Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 3078272, 18 pages
https://doi.org/10.1155/2018/3078272

Research Article

SCCAF: A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context

Xiang Li,[1] Xin Jin,[1] Qixu Wang,[2] Mingsheng Cao,[3] and Xingshu Chen[2]

[1]*College of Computer Science/Cybersecurity Research Institute, Sichuan University, Chengdu, Sichuan Province 610065, China*
[2]*College of Cybersecurity/Cybersecurity Research Institute, Sichuan University, Chengdu, Sichuan Province 610065, China*
[3]*School of Information and Software Engineering, University of Electronic Science and Technology of China, ChengDu, China*

Correspondence should be addressed to Xingshu Chen; chenxsh@scu.edu.cn

Received 22 June 2018; Accepted 27 September 2018; Published 23 October 2018

Guest Editor: Zhiqing Wei

The Internet of Things (IoT) offers a wide variety of benefits to our daily lives in many ways, ranging from smart wearable devices to industrial systems. However, it also brings well-known security and compliance concerns, especially in the physical layer. In addition, due to numerous IoT architectures which have been developed and deployed based on the cloud, the security and compliance of IoT depend on the cloud thoroughly. In this paper, a secure and compliant continuous assessment framework (SCCAF) is proposed to evaluate the security and compliance levels of cloud services in life-cycle. The SCCAF facilitates cloud service to customers to select an optimal cloud service provider (CSP) which satisfies their desired security requirements. Moreover, it also enables cloud service customers to evaluate the compliance of the selected CSP in the process of using cloud services. To evaluate the performance and availability of SCCAF, we carry out a series of experiments with case study and real-world scenario datasets. Experimental results show that SCCAF can assess the security and compliance of CSPs efficiently and effectively.

1. Introduction

The rise of IoT has led to the constant universal connection between people and things (e.g., sensors or mobile devices), and it plays a remarkable role in all aspects of our daily lives [1, 2]. Furthermore, combined with preeminent technologies such as cloud, the cloud-based IoT architecture is becoming a trend in the IoT market. However, as with many new technologies, there are several challenges when it comes to achieving success in cloud-based IoT context adoption [3–5]. Two of the biggest concerns for cloud-based IoT context are security (especially, the physical layer security) and compliance (e.g., lack of customer control mechanism, security assurance and service level agreements (SLAs) guarantee, and dynamic change in the IoT devices) [6, 7]. Nevertheless, there is little literature on the IoT security and compliance assessment [8]. The traditional existing literatures with respect to security of IoT focus on dealing with wireless networks [2, 9, 10]. Therefore, the premise of securing the cloud-based IoT context is to evaluate the security and compliance of cloud service.

Due to massive number of CSPs offering similar kinds of services in the cloud market, it becomes a tricky challenge to select an optimal cloud service. Moreover, from the perspective of cloud service customers (CSCs), it is becoming more and more important to identify which is the real optimal cloud service provider (CSP). A real optimal CSP is supposed to satisfy the security requirements of CSCs in the process of deploying cloud service and the compliance requirements of SLAs continuously while the cloud service is operating. Before CSCs are planning to use cloud services, the major challenge is to select a security CSP among various CSPs based on their security requirements. After that, the main challenge for CSCs is to ensure the conformance between the actual quality of service (QoS) of cloud services and the SLAs claimed by the selected CSP. Intuitively, security and compliance issues are equally important to CSCs throughout the entire process of using the cloud service.

However, the actual situation is that CSCs frequently concentrate on the security or compliance in different periods of using cloud service. Security is the primary concern for CSCs while selecting CSP and the main obstacle of promoting

cloud computing. Nonetheless, research results usually target selecting the security CSP and overlook the compliance issue [11–16]. On the other hand, compliance is the critical concern for CSCs while using cloud services. But the significance of security and the feasibility of assessment tend to be ignored [17–19]. For instance, it is almost impossible for CSCs to evaluate trustworthiness of cloud services by objective and direct means (e.g., QoS monitoring). It is due to the fact that before signing a service contract with CSC, CSP will neither provide the technical details of cloud services nor open interface to CSCs to monitor service QoS for the purpose of confidentiality, security, and competition.

As aforementioned, few literatures take the integration of security and compliance assessment into consideration for evaluating the cloud service. To the best of our knowledge, there is no continuous assessment framework existing in literature which concatenates security and compliance of cloud service from comprehensive perspective. Moreover, the compliance issues of cloud service are urgent and worth studying, especially during the use of cloud services.

In this paper, we propose a novel secure and compliant continuous assessment framework (SCCAF), which evaluates the security level and the compliance level of cloud service. Additionally, a new concept of cloud service life-cycle (CSL) is proposed and elaborated. The CSL enables CSCs to well understand the objects which need to be considered for adopting cloud services. Accordingly, SCCAF can offer more flexibility in the hands of CSCs to evaluate cloud on the basis of their security and compliance requirements.

In a nutshell, the main contributions in this paper are summarized as follows.

(i) We propose a new concept of cloud service life-cycle which enables CSCs to well understand the objectives that need to be considered at each phase of the adoption of cloud services.

(ii) The SCCAF, a novel secure and compliant continuous assessment framework based on CSL, is proposed. It combines assessment methods of security and compliance as mutual complementation. Hence, the SCCAF enables CSCs to continuously evaluate the cloud service provided by CSPs during the full CSL.

(iii) To illustrate the efficiency and effectiveness, we conduct comprehensive experiments to validate our proposed SCCAF from two dimensions, respectively. The results show that SCCAF can achieve better performance and availability.

The rest of the paper is organized as follows. Section 2 surveys related work. Section 3 introduces the proposed concept of CSL and Section 4 elaborates the SCCAF. Section 5 presents the experimental results and their analyses for validating our proposed assessment method. Section 6 concludes this paper with directions for future work.

2. Related Work

A variety of recent research works target selecting an optimal CSP by evaluating cloud services from the dimensions of security and trust. One example is Luna et al. [20] who presented a security metrics framework for CSPs security assessment. In [21], a methodology to quantitative benchmark CSPs security SLA with respect to the security requirements of CSC is presented based on the reference evaluation methodology [22]. Paper [14] presents a methodology for quantizing and evaluating security threats, which weighs each security threat to consider which security controls are required to meet the users' needs in a security SLA, and in [23] a new technique for conducting quantitative and qualitative analysis of the security level provided by CSPs is proposed. Both works are based on the analytic hierarchy process (AHP) [24]. In [11], two evaluation techniques are proposed to conduct the quantitative assessment and analysis of the security SLA based security level provided by CSPs with respect to a set of CSCs security requirements. In [12], a novel cloud security assessment technique is presented which is a more simple and effective approach that can be deployed for the needed online real-time assessment and offers both accuracy and high computational efficiency. Refernce [13] presents a methodology for evaluation and selection of cloud services based on a multicriteria analysis [25] process using a set of evaluation criteria and quantitative metrics. However, the security assessment methods mentioned above are all about selecting CSP before CSCs use of cloud services, and none of them is involved in the case of, after selecting CSP, how to determine the compliance of the SLA claimed by the CSP in the runtime of cloud service.

Besides the security assessment, the assessment techniques to select CSP have also been focused on the evaluation of trust, which has captured researchers' attention in recent years. The assessment methods based on the trust are mainly divided into two aspects, including subjective assessment and objective assessment. From the subjective perspective, [26] presents a distributed framework for determining trustworthiness of federated cloud entities, which uses a reputation manager to capture and store the behavior of cloud entities. In [27], a trust management model is proposed which comprises SLA agent, cloud service directory, cloud provider, and cloud consumer to select most reliable cloud providers by managing trust relationships based on three types of information (local experience of consumers with providers, opinion of others, and reports provided by SLA agent). Paper [28] proposed a model of reputation-enhanced QoS-based web services discovery that combines an augmented UDDI registry to publish the QoS information and a reputation manager to assign reputation scores to the services based on customer feedback ratings on their performance. In [29], a trust management approach is presented, namely, ServiceTrust, and it takes rater's credibility into consideration by combining a user's needs and other personal ratings to estimate a CSP's trust value for the support of reputation-oriented service selection. However, the subjective assessment methods which are difficult to quantify usually makes the evaluation results less accurate and also presents difficulty in its practical adoption.

Many objective assessment methods of service selection have also been proposed, such as those based on monitored QoS data [30–35]. These works mainly focus on determining

the most satisfactory services according to users' requirements and preferences relative to QoS. However, not all of these works apply to cloud environment. Moreover, QoS data of services is hard to be acquired [36] and might not be reliable [34]. To select a satisfactory CSP from objective perspective, [37] proposed a ranking technique that utilizes performance data to measure various QoS attributes and evaluates the relative ranking of cloud providers. In [38], a QoS ranking prediction framework is presented for cloud services by taking advantage of the past service usage experiences of other consumers, which requires no additional invocations of cloud services. Authors of [39, 40] propose an automated framework called CloudGenius and a comparative framework named CloudCmp, respectively. The purpose of the former is automating the decision-making process based on a model and factors specifically for web server migration to the cloud. The purpose of the latter is measuring the elastic computing, persistent storage, and networking services offered by a cloud along metrics that directly reflect their impact on the performance of customer applications. Both of them provide mechanisms to evaluate performance indicators of CSPs in order to help customers pick a cloud that fits their needs.

In addition, there are a few works combining subjective perception and objective measurement to evaluate trustworthiness of cloud services. Reference [19] designs a novel framework named CSTrust for conducting cloud service trustworthiness evaluation by combining QoS prediction and customer satisfaction estimation. Reference [18] proposes a trustworthy selection framework for cloud service selection named TRUSS, which contains an integrated trust evaluation method via combining objective trust assessment and subjective trust assessment. Paper [41] proposes a novel trust evaluation method named UsageQoS for accurately measuring quality of cloud services via leveraging service QoS parameters and user ratings. Although objective assessment methods can yield more accurate results and are easier to implement through existing technical means, they ignore the fact that security is one of the major barriers for adoption of cloud computing and the paramount consideration for CSCs. Moreover, as stated earlier, CSCs are unable to evaluate trustworthiness of cloud services by objective and direct technical means before selecting a CSP to provide cloud services.

As can be seen from the related work discussed above that many existing literatures evaluate security or trustworthiness of CSPs for merely selecting an optimal CSP, but they overlook an important issue; that is, CSCs are concerned about the compliance of SLAs claimed by CSP during the use of cloud services. However, there is no comprehensive and continuous assessment framework that combines security and compliance as a complete and complementary attribute to facilitate CSCs to continuously evaluate CSPs during the full cloud service life-cycle. This paper presents a concept of cloud service life-cycle (CSL) from CSCs' perspective that enables CSCs to clearly understand the items that need to be considered at each phase of the adoption of cloud services. Then a secure and compliant continuous assessment framework is proposed based on CSL, which concatenates security and compliance assessment methods. Such a framework not only enables CSCs to select a security CSP from numerous candidate CSPs out of security perspective, but also allows CSCs to evaluate the compliance of SLAs claimed by the selected CSP in the cloud service runtime. Compliance assessment result can help CSCs make further decisions (e.g., continue to use, change CSP, seek remedies, and claims and even terminate cloud service).

3. Cloud Service Life-Cycle

In this paper, cloud service life-cycle (CSL) is articulated as an assumption or an expectation that a CSC will experience a continuous and integral process about adopting cloud service. This assumption or expectation is based upon a series of more specific phases, which form the components of CSL. As shown in Figure 1, the CSL, an extension from our previous work [43], comprises six phases: initial preparation, alternatives choice, solution deployment, continuous monitoring, decision making, and termination of service. The detailed phases of CLS are described as bellow.

(1) Initial Preparation. Initial preparation is the first phase for all the potential CSCs that are eager to leverage the benefits of cloud services. Customers should analyze the benefits of using cloud computing services based on their data and business types and determine whether the cloud computing services are suitable for them. At the same time, they should determine cloud capabilities types and cloud service categories in accordance with their data and business characteristics. As mentioned above, security is the top primary concern for customers to adopt cloud services. Therefore, CSC should conduct security demand analysis according to the key characteristics and potential security threats of cloud computing. Additionally, the main objective of this phase is that CSC defines the security metrics in accordance with the security analysis results for the preparation of selecting the optimal CSP in next phase.

(2) Alternative Selection. In the alternative selection phase, CSC should select an appropriate CSP in accordance with their security requirements and the security capability of cloud services. Due to the competition among various CSPs, there is large number of CSPs offering similar kinds of cloud services and security provisions. As a result, it has become a challenging task for CSC to identify which service is the best appropriate for them. Hence, to ensure data and business security, CSC should take advantage of the security metrics defined in the previous phase. At the same time, CSC can employ an effective security assessment method to evaluate the security level of CSPs. Customers can select the optimal CSP to provide cloud service based on the security assessment result. The security assessment method involved in this phase is the focus of this paper, which will be elaborated later.

(3) Solution Deployment. In order to ensure robust and efficient use of cloud services, the primary purpose for CSC is to negotiate with the selected optimal CSP to set up the cloud SLAs, which stipulates the QoS of cloud services offered

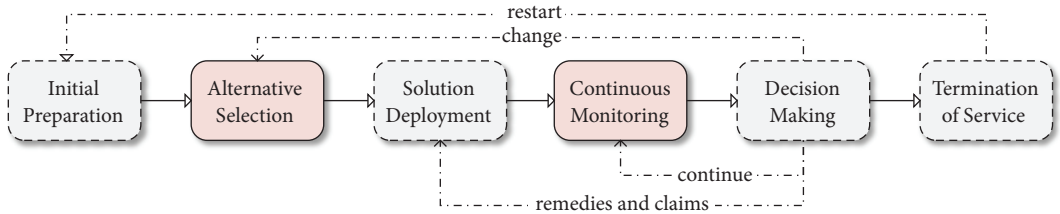


Figure 1: Cloud service life-cycle.

by the CSP. In the meanwhile, CSC should also negotiate with the CSP on the terms including the remedies and claims and change service provider and termination of service in case that the CSP violates the agreed QoS in the operational process of cloud services. Therefore, CSC should define compliance metrics based on the analysis of actual business requirements and the agreed SLAs, which will be used for compliance evaluation of cloud services in the next phase. Finally, CSC should confirm the deployment plan developed by the selected CSP and entrust the CSP to deploy cloud service.

(4) Continuous Monitoring. The primary purpose of CSC in the phase of continuous monitoring is to ensure that actual QoS in the runtime of the cloud service conforms with the QoS agreed in SLAs. In light of planned and unplanned changes that occur in the cloud environment over time, the state of cloud services is not always maintained. Moreover, the CSP may be likely to achieve the benefit maximization at the expense of service quality; that is, CSP not always fully comply with the QoS in the SLAs to offer cloud services, especially that the CSC are not aware of SLAs while the CSP may reduce cloud computing resources (e.g., computing, storage, and network). Therefore, CSC should continuously monitor and record cloud service quality in the process of using cloud services and evaluate the conformance of cloud services through an effective compliance assessment method. The compliance assessment method involved in this phase is the focus of this paper, which will be elaborated later.

(5) Decision Making. In this phase, compliance assessment results in the previous phase can help CSC make decisions. CSC can determine which measures will be taken according to their tolerance to the compliance level of cloud services, which have an impact on their business performance (e.g., reliability and availability). In other words, the CSCs can decide to take corresponding measures according to the violation extent of SLAs. For example, if cloud services are compliant, namely, the monitoring QoS of cloud services is complying with the agreed QoS of SLAs, CSCs can decide to continue to use and evaluate the cloud services. If the cloud services are not compliant, CSC can decide to change CSP or seek remedies and claims to the CSP according to the violation extent, as shown in Figure 1. In the worst case, CSC can choose to terminate the cloud service and exit. The establishment of compliance rules and corresponding measures will be elaborated later.

(6) Termination of Service. The termination of cloud service deals with the exit process, where the use of a cloud service is terminated. Once CSC choose to exit the cloud service, they need to focus on addressing specific termination issues including the exit process and the handling of all classes of data related to the cloud service. For instance, the CSC is able to retrieve their cloud service data and application artifacts. In the meantime, the CSP needs to delete all the CSCs' data. Moreover, the CSC expects that the CSP will not retain any materials belonging to CSC after an agreed period. After exiting cloud service, CSCs can repeat the "Initial Preparation" phase when considering using cloud service again. At the end of the exit process, the CSP should provide the CSC with notification that the process is complete.

4. The Proposed Framework

In this section, the SCCAF, a CSL-based continuous assessment framework, is proposed. This framework can be divided into three main processes, encompassing (1) security assessment, (2) compliance assessment, and (3) taking measures. As shown in Figure 2, the SCCAF includes the following steps.

(1) *Security Assessment*. The CSC evaluates the security level of alternatives (CSPs) according to the conformance between the claimed security provisions provided by CSPs and the security metrics (e.g., facility security, risk management, and information security) defined by the CSC. Then, the CSC selects the optimal CSP to deploy cloud service based on the security assessment result as shown in Figure 3. The security assessment is implemented in initial preparation and alternative selection phases of CSL.

(2) *Compliance Assessment*. After the security assessment is completed, the CSC can select the optimal (high security level) CSP to provide cloud service. During the use of cloud service, the CSC evaluates the compliance level of the cloud services based on the conformance between the claimed cloud SLAs and the actual QoS, as shown in Figure 4. The premise for compliance assessment is that CSC defines the compliance metrics in the solution deployment phase of CSL, namely, specific requirements of SLAs. The compliance assessment is implemented in continuous monitoring phase of CSL.

(3) *Taking Measures*. After the compliance assessment is completed, the CSC can establish compliance

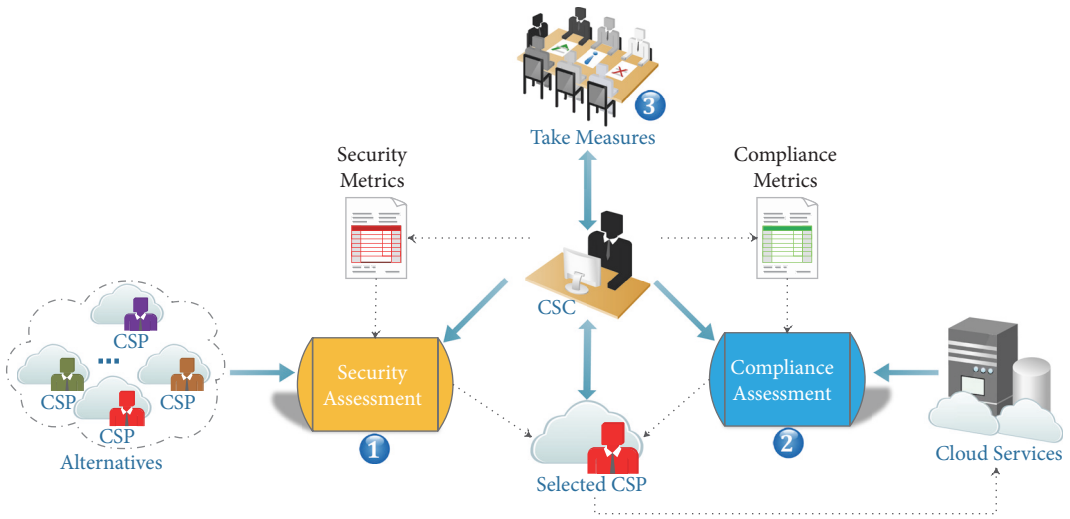


Figure 2: The system architecture of SCCAF.

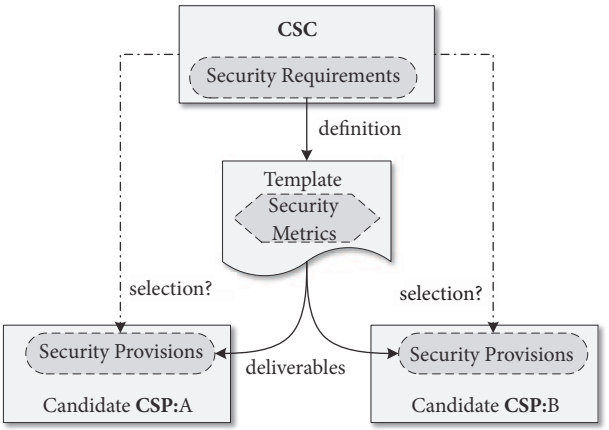


Figure 3: The definition and employment of security metrics.

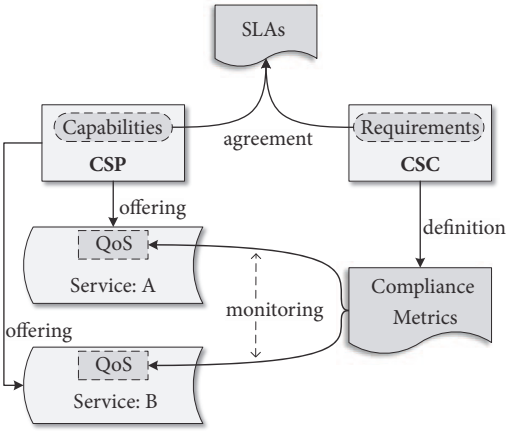


Figure 4: The definition and employment of compliance metrics.

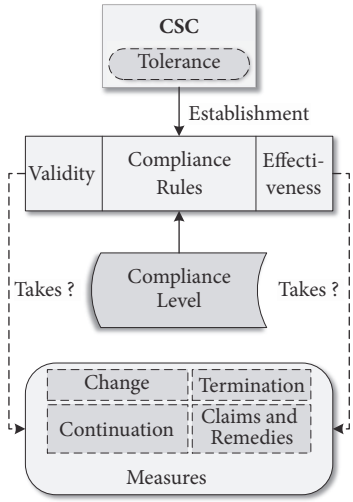


Figure 5: Taking measures according to the compliance level.

tolerance rules based on the impact of compliance level on their actual business. Then, CSC can take corresponding measures (e.g., change CSP, continue to use, and seek remedies and claims) according to the compliance level of the cloud services, as shown in Figure 5. In the worst case, the CSC may consider terminating the cloud service. The process of taking measures is implemented in the decision-making phase of CSL.

4.1. Security Assessment. In security assessment process, the CSC defines security metrics, which include CSC's security requirements related to its data and business. The CSPs determine and describe the conformance between security metrics and their security provisions. According to this conformance, the proposed security assessment approach evaluates the security level of CSPs and ranks them based on the evaluation result. The quantitative security level of CSPs is the primary objective of the security assessment process. For convenience, the key notations used in security assessment are given in Table 1. Specifically, it includes four steps as follows.

(1) Security Metrics Definition. CSC defines a set of security metrics and provides it to CSPs. For instance, CSC can select security controls from the cloud controls matrix (CCM) [44] or consensus assessments initiative questionnaire (CAIQ) [42] according to its security requirements. Then, the CSPs measure their security provisions in accordance with the security metrics and submit measurement results to CSC in the form of deliverables. Deliverables include specific security metrics representing the security provisions of CSPs. The first round using security metrics is to collect information with respect to the security provisions (deliverables) of the CSPs in a uniform format. The deliverables contain n security provisions of m CSPs. The definition of security metrics is implemented in initial preparation phase of CSL.

Table 1: Notations in security assessment.

Symbol	Description
m	the number of CSPs
n	number of security metrics
W_j	weight vector of the pairwise comparison matrix constructed by the *jth* security metric
w	weights assigned to security metrics
K	deliverables set of CSPs
Q_{ij}	quantified security metric in K
$R_{m\times n}$	weighted normalized decision matrix
A^+	ideal solutions of the positive security metric
A^-	ideal solutions of the negative security metric
D_i^+	positive separation measure of the *ith* CSP
D_i^-	positive separation measure of the *ith* CSP
C_i	relative closeness of the *ith* CSP

(2) Security Metrics Quantification. The second round is to quantify the security metrics (deliverables) of each CSP for convenient comparison of their security capabilities. The quantification approach depends on different comparison types of different security metrics. In this step, we can employ the quantification approach proposed by [11, 23]. This approach quantifies security metrics into two categories: Boolean (e.g., a YES/NO measurement result representing the conformable or unconformable to the security metric) and numeric (e.g., a cryptographic key length measurement result representing the extent of conformance to the security metric). The quantitative deliverables are used as input

dataset $Q_{m\times n}$ of security assessment process. The quantification of security metrics is also implemented in initial preparation phase of CSL.

(3) Weights Assignment. After quantifying security metrics, CSC can determine the weights of security metrics by employing the AHP method [24]. In this step, CSC assigns scale of relative importance from 1 to 9 (e.g., such that 9 represents extremely more important and 1 equal importance) for each security metric. These security metrics with specific numerical value can be used to construct a pairwise comparison matrix according to standard AHP method. At the same time, the consistency of this matrix needs to be validated. Then, the weight vector $\boldsymbol{W}$ can be obtained by calculating the eigenvector corresponding to the maximum eigenvalue of the pairwise comparison matrix [45]. The weights of assigning security metrics denoted as $\boldsymbol{w}$ can be obtained by (1), which holds that $\sum \boldsymbol{w} = 1$.

$$\boldsymbol{w} = \left(w_j\right)_{n\times 1} = \frac{W_j}{\sum_{j=1}^{n} W_j} \tag{1}$$

(4) Security Level Evaluation. For the given quantitative security metrics $Q_{m\times n}$ and their weights $\boldsymbol{w}$, CSC can employ the TOPSIS method [46] to evaluate the security level of each CSP and compare their security level in the same context. In this step, a normalized weighted decision matrix needs to be constructed first by (2).

$$R_{m\times n} = \left(\frac{Q_{ij}}{\sqrt{\sum_{i=1}^{m} Q_{ij}^2}} \right)_{m\times n} \times \boldsymbol{w} \tag{2}$$

Then, the ideal solutions A of each security metric can be determined by (3) and (4), which includes positive A^+ and negative A^-.

$$A^+ = \left\{ min\left(r_{ij}\right) \middle| j \in J^- \ or \ max\left(r_{ij}\right) \middle| \ j \in J^+ \right\} \tag{3}$$

$$A^- = \left\{ max\left(r_{ij}\right) \middle| j \in J^- \ or \ min\left(r_{ij}\right) \middle| \ j \in J^+ \right\} \tag{4}$$

where $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, $r_i j \in R$, J^+ represents the security metrics having a positive impact and J^- represents the security metrics having a negative impact.

After that, separation measures D can be calculated by (5) and (6), which represent the geometric distance from alternatives (CSPs) to ideal solutions A. It includes positive D^+ and negative D^-:

$$D_i^+ = \sqrt{\sum_{j=1}^{n} \left(r_{ij} - r_j^+\right)^2} \tag{5}$$

$$D_i^- = \sqrt{\sum_{j=1}^{n} \left(r_{ij} - r_j^-\right)^2} \tag{6}$$

where $i = 1, 2, \ldots, m$, and D_i^+ and D_i^- denote the separation measure from each alternative (CSP) to positive and negative ideal solutions, respectively.

Input: set of deliverables K of alternatives (CSPs), size of the set $m \times n$
1: **Preprocessing:** Initialization and quantifying the deliverables (security metrics) K as Q according to the category of security metrics.
2: **Weight Assignment:** Applying AHP approach to determine the weight vector $\boldsymbol{w}$ for security metrics.
3: **Security level evaluation:** Construct the weighted normalized decision matrix R with the quantitative deliverables Q by TOPSIS method and the obtained weight vector $\boldsymbol{w}$. Calculate the relative closeness (C) for each alternative.

Algorithm 1: Security Assessment.

Next, the relative closeness C representing the degree of conformity between the alternatives (CSP) and the ideal solution can be obtained by (7):

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-} \tag{7}$$

where $i = 1, 2, \ldots, m$ and $0 \le C_i \le 1$. Then, CSC can rank CSPs according to their relative closeness C and select the optimal one with C closest to 1.

To sum up, the security evaluation process is implemented in alternative selection phase of CSL. Algorithm 1 illustrates the security assessment process in the SCCAF. Algorithm 2 demonstrates the procedure of security level evaluation.

After selecting the optimal CSP, the CSC negotiates with the selected optimal CSP on the details of cloud SLAs, namely, specific QoS stipulations. CSC can define compliance metrics in accordance with the agreed SLAs. The compliance metrics should contain the monitorable and measurable QoS attributes belonging to a specific service and their specific compliance values, namely, details of SLAs claimed by the optimal CSP. Such compliance metric can be exploited to evaluate the compliance level of a cloud service during the period of using cloud services, as shown in Figure 4. Actually, since there has been much literature on the establishment of SLAs, CSC can employ existing methods to determine cloud SLAs and define compliance metrics. For instance, the methods proposed by ISO/IEC [47, 48] can be employed to formulate SLAs. The methods proposed by National Institute of Standards and Technology (NIST) [49] and ISO/IEC [50] can be employed to define the compliance metrics. Therefore, the solution deployment phase of CSL is not the focus of this paper.

According to the compliance metrics, the CSC can evaluate the compliance level of the cloud services by employing the compliance assessment method, which we will elaborate its details as follows.

4.2. Compliance Assessment. The compliance assessment process is performed after the security assessment process yields an optimal CSP who will provide cloud service to

Input: set of deliverables K, the number of alternatives (CSPs) m, the number of security metrics n
1: **procedure** SECURITY LEVEL EVALUATION(k, m, n)
2: Create arrays $C_{1\times m}$, $Q_{m\times n} \longleftarrow \emptyset$;
3: Create vector $\boldsymbol{w}$;
4: $index \longleftarrow 0$;
5: The quantized deliverables K is assigned to Q;
6: $\boldsymbol{w} \longleftarrow$ ASSIGNWEIGHTS4METRICS (K, n);
7: $C \longleftarrow$ OBTAIN THE OPTIMAL ALTERNATIVE ($Q, m, n, \boldsymbol{w}$);
8: $index \longleftarrow$ the index of $Max(C)$;
9: **return** *index*;
10: **end procedure**

ALGORITHM 2: Security Level Evaluation.

TABLE 2: Notations in compliance assessment.

Symbol	Description
$T = \{t_1, t_2, \cdots, t_j\}$	a set of compliance evaluation period
$A = \{a_1, a_2, \cdots, a_i\}$	a set of QoS attributes belonged to a service
$C = \{c_1, c_2, \cdots, c_i\}$	a set of compliance metrics values of A
D_{ij}	a set of monitoring data of a_i within t_j
M_{ij}	the mean of D_{ij}
S_{ij}	the variance of D_{ij}
v_{ij}	single conformance of a_{ij}
P_{ij}	the ratio between M_{ij} and the sum including the means of each t_j
H_{ij}	the entropy of a_{ij}
w_{ij}	weight assigned to v_{ij}
f_i	compliance level of a_i
p	monitoring frequency within t_j

the CSC. In the compliance assessment process, CSC continuously evaluates the compliance level of cloud services according to the compliance metrics. Compliance assessment is performed in terms of periods. The quantitative compliance level of cloud services is the primary objective of the compliance assessment process, which can be referred by CSC to make decisions. For convenience, the key notations used in security assessment are given in Table 2.

Specifically, it includes five steps as follows.

(1) Data Collection and Preprocessing. The CSC determines a set of evaluation period T and a monitoring frequency p within each evaluation period t ($t \in T$). For a given evaluation period T, CSC continuously monitor and record the QoS attributes A of a specific service. Then, a monitoring dataset D with respect to A can be obtained. The first round is to collect and preprocess the monitoring dataset of QoS attributes. For convenience, we take a QoS attribute a_i ($a_i \in A$) as an example to describe the compliance assessment process in detail. For a given QoS attribute a_i, its monitoring dataset D_i ($D_i \subset D$) can be obtained from the dataset D. Moreover, for a given evaluation period t_j, the dataset D_i can be divided into smaller datasets D_{ij} ($D_{ij} \subset D_i$) based on t_j. The datasets D_{ij} are used as input data of compliance assessment process to calculate the single conformance v_{ij} of a_i in each t_j. The compliance level of a_i can be obtained by aggregating the weighted v_{ij} within T.

(2) Compliance Interval Construction. The second round is to construct the compliance interval of a_i in accordance with its monitoring dataset D_{ij}. First, we can calculate the mean M_{ij} and variance S_{ij} of D_{ij} by (8) and (9).

$$M_{ij} = \frac{\sum_{k=1}^{p} D_{ij}^k}{p} \tag{8}$$

$$S_{ij} = \frac{\sum_{k=1}^{p} \left| D_{ij}^k - M_{ij} \right|}{p-1} \tag{9}$$

In fact, the actual monitoring QoS of an attribute fluctuates around the compliance metrics value C of SLAs in the runtime of cloud services (in addition to outage, equipment failure, etc.)[36]. Moreover, its fluctuation range of monitoring data cannot be determined accurately [34]. In addition there are only limited monitoring data for a QoS attribute, namely, a small sample. Therefore, we assume that the variation of monitoring data conform to t-distribution [51]. Then, the compliance interval can be constructed by (10) and (11):

$$L = M_{ij} - \frac{\sqrt{S}}{\sqrt{p}} t_{\alpha/2}(p-1) \tag{10}$$

$$U = M_{ij} + \frac{\sqrt{S}}{\sqrt{p}} t_{\alpha/2}(p-1) \tag{11}$$

where L and U represents the lower and upper bounds of the compliance interval, respectively. α is the confidence level assigned by the CSC. $t_{\alpha/2}$ can be obtained by look-up table [51].

(3) Single Conformance. The single conformance is the compliance value of a QoS attribute a_i in an evaluation period t_j. The third round is to obtain single conformance v_{ij} of a_i according to its compliance interval L, U and compliance value c_i. Since different attributes may have different ranges and units, we normalize QoS values into a unified range [0, 1]. Then, the single conformance v_{ij} can be calculated by (12) and (13). The single conformance can be divided into two different types: Positive Factor v_{ij}^{+} representing that higher is better (e.g., throughput) and Negative Factor v_{ij}^{-} representing that lower is better (e.g., response time).

$$v_{ij}^{+} = \begin{cases} 1 & c_i \leqslant L \\ \dfrac{U - c_i}{U - L} & L < c_i \leqslant U \\ 0 & c_i > U \end{cases} \tag{12}$$

$$v_{ij}^{-} = \begin{cases} 0 & c_i \leqslant L \\ \dfrac{c_i - L}{U - L} & L < c_i < U \\ 1 & c_i \geqslant U \end{cases} \tag{13}$$

(4) Weights Assignment. After obtaining the single conformance of a_i, its weight w_{ij} can be determined by employing the entropy method [52]. Firstly, the entropy of a_i in t_j can be calculated according to its mean M_{ij} and (14) and (15), which is denoted as H_{ij}. P_{ij} represents the ratio between M_{ij} and the sum including the means of each t_j.

$$P_{ij} = \frac{M_{ij}}{\sum_{j=1}^{|T|} M_{ij}} \tag{14}$$

$$H_{ij} = -\frac{1}{\ln |T|} \sum_{j=1}^{|T|} P_{ij} \ln P_{ij} \tag{15}$$

Then, for the weight of assigning to a_i in t_j denoted as w_{ij}, it can be obtained in accordance with (16), which holds that $\sum_{j=1}^{|T|} w_{ij} = 1$.

$$w_{ij} = \frac{1 - H_{ij}}{|T| - \sum_{j=1}^{|T|} H_{ij}} \tag{16}$$

(5) Compliance Level Evaluation. This round is to calculate the compliance level of a_i in accordance with the obtained weight and single conformance. For the compliance level of a_i, each of the weighted single conformance needs to be aggregated in T. According to (17), the compliance level f_i of a_i can be obtained, which holds that $0 \leq f_i \leq 1$. The closer the compliance level is to 1, the more compliant the evaluated attribute is.

$$f_i = \sum_{j=1}^{|T|} v_{ij} w_{ij} \tag{17}$$

Broadly, the compliance assessment process is implemented in continuous monitoring phase of CSL. Algorithm 3 illustrates the compliance assessment process in the SCCAF. Algorithm 4 demonstrates the procedure of compliance level evaluation.

4.3. Take Measures. The process of taking measures is performed after the compliance assessment process yields assessment results regarding the cloud services. In this process, CSC establishes relevant compliance tolerance rules (e.g., assessment validity) on the basis of compliance assessment results. Additionally, these rules need to be associated with the corresponding measures (e.g., change CSP). Then, CSC can determine which measure to be taken based on the conformity between compliance level and the compliance tolerance rules. The primary objective of this process is to help the CSC stop loss in time in the event of cloud SLAs compliance violations. For convenience, the key notations given in the compliance assessment apply to the process of taking measures. The details of compliance tolerance rules and corresponding measures will be described in the following.

(1) Validity. The CSC can establish a validity indicator to determine whether the compliance assessment is valid. For a given evaluation period T, the compliance assessment of cloud service is performed t $(t \in T)$ times, and each of the single conformance v is different. A compliance assessment which subjects to $v \neq 0$ is considered as a valid assessment. Then, we define assessment validity as follows.

Definition 1. Let μ and φ denote the number of valid assessment and invalid assessment within the evaluation period T, respectively. The validity of compliance assessment denoted as o can be calculated by

$$o = \frac{\mu}{\mu + \varphi} \tag{18}$$

The CSC can establish assessment validity threshold based on their actual business requirements. For instance, we assume that the acceptable assessment validity threshold of the CSC is α. Thus, for a given evaluation period T (e.g., a year), the compliance assessment is performed in terms of t $(t \in T)$ (e.g., a day). If the assessment validity o is less than α, the CSC may consider changing CSP. The CSC may select another one from the CSPs ranked by security assessment. If the assessment validity o consecutively fails to meet the condition $o \geq \alpha$ for k times, the CSC may consider terminating the cloud service.

(2) Effectiveness. After determining that the validity meets the requirements, the CSC can set up an effectiveness indicator to determine whether the compliance level of cloud services meets its requirements. The effectiveness of compliance level is that the cloud services QoS can support critical business functions of CSC to an acceptable level within an evaluation period of time. Then, we define effectiveness as follows.

Input: set of evaluation period T, evaluation frequency t ($t \in T$), monitoring frequency p, set of compliance metrics values C, set of QoS attributes A

1: **Data Collection and Preprocessing:** During the evaluation period T, monitor and record the actual data QoS attributes A in accordance with evaluation frequency of t and monitoring frequency p. Obtain the monitoring datasets D and categorize it into D_i ($D_i \in D$) by each QoS attribute a_i ($a_i \in A$). The dataset D_i can be further divided into D_i^j according to t_j.

2: **Compliance Interval Construction:** For the QoS attribute a_i, calculate the mean and variance of its monitoring dataset D_i^j. Then, construct the compliance interval according to the relevant features and approach of t-distribution.

3: **Single Conformance:** The single conformance v_{ij} of a_i can be calculated according to its compliance interval and compliance value c_i ($c_i \in C$).

4: **Weight Assignment:** Applying entropy approach to determine the weight w_i^j for the single conformance v_{ij} of QoS attribute a_i. Calculate its weighted conformance by the obtained weight and single conformance.

5: **Compliance Level Evaluation:** Calculate the compliance level f_i of the QoS attribute a_i by aggregating its weighted conformance within evaluation period T. Repeat these steps above with each other attribute to obtain each compliance level of them.

Algorithm 3: Compliance Assessment.

Input: T, D_i, a_i, p, confidence level α, compliance metric value c_i

1: **procedure** Compliance Level Evaluation(D_i, T, p, α, C_i)
2: Create arrays $v^i_{1\times|T|}, m^i_{1\times|T|} \longleftarrow \emptyset$;
3: Create vector $\boldsymbol{w}^i_{1\times|T|}$;
4: $f_i \longleftarrow 0$;
5: **for** $j = 1$ to $|T|$ **do**
6: $v_{ij}, m_{ij} \longleftarrow$ SingleConformance (D_i, p, α, c_i);
7: **end for**
8: $\boldsymbol{w}_i \longleftarrow$ Compliance Weights Assignment (m_i);
9: **for** $j = 1$ to $|T|$ **do**
10: $f_i \longleftarrow f_i + v_{ij}\boldsymbol{w}_{ij}$;
11: **end for**
12: **return** f_i;
13: **end procedure**

Algorithm 4: Compliance Level Evaluation.

Definition 2. Let f denote the compliance level of a QoS attribute within an evaluation period T. Let n denote the number of QoS attributes. The effectiveness denoted as e can be calculated by

$$e = \frac{\sum_{i=1}^{n} f_i}{n} \tag{19}$$

The CSC can establish effectiveness threshold based on their actual business requirements. For instance, we assume that the acceptable effectiveness threshold of the CSC is β. Similarly, for a given evaluation period T (e.g., a year), the compliance assessment is performed in terms of t ($t \in T$) (e.g., a day). If the effectiveness e is less than β, the CSC may consider seeking claims and remedies from the CSP. If the effectiveness e is greater than or equal to β, the CSC can use and evaluate the cloud service continuously.

In general, CSCs have to establish compliance tolerance rules based on their actual business requirements. In practice,

different CSCs may have different compliance tolerance rules. In this process, we provide a feasible and referential method for CSC to make decision according to the compliance level of cloud service.

5. Simulation Studies

This section presents the experiments to validate performance and availability of the proposed security and compliance assessment methods in the continuous assessment framework, respectively. The experiments are conducted by using MATLAB R2017b and performed on a DELL desktop computer with configuration as follows: Intel Core i5 2.7 GHz CPU,8 GB RAM and Windows 10 operating system.

5.1. Security Assessment Validation. First, we conduct the experiments to compare our security assessment method with the Quantitative Hierarchy Process (QHP) method proposed by [11] in terms of performance and accuracy. The QHP method is is an assessment technique that enables ranking of CSPs with respect to CSCs requirements. Due to the similar concepts and evaluation steps, we utilize the same security metrics as QHP, which are developed by Cloud Security Alliance [44]. For facilitating comparison, we employ the same quantification approach for security metrics as QHP. Additional, for convenience, we denote our security assessment method of SCCAF as SAM.

(1) Performance Analysis. To compare SAM with QHP method based on time complexity, we set the number of CSPs to 150 and the number of security metrics to 300. At the same time, we assume that each step in these comparative methods is an operation and the total number of operations represents the time complexity. We vary the number of CSPs from 1 to 150 with a step of 30 and the number of security metrics from 1 to 300 with a step of 60. We simulate that the time complexity of the two methods increases with the number of CSPs and the number of security metrics.

Figure 6 shows that the time complexity of the two methods increases with the number of CSPs in the case that the number of security metrics is constant. Figure 7 shows that the time complexity (operations) of the two methods increases with the number of security metrics in the case that the number of CSPs is constant. Figure 8 shows that the number of operations in both methods increases with the number of CSPs and security metrics. We can observe from these figures that our method outperforms QHP method in both above cases; that is, SAM has the minimum time complexity. With the increase of the number of CSPs or security metrics, the time complexity of QHP increases significantly. This is due to high complexity of algorithms for calculating the priority vector of comparison matrix constructed by all CSPs as per each security metric. In other words, QHP evaluates the security level of CSPs by comparing each security metric of all CSPs and aggregating the comparison results, while SAM is by taking all security indicators as a whole for comparison. It suggests that our method not only is effective but also outperforms QHP method.

(2) Accuracy of SAM. In order to validate accuracy of the SAM method, we compare evaluation results of SAM with evaluation results of QHP through empirical validation. Table 3 presents a sample dataset associated with security metrics used for this scenario. This dataset is excerpted by [11] from the information available in the CSA STAR repository [42], where the values associated to 16 security metrics for the three selected CSPs are presented. As aforementioned, for conveniently comparing the accuracy of both methods, we employ the same quantification approach for security metrics as QHP, which is described below. The selected security metrics comprised both qualitative (e.g., YES/NO) and quantitative (e.g., security levels from 1 to 4) metrics. The YES/NO metrics thresholds are modelled as Boolean 1/0, whereas metrics associated to security levels as $level_1$, $level_2$, $level_3$, and $level_4$ are modelled as 1, 2, 3, 4. For example, the CO3.3 is defined using qualitative thresholds (None, Annually, Quarterly, and Monthly) which are specified as $level_1$, $level_2$, $level_3$, and $level_4$. Similarly, the RI1.1 is defined using qualitative (Internal, External) values. To facilitate the comparison, we take the 16 security metrics in this table as the CSC's security requirements and consider them as the same relative importance ($weight = 0.5$) as described in *caseI* of [11].

In order to obtain the CSPs' security level, we apply the security assessment method presented in Section 5. Table 4 shows the parameters related to security level of CSPs, which are calculated by the algorithms elaborated in Section 5.1. As shown in Table 4, the shortest separation measure from alternative (CSP) to positive and negative ideal solution is CSP_3 and CSP_2, respectively. It means that for the given positive impact security metrics, CSP_3 is most consistent with them and CSP_2 is the most inconsistent with them. By taking the separation measures, we can obtain the relative closeness C of CSPs; the closer it is to 1, the higher the security level of the CSP is. As can been seen from this table, CSP_3 has the highest security level, followed by CSP_1, and CSP_2 is the lowest.

A side by side comparison is shown in Figure 9. As shown in Figure 9, the resulting ranking of CSPs is consistent for both SAM and QHP: CSP_3 is the provider that best satisfies the CSC's security requirements, followed by CSP_1 and CSP_2 respectively. For CSC specifying the security requirements, this means that both methods result in the same evaluation results. However, compared with the QHP method, the SAM method can better reflect the security level of CSPs. For example, in this scenario, since CSP_3 satisfies all the 16 security metrics, its security level should be the maximum, namely, 1, which is not shown in QHP.

5.2. Compliance Assessment Validation. In this section, we evaluate the availability and efficiency of the proposed compliance assessment method, which exploits a synthesized web service dataset from real world [53]. Additionally, we compare performance and certainty of our method with respect to the TRUSS proposed by [18]. For convenience, we denote our compliance assessment method of SCCAF as CAM.

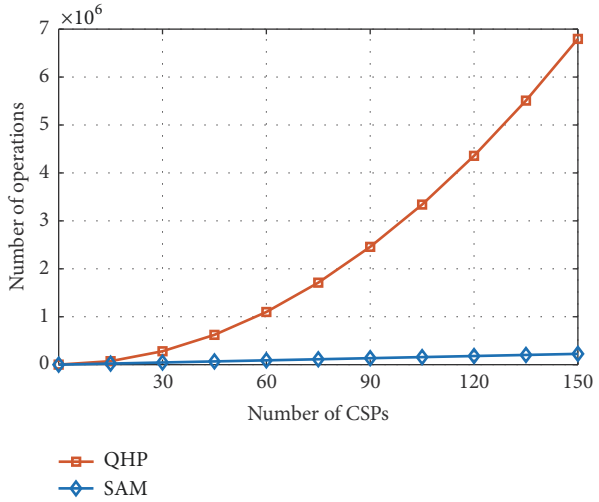


Figure 6: The operation comparison of SAM and QHP with respect to the number of CSPs.

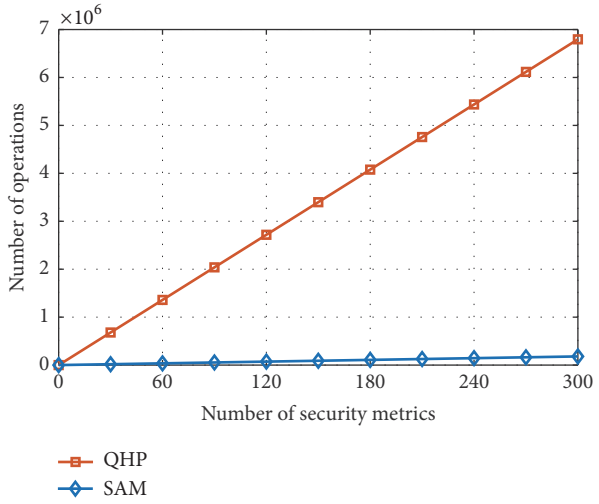
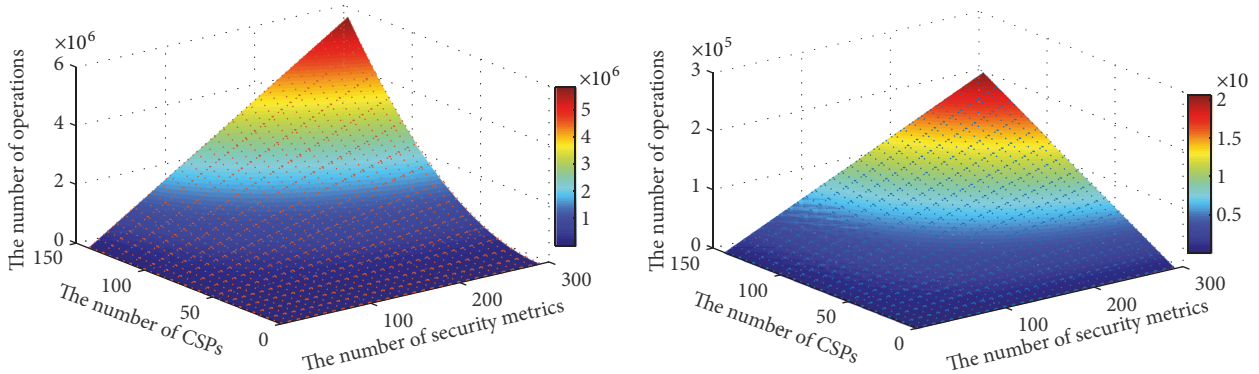


Figure 7: The operation comparison of SAM and QHP with respect to the number of security metrics.



(a) The number of operations of QHP

(b) The number of operations of SAM

Figure 8: The total number of operations comparison between SAM and QHP.

Table 3: Excerpt of CSPs security provisions based on CSCs security requirements [11].

Cloud security SLA element based on CSA STAR [42]			CSP_1	CSP_2	CSP_3
Control Category	Control Group	Security Metric		Value	
Compliance (CO)	Audit Planning (CO1)	CO1.1	*yes*	*yes*	*yes*
		CO1.2	$level_3$	$level_2$	$level_2$
	Independent Audits (CO2)	CO2.1	*no*	*yes*	*yes*
		CO2.2	*yes*	*yes*	*yes*
		CO2.3	*yes*	*yes*	*yes*
		CO2.4	*yes*	*yes*	*yes*
	Third Party Audits (CO3)	CO3.1	*yes*	*yes*	*yes*
		CO3.2	*yes*	*yes*	*yes*
		CO3.3	*Quarterly*	*Annual*	*Monthly*
Facility Security (FS)	Secure Area (FS1)	FS1.1	*no*	Monthly	*yes*
		FS1.2	*yes*	*no*	*yes*
	Asset Management (FS2)	FS2.1	*yes*	*yes*	*yes*
		FS2.2	$level_3$	$level_2$	$level_3$
		FS2.3	*yes*	*yes*	*yes*
Risk Management (RI)	Risk Assessments (RI1)	RI1.1	*Internal*	*Internal*	*External*
		RI1.2	*yes*	*yes*	*yes*

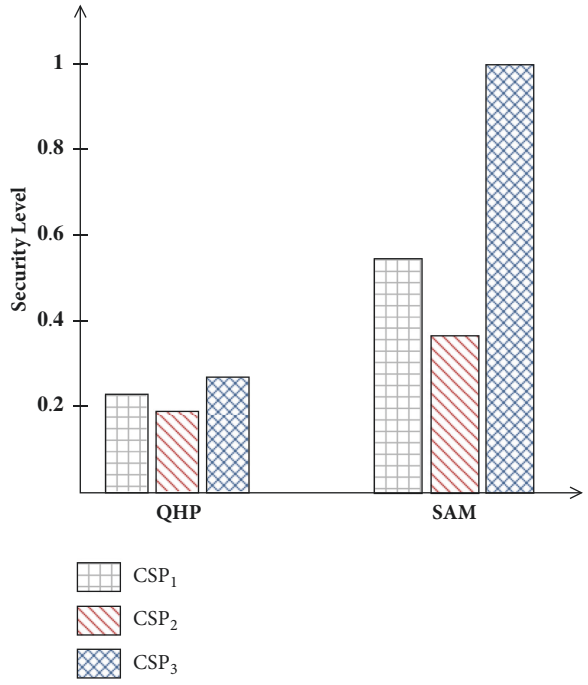


Figure 9: The security assessment results comparison of SAM and QHP.

Table 4: The separation measures and relative closeness of CSPs.

Alternatives		CSP_1	CSP_2	CSP_3
Separation Measures	D^+	0.3	0.43	0
	D^-	0.363	0.25	0.323
Relative Closeness	C	0.548	0.368	1

(1) Availability Validation. We utilize a real-world dataset to simulate the monitorable and measurable QoS attributes of cloud service and verify the availability and efficiency of CAM. This dataset, namely, WSDream dataset2, can be obtained from GitHub website [53]. It records a real-world QoS data from 142 users on 4,500 web services over 64 different time slices (at 15-minute interval). Each service has two QoS attributes in the original dataset, namely, response time (RT) and throughput (TP).

We denote the time slices and the number of users as the evaluation period (EP) and monitoring frequency, respectively. In addition, for facilitating the experiments, we

Table 5: Parameter settings.

QoS Attribute	Dataset	n	m	α	SLA
Response Time	RT_{mon}	64	118	0.05	2.219
Throughput	TP_{mon}	64	118	0.05	0.3901

identify 64 sets of QoS data in both RT and TP dataset, respectively, based on one single service from the original dataset (dataset2) via the keywords, namely, Time Slice ID. Each set contains 118 specific data values generated by users, which represents a set of monitored samples within an EP. As a result, we obtain two smaller QoS datasets, each containing 64×118 records and we denote them as RT_{mon} and TP_{mon}. We use these two datasets as the monitoring QoS value for compliance assessment in the experiments. The parameter settings are given in Table 5, where the number of items is denoted as m and the number of evaluation period is denoted as n. The *SLA* in this table denotes the compliance value with respect to the QoS attribute, which is described in Section 5.2. For convenience, we assumed that the SLA value of two QoS attributes are the mean of the RT_{mon} and the TP_{mon}, as shown in Table 5.

Let us now focus on the considered example. For the negative factor (RT), we first construct the compliance confidence interval according to a set of data in RT_{mon}, namely, the data in an EP. To facilitate the observation of the variation of the monitoring data in ideal case, we employ moving average method to process the monitoring data, which is denoted as smoothing data. Figure 10(a) illustrates the variation of the monitoring data of RT relative to its SLA and compliance confidence interval. As shown in Figure 10(a), the monitoring data vary around the SLA and its smoothing data basically vary within the compliance confidence interval. Because of the actual cloud environment, the QoS monitoring is a continuous process and its values are likely to vary due to the dynamics of the cloud resources (computing, network, and storage) and application workloads. Therefore, we denote the mean of monitoring data as the valid value to be evaluated in this EP. Similarly, Figure 10(b) shows the variation of the monitoring data of TP relative to its SLA and compliance confidence interval.

Then, we calculate the single conformance of RT in this EP according to the corresponding parameters, which includes SLA, compliance confidence interval, and the mean of monitoring data. The single conformance of RT in all EPs (64) can be obtained by the same way. Figure 11(a) shows that the single conformance of RT varies with the relationships across the confidence interval, SLA, and the mean intuitively. As shown in Figure 11(a), the confidence interval of RT does not fully cover the SLA; that is, there are some evaluation periods where RT is completely uncompliant. We can also conclude that the mean of RT varies around the SLA and always varies within the confidence interval. At the same time, it can be seen from this figure that the single conformance of RT is related to its confidence interval and the SLA, which varies between 0 and 1. In the case of a determined SLA, the single conformance of RT decreases with the increase of its confidence interval. When the upper limit of the confidence interval of RT is less than the SLA, the single conformance of RT is the maximum, namely 1. Conversely, the single conformance is the minimum value, namely 0, when the lower limit of the confidence interval of RT is less than the SLA. Similarly, Figure 11(b) shows the single conformance variation of TP.

Next, we determine the weights for the single conformance in each EP. The weight of single conformance of RT can be calculated according to (14), (15), and (16). Then we can use the obtained weights and the single conformance to calculate the weighted conformance of RT as well as TP in each evaluation period. Figure 12(a) shows the weighted single conformance of RT and TP. From this figure, we can observe that the single conformance of RT and TP in each EP is varying. Finally, we obtain the compliance level of RT and TP by aggregating their weighted single conformance in each EP, respectively. Figure 12(b) shows compliance level of RT and TP in form of the interval with every four EPs. From this figure, we can observe that the compliance level of RT and TP increases gradually over EP. This observation of results indicates that if the monitoring data of RT or TP is more stable and compliant over a period of time, its compliance level is closer to 1.

(2) Comparison with TRUSS. In this section, we compare our method of evaluating compliance with TRUSS [18]. The reason is obvious because of the similar direction of study on conformance evaluation of cloud service. Secondly, the sample dataset is derived from WSDream dataset2, so it becomes appropriate to compare both methods. Figure 13 illustrates the comparative computation function of QoS compliance evaluation between the two methods, which describes the effect of different weights and the single conformance on the compliance of an attribute in both TRUSS and CAM methods, respectively. As shown in Figure 13(a), the weighted conformance value varies with weight coefficient in TRUSS method, which means that the compliance computation function is excessively dependent on the weight. It is easy to cause the uncertainty of the conformance value. Figure 13(b) shows that the weighted conformance value has a certain relationship with the weight coefficient in CAM method, which means that the proposed method is more reasonable.

6. Conclusion

In this paper, we propose a new concept of cloud service life-cycle from the perspective of cloud-based IoT context, which enables CSCs to clearly understand the items that need to be considered at each phase of the adoption of cloud services. We have also presented a novel secure and compliant continuous assessment framework based on the cloud service life-cycle. This framework combines assessment methods of security and compliance as mutual complementation to facilitate CSCs to evaluate CSPs during the full cloud service life-cycle. Additionally, this assessment framework ensures the security of cloud-based IoT context by evaluating the security level and compliance level of cloud services. Simulation-based and case study experiments validated the performance and availability of our proposed method.

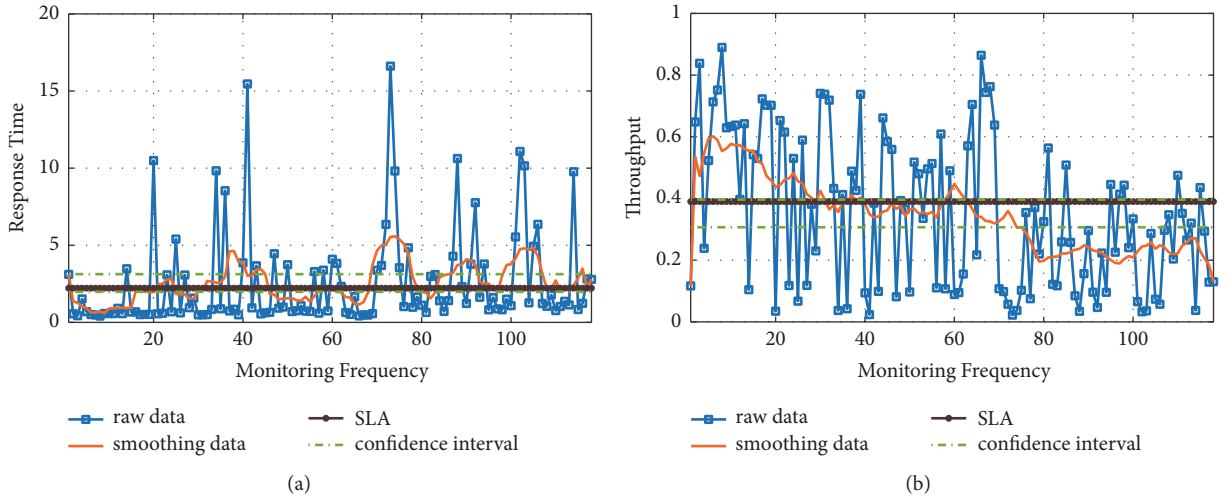


Figure 10: Monitoring data variation of RT and TP within t.

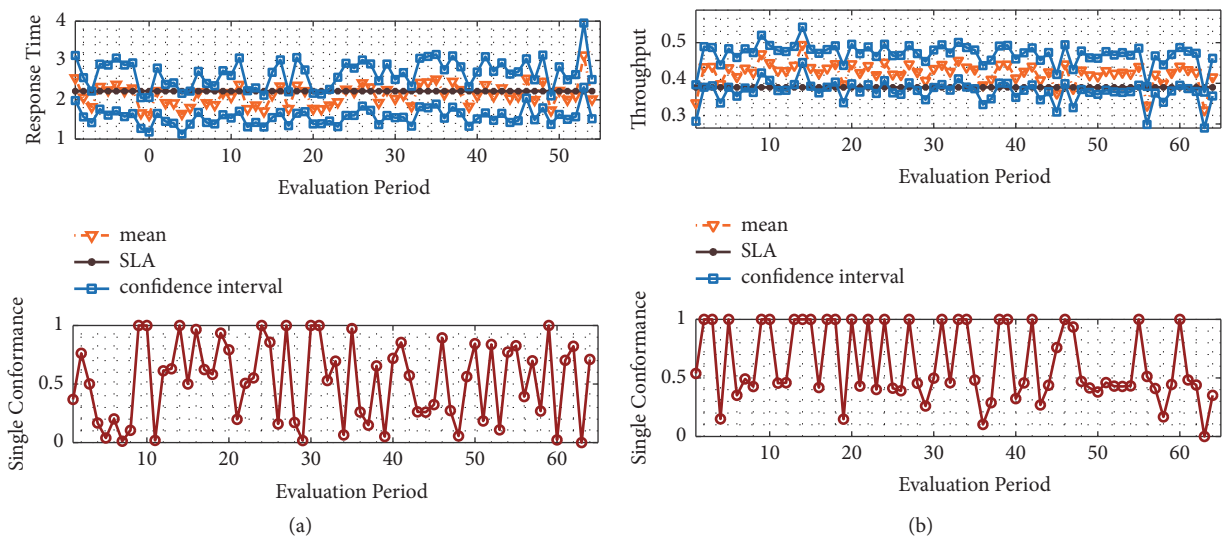


Figure 11: The single conformance o f RT and TP within T.

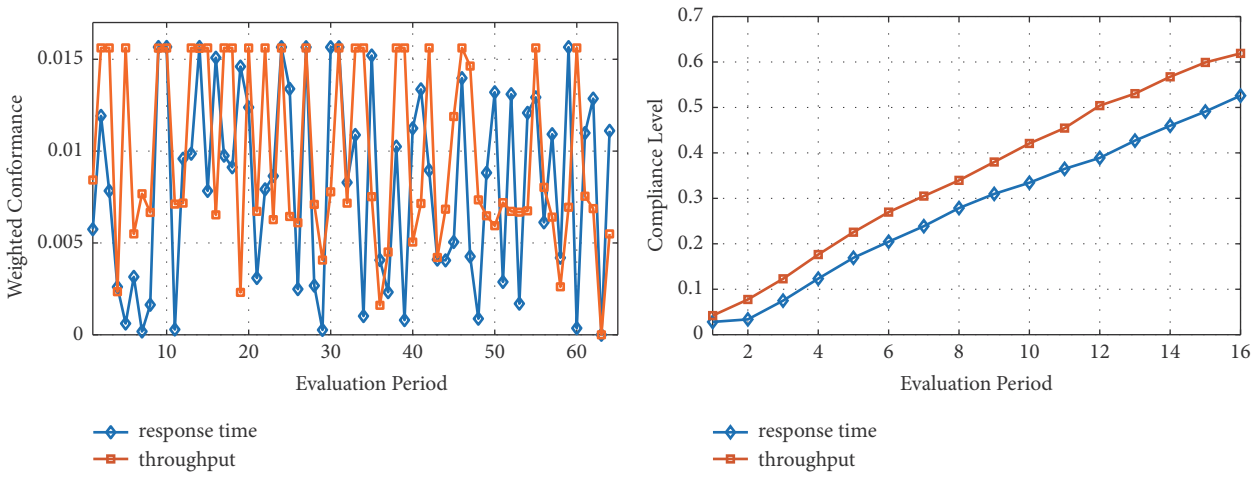


Figure 12: The compliance assessment results of RT and TP within T.

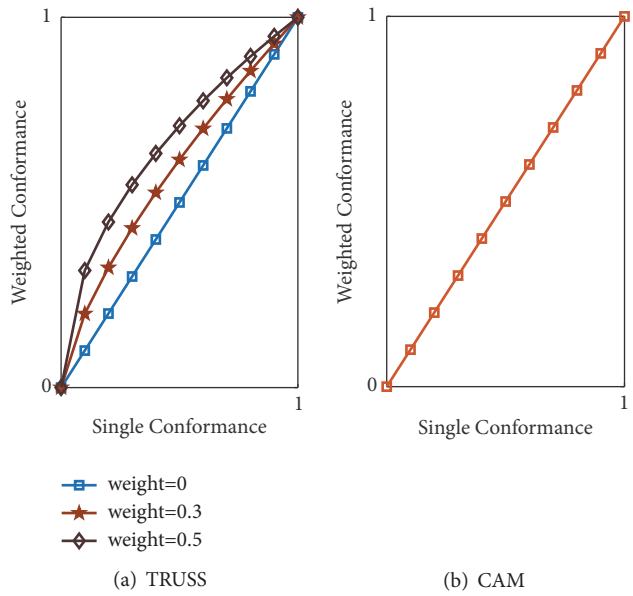


Figure 13: The compliance computation function comparison of CAM and TRUSS.

As future work, we plan extensions to the assessment framework in order to facilitate the evaluation of cloud service from the viewpoints of various stakeholders (e.g., cloud auditors, cloud brokers, or peers). We also plan to develop a prototype for our proposed assessment framework and further improve our evaluation algorithms.

Data Availability

The experimental data used to support the findings of this study are derived from the WSDream dataset2 repository (DOI:10.1109/TSC.2012.34.)

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 61802270 and 61802271 and in part by the Fundamental Research Funds for the Central Universities under Grants SCU2018D018 and SCU2018D022.

References

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[2] D. Chen, N. Zhang, Z. Qin et al., "S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[3] N. Zhang, P. Yang, S. Zhang et al., "Software defined networking enabled wireless network virtualization: Challenges and solutions," *IEEE Network*, vol. 31, no. 5, pp. 42–49, 2017.

[4] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin, "Channel Precoding Based Message Authentication in Wireless Networks: Challenges and Solutions," *IEEE Network*, pp. 1–7.

[5] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[6] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications*, vol. 79, pp. 88–115, 2017.

[7] S. Singh, Y. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.

[8] J. R. C. Nurse, S. Creese, and D. De Roure, "Security Risk Assessment in Internet of Things Systems," *IT Professional*, vol. 19, no. 5, pp. 20–26, 2017.

[9] Q. Wang, D. Chen, and N. Zhang, "LACS: A Lightweight Label-Based Access Control Scheme in IoT-Based 5G Caching Context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.

[10] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: A Privacy-Preserving Content-Based Publish-Subscribe Scheme with Differential Privacy in Fog Computing," *IEEE Access*, vol. 5, pp. 17962–17974, 2017.

[11] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative Reasoning about Cloud Security Using Service Level Agreements," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 457–471, 2017.

[12] J. Modic, R. Trapero, A. Taha, J. Luna, M. Stopar, and N. Suri, "Novel efficient techniques for real-time cloud security assessment," *Computers & Security*, vol. 62, pp. 1–18, 2016.

[13] T. Halabi and M. Bellaiche, "Evaluation and selection of Cloud security services based on Multi-Criteria Analysis MCA," in *Proceedings of the 2017 International Conference on Computing,*

Networking and Communications (ICNC), pp. 706–710, Silicon Valley, CA, USA, January 2017.

[14] S.-H. Na, K.-H. Kim, and E.-n. Huh, *A Methodology for Evaluating Cloud Computing Security Service-Level Agreements*, vol. 5, 2013.

[15] S. K. Garg, S. Versteeg, and R. Buyya, "SMICloud: a framework for comparing and ranking cloud services," in *Proceedings of the 4th IEEE/ACM international conference on utility and Cloud on utility and Cloud computing (UCC '11*, pp. 210–218, Melbourne, Australia, December 2011.

[16] Z. Ruo-xin, X.-j. Cui, S.-j. Gong, H.-k. Ren, and K. Chen, "Model for cloud computing security assessment based on ahp and fce," in *Proceedings of the in Computer Science Education (ICCSE, 2014 9th International Conference on. 1em plus 0.5em minus 0.4em IEEE*, pp. 197–204, 2014.

[17] S. Singh and J. Sidhu, "Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers," *Future Generation Computer Systems*, vol. 67, pp. 109–132, 2017.

[18] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Generation Computer Systems*, vol. 74, pp. 302–312, 2017.

[19] S. Ding, S. Yang, Y. Zhang, C. Liang, and C. Xia, "Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems," *Knowledge-Based Systems*, vol. 56, pp. 216–225, 2014.

[20] J. Luna, H. Ghani, D. Germanus, and N. Suri, "A security metrics framework for the cloud," in *Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference*, pp. 245–250, 2011.

[21] J. Luna Garcia, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," in *Proceedings of the the 2012 ACM Workshop*, p. 103, Raleigh, North Carolina, USA, October 2012.

[22] V. Casola, R. Preziosi, M. Rak, and L. Troiano, "A reference model for security level evaluation: policy and fuzzy techniques," *Journal of Universal Computer Science*, vol. 11, no. 1, pp. 150–174, 2005.

[23] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-based quantitative approach for assessing and comparing cloud security," in *Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014*, pp. 284–291, China, September 2014.

[24] T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9–26, 1990.

[25] J. R. S. C. Mateo, "Multi-criteria analysis," in *Multi Criteria Analysis in the Renewable Energy Industry*, pp. 7–10, Springer, 2012.

[26] J. Abawajy, "Determining service trustworthiness in intercloud computing environments," in *Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks, I-SPAN 2009*, pp. 784–788, Taiwan, December 2009.

[27] M. Alhamad, T. Dillon, and E. Chang, "SLA-Based Trust Model for Cloud Computing," in *Proceedings of the 2010 13th International Conference on Network-Based Information Systems (NBiS)*, pp. 321–324, Takayama, Gifu, Japan, September 2010.

[28] Z. Xu, P. Martin, W. Powley, and F. Zulkernine, "Reputation-Enhanced QoS-based Web Services Discovery," in *Proceedings of the IEEE International Conference on Web Services (ICWS 2007)*, pp. 249–256, Salt Lake City, UT, USA, July 2007.

[29] Q. He, J. Yan, H. Jin, and Y. Yang, "ServiceTrust: Supporting Reputation-Oriented Service Selection," in *Service Oriented Computing and Applications*, vol. 5900 of *Lecture Notes in Computer Science*, pp. 269–284, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[30] S. S. Yau and Y. Yin, "QoS-Based Service Ranking and Selection for Service-Based Systems," in *Proceedings of the 2011 IEEE International Conference on Services Computing (SCC)*, pp. 56–63, Washington, DC, USA, July 2011.

[31] L. Zeng, B. Benatallah, A. H. H. Ngu, M. Dumas, J. Kalagnanam, and H. Chang, "QoS-aware middleware for Web services composition," *IEEE Transactions on Software Engineering*, vol. 30, no. 5, pp. 311–327, 2004.

[32] S. Kalepu, S. Krishnaswamy, and . Seng Wai Loke, "Reputation = f(user ranking, compliance, verity)," in *Proceedings of the Proceedings. IEEE International Conference on Web Services, 2004.*, pp. 200–207, San Diego, CA, USA, July 2004.

[33] L. Vu, M. Hauswirth, and K. Aberer, "QoS-Based Service Selection and Ranking with Trust and Reputation Management," in *On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE*, vol. 3760 of *Lecture Notes in Computer Science*, pp. 466–483, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

[34] S. S. Yau, J. Huang, and Y. Yin, "Improving the Trustworthiness of Service QoS Information in Service-Based Systems," in *Autonomic and Trusted Computing*, vol. 6407 of *Lecture Notes in Computer Science*, pp. 208–218, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[35] X. Liu, K. K. Fletcher, and Mingdong Tang, "Service Selection Based on Personalized Preference and Trade-Offs among QoS Factors and Price," in *Proceedings of the 2012 IEEE International Conference on Services Economics (SE 2012)*, pp. 32–39, Honolulu, HI, June 2012.

[36] Z. Zheng, H. Ma, M. R. Lyu, and I. King, "QoS-aware web service recommendation by collaborative filtering," *IEEE Transactions on Services Computing*, vol. 4, no. 2, pp. 140–152, 2011.

[37] S. K. Garg, S. Versteeg, and R. Buyya, "A framework for ranking of cloud computing services," *Future Generation Computer Systems*, vol. 29, no. 4, pp. 1012–1023, 2013.

[38] Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang, "QoS ranking prediction for cloud services," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 6, pp. 1213–1222, 2013.

[39] M. Menzel and R. Ranjan, "CloudGenius," in *Proceedings of the the 21st international conference*, p. 979, Lyon, France, April 2012.

[40] A. Li, X. Yang, S. Kandula, and M. Zhang, "CloudCmp: comparing public cloud providers," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement (IMC '10)*, pp. 1–14, ACM, Melbourne, Australia, November 2010.

[41] L. Huang, S. Deng, Y. Li, J. Wu, J. Yin, and G. Li, "A Trust Evaluation Mechanism for Collaboration of Data-Intensive Services in Cloud," *Applied Mathematics & Information Sciences*, vol. 7, no. 1L, pp. 121–129, 2013.

[42] *Consensus assessments initiative questionnaire, Cloud Security Alliance*, Standard, 2017.

[43] Information security technology-Security guide of cloud computing services, GB/T 31167-2014, National Information Security Standardization Technical Committee, 2014.

[44] Cloud Controls Matrix, *Cloud Security Alliance*, Standard, 2017.

[45] T. L. Saaty, "Decision making the analytic hierarchy and network processes (AHP/ANP)," *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, 2008.

[46] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius, "A state-of the-art survey of TOPSIS applications," *Expert Systems with Applications*, vol. 39, no. 17, pp. 13051–13069, 2012.

[47] ISO/IEC 19086-1, Information technology-Cloud computing-Service level agreement (SLA) framework-Part 1:Overview and concepts, International Organization for Standardization/International Electrotechnical Commission, 2016.

[48] ISO/IEC 19086-3, Information technology-Cloud computing-Service level agreement (SLA) framework-Part 3: Core conformance requirements, International Organization for Standardization/International Electrotechnical Commission, 2016.

[49] Cloud Computing Service Metrics Description, *National Institute of Standards and Technology, Standard*, 2018.

[50] ISO/IEC FDIS 19086-2, Information technology-Cloud computing-Service level agreement (SLA) framework-Part 2: Metric Model, International Organization for Standardization/International Electrotechnical Commission, 2017.

[51] B. V. Gnedenko, "Theory of probability. 1em plus 0.5em minus 0," *4em Routledge*, 2017.

[52] C. E. Shannon, "A mathematical theory of communication," *Bibliometrics*, vol. 5, no. 1, pp. 3–55, 2001.

[53] Z. Zheng, Y. Zhang, and M. R. Lyu, "Investigating QoS of real-world web services," *IEEE Transactions on Services Computing*, vol. 7, no. 1, pp. 32–39, 2014.