A Framework for Cloud Security Assessment

A Scenario-based, Stakeholder-Oriented Approach

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

Abstract— **Cloud consumers are hesitant in choosing an appropriate cloud service as they are under the assumption that clouds are not safe for their data and operations. This is due to the presence of a trust gap between cloud service consumers and cloud service providers (CSP) as well as a lack of understanding among consumers about what security and privacy (S&P) attributes best fit their requirements. In this paper, we propose a framework to assist consumers in making educated decisions when shopping for cloud S&P . First, the framework illustrates a list of potential S&P issues and recommends evaluative S&P attributes. Second, it enables consumers to assess the degree of security in two or more cloud services against the recommended attributes. Third, it enables consumers to compare their assessments using various instructive graphs. The proposed framework improves S&P of clouds by following a scenario-based and a stakeholder-oriented approach to enable consumers to comprehend their interaction with the cloud for better security. With this tool, we aim to raise the bar for security awareness in cloud computing (CC) and also form the basis for cloud S&P metrics against a standard benchmark in the future.**

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

I. Introduction

Cloud computing (CC) has emerged as the computing model for providing utility-based, on-demand infrastructure, platform and software services for anyone, anywhere and anytime. Despite the potential gains achieved from CC, the security of data and processing aspects is still questionable and impacts CC adoption. Cloud security includes old and well-known issues like the ones related to user access, networks, and authentication as well as emerging issues. Most of the emerging issues are tied to cloud stakeholders' trustworthiness, accountability, and multi-tenancy. As a consequence, cloud adopters find themselves faced with concerns associated with loss of control, and lack of trust. While efforts to improve CC security and privacy (S&P) have proliferated lately, progress toward improvement has been frustratingly slow because:

- Many cloud adopters in their haste to reduce costs focus just on performance at the expense of security.
- Lack of a complete understanding of the Cloud Service Provider's (CSP) environment, applications or services being pushed to the cloud, and operational responsibilities
- The multidimensional nature of CC due to cloud services composability, scalability, and elasticity.
- Lack of consensus among stakeholders on cloud S&P issues, S&P solutions, and accountability.
- The absence of transparency among CC stakeholders and decline of healthy competitiveness among cloud service providers (CSPs) as a result of the lack of consensus on CC standards.
- Organizations have many different CC security objectives (e.g. different requirements, assets, exposure to public, and tolerances to security risks)
- Laws and regulations divergence among industries based in different geographical locations.

Cloud consumers are often unable to evaluate all available alternatives in great depth. While shopping for cloud services, consumers are often using two-stage processes to reach their decisions. At the first stage, consumers typically screen a large set of available cloud S&P attributes to identify the necessary and sufficient ones for a robust service. Subsequently, they evaluate the latter in more depth, perform a comparison of CSPs on important S&P attributes, and make a purchase decision.

Given the different tasks to be performed, we are developing a framework of three interactive tools that provide support to consumers in the following aspects:

(1) Cloud Service Security Recommender (CSSR): supports cloud adopters in the initial screening of available necessary, and sufficient S&P attributes to determine which ones are worth considering further.

(2) CSP Catalogue: supports cloud adopters in storing and viewing the description of cloud services in the form of an organized and curated collection of S&P evaluative attributes and then assessing the attributes readiness to secure and deter by answering a set of polar questions that correspond to each attribute.

(3) Cloud Service Security Assessor (CSSA): supports cloud adopters in the in-depth comparison of multiple cloud services, provisioned by multiple CSPs, before making the actual purchase decision.

This paper is organized in the following way: We briefly survey the related work in Section II. We describe our framework and its conceptual basis, as well as the tools infrastructure in Section III. In Section IV, we present the framework evaluation. Finally, in Section V, we present our future work followed by the conclusion.

II. Related Work

In a nutshell, considerable progress has been made in walking customers through shopping for cloud services and quantitatively ranking cloud services [1,2, 3, 4, 5, 6 and 7]. These efforts in cloud service selection are either:

- Geared towards selecting a service based on its qualities, its non-functional requirements, or QoS with minimal focus on security.
- Focused on a particular cloud service model like software-as-a-service (SaaS), platform-as-a-service (PaaS), or Infrastructure as a service (IaaS).
- Tailored to choose a service based on existing consumers' feedback only, future consumer's requirements only, or neglecting customer participation.
- Designed to treat all selection criteria equally in terms of their importance.
- Focused on assessing risks, threats, or mean failure cost in cloud platforms.

In this paper, we present a framework to assist current or future cloud adopters in shopping for a cloud service by (1) assisting them in identifying the necessary and sufficient S&P attributes for a safe cloud environment, (2) selecting pre-stored CSPs from a service catalog or entering new CSPs into the service catalog and (3) finally comparatively assessing the degree of security in the S&P attributes that each one of the CSPs offer in order to make a purchase decision.

III. The Cloud Security Assessment Framework

This section presents the framework components shown in Fig 1. The framework comprises three interactive tools that are designed to assist consumers in making a well-educated decision. The three tools are illustrated in turn.

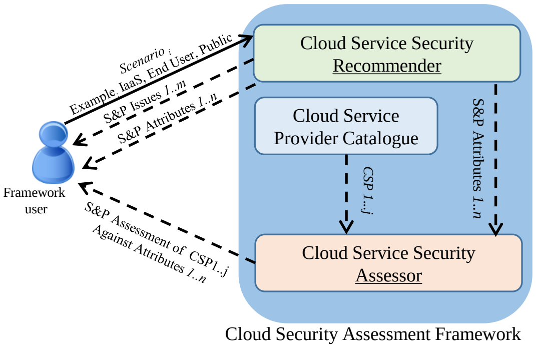

Scenario i
Example. IaaS, End User, Public
S&P Issues 1..m
S&P Attributes 1..n
Framework user
S&P Assessment of CSP1..j Against Attributes 1..n
Cloud Service Security Recommender
Cloud Service Provider Catalogue
CSP 1...j
S&P Attributes 1..n
Cloud Service Security Assessor
Cloud Security Assessment Framework

Fig. 1. Framework User interaction with the components

A) *Cloud Service Security Recommender (CSSR) [8]*

This component of the framework supports cloud adopters in identifying the necessary and sufficient S&P attributes to determine which ones are worth considering further. CSSR (Fig 2.) achieves this by using three taxonomies A, B and C. The three taxonomies enable stakeholders to comprehend their CC model(s), identify potential security issues based on possible attack surfaces and also educates stakeholders about the potential security issues by listing each one's operational impact(s), informational impact(s), and then recommends defensive action(s) and corresponding (set of) security attribute(s). To demonstrate how CSSR taxonomies 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)*

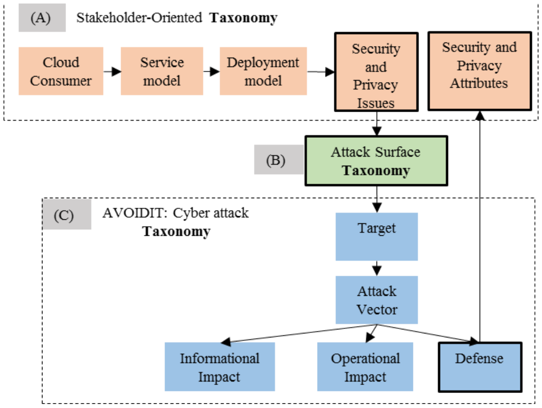
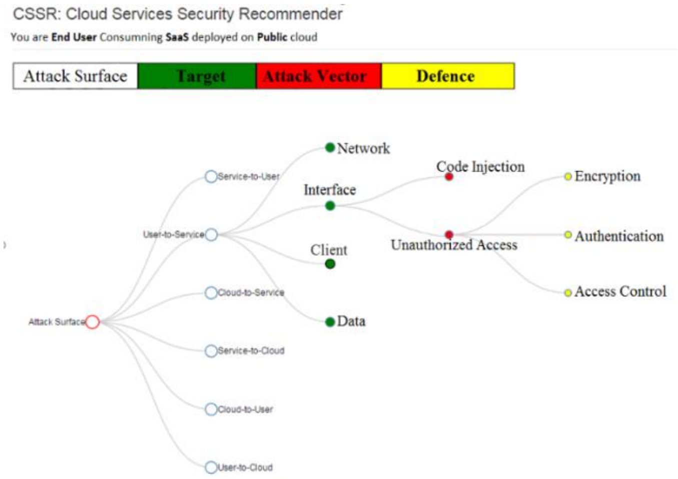


Fig. 2. CSSR Taxonomies

CSSR [12] (i.e. php/mysql tool) 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.

The tool landing page prompts CSSR user to select a service model (e.g. SaaS, Pass, or IaaS), a deployment model (e.g. public, private, community, or hybrid) and identify 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 the S&P issues and their corresponding S&P attributes as in Fig 3.


CSSR: Cloud Services Security Recommender

You are **End User** Consumning **SaaS** deployed on **Public** cloud

Fig. 3. CSSR represents S&P issues (Attack Vector) and recommended Attributes (Defense) for Scenario (End User, SaaS, Public)

This approach is stakeholder-oriented and scenario-based since the taxonomies perform a scenario analysis to identify the issues and recommend S&P attributes. This scenario analysis depends on the type of stakeholder who interacts with the cloud.

B) CSP Catalogue [9]

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. We investigated and identified 25 S&P attributes for the three standard cloud services (SaaS, PaaS, IaaS), that was generated through a thematic analysis of the services offered by real-world CSPs. We highlighted 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 [10]. Table I depicts a sample attributes (i.e. encryption) along with its considerations. A full list of attributes and their classifications shows in Table II.

TABLE I. 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 admins 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?

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 [11] (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 form a CSP catalogue that benefits future cloud consumers.

C) Cloud Services Security Assessor (CSSA)

As illustrated earlier, properties of an attribute are described using a list of considerations (polar questions).

Every S&P attribute has its own set of considerations.

TABLE II. OUR LIST OF ATTRIBUTES AND THEIR CLASSIFICATIONS

Attribute	Service			Tangible?	Default?	Fee Involved?	Service Related?	Function			Protectability[1]							
	SaaS	PaaS	IaaS					Detection?	Prevention?	IR[2]?	1	2	3	4	5	6	7	8
Encryption	X	X	X	Y	Y	Y	Y	X	X	X			X	X				X
Backup	X	X	X	Y	Y	Y	Y			X								X
Authentication and Identity Management	X	X	X	Y	Y	Y	Y	X	X			X	X					X
Dedicated hardware			X	Y		Y	Y		X					X				X
Data Isolation			X	Y	Y		Y		X					X				X
Disaster Recovery	X	X	X	Y	Y	Y	Y			X								
Hypervisor Security			X	Y	Y		Y		X					X				X
Client Side Protection	X	X	X	Y		Y	Y	X	X		X	X	X					X
9) Service Monitoring	X	X	X	Y	Y	Y	Y	X		X	X		X	X				X
Access Control & Customizable profiles	X	X	X	Y	Y		Y	X	X	X	X	X	X	X	X	X	X	X
Secure Data Center Location	X	X	X		Y	Y	Y		X						X	X	X	X
Standards and Certifications	X	X	X		Y		Y	X	X	X	X	X	X	X	X	X	X	X
Data Sanitization	X	X	X	Y	Y	Y	Y		X					X	X	X	X	X
SLA Guarantee and Conformity	X	X	X		Y		Y	X	X	X					X	X	X	
Secure Scalability	X	X	X		Y		Y		X				X	X	X	X		
Secure Service Composition	X	X	X		Y		Y		X	X	X	X	X	X	X	X	X	X
S/w and H/w Procurement	X	X	X		Y				X		X	X	X	X				X
Insider trust	X	X	X		Y				X		X	X	X	X				X
Technology Change	X	X	X		Y			X	X	X	X	X	X	X	X	X	X	X
Service Self-healing	X	X	X	Y	Y			X	X	X		X	X	X				X
Service Availability	X	X	X		Y			X	X	X	X	X	X	X	X	X	X	X
Risk Management	X	X	X		Y			X	X	X	X	X	X	X	X	X	X	X
Security Awareness	X	X	X					X	X	X	X	X						X
Secure Networking infrastructure		X	X	Y	Y			X	X	X		X	X	X				X
Security Insurance	X	X	X	Y						X	X	X	X	X	X	X	X	X

These considerations decide the goodness of each attribute. CSSA relies on these considerations to quantify the degree of S&P in an attribute provided by a CSP. Based on the considerations, each attribute of a CSP will receive a score. If the answer to the consideration question is "Yes", the attribute receives a score of 1, and 0 otherwise. The later denotes that either the provider did not provide an answer to a consideration of an attribute or the answer is "No". The attribute score is simply the weighted summation of all consideration score values of an attribute normalized to a scale of 1-10 as follows:

$$\text{AttributeScore}_{\text{service i}} = \frac{\left(\sum_{j=1}^{n} Consideration_j\right)*10}{n}$$

[1] Protectability: attribute protects cloud environment from the following: **1**=Client Security, **2**=Interface Issues, **3**=Network Security, **4**=Virtualization Security, **5**=Governance Security, **6**=Compliance Security, **7**=Legal Issues, **8**=Data Security

[2] **IR:** Incident Response

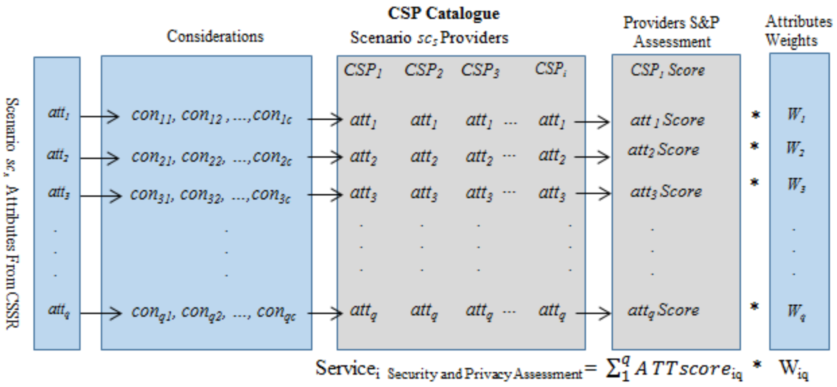

CSP Catalogue
Scenario sc_s Providers
Considerations
Providers S&P Assessment
Attributes Weights
Scenario sc_s Attributes From CSSR
att_1
att_2
att_3
att_q
$con_{11}, con_{12}, \ldots, con_{1c}$
$con_{21}, con_{22}, \ldots, con_{2c}$
$con_{31}, con_{32}, \ldots, con_{3c}$
$con_{q1}, con_{q2}, \ldots, con_{qc}$
CSP_1 CSP_2 CSP_3 CSP_i
CSP_i Score
att_1 Score
att_2 Score
att_3 Score
att_q Score
W_1
W_2
W_3
W_q
$\text{Service}_{i\ \text{Security and Privacy Assessment}} = \sum_1^q ATTscore_{iq} * W_{iq}$

Fig. 4. CSSA operations flow to compute S&P Assessment

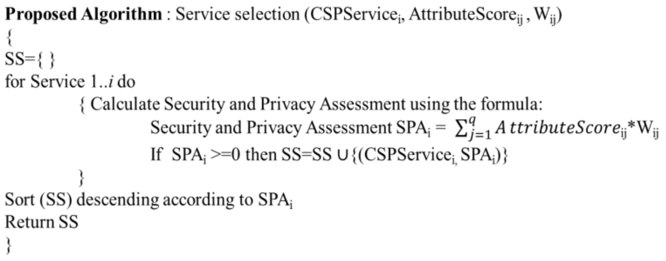
We use a multi-criteria decision-making (MCDM) method to compare, rank, and select from multiple alternatives (CSPs), each having multiple S&P attributes. Once all the attributes composing a service provisioned by a CSP are scored in terms of the degree of S&P they have, a CSP is now ready for assessment tentatively as follows:

$$\text{Service}_{i\ \text{S\&P Assessment}} = \sum_{j=1}^{q} Arttributescore_{ij} * W_{ij}$$

Where, $\text{AttributeScore}_{ij}$ denotes attribute score for attributes from 1 to q of CSP_i, and W_{ij} denotes the importance weight for every attribute composing the scenario. A scenario weights are represented by a fraction of 1 such that the sum of all weights of attributes must equal 1. Attribute weights of a scenario are tentatively treated as of equal importance.

Fig 4 shows how CSSA assesses the degree of S&P in multiple services provided by multiple CSPs. Once CSSR recommends S&P attributes for a particular scenario, CSP catalogue retrieves all CSPs who offer a matching service. After this, the user chooses two or more CSPs from the list to comparatively assess the degree of security in the S&P attributes they offer.

After computing S&P assessment for all the cloud services that were chosen by the user, CSSA then sorts (i.e. ascending, descending) the services according to their degree of S&P in the service according to the assessment. A service selection algorithm is presented in Fig 5.



```
**Proposed Algorithm** : Service selection ($\text{CSPService}_i$, $\text{AttributeScore}_{ij}$ , $W_{ij}$)
{
SS={ }
for Service 1..$i$ do
        { Calculate Security and Privacy Assessment using the formula:
                Security and Privacy Assessment $\text{SPA}_i = \sum_{j=1}^{q} AttributeScore_{ij} * W_{ij}$
                If  $\text{SPA}_i$ >=0 then SS=SS ∪{($\text{CSPService}_i$, $\text{SPA}_i$)}
        }
Sort (SS) descending according to $\text{SPA}_i$
Return SS
}
```

Fig. 5. CSSA service ranking algorithm

IV. Framework Evaluation

Many organizations like National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA) have published S&P controls for cloud services [13 and 14]. 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.

To validate the correctness of framework output, we used a real-world example from recent publications. In late 2014, Code Spaces [16], 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 [17]. 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 framework (CSSR, CSSA in particular), 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.

The presented framework is extensible and updatable due to its taxonomical nature. 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. Also, the framework presented 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) This work also paves the way for cloud S&P metrics against "a standard benchmark" in the future.

V. Future Work and Conclusion

Security cannot be managed, if it cannot be measured. Yet, large CSPs are still finding themselves victims of security and privacy incidents. Also, consumers of cloud services need to understand their security threats, responsibilities, and needs. They need to be able to make well-educated decisions in order to take proactive measures against potential security issues and embrace the cloud with confidence. As such, this work provides important tools that can help shape cloud stakeholders understanding of their responsibilities and needs in the cloud. With the three components of the proposed framework we aim to increases cloud consumers' awareness of the S&P issues; increases cloud consumers' knowledge in the recent S&P solutions that are available in market, increases the CSP willingness to make these S&P solutions available for their clients, increases transparency among consumers and CSPs, and encourages healthier competitiveness among CSPs.

Unfortunately, CSPs cannot be forced to cooperate in entering their offerings details into the CSP catalogue 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 CSP catalogue current.

Also, it is obvious how CC poses many challenges for U.S. law enforcement and national security agencies and commercial organizations. These challenges are mainly security challenges and technical challenges for digital crime-fighters. This work aims to quickly and profoundly change the way the nation addresses growing national CC security challenges posed by the CC revolution and by the increasing global availability of sophisticated CC technologies. It promotes best practices in transparency, accountability, and commitment in the cloud. It enables stakeholders to make well-educated decisions in terms of S&P features in cloud environments. Thus, this project aims to improve national security.

First and foremost, the goal of this work is to appropriately secure CC models. We will continue to enhance our framework and its three components and provide additional S&P attributes and additional capability. For instance, CSSA attributes weights are now treated equally in terms of importance. We are currently working on enabling cloud consumers to prioritize weights so that they can increase the weight of the attributes that are more important to them or decrease attribute's weight if customers can tolerate their risks.

ACKNOWLEDGMENT

This work is partially supported by The Cluster to Advance cyber Security & Testing (CAST) at the University of Memphis.

REFERENCES

[1] Saripalli, Prasad, and Ben Walters. "Quirc: A quantitative impact and risk assessment framework for cloud security." In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pp. 280-288. Ieee, 2010.

[2] Ribas, M., Furtado, C. G., de Souza, J. N., Barroso, G. C., Moura, A., Lima, A. S., & Sousa, F. R. (2015). A Petri net-based decision-making framework for assessing cloud services adoption: The use of spot instances for cost reduction. Journal of Network and Computer Applications, 57, 102-118.

[3] Sun, L., Ma, J., Zhang, Y., Dong, H., & Hussain, F. K. (2016). Cloud-FuSeR: Fuzzy ontology and MCDM based cloud service selection. Future Generation Computer Systems, 57, 42-55.

[4] Steven, J., & Peterson, G. (2003). A Metrics Framework to Drive Application Security Improvement. IEEE Security & Privacy, 1(4), 88-91.

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

[6] Garg, S. K., Versteeg, S., & Buyya, R. (2011, December). SMICloud: a framework for comparing and ranking cloud services. In Utility and Cloud Computing (UCC), 2011 Fourth IEEE International Conference on (pp. 210-218). IEEE.

[7] Alnemr, R., Pearson, S., Leenes, R., & Mhungu, R. (2014, December). Coat: cloud offerings advisory tool. In Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on (pp. 95-100). IEEE.

[8] Abdullah Abuhussein, Sajjan G. Shiva, and F.T Sheldon, CSSR: Cloud Services Security Recommender, IEEE 11th World Congress on Services- Emerging Technology Track: Dependable and Secure Services (DSS 2016), San Francisco, USA, Jun2 26- July 3, 2016.

[9] A. Abuhussein, F. Alsubaei, S. Shiva, and F. Sheldon, "Evaluating Security and Privacy in Cloud Services", In the 2016 IEEE NATA-COMPSAC Symposium on Novel Applications and Technology Advances in Computing, the 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, Georgia, USA - June 10-14, 2016

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

[11] Evaluate A Service Provider, [online] Available: http://www.measure-cloud-security.com/ (2016)

[12] CSSR, [online] Available: http://www.measure-cloud-security.com/ (2016)

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

[16] 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