# Cloud Service Trustworthiness Assessment Based on Cloud Controls Matrix

Jirayu Kanpariyasoontorn, Twittie Senivongse

Computer Science Program, Department of Computer Engineering, Faculty of Engineering, Chulalongkorn University
254 Phyathai Road, Pathumwan, Bangkok, 10330, Thailand
**jirayu.kanp@student.chula.ac.th, twittie.s@chula.ac.th**

***Abstract*— Cloud computing has been widely adopted by corporate and individual customers due to its resource-sharing model that allows on-demand access to scalable and high performance computing services. The growth of such services means there are a lot of service providers who can provide similar services, and hence quality attributes of the services become the criteria for cloud service selection. This paper focuses on cloud service trustworthiness that embraces both security and dependability attributes. A trustworthiness assessment method is proposed based on the CSA Cloud Controls Matrix security guidelines that are mapped to NIST SP800-53 security and privacy recommendations and AICPA trust services principles and criteria in order to classify security and dependability characteristics of each control. Based on the mapping, the provision capabilities of a cloud service as listed in the CSA Consensus Assessments Initiative Questionnaire are assessed and the trustworthiness score of the service is calculated. The assessment method then can assist service consumers in determining and comparing trustworthiness of candidate cloud services as one factor to consider in the service selection process.**

***Keywords*— trustworthiness; security; dependability; cloud computing; assessment**

## I. Introduction

The widely-adopted cloud computing model offers on-demand network access to shared computing resources that can be provisioned, released, monitored, and controlled in a convenient way [1]. Due to the growing number of cloud services, there are a lot of service candidates for a service consumer to choose from, and cloud service selection can become a non-trivial task. Service consumers need to be confident that their data and/or information systems in the cloud are well managed since adverse events (such as system failure, information leakage, or natural disaster) can have a serious impact on their business.

Since cloud providers are likely to offer services with similar functionalities, service consumers are concerned about which services they can trust better. Trustworthiness is a characteristic that, with respect to an information system, “expresses the degree to which the system can be expected to preserve, with some degree of confidence, the confidentiality, integrity, and availability of the information that is being processed, stored, or transmitted by the system across a range of threats.” [2] Service consumers should be assisted in assessing whether cloud services are trustworthy and can operate with a degree of tolerance for system failures, human errors, purposeful attacks, and environmental disruptions.

To assess a cloud service, this paper proposes a trustworthiness assessment method. The assessment is conducted by analyzing service provision capabilities of a cloud service which are published as a response to the Consensus Assessments Initiative Questionnaire (CAIQ) [3] of the Cloud Security Alliance (CSA). The CAIQ contains questions that are a checklist of conduct and are in accordance with the CSA’s Cloud Controls Matrix (CCM) [4] that describes security controls that should be implemented by cloud services. To assess how trustworthy a cloud service is, we first analyze the characteristic of each CCM control. Based on [5], consumer trust is led by dependability and security attributes of the service. The two attributes altogether consist of six subattributes, i.e. confidentiality, integrity, availability, reliability, safety, and maintainability. Therefore, each CCM control is analyzed to see if it is associated with any of these subattributes by considering its association with the security and privacy recommendations by NIST SP800-53 [2] and the trust services principles and criteria by the American Institute of Certified Public Accountants (AICPA) [6]. Then we can determine all subattribute scores and the trustworthiness score of the cloud service from the degree of compliance with the CCM based on the provider response to the CAIQ. In addition, the method differentiates the CMM controls that perform security functions from the ones that are assurance-related, i.e. the ones that are the measures of confidence and, if performed, can lead to trust in the service. The differentiation therefore can refine the scores to better reflect different quality aspects of different cloud services. We conduct a comparative experiment by assessing trustworthiness of five well-known cloud services.

Section II of this paper describes background and related work. Section III proposes the trustworthiness assessment method and section IV presents an experiment and a discussion. The paper concludes in section V.

## II. Related Work

The Cloud Security Alliance (CSA) is a not-for-profit organization that works on the adoption of security best practice and guidelines within cloud computing. Several initiatives are promoted, two of which are of concern here, i.e. CCM and CAIQ. The CCM or Cloud Controls Matrix [4] describes control guidelines for security provision of cloud services. The control guidelines are classified into 16 control domains where each domain is further divided into a number of controls. There are 133 controls in the CCM v.3.0.1. Each control describes what should be done or produced by a cloud service or a service provider. The specification of each control can be traced back to other corresponding security-related standards and recommendations such as those published by NIST and AICPA. The CAIQ or Consensus Assessments Initiative Questionnaire [3] accompanies the CCM and provides a set of yes/no questions to determine whether a cloud service follows each of the CCM controls. The CAIQ can be used by a service provider as a self-checklist for compliance with the CCM and by a cloud customer and auditor who wish to determine what security controls exist in the cloud service. A cloud provider can publish the yes/no responses to the CAIQ questions with the CSA Security, Trust & Assurance Registry (STAR) [7].

Several approaches to measurement of cloud service quality have been proposed but we will focus on those that are based on the CCM. The Cloud Service Measurement Initiative Consortium (CSMIC) publishes a Service Measurement Index (SMI) [8] as a measurement framework to enable cloud service comparison. SMI consists of seven measurement categories and each category is further refined by a number of attributes. Within each attribute, a number of quantitative or qualitative measures are defined. The categories range from the more business-oriented ones (i.e. accountability of provider organizations and the financial aspect) to the more technical ones (i.e. performance, assurance, security & privacy, agility, and usability). Particularly for security & privacy, the the CCM controls are used as the measures. The provider or a customer can assign a weight to each measure (based on the importance of that measure) and a score between 1 and 10 as a level of compliance with that CCM control. Our approach can complement the SMI but we focus only on dependability and security aspects to present a combined view of trustworthiness. In addition, our approach to differentiating between the CCM controls that address security functionality and those that address security assurance can be applied to assign a weight to each SMI security & privacy measure. Another approach is by Bhensook and Senivongse [9] which uses a Goal-Question-Metric approach to develop a CCM-compliance measurement model for comparing security capabilities of cloud services. They transform the questions in the CAIQ into the more assurance-oriented questions that ask for evidence of compliance for scoring the security capabilities. Their model also considers the quality of the evidence in terms of its completeness and its compliance with the controls. Their work only focuses on the security attribute and does not model a broader view of trustworthiness.

Habib et al. [10] propose a different approach toward trust in a cloud service. They use trust-aware framework to validate that the cloud service is compliant with the CCM controls as claimed by the provider in the CAIQ self-assessment. To build trust in a service, they model CCM controls as trust properties that can be validated by certificates (i.e. hard trust) or validated from past experience and behaviour associated with an entity such as a certification authority or cloud provider (i.e. soft trust). They use logic languages in the validation. Our approach addresses consumer trust from a different perspective as we determine trust from trustworthiness of the service based on a quality attributes model.

Other researchers propose non-CCM-based assessment of cloud trustworthiness. An example is the work by Bedi et al. [11] in which a cooperative model of society is used, and trustworthy service providers are selected based on the recommendations given by the customer's trustworthy acquaintances. Another example is the work by Wang and Wu [12] in which their trustworthiness measurement model comprises common trustworthiness factors (such as feedback, recommendation, time, profile, history, risk, friendship) and other unique factors that are specific to each service.

## III. Cloud Service Trustworthiness Assessment Method

The overview of the cloud service trustworthiness assessment method is shown in Figure 1. By definition [5], trustworthiness is a result of security and dependability attributes and their subattributes. That is, security is further characterized by confidentiality, integrity, and availability, whereas dependability is by integrity, availability, reliability, safety, and maintainability. We analyze the specification of each control of the CCM which corresponds to certain controls in the NIST SP800-53 recommendation and AICPA trust services principles and criteria to identify the associated subattributes. Then service trustworthiness is assessed from the provider response to the CAIQ questions which shows the degree of compliance with the CCM controls, and hence the degree of those quality subattributes. In the assessment, complying with the controls that are assurance-related according to NIST SP800-53 will have more impact on the trustworthiness and subattribute scores of the service. The detail of each step of the method is as follows.

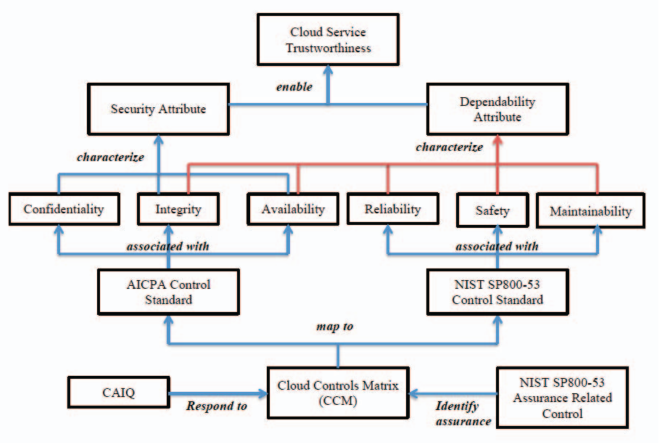

**Figure 1.** Overview of assessment method

### A. *Map CCM and CAIQ to AICPA and NIST SP800-53 Controls*

The CCM control guidelines are classified into 16 control domains as shown in Table 1. Each control domain comprises several controls. Table 2 gives an example of the four controls within the Application & Interface Security control domain. Each control has a number of yes/no questions defined in the CAIQ questionnaire, such as those in Table 3, and cloud providers may publish their response to these questions with the STAR registry. The CCM also maps each of its controls to the controls of several other standards including the AICPA and NIST SP800-53 controls. AICPA has published a set of principles and criteria for evaluating controls that are relevant to the security, availability, and integrity of a system, and the confidentiality and privacy of the information processed by the system. NIST recommends the baseline controls for the information systems of different levels of impact on the organization. Table 4 lists an example of the correspondence between each of the four controls of the Application & Interface Security control domain and the relevant AICPA and NIST SP800-53 controls.

### B. *Associate CCM Controls with Subattributes*

To classify which CCM controls, if implemented by a cloud service, will lead to which subattributes, we examine the specification of each control. We consider that the specification of each CCM control alone may not clearly indicate the relevant subattibutes, so we consult the specifications of the corresponding AICPA and NIST SP800-53 controls.

Since AICPA controls address more on the security attribute, they are helpful in associating the corresponding CCM controls with confidentiality, integrity, and availability subattributes as well as their combination. Table 5 gives an example of a control that is common to all security subattributes as well as those that address particular subattribute.

**TABLE 1.** 16 CCM CONTROL DOMAINS

| | |
|---|---|
| Application & Interface Security (AIS) | Human Resources Security (HRS) |
| Audit Assurance & Compliance (AAC) | Identity & Access Management (IAM) |
| Business Continuity Management & Operational Resilience (BCR) | Infrastructure & Virtualization Security (IVS) |
| Change Control & Configuration Management (CCC) | Interoperability & Portability (IPY) |
| Data Security & Information Lifecycle Management (DSI) | Mobile Security (MOS) |
| Datacentre Security (DSC) | Security Incident Management, E-Discovery & Cloud Forensics (SEF) |
| Encryption & Key Management (EKM) | Supply Chain Management, Transparency and Accountability (STA) |
| Governance & Risk Management (GRM) | Threat & Vulnerability Management (TVM) |

To analyze dependability subattributes, NIST SP800-53 is used. Its controls are organized into 18 families and we use three of them in this paper, i.e. Physical and Environmental Protection, Contingency Planning, and Maintenance. We consider them as related respectively to safety, reliability, and maintainability subattributes. An example is listed in Table 6.

**TABLE 2.** EXAMPLE OF FOUR CCM CONTROLS OF AIS DOMAIN [4]

| Control Domain and Control | Control ID | Control Specification |
|---|---|---|
| Application & Interface Security *Application Security* | AIS-01 | Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g. OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations. |
| Application & Interface Security *Customer Access Requirements* | AIS-02 | Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed. |
| Application & Interface Security *Data Integrity* | AIS-03 | Data input and output integrity routines (i.e. reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse. |
| Application & Interface Security *Data Security/ Integrity* | AIS-04 | Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction. |

**TABLE 3.** EXAMPLE OF CAIQ QUESTIONS FOR CONTROL AIS-02 [4]

| Control Domain and Control | Control ID | CAIQ Question |
|---|---|---|
| Application & Interface Security *Customer Access Requirements* | AIS-02 | Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems? |
| | | Are all requirements and trust levels for customers' access defined and documented? |

TABLE 4. EXAMPLE OF MAPPING BETWEEN CCM CONTROLS AND AICPA AND NIST SP800-53 CONTROLS [4]

| Control Domain and Control | Control ID | AICPA Controls | NIST SP800-53 Controls |
|---|---|---|---|
| Application & Interface Security *Application Security* | AIS-01 | CC7.1 | SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-8, SC-9, SC-10, SC-11, SC-12, SC-13, SC-14, SC-17, SC-18, SC-20, SC-21, SC-22, SC-23 |
| Application & Interface Security *Customer Access Requirements* | AIS-02 | CC5.1 | CA-1, CA-2, CA-5, CA-6 |
| Application & Interface Security *Data Integrity* | AIS-03 | PI1.2,<br>PI1.3,<br>PI1.5 | SI-10, SI-11, SI-2, SI-3, SI-4, SI-6, SI-7, SI-9 |
| Application & Interface Security *Data Security/ Integrity* | AIS-04 | CC5.6 | AC-1, AC-4, SC-1, SC-16 |

TABLE 5. EXAMPLE OF AICPA CONTROLS [6]

| AICPA Criteria | ID | Control Specification |
|---|---|---|
| Criteria common to all subattributes of security (confidentiality, integrity, availability) | CC5.6 | Logical access security measures have been implemented to protect against [insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof] threats from sources outside the boundaries of the system. |
| Additional criteria for confidentiality | C1.2 | Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality commitments and requirements. |
| Additional criteria for availability | A1.2 | Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, monitored, and maintained to meet availability commitments and requirements. |
| Additional criteria for processing integrity | PI1.3 | Data is processed completely, accurately, and timely as authorized in accordance with processing integrity commitments and requirements. |

TABLE 6. EXAMPLE OF NIST SP800-53 CONTROLS [2]

| Attribute | Control Family | Example of Control Specification |
|---|---|---|
| Safety | Physical and Environment al Protection (PE) | (PE-13) Fire Protection<br>The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. |
| Reliability | Contingency Planning (CP) | (CP-6) Alternate Storage Site<br>The organization<br>a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and<br>… |
| Maintaina bility | Maintenance (MA) | (MA-2) Controlled Maintenance<br>The organization:<br>a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;<br>… |

### C. *Define CCM Control Domain-Subattribute Association Matrix*

In this step, we calculate the degree of association that each CCM control domain has with each subattribute in order to define a control domain-subattribute association matrix $D$:

$$D = \begin{bmatrix} d_{1,1} & \dots & d_{1,6} \\ \dots & \dots & \dots \\ d_{16,1} & \dots & d_{16,6} \end{bmatrix}$$

Each element $d_{n,k}$ of $D$ is

$$d_{n,k} = \frac{\sum_{i=1}^{m} a_{n,k,i}}{m} \quad (1)$$

where $d_{n,k}$ = degree of association between control domain $n$ and subattribute $k$, and the degree value is in [0,1];

$a_{n,k,i}$ = value of the association between control $i$ of control domain $n$ and subattribute $k$; the value is 1 if control $i$ is associated with subattribute $k$, and 0 otherwise;

$m$ = number of controls in control domain $n$.

For example, in Table 4, three CCM controls in the AIS control domain, are associated with all the confidentiality, integrity, and availability subattributes, but one is associated with the integrity subattribute only. In other words, 3/4 controls are related to confidentiality and availability, and all four controls are related to integrity. Therefore, the degree of association between the AIS control domain and confidentiality and availability is 0.75 each, and that for integrity is 1. Table 4 also shows that none of the AIS controls map to the PE, CP and MA families of NIST SP800-53. So the degree of association between the AIS control domain and reliability, safety, and maintainability is all 0. The complete matrix *D* is shown in Table 7.

### *D. Calculate Assurance Weights for CCM Control Domains*

According to NIST SP800-53, security functionality and security assurance are two components that affect trustworthiness [2]. Security functionality is concerned with security features, functions, mechanisms, services, procedures, and architectures that are implemented for the information systems. Security assurance is the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome. Some NIST SP800-53 controls focus on security functionality, some on security assurance, and some on both. We then differentiate between these types of controls and give an extra weight to any assurance-related control since, if implemented, it can heighten the confidence and trustworthiness the cloud customers could have in the service. Assurance-related controls produce security evidence such as design/ development artifacts, assessment results, warranties, and certificates. The assurance weight of a CCM control domain is based on the number of NIST assurance-related controls that are related to that control domain. It is computed by

$$as_n = 1 + \left( \frac{ac_n}{ct_n} \right) \tag{2}$$

where $as_{n,}$ = assurance weight score of control domain *n*, and the score is in [1, 2);

$ac_n$ = number of NIST SP800-53 assurance-related controls that are related to control domain *n*;

$ct_n$ = number of all NIST SP800-53 controls that are related to control domain *n*.

For example, in Table 8, there are 35 NIST SP800-53 controls that are related to the AIS control domain (duplicates are counted), and 14 of them are assurance-related. So the assurance weight score of AIS is 1.4 (1+0.4). The assurance scores for all CCM control domains are listed in Table 9.

TABLE 7. CCM CONTROL DOMAIN-SUBATTRIBUTE ASSOCIATION MATRIX

| Control Domain | Confidentiality | Integrity | Availability | Reliability | Safety | Maintainability |
|---|---|---|---|---|---|---|
| AIS | 0.75 | 1 | 0.75 | 0 | 0 | 0 |
| AAC | 1 | 1 | 1 | 0.33 | 0.33 | 0.33 |
| BCR | 0.63 | 0.72 | 1 | 0.45 | 0.36 | 0.54 |
| CCC | 1 | 1 | 1 | 0 | 0 | 0 |
| DSI | 0.85 | 0.85 | 0.85 | 0 | 0.14 | 0 |
| DSC | 1 | 1 | 1 | 0 | 0.5 | 0.22 |
| EKM | 0.5 | 0.5 | 0.5 | 0 | 0 | 0 |
| GRM | 0.81 | 0.81 | 0.9 | 0.18 | 0.18 | 0.36 |
| HRS | 0.9 | 0.9 | 0.9 | 0 | 0 | 0 |
| IAM | 0.61 | 0.61 | 0.61 | 0 | 0 | 0.3 |
| IVS | 0.46 | 0.46 | 0.46 | 0 | 0.07 | 0 |
| IPY | 0 | 0 | 0 | 0 | 0 | 0 |
| MOS | 0 | 0 | 0 | 0 | 0 | 0 |
| SEF | 1 | 1 | 1 | 0.4 | 0 | 0.4 |
| STA | 0.33 | 0.33 | 0.33 | 0.1 | 0.1 | 0.1 |
| TVM | 1 | 1 | 1 | 0.33 | 0 | 0.33 |

TABLE 8. EXAMPLE OF NIST SP800-53 ASSURANCE-RELATED CONTROLS

| Control ID | NIST SP800-53 Control | Assurance-Related Control |
|---|---|---|
| AIS-01 | SC-2, SC-3, SC-4, SC-5, SC-6, SC-7, SC-8, SC-9, SC-10, SC-11, SC-12, SC-13, SC-14, SC-17, SC-18, SC-20, SC-21, SC-22, SC-23 | SC-2, SC-3<br>SC-6, SC-11 |
| AIS-02 | CA-1, CA-2, CA-5, CA-6 | CA-1, CA-2<br>CA-5 , CA-6 |
| AIS-03 | SI-10, SI-11, SI-2, SI-3, SI-4, SI-6, SI-7, SI-9 | SI-10, SI-4,<br>S-I6, SI-7 |
| AIS-04 | AC-1, AC-4, SC-1, SC-16 | AC-1, SC-1 |

TABLE 9. ASSURANCE WEIGHTS OF CCM CONTROL DOMAINS

| AIS | AAC | BCR | CCC | DSI | DSC | EKM | GRM |
|---|---|---|---|---|---|---|---|
| 1.4 | 1.86 | 1.31 | 1.76 | 1.28 | 1.3 | 1 | 0.65 |

| HRS | IAM | IVS | IPY | MOS | SEF | STA | TVM |
|---|---|---|---|---|---|---|---|
| 1.55 | 1.28 | 1.44 | 0 | 0 | 1.5 | 1.72 | 1.53 |

### *E. Calculate Service Capability in Control Domains*

Service capability is based on how compliant the service provision is with the CCM control domains as well as the assurance weights of the control domains. First, the compliance score of a service with regard to a control domain is computed by

$$cp_n = \frac{\sum_{i=1}^{q} y_i}{q} \tag{3}$$

where $cp_n$ = degree of compliance of the service with control domain *n*

$y_i$ = response of the service to CAIQ question *i* in control domain *n*; 1 if yes and 0 if no

*q* = number of CAIQ questions in control domain *n*.

Then the capability of a service with regard to a control domain *n*, or $p_n$, is a product of $cp_n$ as in (3) and $as_n$ as in (2):

$$p_n = cp_n \times as_n \tag{4}$$

Using (4), we obtain a service capability matrix *P*:

$$P = \left[ p_1 \; p_2 \; ... \; p_{16} \right]$$

which represents capability scores of the service in all 16 CCM control domains.

For example, suppose the responses from the provider of a cloud service to the CAIQ questions are listed in Table 10. Using Table 9 and (4), the service capability matrix *P* is shown in Table 11.

### *F. Calculate Service Trustworthiness*

We obtain a service trustworthiness matrix *T* as a product of *P* and *D*:

$$T = P \times D = \left[ C \; I \; A \; R \; S \; M \right] \tag{5}$$

**TABLE 10.** Example of Response to CAIQ and CCM Compliance Scores

| Control Domain | AIS | AAC | BCR | CCC | DSI | DSC | … |
|---|---|---|---|---|---|---|---|
| **No. of CAIQ Questions** | 9 | 13 | 23 | 10 | 17 | 11 | … |
| **No. of Yes Answers** | 7 | 10 | 15 | 5 | 12 | 11 | … |
| **Compliance Score** | 0.78 | 0.77 | 0.66 | 0.5 | 0.71 | 1 | … |

**TABLE 11.** Example of Response to CAIQ and CCM Compliance Scores

| Control Domain | AIS | AAC | BCR | CCC | DSI | DSC | … |
|---|---|---|---|---|---|---|---|
| **Service Capability Score** | 1.09 | 1.43 | 0.86 | 0.93 | 0.90 | 1.3 | … |

where *C, I, A, R, S* and *M* are the scores of confidentiality, integrity, availability, reliability, safety, and maintainability.

Using the service trustworthiness matrix *T*, we can calculate the overall trustworthiness score *TR* as

$$TR = average(C, I, A, R, S, M) \qquad (6)$$

For example, given the service trustworthiness matrix *T* in Table 12, the overall trustworthiness score *TR* is 9.78.

## IV. Experiment and Discussion

In an experiment, a cloud customer selected five cloud services for an assessment. The responses of these services to the CAIQ questions were retrieved from the STAR registry. The assessment result is shown in Figure 2. Note that the reliability, safety, and maintainability scores are low if compared with confidentiality, integrity, and availability scores. This is not surprising though since the control domain-subattribute association matrix *D* in Table 7 already suggests that the CCM controls are associated more with security than dependability. Therefore, it is not necessarily useful to compare between the subattribute scores of the same service, e.g. it should not be concluded that all five providers have high confidentiality and low reliability. Rather, the score for a subattribute may be used to compare across different services, e.g. it would be more useful to conclude that the provider 4 comes last for all subattributes.

## V. Conclusion

In this paper, a method is proposed to assess the degree of trustworthiness of cloud services based on service compliance with the CCM. The method provides a refined view of how the degree of CCM compliance of a service reflects the security, dependability, and trustworthiness quality. Even though a question might be raised about the validity of the service self-assessment information in the STAR, the CSA is a well-received organization and the information can be checked for alignment with third-party certificates that can also published with the STAR. We hence still consider it a useful basis for the assessment.

**TABLE 12.** Example of Service Trustworthiness Matrix

| Subattribute | Confidentiality | Integrity | Availability | Reliability | Safety | Maintainability |
|---|---|---|---|---|---|---|
| Score | 16.15 | 16.62 | 16.78 | 2.78 | 2.49 | 3.86 |

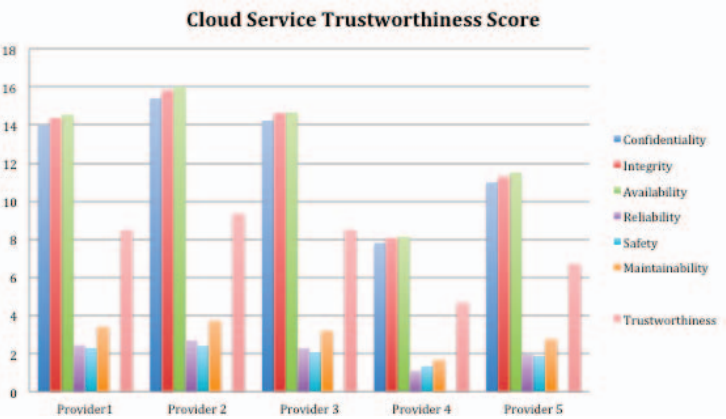

**Figure 2.** Assessment result of experiment

To make the method more automated, the development of a supporting tool is in progress. We will also extend the experiment to more number of cloud customers in real business setting and will statistically evaluate correlation of the scores with other cloud quality measures.

## References

[1] NIST, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, Sep 2011.

[2] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Apr 2013

[3] CSA, *Consensus Assessments Initiative Questionnaire*, Available: https://cloudsecurityalliance.org/research/cai/

[4] CSA, *Cloud Controls Matrix*, Available: https://cloudsecurityalliance.org/research/ccm/

[5] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable and Secure Computing*, vol. 1, no, 1, pp. 11-33, Jan-Mar 2004.

[6] AICPA, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, 2015.

[7] CSA, *Security, Trust & Assurance Registry (STAR)*, Available: https://cloudsecurityalliance.org/star/

[8] CSMIC, *Service Measurement Index (SMI),* Available: http://csmic.org

[9] N. Bhensook and T. Senivongse, "An assessment of security requirements compliance of cloud providers," in *Proc. 4th IEEE Int. Conf. Cloud Computing Technology and Science (CloudCom)*, 2012, pp. 520-525.

[10] S. M. Habib, V. Varadharajan, and M. Muhlhauser, "A trust-aware framework for evaluating security controls of service providers in cloud marketplaces," in *Proc. 12th IEEE Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2013, pp. 459-468.

[11] P. Bedi, H. Kaur, and B. Gupta, "Trustworthy service provider selection in cloud computing environment," in *Proc. Int. Conf. Communication Systems and Network Technologies (CSNT)*, 2012, pp. 714-719.

[12] L. Wang and Z. Wu, "A Novel Trustworthiness Measurement Model for Cloud Service," in *Proc. 7th IEEE/ACM Int. Conf. Utility and Cloud Computing*, 2014, pp.928-933.

**Jirayu Kanpariyasoontorn** was born in Bangkok, Thailand, in 1990. He received the B.Sc. in Computer for Communication from Srinakharinwirot University, Bangkok , Thailand in 2012, and join Computer Science Program, Department of Computer Engineering, Chulalongkorn University, Bangkok, Thailand, in 2013 as a student. His interest research in evaluate, assessment of the cloud security, dependability and trustworthiness on cloud computing

He submitted research "Cloud Service Trustworthiness Assessment Based on Cloud Control Matrix" in international conference on Advance Communication Technology (ICACT2017) on Feb 19 – 22 , 2017.

**Twittie Senivongse** is an associate professor at the Department of Computer Engineering, Faculty of Engineering, Chulalongkorn

University, Thailand. She received B.Sc. in Statistics from Chulalongkorn University in 1989, M.Sc. in Computing Science from Imperial College, UK in 1992, and Ph.D. in Computer Science from University of Kent, UK in 1997. Her research interest includes service computing, software quality measurement, and application of semantic technology.