Sla – Driven Approaches for Enhanced Cloud Data Security

Sai Santosh Achanta[1]
[1]*MBA student, IT Department, Vignan's foundation for science Technology &research (Deemed to be university)*

***Abstract*—Cloud computing has emerged as a cost-effective solution for IT infrastructure management, yet it brings significant concerns regarding data security, privacy, and regulatory compliance. Service Level Agreements (SLAs) are essential instruments to define and manage expectations between cloud providers and customers; however, existing SLAs often emphasize performance over information security. This study aims to bridge that gap by identifying SLA-based information security metrics aligned with the COBIT framework. Through a systematic literature review (SLR), the research identifies key information security threats and attributes pertinent to cloud environments. The Goal Question Metric (GQM) approach is used to derive a set of 41 security metrics from 10 essential IT process areas within COBIT. These metrics serve as a standardized method for both cloud providers and consumers to evaluate and improve the security posture of cloud services. The study provides actionable insights into the development of more security-conscious SLAs, ultimately enhancing trust and assurance in cloud adoption.**

I. INTRODUCTION

As more and more demands for Information Technology (IT) services rise, there are also increasing needs to expand IT architecture and infrastructures to provide more services. As a consequence, IT service providers are faced with challenges of expanding the structures and infrastructures with small expenditure and minimum time in order to provide rising demands from their customers. To address these business challenges and commercial interests, cloud computing architecture was developed. Cloud computing architecture is an environment of IT resources for particular services which is outsourced to customers [1]. In the context of cloud computing, the cloud service provider is known as cloud provider which is an organization that provides cloud computing service. On the other hand, the organization that receives the cloud computing service is known as the cloud customer. Cloud computing is not a novel concept; however, it is rising now and it will have major role in the next 10 years or more [1]. It is an increasing concept because of several reasons including reduction in cost and energy consumption of the shared computing resources (servers, software, storage, and networking) [2]. It also enables effective IT resources usage and increases flexibility for expanding new infrastructures in instant time [2].

Like traditional computing environments, cloud computing brings risks and security concerns to the business that need to be considered appropriately. Such risks and security concerns include challenges in handling privileged user access, ensuring legal and regulatory compliance, ensuring data segregation, maintaining data recovery, difficulty in investigating illegal activities, and lack of assurance of long-term viability of the cloud provider [3] . Due to these challenges cloud customers therefore need to institute mechanisms to measure and improve security of their information assets operating in the cloud. Among the alternatives available to the cloud customer for monitoring, measuring and hence improving information security of the assets managed in the cloud is to develop information security metrics.

Since cloud computing resources are delivered as a service, cloud customer therefore can implement the information security metrics through a Service Level Agreement (SLA). SLA is a legal agreement between a service provider and the customer [4] and is the main basis for managing and controlling the rendered services. SLA metrics are therefore used to assess service level between cloud provider and its customers and serve as basis for service improvement [4]. However, the trend among existing cloud SLAs focuses more on performance measurement than on

security measurement. Example of these SLA include a the GoGrid SLA [5]. Among the issues that hinder the organization from adopting the cloud computing is information security risks [6] [7]. However, we still experience cloud providers not addressing it [6] [7].

We recognize that several studies have been conducted on security metrics, cloud computing as well as SLA. However, none of these studies focused on SLA based information security metrics particularly for cloud computing.

In this study, we therefore select a framework that is suitable to identify information security metrics. We then review the COBIT document and follow the selected framework to identify SLA based information security metrics in cloud computing.

1.1 Aims

The overall aim of this study is to identify SLA based information security metrics in cloud computing using the COBIT framework.

1.2 Objectives

The set objectives of the study which will direct towards achieving our aim are to:

i) Identify relevant information security attributes for cloud computing

ii) Identify information security threats for cloud computing

iii) Select a framework suitable for developing security metrics

iv) Identify SLA based information security metrics in cloud computing aligned with the COBIT framework

II. LITERATURE REVIEW

Several studies have been conducted in the area of SLA metrics, security metrics and cloud computing. Several SLA metrics have been proposed. For instance, Skita et al. [35] propose SLA metric for real-time application on grid architecture. Jain et al. [36] propose SLA management system over IP networks.

In the area of cloud computing several researches have also been conducted. For example, Stantchev [37] proposes an approach of performance evaluation of cloud computing configurations. Rimal and Choi [20] surveyed on architectural approaches of cloud computing system and identified potential further research in cloud computing area.

Moreover, different approaches have been followed in developing security metrics. For instance, Tash and Ghernaouti [38] propose a framework that uses risk assessment to derive efficient metrics for measuring information security. Tanna et al. [39] propose a model for identifying metrics based on threat model. Another approach is the one described by SANS

[40] which presents seven steps for generating security metrics.

III. METHODOLOGY

Research questions, research methodologies and research plan are presented in this section.

3.1 Research questions

To achieve aims and objectives stated in sections 1.1 and 1.2 respectively, these following research questions are addressed:

RQ1. What information security attributes are relevant in cloud computing?

This research question is formulated in order to identify information security attributes relevant in cloud computing. The answers to this question also assist us to identify information security metrics in cloud computing as required in RQ3. The RQ1 is indirectly answered through RQ 1.1.

RQ1.1 What information security threats are relevant in cloud computing?

The main objective of this research question is to understand information security threats relevant in cloud computing. In addition, the answers to this question will enable us to be focused on cloud computing issues when identifying information security metrics rather than the traditional computing environment.

RQ2. Which framework is suitable for developing security metrics?

This research question aims at selecting a framework that will be followed in identifying information security metrics. This is important because several frameworks might be found in literature some of which may not be effective in identifying security metrics. This is also important because in the absence of a suitable framework numerous information security metrics might be found in the study hence becoming unmanageable.

3.2 Research methods and rationale

We conduct two methods in this study, systematic literature review (SLR) and thorough analysis of COBIT framework. The rationales for conducting these methods are as follows:

3.2.1 Rationale for systematic literature review

According to Jeffery and B. Neidecker-Lutz [1] cloud computing is emerging in Europe at this moment. Hence there is less information to collect from industry practitioners. For this reason, we only rely on information from literature to attain some of the objectives of this study. We therefore collect data required in this study through SLR. We adopt SLR as proposed by Kitchenham [42]. We adopt SLR as it is a systematic, comprehensive, structured and repeatable process that is used to identify and analyze published studies [42]. In this study we use SLR to gather information regarding security threats and information security attributes in cloud computing as well as selecting a framework suitable for identifying information security metrics.

3.2.2 Rationale for thorough analysis of the COBIT framework

In this study, we follow the COBIT framework besides other existing security framework such as ISO 27001. This is because the COBIT framework is more focused on business and it aims at ensuring that IT functions enable organizations in meeting strategic and business objectives while reasonably managing IT risks [10]. Since cloud computing is business architecture, we therefore consider the COBIT framework to be more appropriate in the study than other existing security frameworks. Moreover, the COBIT is a measurement-driven framework which provides several metrics to measure IT processes including metrics for measuring SLA and security performance. We will therefore identify metrics from COBIT that can be applicable in cloud computing.

3.3 Research plan

To achieve the objectives, we divide the study into three main phases as described in following subsections and presented in figure 5.

IV. RESULTS

In this section, the results of the study are presented. Section 5.1 presents study selection for SLR1, and 5.2 presents study selection for SLR2. The identified relevant security attributes and security metrics framework are presented in section 5.3 and 5.4 respectively. Lastly, section 5.5 presents results of the identified information security metrics.

Study selection for SLR1

Results for study selection and inclusion/exclusion process for SLR1

To collect relevant data for the study, we conducted SLR in the Engineering Village, Scopus and other electronic databases. We used the following search strings:

- Engineering Village: (((\$cloud \$computing) WN KY) AND ((\$security OR \$threats OR \$risk* OR \$vulnerabilit) WN KY))
- Scopus: TITLE-ABS-KEY (((cloud computing) AND (\$security OR \$threat* OR \$risk* OR \$vulnerabilit*))) AND PUBYEAR AFT 1969
- Other databases (ISACA, NIST, SANS, ENISA): We used simple search string for the keywords cloud computing, security, risks, vulnerabilities.

We did not restrict the publication year of literatures as we did not have background when exactly cloud computing concept started. We therefore intended to discover as much researches in the area as possible. However, publication year 1969 as seen in search string above is the earliest records of year found in Scopus database.

The built-in characteristics of our databases were used to apply the first and second selection criterion in table 2. Figure 6 shows that those electronic databases yielded 1058 studies. The studies were combined and duplicates deleted using Endnote [45]. We manually deleted duplicates after Endnote failed, leaving 625 studies for analysis. Figure 6 shows phase 1 study outcomes.

We shared 625 studies to discover relevant ones based on table 2's study second filter criteria. The second filter criteria identified 252 relevant studies for our study. After deleting 61 non-full text studies and 109 papers we could not draw information from, we found 82 relevant research.

Distribution of studies per year of publication

It is observed that out of 82 studies identified, many studies were published in the year of 2000 and later with 2009 recording the highest number of studies as presented in figure 7. The details of the 82 studies together with the year of publications are presented in the appendix G.

V. DISCUSSION

Information security attributes and threats in cloud computing

This study has shown that many studies were published in 2006 and later with the year 2009 recording the largest number of publications as presented in section 5.1.3 figure 7. This suggests that information security in cloud computing environment is gaining more attention from the academia. Further, this suggests that the public community is striving to address information security issues in the cloud which has been among the obstacles for its adoption.

In traditional computing researchers have attempted to identify commonly experienced information security threats or risks. For instance, Pfleeger and Pfleeger [46] present that espionage, organized crime, cyberterrorism, eavesdropping, wiretapping, spoofing, session hijacking and denial of service are among the threats in traditional computing. Pfleeger and Pfleeger [46] argue that information security threats ultimately compromise the security attributes namely confidentiality, integrity and availability.

A recent study conducted by Samy et al. [56] presents 22 threats to health information security. Among the threats identified by [56] include repudiation, social engineering attacks, deliberate acts of theft, willful damages, unauthorized use, and deviations in quality of service.

We observe some commonality when we consider the threats identified in this study as presented in section 6.2 with those presented by Pfleeger and Pfleeger [46] as well as by Samy et al. [56]. This suggests that cloud computing is exposed to the same information security threats as the traditional computing. This conclusion is in agreement with CSA [57] who argues that security controls in the cloud computing are the same as those in traditional computing environment. As CSA further argues that depending on cloud computing model deployed organizations operating in the cloud are likely to face more challenging threats [57].

The results presented in figure 9 identify four information security attributes namely confidentiality, integrity, availability and accountability. Figure 9 further presents that confidentiality, integrity, availability and accountability recorded 36%, 22%, 25% and 17% respectively. These results suggest that of the four attributes identified, confidentiality is considered more important followed by availability, integrity and accountability. Based on these results, it is apparent that the identified attributes are the same as those presented by previous researchers for traditional computing [30] [46]. The fact that non-repudiation was not identified as one of the attributes of information security may be due to lack of common vocabulary in information security as a discipline. This argument maybe considered true as even Pfleeger and Pfleeger [46] do not present non-repudiation as an attribute of information security.

Selection of GQM framework

As described in section 5.4, phase 2 (identifying framework for creating metrics) produces an acceptable security metric framework. The requirement for a metric framework stem from the difficulty of finding a manageable number of security indicators due to the abundance of proposed metrics. Figure 16 shows that the COBIT framework [10] describes 340 metrics. Not all COBIT measures are relevant to cloud computing and SLAs, but without an appropriate paradigm for finding metrics, researchers may have identified a significant number of security metrics. According to Basili et al. [28], without a good model and goal specification, it may be unclear what metrics to employ and how to interpret them.

Section 5.4 of the results lists eight frameworks. Each framework has flaws. Bottom-up approach may not yield superior measurements because there are too many object attributes to observe [28]. We found top-down approaches in NIST SP800-55 [34], SANS security metrics recommendations [40], and GQM [26] [28]. Several metric frameworks scored low in acceptability and universality when we used the selection criteria.

We used the GQM framework to generate the measures since it scored highest on simplicity, acceptability, universality, and intended usage. GQM has the greatest score and is top-down, starting with aim (conceptual) and moving down to questions (operational) and measurements. Thus, GQM clarified our selection of cloud computing-relevant SLA-based information security metrics.

SLA based information security metrics

In this study, we identify SLA based information security metrics that can be used by cloud customer to measure information security performance of the cloud services. Although organizations may use in their cloud environment all of the metrics presented in

this study as is, a better understanding of their environment is of paramount. In understanding their cloud environment organization may consider such issues as the type of cloud services and cloud deployment model adopted. Other issues may include regulatory issues governing their business and industry.

Tashi and Ghernaouti [38] suggest that a scope (what to measure) is the primary and first step in undertaking a successful security measurement programme. It is also apparent that without a clear measurement scope organization would end up identifying too many security metrics that are costly and impossible to measure for control and improvements. In this study we focus on ten objects that we consider to be more important in the cloud environment. These objects and their descriptions are presented in section 6.4. The objects were identified based on the COBIT framework. However, we see that these objects are closely related with the issues CSA [47] considers as critical areas in cloud computing. The areas that CSA [47] considers critical include compliance and audit, information lifecycle management, traditional security, business continuity, and disaster recovery, incident response, notification, and remediation, application security, identity and access management. Therefore, we argue that the objects we identified in this study for SLA measurement respond to the business need in addressing information security issues in the cloud computing.

While we identify the metrics we had in mind the characteristics of a good metric as suggested by Jaquith [31] . The suggested characteristics are that the metrics should be consistently measured, cheap to gather, expressed as a cardinal number or percentage, expressed using at least one unit of measure and contextually specific. The metrics presented in this study are in viewpoint of the decision makers so that they can timely take appropriate actions regarding their services in the cloud computing. We also considered the five principles of selecting SLA metrics as suggested by Hayes [4]. The suggested principles are that SLA metrics have to motivate the right behaviour (meet expectation and goals of the customer), reflect factors within the provider's control, easily gathered, not too excessive number of metrics and that set reasonable attainable performance levels.

As shown in figure 16, we observed that a single COBIT domain of Deliver and Support (DS) has 120 metrics which is 35% when compared with a total of 340 metrics presented in the COBIT framework. Such a huge number of metrics as observed in the COBIT framework or a single DS domain may be costly to implement. It may also become merely impossible for an organization to successfully collect the data and measure their information security processes for control and improvement purposes. Moreover, it may not be consistent with the five SLA principles suggested by Hayes [4].

VI. VALIDITY RISKS

Validity risks or commonly known as validity threats concern with how valid the results of a study are [58]. In this study we use validity risks instead of validity threats to avoid confusion with the term "threat" used in this study.

To answer research questions stated, this study solely based on literature identified in several databases such as Engineering Village and Scopus. The identified literatures were analyzed particularly to identify information security attributes in cloud computing. Moreover, we selected a framework for identifying information security metrics from literatures. However, by relying on databases mentioned we could have missed some important studies. To mitigate this risk, we covered several security specific organizations sites such as NIST, SANS, and ISACA that are known to contribute on security related issues and their researches are close to the industry practices.

When conducting SLR1, we expected two validity risks. The first danger was that two of us conducted the study, making data consistency and completeness difficult. We reduced risk by creating data collection form. The data extraction form helped us resolve issues during data extraction. We also expected the data gathering form to have errors that could have influenced the results. We reduced this risk by detecting and fixing form flaws via pilot data extraction.

In SLR2, we anticipated the risk of choosing a metric framework that wasn't acceptable for this study. We reduced risk by applying stringent selection criteria. Each of us applied the selection criteria separately. We then reviewed our results to create a framework. This strategy decreased bias and helped resolve disagreements. The sample size of two of us applying the criteria may not be enough to establish that the

specified framework is feasible. Cloud computing is very young, therefore it's hard to get a large sample of industry experts who may have helped us score the criterion.

Another risk we considered was that the framework may not apply to all industries. We addressed the problem by defining universality criteria to test if the literature's frameworks could be applied to all industries worldwide. We also appreciate that we had to interact with a big population sample from many businesses to generalize our conclusions.

We understand that our results may not apply to IaaS, PaaS, or SaaS because we concentrated on cloud computing. Private, communal, public, and hybrid cloud computing deployment methods may potentially be affected. We suggest future study on alternative services and models.

VII. CONCLUSION AND FUTURE WORK

Cloud computing is an emerging and growing subject in IT industry. Many organizations are exploring cloud computing as a prospering cost-effective computing option for their enterprise needs. Some organizations have already entrusted their sensitive information to be stored in cloud computing environment. Besides that, there are a number of issues that hinders adoption of cloud computing. Among these issues are security, privacy issues, lack of standard for measuring the SLA, complexity in adherence to compliance and audit, regulatory and legal issues as the data might be processed and stored beyond the cloud customer boundaries. This study has addressed the issue of improving information security in the cloud using SLA metrics.

It has been revealed in this study that cloud computing is exposed to the same threats as those facing traditional computing environment. Due to the nature of cloud computing service delivery and deployment models, cloud customers become exposed to more challenging security threats and risks than the traditional computing counterparty. As it has been established in this study, cloud providers have key responsibilities for creating not only a cost effective but also a secure cloud computing service.

Many researchers have suggested that SLA may be used by both cloud customers and providers as a tool for establishing common expectations and goals. For instance, ISACA

[59] suggests that SLA is an effective tool to address cloud computing risks. In this study we therefore assist both cloud provider and customers on the security issues that we believe are to be considered for inclusion in their SLA. We further help them with a number of SLA based information security metrics that might be considered in measuring whether the anticipated security performance and goals of the cloud services are being met.

The SLA based information security metrics identified in this study are generic. The metrics are intended for all cloud computing services and deployment models. Because of time constraint, it is not possible for us to study the metrics to be applicable specifically for each cloud computing type of service and deployment model.

We have learnt that electronic citation databases work based on semantic analysis. However, overtime concepts especially in technology changes. Therefore, researchers need to be aware of these changes in order to obtain reliable search results.

We found that the security in cloud computing architecture is challenging as the subject of cloud computing itself is still developing and evolving. Considering the case of Europe, cloud computing is emerging in the region. This situation has necessitated us to obtain information of this study only based on systematic literature review of published academic studies. Nevertheless, we believe cloud computing gains attention from IT professionals in industry now and even much more in the future. Several researchers also believe that cloud computing will be widely integrated in the industry. In spite of immature state of cloud computing, the study identified SLA based information security metrics in cloud computing environment as the end results. As a potential future work, we can demonstrate the output of this study in academia or industry for validation.

REFERENCES

[1] K. Jeffery, and B. Neidecker-Lutz, The Future of Cloud Computing Opportunities for European Cloud Computing Beyond 2010, European Commission Information Society and Media.

[2] R. Barga, J. Bernabeu-Auban, D. Gannon et al., “Cloud computing architecture and application

programming," SIGACT News, vol. 40, no. 2, pp. 94-5, 2009.

[3] B. R. Kandukuri, V. R. Paturi, and A. Rakshit, "Cloud security issues," 2009 IEEE International Conference on Services Computing (SCC). pp. 517-20.

[4] S. I. Hayes, "Metrics for IT outsourcing Service Level Agreements," http://www.clarity-consulting.com/MetricsforIToutsourcing.pdf, 2004].

[5] GoGrid, "GoGrid Service Level Agreement (SLA)," http://www.gogrid.com/legal/sla.php, [August 10, 2010, 2010].