Our ultimate goal is to provide the opportunity to improve the S&P in CC.

We would argue that the presented approach will require significant change in attitude from all CC stakeholders in order to lead to better security culture and improve the security for all actors within the cloud environment. This tool aims to raise the bar for security awareness in CC and forms the basis for S&P assessment tool that will be presented in the future.

REFERENCES

[1] Hackenberger, B., "Encryption can make cloud computing safer, Special for CyberTruth, accessed from: http://www.usatoday.com/story/cybertruth/2013/05/31/cloud-security-hacking-encryption/2375689/

[2] Arkin B, "Important Customer Security Announcement", accessed from: http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html

[3] Salcedo, H. "Google Drive, Dropbox, Box and iCloud reach the Top 5 Cloud Storage Security Breaches List", Nov 2014 , accessed from http://psg.hitachi-solutions.com/credeon/blog/google-drive-dropbox-box-and-icloud-reach-the-top-5-cloud-storage-security-breaches-list

[4] Abuhussein, A., Harkeerat B., and Shiva, S.. "Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing." IEEE Cloud, 2013.

[5] Top Threats Working Group. (2013). The notorious nine: cloud computing top threats in 2013 [online]. Cloud Security Alliance.

[6] 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.

[7] Wang, S., Zheng, Z., Sun, Q., Zou, H., & Yang, F. (2011, April). Cloud model for service selection. In Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on (pp. 666-671). IEEE. Chicago

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

[9] CloudPassage, Agile security for agile enterprises, (2015), [online], accessed from: http://www.cloudpassage.com/

[10] CipherCloud, Cloud Data Security, Solutions (2015), [online], accessed from: http://www.ciphercloud.com/

[11] CloudLock, Cloud Security Software, (2015), [online], accessed from: http://www.cloudlock.com/

[12] John Edwards, Securing the commercial cloud, Solving commercial cloud's security puzzle, (2015), [online], accessed from:http://www.c4isrnet.com/story/military-tech/it/2015/02/20/securing-commercial-cloud/23738771/

[13] CSA: Cloud Control Matrix. Cloud Security Alliance [online], CSA CCM v3.0 (2013)

[14] DRAFT, F. P., Recommended security controls for federal information systems and organizations. NIST Special Publication, 800, 53. Chicago, 2009

[15] Catteddu, D., Hogben, G. (eds.): Cloud Computing: Benefits, Risks and Recommendations for Information Security. ENISA Report (2009)

[16] U.S. Department of Education, Family Educational Rights and Privacy Act (FERPA), [online] accessed from: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[17] Department of Health, HIPAA: Health Insurance Portability and Accountability Act (2015), [online] accessed from: http://health.state.tn.us/hipaa/

[18] Dan Morrill, "CloudPassage Cloud Security Survey" [online], accessed from: http://www.cloudave.com/25217/cloudpassage-cloud-security-survey/

[19] Cloud Computing Use Case Discussion Group: Cloud Computing Use Cases White Paper, Version 4.0 (2010)

[20] Qu, L., Wang, Y., & Orgun, M. A., Cloud service selection based on the aggregation of user feedback and quantitative performance assessment. In Services Computing (SCC), 2013 IEEE International Conference on (pp. 152-159). 2013

[21] Kossmann, D., Kraska, T., & Loesing, S., An evaluation of alternative architectures for transaction processing in the cloud. In Proceedings of ACM SIGMOD International Conference on Management of data, 2010

[22] Barker, S. K., & Shenoy, P., Empirical evaluation of latency-sensitive application performance in the cloud. In Proceedings of ACM SIGMM Conference on Multimedia systems, 2010

[23] Zeng, W., Zhao, Y., & Zeng, J., "Cloud service and service selection algorithm research". In Proceedings of ACM/SIGEVO Summit on Genetic and Evolutionary Computation, 2009.

[24] Hussain, F. K., & Hussain, O. K.. Towards multi-criteria cloud service selection. In Innovative Mobile and Internet, Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on (pp. 44-48). 2011

[25] Han, S et al. Efficient service recommendation system for cloud computing market. the 2nd International Conference on Interaction Sciences: Information Technology, Culture, and Human, 2009

[26] Ruiz-Alvarez, A., & Humphrey, M., An automated approach to cloud storage service selection. In 2nd international workshop on Scientific Cloud Computing, 2011

[27] Li, G., et al., Approach to Trust-Aware Service Recommendation. In the 4th int'l CENet 2015.

[28] Jackson, K. A., DuBois, D. H., & Stallings, C. A. (1991). An expert system application for network intrusion detection (No. LA-UR-91-558; CONF-911059--1). Los Alamos National Lab.

[29] Bauer, D. S., & Koblentz, M. E. (1988, April). NIDX-an expert system for real-time network intrusion detection. In IEEE Computer Networking Symposium, 1988.

[30] O'Sullivan, J., Edmond, D., Ter Hofstede, A. What's in a Service?. Distributed and Parallel Databases, 12(2-3), 117-133, 2002

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

[32] Aaker, David A. (2001). Strategic Market Management. New York: John Wiley & Sons. pp. 108 et seq. ISBN 0-471-41572-3.

[33] Gruschka, N., & Jensen, M. Attack Surfaces: A Taxonomy for Attacks on Cloud Services. In IEEE CLOUD (pp. 276-279). 2010

[34] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2014, June). AVOIDIT: A cyber attack taxonomy. In 9th Annual Symposium on Information Assurance (ASIA'14) (pp. 2-12).

[35] Abuhussein, A., Bedi, H., & Shiva, S., Evaluating security and privacy in cloud computing services: A Stakeholder's Perspective. In Internet Technology And Secured Transactions, 2012

[36] Abuhussein, A, Alsubaei, F., Shiva, S., Sheldon, F., "Evaluating Security and Privacy in Cloud Services", NATA Symposium, the IEEE 40th Annual COMPSAC, Atlanta, Georgia, USA, 2016

[37] CSSR, (2016) [online], accessed from : http://measure-cloud-security.com/

[38] Code Spaces, (2015), accessed from: http://www.codespaces.com/

[39] S., Ragan, Code Spaces forced to close its doors after security incident (2015) [online], Accessed from: http://www.csoonline.com/article/2365062/disaster-recovery/code-spaces-forced-to-close-its-doors-after-security-incident.html

[40] ENISA, C. C. (2009). Benefits, risks and recommendations for information security. European Network and Information Security