Evaluating Security and Privacy in Cloud Services

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

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

***Abstract*—Moving data and applications to the cloud implies shifting their control from cloud consumers to the cloud service provider (CSP) indefinitely. Hence, the security and privacy (S&P) of the consumers' assets becomes an important issue. Assessing and comparing potential cloud computing (CC) services, poses an issue for CC adopters to choose S&P options that are sufficient and robust at the same time. In this paper, we describe CC adopters' S&P concerns. We identify a set of attributes that reflect various aspects of cloud S&P in an attempt to alleviate those concerns. We classify the attributes based on their tangibility and their relevance to S&P threats. Every attribute in our list is represented by a set of considerations (i.e. polar questions) to assess its quality. We present a tool that embodies our set of attributes. We aim to enable consumers to assess and compare CC services, in terms of S&P, so that they can make well-educated choices. CSPs can also make use of these attributes to offer better cloud S&P.**

Cloud Computing, Security, Privacy Standardization, Legal Aspect, Security Assesment, Cloud Economics

I. INTRODUCTION

The emerging success of cloud computing (CC) in the current Internet commercial landscape has opened new doors for attackers to exploit potential business and industries. This can be largely credited to the ubiquitous connectivity provided by CC platforms where an attacker can inflict damage from almost any geographical location independent of where the cloud itself is located. Thus, establishing a secured cloud has been a matter of significant importance to cloud service providers (CSPs) and consumers.

While efforts to improve CC security and privacy (S&P) have proliferated lately, progress toward improvement has been frustratingly slow. Some of this lag in progress may be attributable to consumers' *lack of awareness* in cloud S&P, and the *lack of consensus* among stakeholders on cloud S&P issues, S&P solutions, and accountability. These deficiencies (1) discouraged competitiveness among CSPs and transparency among stakeholder and (2) undermined the establishment of clear systems of accountability.

In this paper, we identify and categorize the attributes that highlight the S&P provided by CC services. Then we proceed to present how one can use these attributes for evaluating potential CC services from a consumer standpoint. The importance of such an evaluation resides in that it: (1) increases cloud consumers' awareness of the S&P issues, and the recent S&P solutions, (2) increases the willingness of CSPs to make these S&P solutions available for their clients, (3) increases transparency among consumers and CSPs, and (4) encourages healthier competitiveness among CSPs.

In section II, we highlight some recent work and solutions that assess and compare the S&P of clouds. In section III, we illustrate the potential S&P attributes that we believe sufficient to fulfill the consumers' S&P needs. In section IV, we demonstrate how such attributes are used to compare and assess the S&P of CC services. In section V, we highlight our future work and conclude in section VI.

II. RELATED WORK

There have been several attempts from research and industry to cope with the consumer issues in choosing the appropriate cloud service [1, 2, 3, and 4]. For example, Amazon Web Services (AWS) has published a white paper [1] to assist customers with integrating AWS into their IT environment. The Australian Department of Communication has published a consumer factsheet [2] to assist potential consumers in shopping for cloud services.

The attempts above may be among the first steps to address the S&P challenges from a stakeholder perspective. However, some of them focus on a single service model [1] (i.e. SaaS, PaaS, or IaaS) whereas others have a small list of considerations with plans to expand in the future [2, 3, and 4]. Also, because stakeholders have different requirements and tolerances to S&P risks, there is a need for an approach that assists stakeholders in choosing the desired S&P in every component of the service (e.g. less client-side protection and more data protection). In addition, to enable stakeholders to make accurate decisions, they need to be able to quantify the service S&P. Furthermore, existing efforts do not provide consumers with a tool to enter cloud service properties and evaluate their entries to make educated decisions. Finally, most of the existing attempts have yet to observe their benefits in the real world in terms of guiding stakeholders and improving S&P.

Our work is significantly different from the existing efforts in that we provide a tool that guides consumers throughout their decision-making process. The tool enables the consumer to view their S&P requirements in the form of assessments and various charts. The output of the tool enables consumers to compare and decide how safe their data/application will be in the various CSPs' hands.

III. A FRAMEWORK OF S&P ATTRIBUTES

A cloud service offered by a CSP comprises a set of S&P choices (i.e. S&P attributes) to secure and deter. The set of

attributes together specifies the S&P of service offered. A CSP may have multiple offerings of the same S&P attribute (e.g. single factor authentication, multifactor authentication) or may allow consumers to obtain an attribute from a third party vendor. When obtaining a cloud service, hesitant consumers are left to decide on (1) the necessary S&P attributes and (2) the appropriateness of each S&P attribute in terms of the degree of security it provides. In this work, we identify and illustrate 25 S&P attributes for the three standard cloud services (SaaS, PaaS, IaaS). We highlight attribute aspects that should matter to consumers when researching different CSPs. We refer to these aspects as considerations. In this work context, the considerations consist of more than 200 polar questions (i.e. Yes/No questions) that assess the degree of S&P in all attributes. These questions enable cloud consumers to decide whether their goals for cloud S&P are met. This is widely known as the Goal Questions Metric (GQM) approach [5]. By visiting a CSP website, consumers can collect and log the various security, privacy, and service-level policies and procedures to answer the attribute questions. Then, consumers themselves can recognize when security goals are met based on their requirements and the tool output. We developed an online tool [6] (php/mysql) that encompasses our list of attributes along with their corresponding considerations. The tool enables consumers to save their entries for a CSP and view results in various informative charts. All saved entries create a service catalog that benefits future consumers. Consumers can also evaluate multiple CSPs to compare and choose among them. In subsections A and B, we illustrate our attributes and the classifications.

A. S&P Attributes

At present, the following 25 S&P attributes have been selected for inclusion in the tool. More attributes will be included as they are identified. Each attribute is followed by a sample of two considerations.

1) *Backup:* measures service readiness to respond to failure, loss, or damage in clouds (e.g. Virtual Machines (VMs), data, etc.) by making duplicate(s) of originals. Considerations include: (1) Is backup/restore bandwidth unlimited? (2) Is the backup service automated?
2) *Encryption:* identifies data protection on its way from consumer to cloud and in transit against unauthorized use by scrambling the contents so that it can be read only by someone who has the encryption key to unscramble it. Considerations include: (1) Is data transferred to and from the cloud encrypted by default? (2) Is the encryption attribute FIPS 140-2 [7] compliant?
3) *Identity Management and Authentication:* identifies the service robustness against unauthorized access to the CC components (e.g. control panel, VMs, GUI, database, etc.) by verifying login credentials. Considerations include: (1) Is multi-factor authentication (MFA) supported?, (2) Is the authentication system synchronized with the organization "active directory"?
4) *Dedicated hardware:* measuring service readiness to cope with the availability issues that result from sharing resources. Considerations are: (1) Does the CSP offer dedicated machines to a single consumer?, (2) Does the CSP apply the same security countermeasures that apply to VMs on dedicated machines?
5) *Data Isolation:* measures the degree to which data in the cloud (e.g. VMs, or storage, etc.) is isolated from modifications made by other tenants. Considerations include: (1) Does the CSP isolate data sharing the same resources?, (2) Does the CSP make best effort to protect VMs that are sharing the same partitions from DoS?
6) *Disaster Recovery:* measures service readiness to recover and protect the cloud service in the event of a disaster. Considerations include: (1) Does the CSP offer a disaster recovery plan? (2) Is the recovery process automated?
7) *Hypervisor Security:* measure the robustness of the process of ensuring the VM manager (VMM) is secure. This includes its computations, networking, and storage. Considerations include: (1) Does the CSP prevent deployment of insecure or tampered VMs?, (2) Can the CSP identify and defend against VM side-channel attack?
8) *Client Side Protection:* assesses the CSP countermeasures to protect the consumer against malicious activities. Considerations include: (1) Does the CSP encourage secure protocols like SSL, VPN? (2) Does the CSP make best effort to increase consumers' S&P awareness?
9) *Monitoring:* measures the CSP readiness to collect, analyze, and escalate indications and warnings in cloud service. Considerations include: (1) Does the CSP notify consumers about any possible threats and how to mitigate them? (2) Can consumers view the cloud health monitors?
10) *Access Control and Customizable Security Profiles:* measures the physical and logical countermeasures that can be used to regulate who or what (e.g. VMs) can view/use resources. This includes the ability to audit profiles. Considerations include: (1) Does the CSP provide Separation of Duties and Administrator Access?, (2) Does the CSP allow full control on the ACLs?
11) *Datacenter Location:* identifies the CSP readiness to protect cloud service data centers (i.e. compute, storage, etc.) against the physical security risks. Considerations include: (1) Does the CSP hide the exact locations of the data centers from the public?, (2) Can consumers choose the geographical location of where to store their data?
12) *Security Standards and Certification:* identifies CSP compliance to standards and assesses CSP background, qualifications, and legitimacy in information security, privacy, healthcare, education, etc. Considerations include: (1) Is the CSP and Service certified?, (2) can consumers see standards, certifications, and reports from granting organizations including employee training?
13) *Data Sanitization:* identifies the security measures that CSP take to deliberately, permanently, and irreversibly remove or destroy data (in storage media, documents,

etc.) so that it can never be recovered or retrieved. Consideration are: (1) Is the data destroyed securely when the service is terminated?, (2) Does the CSP sanitize the storage media before being reused?

14) *SLA Guarantee and Conformity:* identifies whether the running service conforms with the SLA. Consideration are: (1) Does the CSP consider complexity of the cloud architecture in SLA?, (2) Does SLA consider different impacts of service outage on different business natures?

15) *Secure Scalability:* assesses the CSP countermeasures to maintain S&P in cloud services against unpredictable failures when services scale up/down to meet consumer needs. Considerations include: (1) Does the CSP guarantee availability while scaling up/down?, (2) Does the CSP allow scaling to different geographical zones?

16) *Secure Service Composition:* measures the CSP capability to guarantee secure and trustworthy service composition to protect the cloud services against unpredictable failures. Considerations include: (2) Does the CSP regularly check S&P of the composite services?, (2) Does the CSP have a clear outsourcing policy?

17) *Software and Hardware Procurement:* assesses the CSP policies, strategies, and procedures used to validate S&P legitimacy and compatibility of the purchased hardware and software that are used in clouds. Considerations include: (1) Does the CSP purchase/lease hardware and software from a legitimate source? (2) Does the CSP purchase/lease hardware and software that are all tested, certified, and conform to standards?

18) *Insider Trust:* assesses the CSP policies, strategies, and procedures to prevent, detect, and/or respond to malicious attack perpetrated on cloud service by a person with authorized access. Considerations include: (1) Does the CSP have a formalized insider threat program?, (2) Does the CSP perform background check on employees?

19) *Technology Change:* measures the CSP readiness to cope with the S&P issues that may occur as a result of technology evolution or vanishing. Considerations include: (1) Can the CSP change security features in case of technology emergence/ obsolescence without affecting the service?, (2) Does the CSP guide consumers to make educated choices if technology or S&P attributes or risks change?

20) *Service Self-healing:* measures service readiness with pre-configured responses and actions to face S&P failures. This includes automatic detection, prevention and response to failures. Considerations include: (1) Does the CSP make the best effort to identify triggers that lead to abnormal behavior in the cloud?, (2) Does the CSP have tools to automatically prevent S&P risks?

21) *Service Availability:* identifies the CSP readiness to ensure that a cloud user can access information or resources in a specified time/location and the correct format. Considerations include: (1) Does the CSP ensure fair availability for all tenants on a physical machine?, (2) Does the CSP make best effort to protect isolated VMs that share the same partition from DoS attacks?

22) *Risk Management:* assesses the CSP goodness in identifying, assessing, and prioritizing, monitoring, and controlling risks. Considerations include: (1) Does the CSP have a risk management plan for the offered services?, (2) Does the CSP allow for certified external auditors' involvement in all risk management activities?

23) *Security Awareness:* measures the CSP's ability to provide knowledge to all cloud stakeholders to increase protection of the physical, and informational assets in clouds. Considerations include: (1) Does the CSP provide recommendations for better security?, (2) Does the CSP warn consumers of possible vulnerabilities?

24) *Secure Networking infrastructure:* identifies the CSP's effectiveness in preventing unauthorized access, misuse, modification, or denial of cloud physical and virtual networks. Considerations include: (1) Does the CSP allow consumers to build geographically dispersed networks?, (2) Does the CSP provide countermeasures for all network attacks (e.g. MITM, DDoS, etc.)?

25) *Security Insurance:* refers to the CSP's willingness to compensate cloud consumers for specific potential service failures. Considerations include: (1) Does the CSP provide insurance for the services?, (2) Does the CSP have more than one insurance plan?

B. Attribute Classifications

We classified our list of attributes to reveal additional information to consumers. The following are the classification criteria. Table I depicts the different classifications for the S&P attributes.

- Tangibility: shows attribute tangible nature. Tangible attributes comprise an algorithm, instrument, etc., that can be measured in terms of use and cost (e.g., backup, encryption, etc.). Intangible ones deal with organizational and behavioral measures (e.g. insider trust, etc.).
- Service Model: shows attribute's applicability to a cloud service model (i.e. SaaS, PaaS, or IaaS attributes).
- Functionality: shows attribute's functionality as detection (D), prevention (P) and incident response (IR).
- Protectability: shows the type of S&P issue(s) that an attribute can protect the cloud service from. Protectability classes are client, interface, network, virtualization, governance, compliance, legal aspects, and data S&P issues. Refer to [8] for examples of S&P issues and types.
- Default: Cloud services by default have monitors for service health. However, consumers can purchase advanced monitors at their expense. This classification shows whether an attribute is included by default.

IV. An Empirical Evaluation

We have evaluated the tool by gathering publicly available data to answer S&P attributes questions for two IaaS CSPs. For every consideration of an attribute, a CSP received a score (1) if the answer is yes, (-1) if the answer is no, and (0) if no information is available in the CSP website. For every attribute, we summed attribute score and normalized it to 10 since the number of considerations varies from one attribute to another. Fig.1 represents the degree of S&P (out of 10) for each attribute. It is clear that CSP1 attributes "monitoring", "data center location", and "security standards and certifications" attributes received the highest degree of S&P, almost 10, whereas the lowest degree of S&P, below 4, is in "secure scalability". This indicates that CSP1 focuses less on security as applied to services scaling up/down and that the probability of scalability S&P risks is higher than other risks. Fig.2 represents the functionalities of CSP1 and CSP2 attributes. It is also clear that the service provisioned by CSP1 is more effective than the one of CSP 2 in terms of its ability to detect, prevent, and respond to risks.

TABLE I. S&P Attributes Classifications

Attrib. No.	***Services***			***Tangibility***	***Default***	***Function***			***Protectability***							
	SaaS	***PaaS***	***Iaas***			***D***	***P***	***IR***	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***
1	X	X	X	•				X								•
2	X	X	X	•		X	X	X			•	•				•
3	X	X	X	•	•	X	X			•	•					•
4			X	•			X					•				•
5			X	•	•		X					•				•
6	X	X	X	•	•			X					•	•		•
7			X	•	•		X					•				•
8	X	X	X	•		X	X		•	•	•					•
9	X	X	X	•	•	X		X	•		•					
10	X	X	X	•		X	X	X	•	•	•	•	•	•	•	•
11	X	X	X	•			X						•	•	•	•
12	X	X	X		•	X	X	X	•	•	•	•	•	•	•	•
13	X	X	X	•	•		X					•	•	•	•	•
14	X	X	X		•	X	X	X					•	•	•	
15	X	X	X	•	•		X				•	•	•	•		
16	X	X	X		•		X	X	•	•	•	•	•	•	•	•
17	X	X	X		•		X			•	•	•				•
18	X	X	X		•		X		•	•	•	•				•
19	X	X	X		•	X	X	X	•	•	•	•	•	•	•	•
20	X	X	X	•	•	X	X	X		•	•	•				•
21	X	X	X		•	X	X	X	•	•	•	•	•	•	•	•
22	X	X	X		•	X	X	X	•	•	•	•	•	•	•	•
23	X	X	X			X	X	X	•	•						•
24		X	X	•	•	X	X	X		•	•	•				•
25	X	X	X	•				X	•	•	•	•	•	•	•	•

V. Conclusion

Securing the cloud is not an easy task especially after vulnerable incidents we see and hear every day. We presented a list of S&P attributes that help cloud services consumers to secure cloud. To the best of our knowledge, this is perhaps the only published tool that aims to evaluate the degree of S&P of a cloud service. Our goal is to provide hesitant future and current cloud consumers with a set of evaluating criteria to end their confusion. 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 S&P 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. We will continue enriching this research with emerging attributes that appear on the scene. We are also working on developing metrics that aid in better quantifying these attributes.

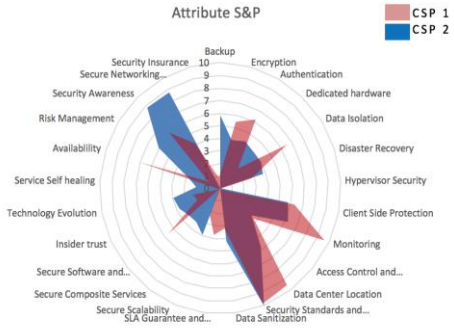

Figure 1. A comparison of the degree of S&P in CSP1 and 2 attributes

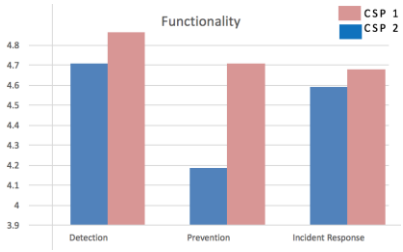

Figure 2. A comparison of S&P attributes functionality for CSP1 and 2

Acknowledgment

This work is an expansion on a paper presented at the ICITST in 2012 [8]. This work contributes to a project that is partially supported by The Cluster to Advance Cyber Security & Testing (CAST) at the University of Memphis.

References

[1] Amazon Web Services: Risk and Compliance [online], Available: https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

[2] Cloud computing and privacy: Consumer factsheet, Australian Government- Department of Communications, [online] Available: https://www.communications.gov.au/sites/g/files/net301/f/2014-112101-CLOUD-Consumer-factsheet.pdf

[3] Pauley, Wayne A. "Cloud Provider Transparency: An Empirical Evaluation." IEEE Security & Privacy 6, no. 8 (2010): 32-39.

[4] Garg, S. K., Versteeg, S., & Buyya, R. (2013). A framework for ranking of cloud computing services. Elsevier Journal of Future Generation Computer Systems, 29(4), 1012-1023, .

[5] Van Solingen, R., Basili, V., Caldiera, G., & Rombach, H. D. (2002). Goal question metric (gqm) approach. Encyclopedia of software engineering.

[6] Service Catalog, [online] Available: http://www.measure-cloud-security.com/ (2016)

[7] FIPS PUB 140-2, NIST [online] Available: http://csrc.nist.gov/groups/STM/cmvp/standards.html

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