IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 12, 2018, accepted December 26, 2018, date of publication January 3, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2890432

Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach

XIANG LI[1], QIXU WANG[2], XIAO LAN[2], XINGSHU CHEN[2], NING ZHANG[3], (Member, IEEE), AND DAJIANG CHEN[4], (Member, IEEE)

[1]College of Computer Science, Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China
[2]College of Cybersecurity, Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China
[3]Department of Computing Science, Texas A&M University Corpus Christi, TX 78412, USA
[4]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

Corresponding author: Qixu Wang (qixuwang@scu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61802270, Grant 61802271, Grant 61872059 and Grant 61502085, and in part by the Fundamental Research Funds for the Central Universities under Grant SCU2018D018 and Grant SCU2018D022.

ABSTRACT The Internet of Things (IoT) provides a new paradigm for the development of heterogeneous and distributed systems, and it has increasingly become a ubiquitous computing service platform. However, due to the lack of sufficient computing and storage resources dedicated to the processing and storage of huge volumes of the IoT data, it tends to adopt a cloud-based architecture to address the issues of resource constraints. Hence, a series of challenging security and trust concerns have arisen in the cloud-based IoT context. To this end, a novel trust assessment framework for the security and reputation of cloud services is proposed. This framework enables the trust evaluation of cloud services in order to ensure the security of the cloud-based IoT context via integrating security- and reputation-based trust assessment methods. The security-based trust assessment method employs the cloud-specific security metrics to evaluate the security of a cloud service. Furthermore, the feedback ratings on the quality of cloud service are exploited in the reputation-based trust assessment method in order to evaluate the reputation of a cloud service. The experiments conducted using a synthesized dataset of security metrics and a real-world web service dataset show that our proposed trust assessment framework can efficiently and effectively assess the trustworthiness of a cloud service while outperforming other trust assessment methods.

INDEX TERMS Cloud-based IoT, cloud service trust assessment, security and reputation assessment, trustworthy cloud service selection.

I. INTRODUCTION

The Internet of things (IoT) is an emerging technology that has developed rapidly in recent years. The concept of the IoT is defined as the network of physical objects, devices, vehicles, buildings and other items that are embedded with electronics, software, sensors, and network connectivity that permits these objects to gather and exchange data [1]. The IoT has led to the constant universal connection between people and things. Therefore, the IoT has been widely applied in various applications and is the next major link in the new technology domain. However, due to the resource constraints of IoT devices, the tasks with high computational complexity and the large volume of data storage in the IoT context are always handled by the resource-rich cloud paradigm, which considerably enhances their efficiency. For instance, IoT devices generate vast amounts of data that put huge strains on the IoT. The Cloud can be used to process and store the big data generated by IoT devices, which will improve the overall efficiency of cloud- based IoT context [2]. The cloud-based IoT architecture is illustrated in Figure 1.

Through the integration of the IoT and the Cloud, we have the opportunity to expand the use of the available technology that is provided in cloud environments [3]. However, as with many new technologies, there are several challenges with regards to achieving success in the cloud-based IoT context [4]–[6] and IoT environment [7], [8]. Two of the challenges for the cloud-based IoT context are security (e.g., the physical layer security and access

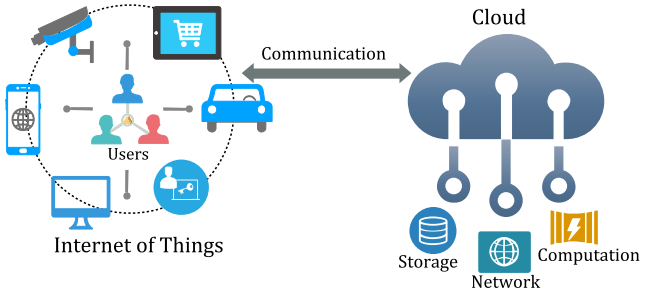


FIGURE 1. Cloud-based IoT context.

control management) and trust (e.g., malicious nodes and data misuse). Therefore, the adoption of the cloud-based IoT paradigm transfers the security and trust issues of the IoT to the cloud. To address this issue, the security of the IoT context can be ensured through a trustworthy cloud, as shown in Figure 2. Nevertheless, there is little literature on the cloud-based IoT context trust assessment, while the traditional existing literature with respect to the security of the IoT address wireless networks [9]–[11]. Therefore, this paper focuses on ensuring the security of the cloud-based IoT context by assessing the trustworthiness of a cloud service using an integrated approach of security and reputation.

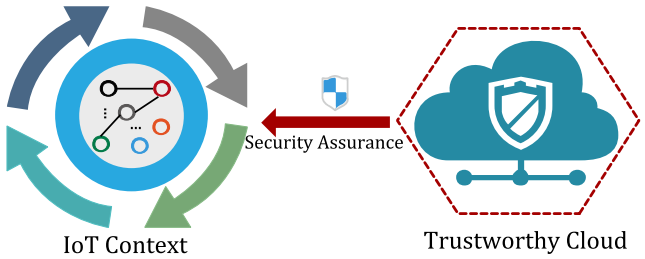


FIGURE 2. Trustworthy Cloud ensures security of the IoT context.

Since there are increasingly more competing cloud service providers (CSPs) that have similar functional properties, determining the trustworthiness of cloud service providers (CSPs) has become one of the most challenging issues. It also has truly brought about a tough choice for the cloud service customers (CSCs) to select the most trustworthy CSPs out of a large pool of already existing CSPs with similar offerings. The trust assessment or selection of CSPs reflects the cognition of CSCs with respect to the multiple cloud service attributes, such as reliability, scalability, availability, safety, and security. To address these issues related to trust, various trust-based cloud service studies have attracted considerable interest. These studies focus on evaluating the trustworthiness of the cloud services of CSPs by leveraging multiple different attributes related to cloud services, which can be deemed as a comprehensive quality measure of the services.

Some existing studies attempt to assess the trustworthiness of CSPs based on the quality of service (QoS) of their cloud service [12]–[15]. These studies focus on evaluating the compliance degree between the QoS values of the cloud service of each candidate CSP and the QoS requirements of the CSCs or the cloud service level agreements (SLAs) in order to determine their trustworthiness, and then recommend the CSP with the highest trustworthiness to the CSC. There are also some studies that attempt to assess the trustworthiness of CSPs by employing the feedback ratings of CSCs [16]–[19], namely, the rating-based reputation evaluation, which has been widely adopted in web service-based applications (e.g., e-commerce and peer-to-peer (P2P) networks). They focus on evaluating the reputation of each candidate CSP by using the feedback ratings of CSCs among all the ratings of its cloud service. Both the QoS and reputation are typically represented by a comprehensive score reflecting the overall quality and opinion or by a small number of scores on several major aspects of performance.

The QoS and reputation of CSPs will undoubtedly impact the choice of the cloud services of CSCs. Consequently, CSPs attempt to build and maintain higher QoSs and reputations for their cloud services. One of the most obvious flaws in previous works was the failure to consider security in the trust assessment. Although both QoS and feedback ratings can capture some trust features of cloud services, they are far from being perfect measures of the trustworthiness of CSPs without also including security. Therefore, it is widely recognized that without a sufficient security assessment, the accurate and true trustworthiness of a cloud service cannot be obtained. To the best of our knowledge, no comprehensive trust assessment framework that evaluates the trustworthiness of a CSP by combining its security and reputation has been published. Though there are some works that attempt to evaluate the trustworthiness of a CSP by taking security into consideration [20], [21], they do not highlight the importance of security because of the lack of fine-grained security metrics.

Contrary to this, we propose a novel trust assessment framework for cloud services that takes into account both the security and reputation of cloud services as complementary features to evaluate the trustworthiness of cloud services. In addition, it also facilitates CSCs in selecting the most trustworthy CSPs out of various candidate CSPs in order to provide cloud services according to the trust assessment results.

This paper addresses the issues for the trustworthiness of a cloud service by presenting a trust assessment framework that integrates security and reputation in order to assess the trustworthiness of cloud service through the following contributions:

- A novel trust assessment framework for cloud services is proposed to assess the trustworthiness of cloud services by integrating security and reputation. The proposed framework ensures the security of the cloud-based IoT context by assessing the trustworthiness of cloud services.
- To evaluate the trustworthiness of cloud services with respect to security, a security-based trust assessment method is proposed, which exploits cloud-specific

security metrics to evaluate the security of cloud services. For evaluating the trustworthiness of cloud services with respect to reputation, we propose a reputation-based trust assessment method to evaluate the reputation of cloud services by using the feedback ratings on the QoS of cloud services.
- To effectively integrate the assessment results of security and reputation into the trust assessment of cloud services, an integrated trust assessment method is presented. It employs an objective weight assignment approach to assign the respective relative importance weight factors to the security level and reputation level and aggregate them in order to obtain the quantitative trustworthiness of cloud services.
- To illustrate the feasibility and efficacy of the proposed framework, we conduct comprehensive experiments from two dimensions (i.e., availability and performance). The experimental results show that the proposed framework is effective and efficient in the trust assessments of cloud services.

The remainder of the paper is structured as follows. Section 2 discusses the related work. Section 3 presents the system model and the design goals. Section 4 details the proposed trust assessment framework of cloud services and elaborates on the proposed trust assessment methods. Section 5 presents the experiments and results analysis, and finally, Section 6 presents this paper's conclusions and outlines directions for future work.

II. RELATED WORK

Some widely adopted trust assessment methods for evaluating the trustworthiness of cloud services have been proposed from different perspectives. The QoS-driven trust assessment method for cloud services is one of them. In [15], a compliance-based multi-dimensional trust evaluation system was proposed, which enabled CSCs to determine the trustworthiness of a CSP. This system helps CSC to choose a CSP from candidate CSPs that satisfy its desired QoS requirements. Somu *et al.* [22] presented a trust-centric approach based on hypergraph-binary fruit fly optimization for the identification of suitable and trustworthy CSPs. Yang *et al.* [23] proposed a novel method and trust mechanism based on cloud model theory. This mechanism takes trust, costs and time into account and employs the analytic hierarchy process method to help CSCs select the appropriate cloud service. In [24], a trust evaluation framework that uses the compliance monitoring mechanism to determine the trustworthiness of CSPs was proposed. However, the QoS data of cloud services is difficult to be acquired and often incomplete. In addition, the QoS data of cloud services might be unreliable. Therefore, it is impossible to determine the accurate trustworthiness of CSPs only based on the QoS value.

It is also common to assess the trustworthiness of cloud services based on experiences and opinions (i.e., feedback ratings) from CSCs. Nagarajan *et al.* [25] advocated a big data processing framework for evaluating the trustworthiness of cloud services. It pre-processes the feedback ratings of CSCs by employing a cloud broker that incorporates the MapReduce framework. In [26], a novel trust evaluation method combined the feedback evaluation component and the Bayesian game model to recognize malicious CSCs and their feedback ratings. The former is used to examine and identify fake identities and the latter is used to detect malicious users and their feedback. Noor *et al.* [19] designed and implemented a reputation-based trust management framework. This framework can measure the credibility of feedback ratings to protect cloud services from malicious CSCs. In [18], a lightweight reputation measurement approach for cloud services based on the cloud model was proposed. This method uses fuzzy set theory to obtain the reputation scores of cloud services according to the feedback ratings of CSCs. However, there are malicious users and unfair feedback ratings in the real cloud environment, which significantly affect the reputation of CSPs. Similarly, it is impossible to obtain the true trustworthiness of CSPs only based on the feedback ratings of users.

There are also some studies that combined objective and subjective assessment methods. Tang *et al.* [27] proposed a trustworthy selection framework for cloud service selection. This framework presented an integrated trust evaluation method that combines an objective trust assessment (QoS monitoring) and a subjective trust assessment (feedback ratings). However, the one-size-fits-all algorithm for identifying untrustworthy users can mistakenly exclude trustworthy users and their true feedback ratings. In [20], a novel framework for conducting cloud service trust evaluations that combines QoS predictions and customer satisfaction estimations was proposed. This framework focused on improving the accuracy of the QoS value predictions of quantitative trustworthy attributes and estimating the customer satisfaction for a target cloud service. However, it did not consider the influence of the time factor and unfair feedback ratings on the QoS predictions. Huang *et al.* [21] proposed an algorithm to measure the quality of cloud services that leverages the service QoSs and feedback ratings of CSCs. Though it considered both the trustworthiness of individual partner services and their relation, it had a particular representation for the subjective attributes and neglected the dynamic features of the QoS. Reference [28] aimed to select the trustworthy service provider by evaluating trustworthiness based on the in-context feedback from different sources, which included customer feedback, global advisory feedback and third-party feedback. However, it relies too much on subjective feedback and ignores the importance of objective aspects.

In addition to the trust assessment methods mentioned above, there are some other methods to ensure the trustworthiness of the cloud environment. Kim [29] proposed an enhanced trusted cloud computing platform to protect the confidentiality and integrity of the user's data and computations. This trusted platform provides secure and efficient virtual machine management protocols to protect against

eavesdropping and tampering during transfer and guarantee the security of the virtual machine against inside attackers. In [30], a new trust model based on fuzzy mathematics in the cloud environment was proposed. According to the successful and failed interactions between cloud entities, the trustworthiness of cloud systems was computed based on the properties and semantics of trust. Li *et al.* [31] proposed a trust quantification method based on fuzzy comprehensive evaluation theory for cloud computing. Furthermore, it introduced the trust ontology for cloud services that defines user preference trust values to protect user data.

It can be seen from the related work discussed above that many existing studies on the trust assessment of cloud services are mainly classified into two categories, namely, QoS-based and feedback rating-based approaches, which have been widely adopted in cloud service trust assessment. However, one of the most indispensable factors to ensure that cloud services are trustworthy, namely, security, is not taken into account by these works. Unlike previous works that do not consider the problem of security in cloud service trust assessments, we present a comprehensive trust assessment framework combining the features of security and reputation for cloud services. This framework not only assesses the security level of cloud services based on various security metrics, but it also assesses the reputation of cloud services based on the feedback ratings of CSCs. Furthermore, it has the ability to adaptively adjust the trustworthiness of cloud services according to the security level and reputation level.

III. SYSTEM MODEL AND DESIGN GOALS

In this section, we present the system model that comprises two assessment models, namely, the security assessment model and the reputation assessment model. The security assessment model mainly describes the elements and components constituting the security-based trust assessment method. The reputation evaluation model mainly introduces the weight factors that are used to mitigate the common attacks impacting the reputation evaluation results. Finally, we end this section with the details of the design goals.

A. SECURITY ASSESSMENT MODEL

We consider the security assessment model including m CSPs and n security metrics covering multifaceted security features (e.g., facility security, risk management and information security). These security metrics can be defined and formatted as a deliverable template by the CSC. Then, the security assessment model consists of many CSPs and a deliverable template containing numerous security metrics. This model evaluates the security of CSPs by employing the security metrics in the deliverable template, which is called the security controls deliverable (SCD).

1) *Standardization:* The SCD acts as the standardized artifact that can demonstrate the security controls that are implemented in the cloud service of a CSP. The security metrics in the SCD are defined according to the common security requirements of CSCs in practice. Many security metrics have been developed by multidisciplinary working groups on security standards (e.g., CSA [32], FedRAMP [33], NIST [34], [35], ISO/IEC [36], [37], SMI [38], etc.). We can select the appropriate security metrics from these existing standards to develop the SCD. These security metrics ensure that CSCs are comfortable using the secure cloud service.
2) *Conformity:* The CSP measures and verifies the security controls that are implemented in its cloud services according to the SCD. Then, the CSP fills in the SCD according to the conformance between the security metrics and its security controls. In our model, we assume that the content in the SCD provided by the CSP, namely the conformity between security metrics and security capability of CSP, are true and credible. After that, the SCD will be used to evaluate the security level of the cloud service provided by the CSP.

B. REPUTATION ASSESSMENT MODEL

In the reputation assessment model, a CSC either gives a feedback rating regarding the trustworthiness of a holistic cloud service or the quality of service (QoS) of a specific cloud service. From the feedback ratings of CSCs, the trustworthiness of a cloud service is actually a collection of the historic invocation records. The feedback rating is denoted by a multituple $(C_{id}, S_{id}, S_{id}(A_{id}), F, \Delta t)$, where C_{id} and S_{id} respectively represent the identity of the CSC and the cloud service, $S_{id}A_{id}$ is the resource or attribution of $S_{id}A_{id}$, F represents the feedback rating on the QoS of a cloud service attribution $S_{id}(A_{id})$ or the holistic cloud service S_{id}, and Δt is the time when the F is offered by CSC. Each multituple represents a feedback rating on a specific attribute or service of a cloud service from a CSC. Therefore, the credibility and certainty of feedback ratings play important roles in this model for evaluating the trustworthiness of cloud services. To mitigate the negative impacts of unfaithful feedback ratings from malicious CSCs on the reputation evaluation, we introduce the following weight factors.

1) *Credibility*: In the practical scenario, some malicious customers may cooperate to provide a large amount of unfaithful feedback ratings in order to increase or decrease the reputation of a specific cloud service. In addition, a CSP may hire several malicious customers to launch a self-promotional attack [39] or slandering attack [40] to boost the reputation of its cloud service. These two common attacks are belonged to collusion attacks. The weight factor of credibility that is introduced in the reputation assessment model can adaptively adjust the credit of customers according to their feedback rating on the cloud service in order to mitigate the impacts of the collusion attacks on the reputation evaluation results. In our model, we assume that the majority of CSCs offering feedback rating on cloud service are not malicious.

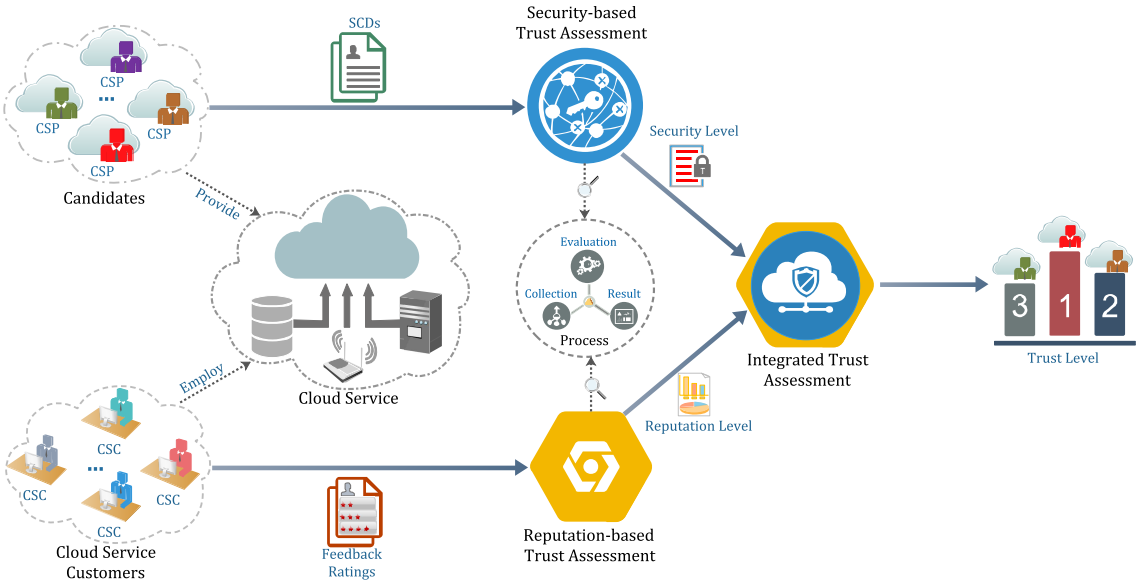


FIGURE 3. The proposed trust assessment framework for cloud service.

2) *Certainty*: It is worth considering that some malicious CSCs subvert the reputation assessment model by creating a large number of pseudonymous identities and using them to give numerous unfaithful feedback ratings for the purpose of conducting a self-promotional or slanderous attack in a short period of time. The weight factor of certainty presented in the reputation assessment model can mitigate the impacts of these attacks on the reputation evaluation results by retaining a constant number of valid feedback ratings of customers over a short period of time.

C. DESIGN GOALS

The design goal is to develop a trust assessment framework based on security and reputation for assessing the trustworthiness of cloud services. Specifically, we aim to achieve the following objectives.

1) *Security Goal*: The purpose here is to evaluate the security of the cloud services provided by CSPs. The unambiguous and understandable assessment results (i.e., quantitative value) are obtained by employing the security-based trust assessment method proposed in this paper. The quantitative assessment results that represent the security of cloud services are used to evaluate their trustworthiness.
2) *Reputation Goal*: The primary objective here is to evaluate the reputation of cloud services according to the feedback ratings. Similar to the security assessment, the quantitative assessment results, representing the reputation of cloud services, are obtained by using the reputation-based trust assessment method proposed in this paper. The quantitative reputation of cloud services are used to evaluate their trustworthiness.
3) *Trust Goal*: The trust goal evaluates the trustworthiness of cloud services by combining the security and the reputation of the cloud services that were obtained in the previous two processes. By exploiting the proposed relative importance weight assignment approach, the security and reputation are given reasonable weights. Ultimately, the quantitative trustworthiness of cloud services are obtained by utilizing the integrated trust assessment method proposed in this paper.

IV. THE PROPOSED TRUST ASSESSMENT FRAMEWORK

In this section, the STRAF, a novel trust assessment framework for cloud service based on security and reputation, is proposed. This framework is an extension from our previous work [41] and can be divided into three main components, encompassing 1) security-based trust assessment (SeTA), 2) reputation-base trust assessment (ReTA) and 3) integrated trust assessment (InTA). In addition, we further analyze the availability and feasibility of SeTA and ReTA. As shown in Figure 3, the STRAF includes the following components.

A. SECURITY-BASED TRUST ASSESSMENT

The SeTA, a security-based trust assessment method, is proposed and detailed in this section. The SeTA comprises three main procedures, including 1) security metrics definition, 2) security metrics quantification, and 3) security level evaluation. For convenience, the key notations used in SeTA are given in Table 1. Specifically, the SeTA includes the following steps.

1) SECURITY METRICS DEFINITION

In this stage, the SeTA first defines security metrics and accordingly forms security control deliverable (SCD).

TABLE 1. Notations in security-based trust assessment.

Symbol	Description
m	the number of CSPs
n	the number of security metrics
K	a set of SCDs from CSPs
Q	a set of quantitative K
R	the normalized decision matrix
A	the ideal solutions of security metrics
D	the separation measures of CSPs
C	the relative closeness of CSPs

The SCD contains n multifaceted and cloud-specific security metrics which represent various security requirements of CSCs. Then, the SCD is provided to the m candidate CSPs for fulfillment. These security metrics in SCD are supposed to be ensured by CSPs implementing specific security controls or security mechanisms. Finally, The CSPs self-evaluates its security capability according to security metrics and provide their conformity with security metrics. The first round using SCD is to collect data with respect to the security capability of the candidate CSPs in a uniform format and fashion. Therefore, the collected SCDs K contain m CSPs, where each of them has n security metrics. Furthermore, some existing researches and standards (e.g., CSA CCM [32], FedRAMP [33] and ISO/IEC [36], [37]) on cloud security control have been well developed, which can be used as baseline repository by CSCs to define bespoke security metrics.

2) SECURITY METRICS QUANTIFICATION

The second round is to quantify the security metrics of each candidate CSP included in SCDs for convenient comparison of their security capabilities. The quantification approach depends on different types of the security metrics. In this step, we employ the quantification approach proposed by [42]. 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 SCDs are used as input dataset $Q_{m\times n}$ of security level evaluation process.

3) SECURITY LEVEL EVALUATION

For the given quantitative SCDs $Q_{m\times n}$, SeTA employs the method based on technique for order preference by similarity to ideal solution (TOPSIS) [43] to evaluate the security level of each candidate CSP and compare their security level in accordance to evaluation results. Firstly, a normalized decision matrix needs to be constructed by Equation (1).

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

Then, the ideal solution A of each security metric can be determined by Equations (2) and (3), which includes positive A^+ and negative A^-.

$$A^+ = \{min(r_{ij})|j \in J^- \ or \ max(r_{ij})|j \in J^+\} \tag{2}$$

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

where, $i = 1, 2, \cdots, m$, $j = 1, 2, \cdots, n$, $r_ij \in R$, 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 Equations (4) and (5), which represent the geometric distance from each CSP to ideal solutions A. It also includes positive D^+ and negative D^-.

$$D_i^+ = \sqrt{\sum_{j=1}^{n}(r_{ij} - r_j^+)^2} \tag{4}$$

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

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

Next, the relative closeness C representing the degree of conformity between the each of CSPs and the ideal solution can be obtained by Equation (6).

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-} \tag{6}$$

where $i = 1, 2, \cdots, m$ and $0 \leq C_i \leq 1$. Then, SeTA can rank CSPs according to their relative closeness C, which represents the security capability of CSP. The closer the relative closeness C of CSP is to 1, the higher its security level is.

Algorithm 1 Security-Based Trust Assessment

Input: the number of candidate CSPs m and security metrics n

1: **Data Collection and Preprocessing:** Define and select n security metrics according to the common security issue of cloud service and form the security metric template. m candidate CSPs fill out the SMT and submit it as security control deliverables (SCDs). Integrate and normalize the SCDs as a dataset K.

2: **Security Controls Deliverables Quantification:** In terms of CSP, the contents of dataset K (e.g., security metrics) is quantified as dataset Q according to the category of security metrics.

3: **Security Level Evaluation:** Construct the normalized decision matrix R with the quantitative SCDs Q by TOPSIS method. Determine the positive (A^+) and negative (A^-) ideal solutions for each security metric. Calculate the separation measures ($D^+ and \ D^-$) in accordance with ideal solutions. Calculate the relative closeness (C) for each CSP.

Algorithm 1 illustrates the security-based trust assessment process. Algorithm 2 demonstrates the procedure of the security level evaluation.

Algorithm 2 Security Level Evaluation

Input: set of SCD Q, size of the set $m \times n$

procedure Security Level Evaluation(Q, m, n)
  Create arrays $C_{1\times m}, A^{+}_{1\times n}, A^{-}_{1\times n}, D^{+}_{1\times m}$,
  $D^{-}_{1\times m} \leftarrow \emptyset$;
  Create matrix $R_{m\times n} \leftarrow \emptyset$;
  $R \leftarrow$ MatrixNormalization (Q, m, n);
  $A^{+}_{1\times n}$, $A^{-}_{1\times n} \leftarrow$ IdealSolutions (R);
  $D^{+}_{1\times m}, D^{-}_{1\times m} \leftarrow$ SeparationMeasures(R,
  $A^{+}_{1\times n}, A^{-}_{1\times n}$);
  $C \leftarrow$ RelativeCloseness $\left(D^{+}_{j}, D^{-}_{j}\right)$;
  $Sort(C)$;
  return C;
end procedure

4) SECURITY ASSESSMENT ANALYSIS

The security metrics used in SeTA are derived from international and industrial security standards (i.e., ISO/IEC, CSA and FedRAMP). These security metrics are developed based on the best practices from industry, organizations and government departments. The availability and feasibility of security metrics are endorsed by the international working groups on security standards. In the process of SeTA, we assume that the content in the SCDs provided by CSPs, namely the conformity between security metrics and their security capabilities, are true and credible. We can obtain the maximum and minimum of each security metric from the quantitative SCDs Q. For the positive security metric, A^{+} and A^{-} represent the set of maximum and minimum for each security metric, respectively. Moreover, we can respectively obtain the geometric distances (i.e., D^{+} and D^{-}) from a CSP to the best and the worst security metrics (i.e., A^{+} and A^{-}). Therefore, it can be considered that the smaller D^{+} of a CSP is, the closer each security metric of the CSP to its corresponding maximum in A^{+} is, that is, the security level of the CSP is high. Conversely, the smaller D^{-} of a CSP is, the closer each security metric of the CSP to its corresponding minimum in A^{-} is, that is, the security level of the CSP is low. Then, we can state that if a CSP has a larger D^{-} and a smaller D^{+}, its security level must be higher.

B. REPUTATION-BASED TRUST ASSESSMENT

In this process, the ReTA continuously evaluates the reputation of cloud services within several fixed-sized consecutive time windows. In each time window, the local objective reputation (LOR) is evaluated in accordance with the feedback ratings provided by CSCs. The feedback ratings are the single or holistic feedback on a specific service generated by CSCs in the process of using cloud services. The LOR represents the current reputation level of a specific cloud service offered by a CSP in a given time window. The global objective reputation (GOR), representing the holistic reputation level of all services provided by a CSP, will be obtained by aggregating the time-based weighted LOR. After that, the ReTA quantifies the reputation (i.e., GOR) of each CSP and submits it to the InTA for the integrated trust assessment, as shown in Figure 3. Specifically, the ReTA includes three stages as follows.

1) LOCAL OBJECTIVE REPUTATION

In this stage, we assume that CSCs are willing to give feedback ratings to a service that he/she has invoked, and these ratings can be collected for service reputation evaluation purpose. Since LOR is evaluated by the feedback ratings on a specific service provided by CSCs within a fixed time of period, LOR can be considered as a time window-based reputation metric for cloud service. LOR is generated in a time window when interactions have been taken place between CSCs and services.

Definition 1: Let $\Omega = \{S_1, S_2, \cdots, S_m\}$ denote m cloud services; Let $\Psi = \{C_1, C_2, \cdots, C_n\}$ denote n CSCs. Let $F_{ij}(\Delta t_k)$ denotes the feedback rating of CSC C_j on cloud service S_i within the time window Δt_k. Let $L_{S_i}(\Delta t_k)$ denote the LOR of cloud service S_i ($S_i \in \Omega$) within the k^{th} time window Δt_k. We define the $L_{S_i}(\Delta t_k)$ as follows.

$$L_{S_i}(\Delta t_k) = \sum_{j=1}^{n} (F_{ij}(\Delta t_k) \times \gamma_j^{\Delta t_k} \times \lambda_j^{\Delta t_k}) \tag{7}$$

where $\gamma_j^{\Delta t_k}$ and $\lambda_j^{\Delta t_k}$ respectively represent the credibility of CSC C_j and the certainty of its feedback ratings within the k^{th} time window Δt_k, which will be detailed later. The dimensions included in a feedback rating $F_{ij}(\Delta t_k)$ depends on the type of feedback rating from the CSCs. For instance, if there are κ resources or attributes of a cloud service S_i that CSCs focus on, $F_{ij}(\Delta t_k)$ represents the feedback rating offered by CSC on the QoS of a cloud service attribute or the holistic cloud service within the Δt_k time window, which has been detailed both in reputation assessment model and step 1 of Algorithm 3. In a real-world scenario, the feedback rating F offered by a CSC is a quantitative value related to a specific cloud service attribute (e.g., response time and throughput).

2) WEIGHT FACTOR ASSIGNMENT

In traditional trust evaluation systems, all feedback ratings on a service are usually exploited to evaluate their reputation. Although these methods are simple and effective, they cannot cope well with the impact of unfair feedback ratings offered by malicious users (e.g., self-promotional attack or slandering attack) on reputation evaluation. Thus the result of reputation evaluation is not accurate and reliable enough. In this stage, in order to effectively solve the issues, we define respectively two weight factors which are named as credibility and certainty to improve the accuracy of the reputation assessment model of cloud services and mitigate the impact of reputation attacks initiated by malicious users.

Definition 2: For a given time window Δt_k, let ω_{C_j} ($\omega_{C_j} \subseteq \Omega$) denotes the subset of services which are invoked by the CSC C_j; Let ψ_{S_i} ($\psi_{S_i} \subseteq \Psi$) denotes the subset of CSCs which invokes the service ω_{C_j}; Let f_{ij} denotes the feedback

Algorithm 3 Reputation-Based Trust Assessment

Input: identity of CSC C_{id}, identity of cloud service S_{id}, a resource or attribution of cloud service $S_{id}(A_{id})$, feedback F on quality of service (QoS) of $S_{id}A_{id}$ or the feedback rating on the overall QoS of S_{id}, timestamp t of feedback rating, consecutive time window z in terms of Δt

1: **Data Collection and Preprocessing:** Continue collecting the required information with respect to the feedback ratings on cloud services of CSC within a given continuous time window z. According to the time stamp of the feedback rating and the given time slice Δt, normalize the required information regarding feedback ratings into the form of multi-tuple $(C_{id}, S_{id}, S_{id}(A_{id}), F, \Delta t)$. Develop a data repository Θ with each multi-tuple as a record stored in it.

2: **Weight Factor Assignment:** For a given time window Δt_k, the identity of CSC is used as keyword to retrieve its feedback rating information (e.g., multi-tuple) in Θ. The credibility γ and certainty λ weight factors of each CSC can be obtained according to the calculation approaches proposed in the ReTA process.

3: **Local Objective Reputation:** Based on the credibility and certainty of each CSC that has been obtained, and combined with their feedback ratings, the LOR of a cloud service given by each CSC can be calculated within the time window Δt_k. The LOR $L_{(S_i)}$ for each cloud service can be obtained by aggregating the feedback rating of each CSC.

4: **Global Objective Reputation:** According to the given time window Δt_k, the corresponding time attenuation weighting factor assigned to the LOR of each cloud serive can be determined. The GOR $G_{(S_i)}$ for each cloud service can be obtained by aggregating time-based weighted LOR within each time window Δt_k.

rating of CSC C_j on cloud service S_i; Let $\gamma_j^{\Delta t_k}$ denotes the credibility weight factor of CSC C_j within the k^{th} time window; The credibility weight factor of the CSC C_j is define as follows.

$$\gamma_j^{\Delta t_k} = 1 - \frac{\sqrt{\frac{\sum_{|\omega_{C_j}|}(f_{ij} - E_{\omega_{C_j}})^2}{|\omega_{C_j}|}}}{|\psi_{S_i}|} \tag{8}$$

where f_{ij} depends on the number p of feedback ratings offered by the CSC C_j on the service $S_i\,(S_i \in \omega_{C_j})$, which can be obtained by the Equation (9).

$$f_{ij} = \begin{cases} F_{ij}, & p = 1 \\ \dfrac{\sum_{q=1}^{p} F_{ij}^q}{p}, & p > 1 \end{cases} \tag{9}$$

$E_{\omega_{C_j}}$ denotes the average of feedback ratings offered by the other CSCs (i.e., all CSCs except C_j) on the service ω_{C_j}, which can be obtained by the Equation (10).

$$E_{\omega_{C_j}} = \frac{1}{|U_{ij}|} \times \sum_{U_{ij} \in \psi_{S_i}} f_{ij} \tag{10}$$

where U_{ij} denotes the other CSCs (except C_j) invoking the service $S_i\,(S_i \in \omega_{C_j})$.

For the certainty weight factor, we can describe it in detail with the following definition.

Definition 3: For a given time window Δt_k, let d_{ij} denotes the number of feedback ratings offered by a CSC C_j on a service $S_i\,(S_i \in \omega_{C_j})$; Let $|D_i|$ denotes the total number of feedback ratings received by the service S_i; Let $\lambda_j^{\Delta t_k}$ denotes the certainty weight factor of CSC C_j within the k^{th} time window. We define the $\lambda_j^{\Delta t_k}$ as follows.

$$\lambda_j^{\Delta t_k} = 1 - \frac{d_{ij} - E(|D_i|)}{|D_i|} \tag{11}$$

where $E(|D_i|)$ denotes the average of feedback ratings number received by the service S_i, which can be obtained by Equation (12).

$$E(|D_i|) = \frac{\sum_{j=1}^{|J|}(d_{ij} - \epsilon)}{|J|} \tag{12}$$

where ϵ denotes the valid threshold of the number of feedback ratings offered by a CSC on a service. In other words, a CSC can only provide ϵ feedback ratings to a service within a specific time window, and the excess will be discarded. $|J|$ denotes the number of CSCs offering feedback ratings to service $S_i\,(S_i \in \omega_{C_j})$.

According to definition 2 and definition 3, we can obtain the weight factors (i.e., credibility and certainty) of all CSCs who invoked a service S_i within a k^{th} time window. We denote the credibility and certainty as $\Gamma(\Delta t_k) = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ and $\Lambda(\Delta t_k) = \{\lambda_1, \lambda_2, \cdots, \lambda_n\}$, respectively. At the same time, the feedback ratings F_{ij} of CSCs on the service S_i are generalize as $F(\Delta t_k) = \{F_{i1}, F_{i2}, \cdots, F_{in}\}$. Therefore, the Equation (7) can be revamped as follows.

$$L_{S_i}(\Delta t_k) = \boldsymbol{F}(\Delta t_k) \times \boldsymbol{\Gamma}(\Delta t_k) \times \boldsymbol{\Lambda}(\Delta t_k) \tag{13}$$

3) GLOBAL OBJECTIVE REPUTATION

In the previous two stages, the LORs, representing the reputation level of each cloud service in each time window, have been obtained. In this stage, the global objective reputation (GOR) which denote the reputation level of each cloud service within an evaluation time period can be obtained by aggregating the LOR of each cloud service with time-based weights. Therefore, GOR can be described in detail with the following definition.

Definition 4: For a given consecutive time window z, let $\Upsilon = \{\upsilon_1, \upsilon_2, \cdots, \upsilon_z\}$ denote a time-based weight assigned to the LOR of a service S_i within different time windows $L_{S_i}(\Delta t_k)\,(k \in [1, z])$. Let $G_{S_i}(\Delta t_z)$ denote the GOR of service S_i within current time window Δt_z; The GOR of service S_i is

defined as follows.

$$G_{S_i}(\Delta t_z) = \sum_{k=1}^{z} (L_{S_i}(\Delta t_k) \times \upsilon_k) \tag{14}$$

where $\sum_{k=1}^{z} \upsilon_k = 1$ and $\upsilon_k \in [0, 1]$.

According to human social behavior habits, older knowledge has less impact, whereas new knowledge makes more contribution to trust decision making [44]. Thus, we can define the υ as a time-based attenuation function as follows.

$$\upsilon_k = \mu + (1 - \mu) \times \exp(-\tau \times (1 - \frac{k}{z})) \tag{15}$$

where $\mu \in [0, 1]$ is used to adjust the effect of the time-based attenuation function. $\tau \in [0, 1]$ is an adjustable positive constant, and can be tuned accordingly. For convenience of rank and comparison, the reputation level of each cloud service G_{S_i} can be normalized to the range [0,1] in a uniform fashion.

Algorithm 4 Local Objective Reputation

Input: time windows Δt, cloud service identity S_{id}, feedback ratings dataset Θ, size of dataset $|\Theta|$

procedure LOR Evaluation(Θ, $|\Theta|$, Δt, S_{id})
  $C_{size}, L \leftarrow 0$;
  $C_{size} \leftarrow$ GetCSCsSize (Θ, $|\Theta|$, Δt);
  Create arrays $\Gamma_{C_{size}}, \Lambda_{C_{size}}, F_{C_{size}} \leftarrow \emptyset$;
  $\Gamma, \Lambda \leftarrow$ WeightFactorAssignment (Θ, $|\Theta|$, Δt);
  $F \leftarrow$ CalWeightedFeedback(Θ, $|\Theta|$, Γ, Λ, Δt, S_{id});
  for $i = 0$ to C_{size} **do**
    $L = L + F[i]$;
  end for
  return L;
end procedure

Algorithm 3 illustrates the reputation-based trust assessment process. Algorithm 4 and 5 demonstrate the evaluation procedure of the LOR and GOR, respectively.

4) REPUTATION ASSESSMENT ANALYSIS

Feedback rating based reputation assessments are often subject to malicious attacks (e.g., self-promotional attack or slandering attack), that is, malicious CSCs often give unfaithful feedback ratings in various irregular ways to influence the outcome of the reputation evaluation. To address these problems, we propose credibility and certainty weight factors. The credibility weight factor used in the ReTA can mitigate the impact of collusion attacks on the reputation evaluation results by distinguishing abnormal feedback ratings from all feedback ratings. It reduces the credit of a CSC based on its abnormal feedback ratings. Furthermore, the certainty weight factor introduced in the ReTA can mitigate the impact of these attacks on the reputation evaluation results by filtering out the feedback ratings that exceeds a reasonable and valid threshold in a short period of time. The weight factors of credibility and certainty make the reputation evaluation based on feedback ratings better able to resist malicious attacks. They also make the results of ReTA more accurate and trustworthy.

Algorithm 5 Global Objective Reputation

Input: time windows z, feedback ratings dataset Θ of CSCs, size of dataset $|\Theta|$

procedure GOR Evaluation(Θ, $|\Theta|$, z)
  $S_{size} \leftarrow 0$;
  $S_{size} \leftarrow$ GetServicesNumber (Θ, $|\Theta|$);
  Create arrays $Sid_{S_{size}}, L_{S_{size} \times z}, \Upsilon_z, G_{S_{size}} \leftarrow \emptyset$;
  $SID \leftarrow$ GetServicesID (Θ, $|\Theta|$);
  for $i = 0$ to z **do**
    $\Upsilon[i] \leftarrow$ TimeWeightsAssignment (Δt_i);
    for $j = 0$ to S_{size} **do**
      $L[j][i] \leftarrow$ LocalObjectiveReputation(
      Θ, $|\Theta|$, Δt_i, $Sid[j]$);
    end for
  end for
  for $j = 0$ to S_{size} **do**
    $G[j] \leftarrow L[j] \times \Upsilon^T$;
  end for
  Normalize G into a unified range [0,1];
  return G;
end procedure

C. INTEGRATED TRUST ASSESSMENT

After the processes of SeTA and ReTA, the security level and reputation level of a cloud service can be obtained. Then, in the integrated trust assessment (InTA) process, the trust level of targeted cloud services can be obtained by integrating the security level and reputation level based on the objective weight assignment approach. In practice, the more important a resource or attribute in the cloud service, the more the number of security controls or security mechanisms will be enforced, namely more security metrics. For the same reason, the more resources or attributes a cloud service provide, the more competitive and reputable it is.

Inspired by this scenario, we employ objective weight assignment approach based on the actual situation to determine the relative importance weights of the security level and the reputation level obtained respectively from SeTA and ReTA. In other words, the relative importance weight of security level is determined by the ratio of its elements (i.e., security metrics) to the total number of elements involved in InTA. Similarly, the relative importance weight of reputation level is determined by the number of its elements (i.e., resources or attributes) involved in InTA. Furthermore, in order to make our trust evaluation methods applicable to different scenarios and datasets, we introduce a parameter φ to adjust the trade-off between SeTA and ReTA. Therefore, the relative importance weights of SeTA and ReTA can be determined by φ.

Definition 5: Suppose that S_i is a targeted cloud service to be evaluated, $M = \{m_1, m_2, \cdots, m_u\}$ are its security metrics, and $A = \{a_1, a_2, \cdots, a_v\}$ are its resources or attributes; Let U and V denote respectively the number of security metrics and attributes; Let α denotes the relative importance weight

TABLE 2. Excerpt of cloud-specific security metrics.

Cloud security controls derived from CSA, FedRAMP and IOS/IEC			CS_1	CS_2	CS_3	CS_4	CS_5	CS_6
Control Category	Control Name	Control ID						
System and Information Integrity	Information system Monitoring	SI-4	Ongoing	Ongoing	Weekly	Weekly	Ongoing	Weekly
	Flaw Remediation	SI-2c	Monthly	Monthly	Quarterly	Monthly	Quarterly	Monthly
		SI-2(2)	Monthly	Weekly	Monthly	Weekly	60 days	Monthly
	Security Functionality Verification	SI-6	Monthly	Monthly	Quarterly	Quarterly	Monthly	60 days
Physical and Environmental Protection	Access Records	PE-8b	60 days	Weekly	Monthly	Quarterly	Monthly	Weekly
	Monitoring Physical Access	PE-6b	Monthly	Monthly	Monthly	60 days	Quarterly	Quarterly
	Physical Access Control	PE-3f	Annually	Quarterly	Annually	Annually	Quarterly	Quarterly
		PE-3g	Annually	Quarterly	Annually	Annually	Quarterly	Annually
Audit Assurance & Compliance	Audit Planning	AAC-01	Yes	Yes	Yes	No	Yes	Yes
	Independent Audit	AAC-02.2	Yes	Yes	Yes	Yes	Yes	Yes
		AAC-02.7	Yes	Yes	Yes	Yes	Yes	Yes
		AAC-03.3	Yes	Yes	Yes	No	No	Yes
Datacenter Security	Asset Management	DCS-01.1	Yes	Yes	No	Yes	Yes	No
		DCS-01.2	Yes	Yes	Yes	No	No	Yes
	Equipment Identification	DCS-03.1	No	Yes	Yes	Yes	Yes	No
	Secure Area Authorization	DCS-07.1	Yes	Yes	Yes	Yes	Yes	Yes
Cloud Service Level Agreements	Service Availability	Cloud service downtime (hr)	3	1	5	8	6	2
	Service Reliability	Mean time to service recovery (hr)	1.5	0.5	1	2	2.5	3
		Number of service failures	100	80	120	70	130	150
		Retention period for backup data (day)	360	360	180	90	180	90

of SeTA. We define the α as follows.

$$\alpha = \frac{U \times \varphi}{U \times \varphi + V \times (1 - \varphi)} \tag{16}$$

where $\varphi \in [0, 1]$ is an adjustable positive constant, which can be tuned accordingly.

After that, we can calculate the trust level of the targeted cloud services according to their security level, reputation level and relative importance weight α.

Definition 6: Suppose that SL_i and RL_i denote the security level and reputation level of cloud service S_i; Let T_{S_i} denotes the trust level of cloud service S_i; We define the T_{S_i} as follows.

$$\mathrm{T}_{S_i} = \alpha \times SL_i + (1 - \alpha) \times RL_i \tag{17}$$

The introduction of parameter φ makes the trust assessment method more adaptable to different application scenarios, especially in reputation-based trust assessment model or system. For instance, in an application scenario that CSCs give feedback ratings on the service quality of holistic cloud service provided by a CSP rather than the resources or attributes of cloud service, the proposed reputation-based trust assessment methods can also work. In this scenario, the V, representing the number of resources or attributes of a cloud service in definition 5, denotes a cloud entity (i.e., the holistic service quality of a cloud service or a CSP) and its value is 1. This will lead to an overweighting of relative importance assigned to security level in InTA. Hence, to address this issue, the parameter φ is used as a regulatory factor to leverage the trade-off between SeTA and ReTA.

V. EXPERIMENTS AND RESULTS ANALYSIS

This section first introduces the setup of the experiments for the validation of the STRAF. Then, it conducts the experiments to validate the availability and performance of the STRAF and analyzes the experimental results.

A. EXPERIMENTAL SETUP

The experiments are conducted by using MATLAB R2017b and are performed on a DELL desktop computer with the following configuration: an Intel Core i5 2.7 GHz CPU, 8 GB RAM, and the Windows 10 operating system. There is currently no integrated and available dataset fit for the validation of the STRAF (the assessment framework), namely, that are available for both SeTA and ReTA. Therefore, we use a synthesized dataset that contains some security metrics and a real-world web service dataset to validate the methods of SeTA and ReTA, respectively.

The synthesized dataset comprises security metrics that were derived from the cloud SLAs of the ISO/IEC 19086 standards [36], [37], the CSA STAR repository [45] and the FedRAMP security control baseline [33]. We denote the dataset as SecData. SecData are utilized to validate the availability of SeTA, as shown in Table 2. Table 2 presents a sample dataset associated with the security metrics used for this scenario, wherein the values associated with 20 security metrics are presented. These security metrics comprise both qualitative (e.g., *Yes*/*No*, *weekly*, *monthly*, etc.) and quantitative (e.g., seconds, days, etc.) metrics. The *Yes*/*No* metrics are modeled as boolean 1/0, whereas metrics associated with the control frequency, such as *Ongoing*, *Weekly*, $\cdots$, *Annually* are modeled as 6, 5, $\cdots$, 1. In this scenario, we assume that 6 CSPs need to be evaluated. The quantified security metrics of CSPs are used to evaluate their security in SeTA.

The real-world web service dataset, namely, the WSDream dataset2 [46], can be obtained from its github website. It records the real-world QoS data from 142 users of 4,500 web services over 64 different time slices (with the step size of 15 minutes). Each service has two QoS attributes in the original dataset, namely, the response time (RT) and the throughput (TP). For objectivity and convenience, we randomly select 6 services within 10 different time slices and identify the feedback ratings from the top 100 users as the valid data. As a result, we obtain two smaller datasets that

respectively contains $6 \times 100 \times 10$ entries. To facilitate the integrated trust assessment, we assign these 6 services to the 6 CSPs selected in the SeTA as their cloud service. The two smaller QoS datasets (i.e., response time and throughput) are used to evaluate the reputation of the 6 CSPs in ReTA.

As aforementioned, the trustworthiness of CSP are determined by combining its security and reputation in InTA. The relative importance weight of SeTA and ReTA are determined by their respective number of metrics or attributes involved in InTA. In this scenario, we set $\varphi = 0.2$ according to the number of security metrics in SeTA and the number of attributes in ReTA to achieve the better effect. The settings of the parameters used in our experiments are given in Table 3.

TABLE 3. Parameter settings.

Method Name		SeTA	ReTA
Number of metrics		20	2
Data Type		Quantitative and Qualitative	Quantitative
Data Source		FedRAMP, CSA and ISO/IEC	WSDream
Parameters	ϵ	*N/A*	1
	μ	*N/A*	0.2
	τ	*N/A*	0.5
	φ	*N/A*	0.2
	α	0.29	0.71

B. AVAILABILITY VALIDATION

This section presents the experimental results based on the above datasets and parameter settings. For the purpose of validating the availability, we first implement the security assessment for the cloud services by employing the SeTA method with the SecData dataset. Then, we perform the reputation assessment for the cloud services by using the ReTA method with the WSDream dataset. Finally, we evaluate the trustworthiness of CSPs by applying the InTA method with the assessment results of SeTA and ReTA.

1) SeTA

To validate the availability of SeTA, we use the security metrics of TABLE 2 to evaluate the security of the 6 CSPs by implementing the SeTA method. We can obtain the separation measures and relative closeness of each CSP according to Equations (1)-(6) and SecData, as shown in Figure 4. Figure 4 shows that the separation measures, namely, D^+ and D^-, respectively denote the distance from its security metric to the positive and negative security metrics. The relative closeness, namely, C, represents the security level of CSPs. We can observe that CSP_2 is the CSP that best satisfies the security metrics, followed by CSP_1, CSP_5, CSP_3, CSP_6 and CSP_4 respectively.

2) ReTA

For the availability validation of ReTA, we employ the QoS datasets extracted from the WSDream dataset2 to evaluate the reputation of the 6 CSPs by implementing the ReTA method.

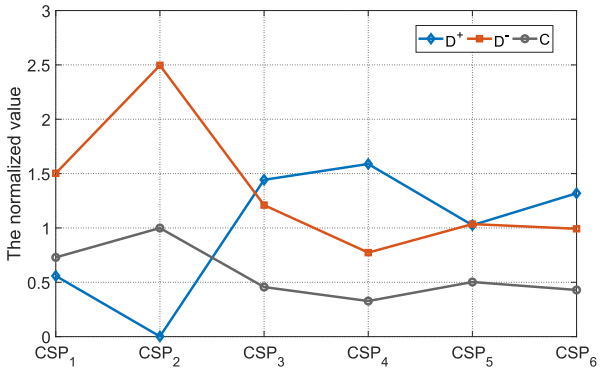


FIGURE 4. The security evaluation results of SeTA.

For the response time attribute of a service, we can obtain the LOR of a CSP according to Equations (7)-(13), as shown in Figure 5.

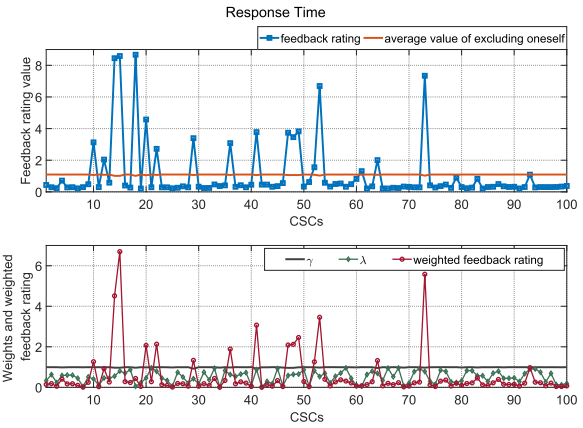


FIGURE 5. The feedback ratings and weight factors of CSCs on the response time of a service within a unit time window.

The top subgraph of Figure 5 shows the feedback ratings of CSCs and the average value of the feedback ratings excluding the CSCs itself within a unit time window, where the x-axis represents the CSC and the y-axis represents the related parameter value. The bottom subgraph of Figure 5 shows the credibility and certainty weighting factors of CSCs and their weighted feedback ratings. From Figure 5, we can observe that the feedback ratings of CSCs are proportional to their weights. The bigger the weight is, the bigger the feedback rating, and vice versa. In other words, the feedback ratings of CSCs are affected by their credibility and certainty weights. Since this method can effectively reduce the impacts of malicious CSCs on the feedback ratings of a service attribute, the weighted feedback ratings of CSCs on a service are more reasonable. Similarly, we can obtain the feedback ratings of CSCs on the throughput attribute of the service, as shown in Figure 6.

After obtaining the LOR of each CSP, the GOR of CSPs can be calculated by aggregating their LORs with the time-based weights. In our experiment, we assume that

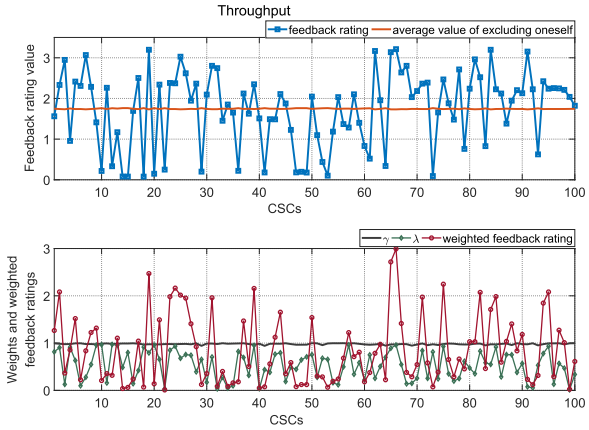


FIGURE 6. The feedback ratings and weight factors of CSCs on the throughput of a service within a unit time window.

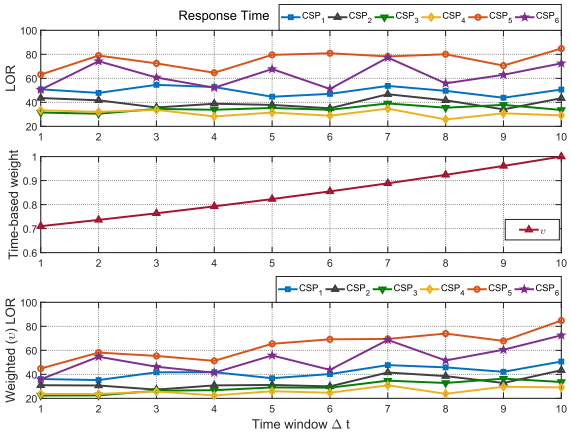


FIGURE 7. The time-based weight and weighted LOR of CSPs on the response time of a service within 10 unit time window.

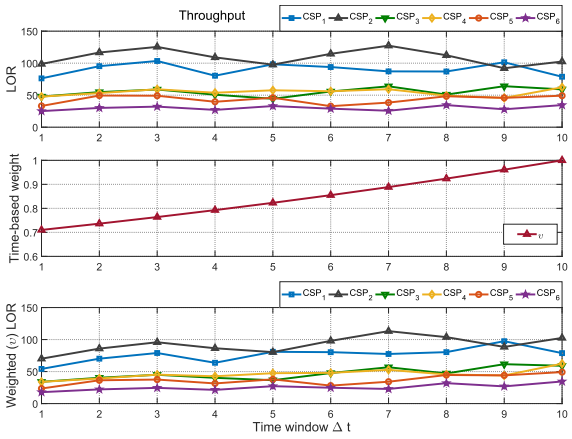


FIGURE 8. The time-based weight and weighted LOR of CSPs on the throughput of a service within 10 unit time window.

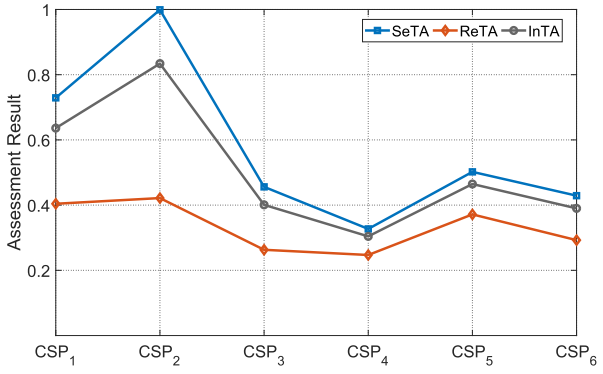


FIGURE 9. The assessment results of SeTA, ReTA and InTA.

10 time windows are selected to calculate the GOR of CSPs. For the response time attribute, we can obtain the GOR of each CSP according to Equations (14) and (15), as shown in Figure 7, where the x-axis represents the time window Δt.

The top subgraph of Figure 7 shows the LOR of each CSP. The center subgraph of Figure 7 shows the time- based weight. The bottom subgraph of Figure 7 shows the weighted LOR of each CSP. From this figure, we can observe that the larger the time window is, the larger the weighted LOR of the CSP. In other words, the closer the time to perform the assessment, the higher the reliability of the LOR. After that, we can obtain the GOR of each CSP by aggregating its weighted LOR. In the same way, the weighted LOR of the throughput attribute of CSPs can be obtained, as shown in Figure 8.

3) InTA

The trust level of each CSP can be obtained by combining the security level and reputation level, which have been calculated in SeTA and ReTA, respectively. The GORs of all attributes of a CSP need to be normalized and aggregated as an integrated value before calculating its trustworthiness. According to Equations (16) and (17), we can obtain the relative importance weights of SeTA and ReTA and then calculate the trustworthiness of each CSP, as shown in Figure 9. Figure 9 shows the security, reputation and trustworthiness of the CSPs respectively obtained from the SeTA, ReTA and InTA. From this figure, we can observe that CSP_3 has a higher security level than CSP_6, while CSP_6 has a higher reputation level than CSP_3. From the perspective of trust assessment, CSP_3 has higher trust level than CSP_6. This is because we set the relative importance weight of SeTA higher than that of ReTA in this experiment. In practice, the relative importance weights can be adjusted to find the best effect based on the requirements of actual business or CSCs. As shown in this figure, CSP_2 is more trustworthy than the others.

C. PERFORMANCE VALIDATION

This section presents the experimental results for validating the performance. Since there is no trust assessment method combining security and reputation, we respectively compare some existing security assessment methods and reputation assessment methods with our trust assessment methods (SeTA and ReTA).

1) SeTA

For the performance comparison, we analyze the time complexity of several other security assessment methods in terms of the operations in their algorithms. The comparative methods are described as follows.

- Cloud security evaluation method based on quantitative hierarchy process (denoted as QHP) [42]. The QHP method is an assessment technique that evaluate different CSPs based on the various security specifications with respect to user's security requirements by applying the AHP-based quantitative evaluation method.
- A methodology for performance quantification and the evaluation of cloud security services based on a set of quantitative evaluation metrics [27]. These metrics are developed by using the Goal-Question-Metric (denoted as GQM) paradigm.
- A broker-based cooperative security-SLA evaluation methodology (denoted as BCSE) for personal cloud computing [47]. To address the issues of the quantitative measurement of security metrics, the BCSE uses a multi-dimensional approach and a cooperative model to acquire a set of general indicators based on cloud brokers.

To compare SeTA with the other methods based on time complexity, we set the number of CSPs to 150 (refer to the number of cloud service providers authorized by FedRAMP [33]) and the number of security metrics to 300 (refer to the number of security controls in CSA CAIQ [45]). In addition, 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 30 and the number of security metrics from 1 to 300 with a step of 60. We simulate that the time complexity of the comparative methods increase with the number of CSPs and the number of security metrics, as shown in Figure 10.

Figure 10 (a) shows that the time complexity (operations) of the comparative methods increases with the number of security metrics when the number of CSPs is constant. Figure 10 (b) shows that the time complexity of the comparative methods increases with the number of CSPs when the number of security metrics is constant. We can observe from this figure that our method outperforms the other methods in both cases, that is, SeTA has the minimum time complexity among the comparative methods. With the increase of the number of CSPs or security metrics, the time complexity of both QHP and BCSE increase significantly. This is due to the high complexity of the weight assignment and evaluation algorithms. The reason for the low time complexity of the GQM is its simple weight assignment approach. Since there is no weight assignment process in SeTA and the evaluation approach of SeTA is concise, it has little impact on the SeTA method. It suggests that our method is effective and outperforms the other methods.

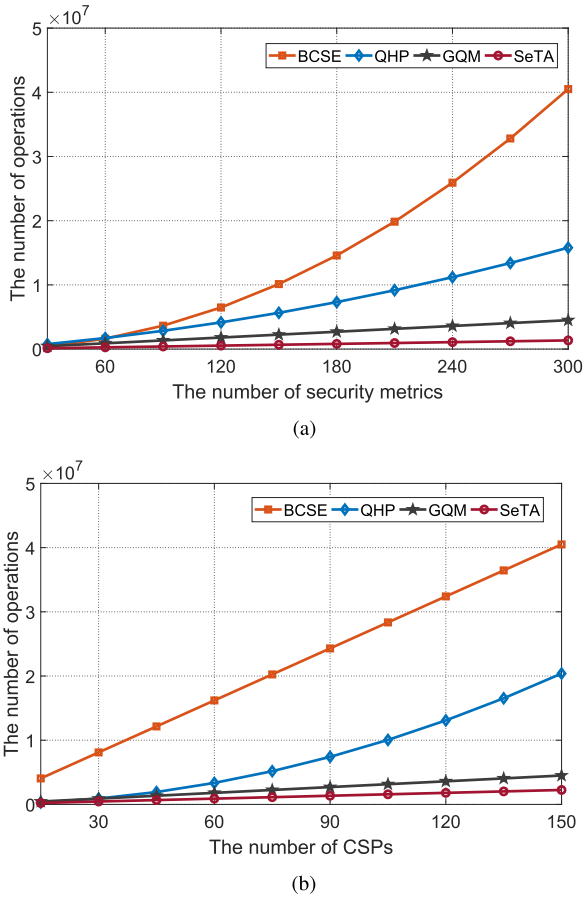


FIGURE 10. Performance comparison between SeTA and some other methods. (a) Time complexity varies with the number of security metrics. (b) Time complexity varies with the number of CSPs.

2) ReTA

For the performance comparison, we compare several other reputation evaluation methods with ReTA. The comparative methods are described as follows:

- Reputation method based on averaging the rating scores (denoted as ReA) [48]. This method calculates the reputation for each service by averaging the ratings for the services from the invoking users and then recommends services with higher reputations.
- An unfair rating filtering method based on reputation revisions (denoted as ReM) [17]. This method uses prior knowledge as the basis of similarity when calculating the average ratings, which facilitates the recognition and filtering of unfair ratings.
- A reputation computation approach for measuring the reputation of Web services (denoted as ReC) [49]. The approach uses three phases to measure and compute the reputation of service and improves the computational accuracy of reputation.

To implement the comparison experiment, we select the feedback ratings of 100 CSCs on the throughput within a unit time window from the dataset mentioned in ReTA. These feedback ratings are used to evaluate reputation by

employing these comparative methods. We vary the percentage of malicious feedback ratings from 0% to 25% with a step size of 5% and observe the impacts on and changes in reputation. Furthermore, we normalize the reputation obtained by these comparative methods.

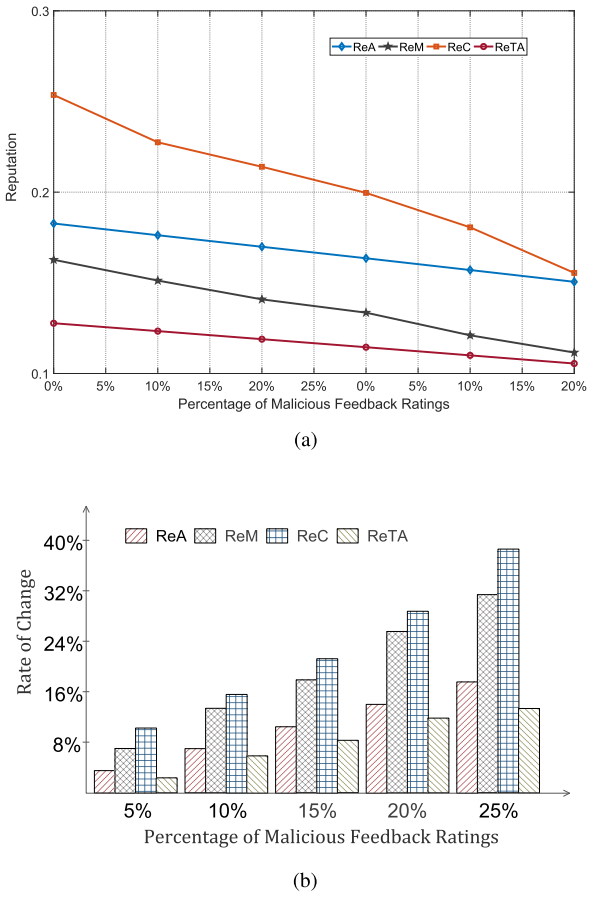


FIGURE 11. The impact of malicious feedback ratings on reputation evaluation. (a) The reputation evaluation results of comparative methods. (b) The rate of change on reputation evaluation results.

Figure 11 shows the reputation and the rate of change of the comparative methods with different percentages of malicious feedback ratings, respectively. From this figure, we can observe that as the percentage of malicious feedback ratings increases, the reputation of all the comparative methods decrease, as shown in Figure 11 (a). However, the rate of change of the reputation for each method is different. As can be seen from Figure 11 (b), the ReC method has the highest rate of change, that is, its reputation is most vulnerable to malicious feedback ratings, and it is followed by ReM, ReA and ReTA, respectively. This demonstrates that our method outperforms the other methods, especially when the percentage of malicious feedback ratings increases.

As anticipated, the above experimental results indicate that the STRAF combining the security-based trust assessment method and the reputation-based trust assessment method is indeed helpful in improving the trust assessment of cloud services.

VI. CONCLUSIONS

In this paper, we propose a novel trust assessment framework for cloud services (named STRAF) that combines its security and reputation characters. This framework has the ability to enhance the security of the cloud-based IoT context through trustworthy cloud services. It also facilitates CSCs in assessing the trustworthiness of the cloud services provided by the functionally equivalent CSPs and selecting the most trustworthy one from them to on which to deploy the cloud service. It is worth noting that the advantage of the STRAF is that it takes into account both security and reputation as complementary features to evaluate trustworthiness of cloud services and accordingly obtain the quantitative trustworthiness of cloud services. Additionally, in order to incorporate the security metrics in the trust assessment, we present a security-based trust assessment method (namely, SeTA). In addition, for the improvement of the accuracy and reliability of the feedback rating-based reputation assessment model, we present a reputation-based trust assessment method (namely, ReTA). Furthermore, for the sake of the potent combination of SeTA and ReTA, an integrated trust assessment method (namely, InTA) is proposed to assess the overall trustworthiness of cloud services. Simulation-based experiments validated the performance and availability of our proposed methods.

As future work, We aim to build a working prototype for our proposed trust assessment framework and implement the proposed trust assessment methods in a practical cloud environment.

REFERENCES

[1] S. K. Lee, M. Bae, and H. Kim, "Future of IoT networks: A survey," *Appl. Sci.*, vol. 7, no. 10, p. 1072, 2017.

[2] W. Li *et al.*, "System modelling and performance evaluation of a three-tier Cloud of Things," *Future Gener. Comput. Syst.*, vol. 70, pp. 104–125, May 2017.

[3] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.

[4] N. Zhang *et al.*, "Software defined networking enabled wireless network virtualization: Challenges and solutions," *IEEE Netw.*, vol. 31, no. 5, pp. 42–49, May 2017.

[5] 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 Netw.*, 2018, doi: 10.1109/MNET.2018.1700392.

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

[7] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.

[8] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[9] D. Chen *et al.*, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017.

[10] Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, "LACS: A lightweight label-based access control scheme in IoT-based 5G caching context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.

[11] 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.

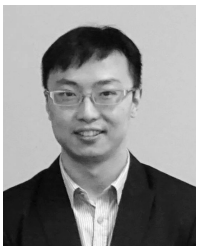
[12] Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang, "QoS ranking prediction for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1213–1222, Jun. 2013.
[13] H. Ma, Z. Hu, K. Li, and H. Zhang, "Toward trustworthy cloud service selection: A time-aware approach using interval neutrosophic set," *J. Parallel Distrib. Comput.*, vol. 96, pp. 75–94, Oct. 2016.
[14] T. Halabi and M. Bellaiche, "Towards quantification and evaluation of security of cloud service providers," *J. Inf. Secur. Appl.*, vol. 33, pp. 55–65, Apr. 2017.
[15] S. Singh and J. Sidhu, "Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers," *Future Gener. Comput. Syst.*, vol. 67, pp. 109–132, Feb. 2017.
[16] T. H. Noor, Q. Z. Sheng, and A. Alfazi, "Reputation attacks detection for effective trust assessment among cloud services," in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Jul. 2013, pp. 469–476.
[17] Q. Wu, X. Zhang, M. Zhang, Y. Lou, R. Zheng, and W. Wei, "Reputation revision method for selecting cloud services based on prior knowledge and a market mechanism," *Sci. World J.*, vol. 2014, Feb. 2014, Art. no. 617087.
[18] S. Wang, L. Sun, Q. Sun, J. Wei, and F. Yang, "Reputation measurement of cloud services based on unstable feedback ratings," *Int. J. Web Grid Services*, vol. 11, no. 4, pp. 362–376, 2015.
[19] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustdar, and A. H. H. Ngu, "CloudArmor: Supporting reputation-based trust management for cloud services," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 367–380, Feb. 2016.
[20] 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," *Knowl.-Based Syst.*, vol. 56, pp. 216–225, Jan. 2014.
[21] 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," *Appl. Math. Inf. Sci.*, vol. 7, no. 1L, pp. 121–129, 2013.
[22] N. Somu, M. R. Gauthama Raman, K. Kirthivasan, and V. S. Shankar Sriram, "A trust centric optimal service ranking approach for cloud service selection," *Future Gener. Comput. Syst.*, vol. 86, pp. 234–252, Sep. 2018.
[23] Y. Yang, X. Peng, and D. Fu, "A framework of cloud service selection based on trust mechanism," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 25, no. 3, pp. 109–119, 2017.
[24] J. Sidhu and S. Singh, "Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers," *J. Grid Comput.*, vol. 15, no. 1, pp. 81–105, 2017.
[25] R. Nagarajan, R. Thirunavukarasu, and S. Shanmugam, "A fuzzy-based intelligent cloud broker with MapReduce framework to evaluate the trust level of cloud services using customer feedback," *Int. J. Fuzzy Syst.*, vol. 20, no. 1, pp. 339–347, 2018.
[26] S. Siadat, A. M. Rahmani, and H. Navid, "Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model," *J. Supercomput.*, vol. 73, no. 6, pp. 2682–2704, 2017.
[27] M. Tang, X. Dai, J. Liu, and J. Chen, "Towards a trust evaluation middleware for cloud service selection," *Future Gener. Comput. Syst.*, vol. 74, pp. 302–312, Sep. 2017.
[28] P. Varalakshmi and T. Judgi, "Multifaceted trust management framework based on a trust level agreement in a collaborative cloud," *Comput. Elect. Eng.*, vol. 59, pp. 110–125, Apr. 2017.
[29] H. Kim, "Enhancing trusted cloud computing platform for infrastructure as a service," *Adv. Elect. Comput. Eng.*, vol. 17, no. 1, pp. 9–14, 2017.
[30] A. Mohsenzadeh, H. Motameni, and M. J. Er, "A new trust evaluation algorithm between cloud entities based on fuzzy mathematics," *Int. J. Fuzzy Syst.*, vol. 18, no. 4, pp. 659–672, 2016.
[31] X. Li, J. He, B. Zhao, J. Fang, Y. Zhang, and H. Liang, "A method for trust quantification in cloud computing environments," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 2, p. 5052614, 2016.
[32] Cloud Security Alliance. (2015). *Cloud Controls Matrix v3*. [Online]. Available: https://cloudsecurityalliance.org/research/ccm/
[33] *Continuous Monitoring Strategy Guide, Version 3.2*, Federal Risk and Authorization Management Program, Apr. 2018.
[34] *Cloud Computing Service Metrics Description*, Standard, National Institute of Standards and Technology, Special Publication 500-307, Apr. 2018.
[35] *Security and Privacy Controls for Federal Information Systems and Organizations*, Standard, National Institute of Standards and Technology, Special Publication 800-53, Apr. 2013.
[36] *Information Technology-Cloud Computing-Service Level Agreement (SLA) Framework—Part 2: Metric Model*, Standard ISO/IEC DIS 19086-2, International Organization for Standardization and International Electrotechnical Commission, Oct. 2017.
[37] *Information Technology-Cloud Computing-Service Level Agreement (SLA) Framework—Part 3: Core Conformance Requirements*, Standard ISO/IEC DIS 19086-2, International Organization for Standardization and International Electrotechnical Commission, Oct. 2016.
[38] J. Siegel and J. Perdue, "Cloud services measures for global use: The service measurement index (SMI)," in *Proc. Annu. SRII Global Conf.*, San Jose, CA, USA, 2012, pp. 411–415.
[39] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," *ACM Comput. Surv.*, vol. 42, no. 1, 2009, Art. no. 1.
[40] P. Chandrasekaran and B. Esfandiari, "A model for a testbed for evaluating reputation systems," in *Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Nov. 2011, pp. 296–303.
[41] X. Li, X. Jin, Q. Wang, M. Cao, and X. Chen, "SCCAF: A secure and compliant continuous assessment framework in cloud-based IoT context," *Wireless Commun. Mobile Comput.*, vol. 2018, Oct. 2018, Art. no. 3078272.
[42] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative reasoning about cloud security using service level agreements," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 457–471, Sep. 2017.
[43] M. Behzadian, S. K. Otaghsara, M. Yazdani, and J. Ignatius, "A state-of-the-art survey of TOPSIS applications," *Expert Syst. Appl.*, vol. 39, no. 17, pp. 13051–13069, 2012.
[44] X. Li, F. Zhou, and X. Yang, "A multi-dimensional trust evaluation model for large-scale P2P computing," *J. Parallel Distrib. Comput.*, vol. 71, no. 6, pp. 837–847, 2011.
[45] Cloud Security Alliance. *Consensus Assessments Initiative*. Accessed: Oct. 2017. [Online]. Available: https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-0-1/
[46] Z. Zheng, Y. Zhang, and M. R. Lyu, "Investigating QoS of real-world Web services," *IEEE Trans. Services Comput.*, vol. 7, no. 1, pp. 32–39, Jan./Mar. 2014.
[47] S.-H. Na and E.-N. Huh, "A broker-based cooperative security-SLA evaluation methodology for personal cloud computing," *Secur. Commun. Netw.*, vol. 8, no. 7, pp. 1318–1331, 2015.
[48] 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," *Appl. Math. Inf. Sci.*, vol. 7, no. 1L, pp. 121–129, 2013.
[49] S. Kumar and C. Nayak, "An approach to detect malicious feedback rating for measuring Web service reputation," *Int. J. Grid Distrib. Comput.*, vol. 9, no. 3, pp. 109–116, 2016.

XIANG LI received the B.S. degree from Hainan University, in 2009, and the M.S. degree from the Chongqing University of Posts and Telecommunications, in 2012. He is currently pursuing the Ph.D. degree with the College of Computer Science, Sichuan University. His research interests include both theoretical and experimental and are focused on automated security assessment methodologies of design and evaluate cloud-based systems, quantification and monitoring of security metrics, and enforcing security in cloud environments.

QIXU WANG received the B.Sc. degree from the Southwest University of Science and Technology, in 2009, and the Ph.D. degree in computer science and technology from the University of Electronic Science and Technology of China, in 2017. He is currently an Assistant Researcher with the College of Cybersecurity, Sichuan University. His current research interests include cloud computing security, wireless network security, trusted computing, and data privacy protection.

XIAO LAN received the Ph.D. degree from the Institute of Information Engineering, Chinese Academy of Sciences, in 2018. She is currently an Assistant Researcher with the Cybersecurity Research Institute, Sichuan University. Her research interests include applied cryptography, authenticated key exchange protocol, and blockchain.

XINGSHU CHEN received the Ph.D. degree from Sichuan University, in 2004. She is currently a Professor with the College of Computer Science, Cyber-Security Research Institute, Sichuan University. Her research interests include cloud computing, cloud security, distributed file system, big data processing, network protocol analysis, and new media supervision. She is also a member of the China Information Security Standardization Technical Committee.



NING ZHANG (M'15) received the B.Sc. degree from Beijing Jiaotong University, Beijing, China, in 2007, the M.Sc. degree from the Beijing University of Posts and Telecommunications, Beijing, in 2010, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2015. He was a Postdoctoral Fellow with the University of Waterloo and the University of Toronto. He is currently an Assistant Professor with Texas A&M University-Corpus Christi, Corpus Christi, TX, USA. His current research interests include physical layer security, dynamic spectrum access, 5G, and vehicular networks.

DAJIANG CHEN (M'15) received the B.Sc. degree from Neijiang Normal University, in 2005, the M.Sc. degree from Sichuan University, in 2009, and the Ph.D. degree in information and communication engineering from the University of Electronic Science and Technology of China (UESTC), in 2014. He was a Postdoctoral Fellow with the School of Information and Software Engineering, UESTC, from 2014 to 2017, and the University of Waterloo, Waterloo, ON, Canada, from 2015 to 2017. He is currently an Assistant Professor with the School of Information and Software Engineering, UESTC. His current research interests include information theory, secure channel coding, and their applications in wireless network security, wireless communications, and other related areas. He has serves/served as a Technical Program Committee Member for the IEEE Globecom, the IEEE VTC, the IEEE WPMC, and the IEEE WF-5G.