An Assessment of Security Requirements Compliance of Cloud Providers

Nuntapun Bhensook and Twittie Senivongse
Software Engineering Program, Department of Computer Engineering
Faculty of Engineering, Chulalongkorn University
Bangkok, Thailand
nuntapun.b@student.chula.ac.th, twittie.s@chula.ac.th

Abstract—Cloud provider assessment is important for cloud consumers to determine, when outsourcing computing work, which providers can serve their business and system requirements. This paper presents an initial attempt to assess security requirements compliance of cloud providers by following the Goal Question Metric approach and defining a weighted scoring model for the assessment. The security goals and questions that address the goals are taken from Cloud Security Alliance’s Cloud Controls Matrix and Consensus Assessments Initiative Questionnaire. We then transform such questions into more detailed ones and define metrics that help provide quantitative answers to the transformed questions based on evidence of security compliance provided by the cloud providers. The scoring is weighted by quality of evidence, i.e. its compliance with the associated questions and its completeness. We propose a scoring system architecture which utilizes CloudAudit and assess Amazon Web Services as an example.

Keywords—security; assessment; cloud computing.

I. INTRODUCTION

It is desirable for cloud consumers to be able to determine, when outsourcing computing work, which cloud providers can provide computing services that can serve their business and system requirements. According to [1], three cloud service models are commonly defined with respect to types of computing services, i.e., Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Choosing between different cloud providers of either service model can be difficult for cloud consumers, particularly when it is not easy to determine or compare many quality attributes of the providers, such as security.

Standard organizations issue security-related standards and guidance which can be used in cloud environment such as ISO/IEC 27001 [2] and the Governance, Risk Management, and Compliance (GRC) stack [3] proposed by the Cloud Security Alliance (CSA). We present an initial attempt to assess cloud providers’ security provision by following CSA initiatives within the GRC stack in two steps. First, with the Goal Question Metric approach to quality measurement (GQM) [4], security goals of cloud providers and questions that address the goals are taken from CSA’s Cloud Controls Matrix (CCM) [5] and Consensus Assessments Initiative Questionnaire (CAIQ) [6]. We transform CAIQ questions into more detailed ones in order to help define the metrics, which provide quantitative answers to the transformed questions based on security evidence provided by the providers. Cloud auditors or the providers can then assess security compliance of the cloud services by considering existing evidence and its quality, i.e. its compliance with the associated questions and its completeness. The second step is that we devise a weighted scoring model for determining the degree of security compliance of providers’ offerings. Security compliance scores can help cloud consumers to determine how well their security requirements can be fulfilled if services of certain providers are used. They can also compare the security attribute of different providers. A scoring system architecture, which collects assessment results from cloud providers based on CSA’s CloudAudit deliverables [7] and calculates and ranks security compliance scores, is presented.

The rest of this paper is organized as follows. Section II discusses related work. Section III applies the GQM method to CCM and CAIQ and defines cloud security metrics. The security compliance scoring model is proposed in Section IV together with the system architecture that supports the model. Section V shows as an example the assessment of Amazon Web Services. The paper concludes in Section VI with discussion and future work.

II. RELATED WORK

One of the key barriers to cloud service adoption is the consumer concern over data security. The issue of transparent security [8] is addressed for cloud providers to build consumer trust by disclosing sufficient information about security design, practices, and procedures that will protect consumer data, as well as how compliance with regulations will be met. But at the same time, the providers will have to protect critical security information for overall governance. The effort by the Cloud Security Alliance (CSA), which is the foundation of our work, also aims to promote the use of best practices for providing security assurance within cloud computing. CSA proposes the GRC stack [3] which consists of four initiatives: (1) CloudAudit [7] which provides a common interface and namespace to allow cloud providers to expose audit, assertion, assessment, and assurance information of their cloud services to cloud consumers, (2) Cloud Controls Matrix (CCM) [5] which provides security principles for assessing security provision of cloud consumers, (3) Consensus Assessments Initiative Questionnaire (CAIQ) [6] which provides a set of questions to a cloud consumer and cloud auditor may wish to ask of a cloud provider to determine what security controls exist in
the cloud service, and (4) Cloud Trust Protocol (CTP) which offers cloud consumers a mechanism to find out important information about security in the cloud while offering cloud providers a standard technique to prepare and deliver the information to the consumers. Among the four CSA initiatives, we will later focus on the first three.

Knobe and Egan [9] present the Cloud Trust Protocol (CTP) as the enabling mechanism to create digital trust by making cloud activities visible and controllable by cloud consumers. We see that this protocol shares with us the view of transparent security since it allows the consumers to request from the providers the access to elements of transparency, i.e. pieces of information seen as trust evidence such as configuration, vulnerability, audit log, and service statistics. The elements of transparency can be negotiated between a specific cloud consumer and a provider, and hence, unlike our approach, the protocol builds trust for existing consumers rather than prospective consumers who are choosing between different cloud providers.

Pauley [10] defines a scorecard for cloud consumers to evaluate cloud transparency on the basis of the providers’ use of standards, best practices, policies, and procedures with regard to security, privacy, audit, and service levels. The evaluation considers the information available on the service portals as well as other published Web content related to previous service breaches and downtime. For each aspect, the evaluation is guided by a number of “yes or no” questions and requires a visit to relevant Web sites to analyze the necessary information. In addition, a “yes or no” answer means the provider performs some activity or has some evidence in response to the question but it does not necessarily say about the quality of the activity and evidence.

A different approach toward scoring of trust in the providers is by Sumetanupap and Senivongse [11]. Since provider quality always has a strong influence on service selection, they look at trust from the Social Psychology perspective and compile a list of questions regarding the provider’s competence, benevolence, and integrity. Their scoring model is based on the fuzzy set theory.

III. SECURITY REQUIREMENTS COMPLIANCE

This section describes the first step of our approach in which security compliance of cloud providers can be assessed. We apply the GQM approach to quality measurement [4] and follow CSA’s CCM and CAIQ in the assessment.

The overview of the assessment is depicted in Fig. 1. GQM is defined in a top down fashion. First, a goal (i.e. security attribute) which involves an object under measurement (i.e. cloud provider’s offering) will be defined, followed by a set of questions which characterize the object under measurement with regard to its achieving the goal. Associated with each question are metrics or a set of data which help provide a quantitative answer to the question. CCM defines a list of security control requirements which cloud providers and their offerings should fulfill. There are 11 control groups which can be seen as security goals, and each control group has several control areas. Each control area is associated with a control specification which defines what should be done in that control area. CAIQ provides “yes or no” control questions for each control area in the CCM to assist in vetting the providers on the security of their service offerings and on their security profiles. These questions help us understand the activities that the providers are expected to perform and the artifacts that the providers are expected to produce in order to meet the requirements in the CCM. However, we need evidence to ensure that the providers really perform or produce as expected. Hence we transform CAIQ questions into more detailed ones before defining metrics that answer the transformed questions.

A. Mapping CCM to GQM Goals

The 11 control groups in the CCM can be formulated into the measurement goals since they are what the cloud provider is expected to attain. We use the goal definition template [4] for specifying that a goal is to: (1) Analyze the object under measurement, (2) For the purpose of understanding, controlling or improving the object, (3) With respect to the quality focus of the object that the measurement focuses on, (4) From the viewpoint of the people who measure the object, and (5) In the context of the environment in which measurement takes place. As an example, the definition of the goal G-01 Compliance (i.e. the control group CO) is given in Table I.

B. Mapping CAIQ to GQM Questions to Derive GQM Metrics

The “yes” or “no” answers to CAIQ control questions cannot tell whether the activities that the providers are expected to perform and the artifacts that the providers are expected to produce for CCM control areas really do exist or have good quality. Since we aim to put an emphasis on the existence of evidence as well as its quality so that it can help confirm whether and how well the providers comply with the best practices in the control areas, we define GQM questions by transforming CAIQ questions as in Table II.

---

**A different approach toward scoring of trust in the providers is by Sumetanupap and Senivongse [11]. Since provider quality always has a strong influence on service selection, they look at trust from the Social Psychology perspective and compile a list of questions regarding the provider’s competence, benevolence, and integrity. Their scoring model is based on the fuzzy set theory.**

---

**III. SECURITY REQUIREMENTS COMPLIANCE**

This section describes the first step of our approach in which security compliance of cloud providers can be assessed. We apply the GQM approach to quality measurement [4] and follow CSA’s CCM and CAIQ in the assessment.

The overview of the assessment is depicted in Fig. 1. GQM is defined in a top down fashion. First, a goal (i.e. security attribute) which involves an object under measurement (i.e. cloud provider’s offering) will be defined, followed by a set of questions which characterize the object under measurement with regard to its achieving the goal. Associated with each question are metrics or a set of data which help provide a quantitative answer to the question. CCM defines a list of security control requirements which cloud providers and their offerings should fulfill. There are 11 control groups which can be seen as security goals, and each control group has several control areas. Each control area is associated with a control specification which defines what should be done in that control area. CAIQ provides “yes or no” control questions for each control area in the CCM to assist in vetting the providers on the security of their service offerings and on their security profiles. These questions help us understand the activities that the providers are expected to perform and the artifacts that the providers are expected to produce in order to meet the requirements in the CCM. However, we need evidence to ensure that the providers really perform or produce as expected. Hence we transform CAIQ questions into more detailed ones before defining metrics that answer the transformed questions.

**A. Mapping CCM to GQM Goals**

The 11 control groups in the CCM can be formulated into the measurement goals since they are what the cloud provider is expected to attain. We use the goal definition template [4] for specifying that a goal is to: (1) Analyze the object under measurement, (2) For the purpose of understanding, controlling or improving the object, (3) With respect to the quality focus of the object that the measurement focuses on, (4) From the viewpoint of the people who measure the object, and (5) In the context of the environment in which measurement takes place. As an example, the definition of the goal G-01 Compliance (i.e. the control group CO) is given in Table I.

**B. Mapping CAIQ to GQM Questions to Derive GQM Metrics**

The “yes” or “no” answers to CAIQ control questions cannot tell whether the activities that the providers are expected to perform and the artifacts that the providers are expected to produce for CCM control areas really do exist or have good quality. Since we aim to put an emphasis on the existence of evidence as well as its quality so that it can help confirm whether and how well the providers comply with the best practices in the control areas, we define GQM questions by transforming CAIQ questions as in Table II.
Cloud auditors, or providers as in the case of self-assessment, will assign such scores to the evidence given by the providers. In a certain case, cloud providers may not disclose some security information and evidence unless a confidentiality agreement is made before the assessment. In the case that providers advertise their security processes and policies without any concrete evidence, reputation and trustworthiness of their Web sites rated by trusted sources may be consulted to assist in the assessment.

IV. SECURITY COMPLIANCE SCORING

This section describes the second step of our approach in which security compliance scores of cloud providers can be computed.

A. Weighted Scoring Model

Given the result of the GQM method, we devise a security scoring model for cloud providers based on documentation the providers present as evidence of goal attainment. The measurements of evidence quality are used as weighting factors in the model that comprises the following equations.

The overall security score $S_c$ (in %) of a cloud provider is computed by

$$S_c = \sum_{g=1}^{k} \frac{S_g}{k}$$

where $S_g$ = security score with regard to a goal $g$ as computed by (2),

$k$ = number of goals.

### TABLE II. EXAMPLE OF QUESTION TRANSFORMATION

<table>
<thead>
<tr>
<th>CAIQ Questions</th>
<th>Transformed Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Area</strong>: Audit Planning</td>
<td><strong>Control Specification</strong>: Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e. internal/external audits, certifications, vulnerability and penetration testing).</td>
</tr>
<tr>
<td>CO-01.1 Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA’s Cloud Computing Management Audit/Assurance Program, etc.)?</td>
<td>Q-01.1 What is the quality of evidence of audit assertions, using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA’s Cloud Computing Management Audit/Assurance Program, etc.), that you produce?</td>
</tr>
<tr>
<td>CO-02.1 Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISA4302 or similar third party audit reports?</td>
<td>Q-01.2 What is the quality of evidence of SAS70 Type II/SSAE 16 SOC2/ISA4302 or similar third party audit reports that you allow tenants to review?</td>
</tr>
<tr>
<td>CO-02.2 Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?</td>
<td>Q-01.3 What is the quality of evidence of network penetration tests of your cloud service infrastructure that you conduct regularly as prescribed by industry best practices and guidance?</td>
</tr>
</tbody>
</table>

Regarding quality of evidence, there are two types of quality in the assessment.

1) **Compliance of Evidence**: Evidence will be assessed if it complies with the required documentation addressed by the questions, or follows known international or industry standards and guidelines, such as ISO or ITIL specifications and others. In the case that the evidence proves to be in the context of the question but is not clear that it is fully compliant, the compliance level can be partial. For example, if a question is associated with an international standard but the provider provides evidence that conforms to an internal security checklist which follows some best practices, its compliance can be partial. We define compliance score of evidence as in Table III.

2) **Completeness of Evidence**: If producing evidence for a question is considered as a project with several groups of processes to run within the project [12], the documentation presented as evidence at any one time can be in different forms depending on the stage of the project. We can specify completeness level of the evidence by first determining the project document to which the evidence correspond. Then the process group in which the document belong indicates the completeness score of the evidence as in Table IV.

### TABLE III. COMPLIANCE SCORE OF EVIDENCE

<table>
<thead>
<tr>
<th>Compliance Level</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Compliance</td>
<td>1</td>
</tr>
<tr>
<td>Partial Compliance</td>
<td>0.5</td>
</tr>
<tr>
<td>Noncompliance</td>
<td>0</td>
</tr>
</tbody>
</table>

### TABLE IV. COMPLETENESS SCORE OF EVIDENCE

<table>
<thead>
<tr>
<th>Completeness Level (Process Group)</th>
<th>Related Document Type</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Evidence</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Initial</td>
<td>Project charter, Preliminary project scope statement</td>
<td>0.1</td>
</tr>
<tr>
<td>Planning</td>
<td>Project scope management plan, Work breakdown structure (WBS), WBS dictionary, Scope baseline, Activity list, Milestone list, Project schedule</td>
<td>0.3</td>
</tr>
<tr>
<td>Executing</td>
<td>Project management plan (update), Recommended corrective actions, Project staff assignments, Team performance assessment</td>
<td>0.5</td>
</tr>
<tr>
<td>Monitoring and Control</td>
<td>Recommended corrective actions, Recommended preventive actions</td>
<td>0.8</td>
</tr>
<tr>
<td>Closing</td>
<td>Final product/service/result, Closed contract</td>
<td>1</td>
</tr>
</tbody>
</table>

The metrics are defined in Table V for measuring the quality score, i.e. compliance score and completeness score, of related evidence.
The security score $S_g$ (in %) with regard to a goal $g$ is computed by

$$S_g = \frac{\sum_{i=1}^{m} \text{Actual}S_{q_{i}} \times 100}{\sum_{i=1}^{m} \text{Total}S_{q_{i}}}$$  \hspace{1cm} (2)$$

where $\text{Actual}S_{q_{i}}$ = actual security score with regard to a question $q$ of goal $g$ as computed by (3),

$$\text{Total}S_{q} = \text{possible total security score with regard to a question } q \text{ of goal } g \text{ as computed by (3)},$$

$m = \text{number of questions of goal } g.$

The security score $S_m$ (in %) with regard to a metric $m$ is computed by

$$S_m = \frac{\sum_{i=1}^{p} \text{Actual}S_{m_{i}} \times 100}{\sum_{i=1}^{p} \text{Total}S_{m_{i}}}$$  \hspace{1cm} (3)$$

where $\text{Actual}S_{m_{i}} = \text{actual security score with regard to a metric } m \text{ of question } q \text{ as computed by (4)},$

$$\text{Total}S_{m} = \text{possible total security score with regard to a metric } m \text{ of question } q \text{ as computed by (4)},$$

$p = \text{number of metrics of question } q.$

The security score $S_e$ (in %) with regard to a metric $e$ that is associated with metric $m$ (i.e. 1 if evidence exists and 0 if there is no evidence),

$$S_e = \frac{\sum_{i=1}^{r} (S_e \times W_{e_{i}}) \times 100}{(\text{max}(W_{e_{j}}) + \text{max}(W_{e_{j}})) \times r}$$  \hspace{1cm} (4)$$

where $S_e = \text{existence score of evidence } e \text{ that is associated with metric } m$ (i.e. 1 if evidence exists and 0 if there is no evidence),

$W_{e_{i}} = \text{compliance score of metric } m \text{ for evidence } e \text{ as in Table III},$

$W_{e_{j}} = \text{completeness score of metric } m \text{ for evidence } e \text{ as in Table IV},$

$\text{max}(W_{e_{j}}) = \text{maximum compliance score (i.e. 1),}$

$\text{max}(W_{e_{j}}) = \text{maximum completeness score (i.e. 1),}$

$r = \text{number of evidence associated with metric } m.$

For a cloud consumer to select a provider, a choice should be made first on the service model, i.e. whether the required service is IaaS, PaaS, or SaaS. Then the scoring model can be used to compute the scores of different providers of the same service model for comparison.

Although the security level of a specific cloud provider does not directly depend on its deployment model (i.e. private, public, community, and hybrid) but rather on its security assurance, the deployment type does contribute to the degree of control the consumer has over security in the cloud [1]. Private cloud is operated exclusively for a consumer organization and therefore the consumer control over security and governance is the highest whereas it is the
lowest for public cloud which is operated for general public outside the consuming organization. The security control of community cloud and hybrid cloud should fall between those two. Community cloud is closer to private cloud than public cloud as it is operated for multiple organizations which have common security and regulatory consideration. Hybrid cloud involves a composition of two or more clouds, e.g. a cloud service which combines a public cloud and a private cloud. A consumer who is, for example, concerned with control over security may prefer a private cloud provider with a lower security score over a public cloud provider with a higher score.

B. Scoring System Architecture

Since a large number of control areas and control questions can make the assessment infeasible for cloud stakeholders, CSA therefore encourages automated assessment. Using CloudAudit interface and namespace, our scoring system architecture in Fig. 2 can automate security compliance measurement by allowing cloud providers to make necessary security information accessible. A template called a GQM Matrix (GQMM) template is provided for the providers to present security assurance information including results of the assessment by cloud auditors or by the providers themselves (i.e. results from Section III) as well as associated evidence. Since such information can be updated over time, the architecture includes Web feed and feed reader features for provider information updates. Given the security information fed by the providers, the scoring engine can compute security compliance scores of the providers using the model in Section IV.A. Via the user interface, cloud consumers can specify criteria for viewing and ranking security scores of providers of a particular service model or deployment model, or the scores for a particular goal.

V. EXAMPLE

As an example, we apply the assessment and scoring model to Amazon Web Services (AWS). The scores cannot be treated as the actual scores of Amazon AWS since only the questions and metrics of the Compliance (G-01) and Information Security (G-05) goals in Table V are considered. Due to space limitation, suppose security information and relevant evidence is made available by Amazon AWS for assessment as summarized in Table VI. Note that only a number of metrics are provided with associated evidence.

A cloud auditor considers the metrics and existing evidence and then assesses evidence compliance and completeness. For example, for the metric M-01.3.1 Network Penetration Test Policy, AWS does not conduct penetration testing, but a policy for customers to conduct penetration tests by themselves or by a third party is in place [15]. The auditor considers this policy as partially compliant. Since this policy states how to request authorization to conduct the tests, it is in the initial phase of testing. Evidence associated with other metrics gives detailed or fully compliant documentation, and the completeness level is closing.

When this assessment information is fed to the scoring system, the security compliance score is computed as follows.

For the goal G-01 Compliance and using (4) and Tables III-IV, we obtain

![Figure 2. Scoring system architecture.](image-url)
The reliability of assessment results depends on the security information that is provided by cloud providers. By emphasizing the existence and quality of compliance evidence, the approach tries to alleviate the problem of provider fraud. Also, transparent security is still an open issue since the providers need to consider which necessary information should be disclosed to improve consumer confidence in service offerings, while also concealing potentially sensitive information. Apparently, missing or low quality evidence can affect security scores, and cloud consumers should be able to trust cloud offerings which provide more evidence of higher quality.

We can enhance the assessment by considering other quality aspects of the evidence. For example, a cloud provider presenting up-to-date evidence, such as third-party certificates renewed regularly, would be preferred to another provider who gives out-of-date evidence. For better selection, the GQM approach can be applied to measuring other nonfunctional aspects of cloud providers, e.g. availability of management tools, usability, and pricing.

VI. DISCUSSION AND CONCLUSION

This paper presents an approach to security assessment of cloud providers. The scope of security requirements to be assessed includes those best practices and guidance listed in CSA’s CCM and the questions given in CSA’s CAIQ. We apply the GQM method and derive relevant metrics with an emphasis on the existence and quality of the evidence. A scoring model and system architecture are proposed.

We consider our approach as an initial attempt to assess security compliance because the questions/metrics are transformed/derived in a straightforward manner from CAIQ questions. Given that CAIQ questions are quite generic and address CCM control areas whose control specifications are also broad, we see that our approach lists an initial or default set of questions and metrics for assessment. To accommodate different assessment needs of different cloud stakeholders, service models, and deployment models, more detailed control areas and control questions should be derived in order for the assessment to better address such needs.

For the goal G-05 Information Security and using (4) and Tables III-IV, we obtain

- score of G-05.1.1 = 0%
- score of G-05.1.2 = 0%
- score of G-05.1.3 = 0%
- score of G-05.1.4 = 0%
- score of G-05.1.5 = 0%
- score of G-05 = (0+0+0+100+100) / 500 = 40%

Using (2), we obtain

- score of G-05 = (40*100) / 100 = 40%

REFERENCES