# Evaluating Cloud Users' Credibility of Providing Subjective Assessment or Objective Assessment for Cloud Services

Lie Qu[1], Yan Wang[1], Mehmet Orgun[1], Duncan S. Wong[2],
and Athman Bouguettaya[3]

[1] Macquarie University, Sydney, Australia
{lie.qu,yan.wang,mehmet.orgun}@mq.edu.au
[2] City University of Hong Kong, Hong Kong, China
duncan@cityu.edu.hk
[3] RMIT University, Melbourne, Australia
athman.bouguettaya@rmit.edu.au

**Abstract.** This paper proposes a novel model for evaluating cloud users' credibility of providing subjective assessment or objective assessment for cloud services. In contrast to prior studies, cloud users in our model are divided into two classes, i.e., ordinary cloud consumers providing subjective assessments and professional testing parties providing objective assessments. By analyzing and comparing subjective assessments and objective assessments of cloud services, our proposed model can not only effectively evaluate the trustworthiness of cloud consumers and reputations of testing parties on how truthfully they assess cloud services, but also resist user collusion to some extent. The experimental results demonstrate that our model significantly outperforms existing work in both the evaluation of users' credibility and the resistance of user collusion.

## 1 Introduction

Due to the diversity and complexity of cloud services, the selection of the most suitable cloud services has become a major concern for potential cloud consumers. In general, there are three types of approaches which can be adopted to conduct cloud service evaluation prior to cloud service selection. The first type is based on cloud users' subjective assessment extracted from their subjective ratings [5]. The second type is based on objective assessment via cloud performance monitoring and benchmark testing [10] provided by professional organizations, such as CloudSleuth[1]. The third type is based on the comparison and aggregation of both subjective assessment and objective assessment [7,8].

Whichever type of approaches are adopted, the credibility of cloud users providing assessments has a strong influence on the effectiveness of cloud service selection. In cloud environments, cloud users can be generally classified into two classes according to the different purposes of consuming cloud services. The first class comprises ordinary cloud consumers whose purpose is to consume a

[1] www.cloudsleuth.net

X. Franch et al. (Eds.): ICSOC 2014, LNCS 8831, pp. 453–461, 2014.

cloud service having high quality performance and spend as little money as possible. They usually offer subjective assessment of cloud services through user feedback. The second class comprises professional cloud performance monitoring and testing parties whose purpose is to offer objective assessment of cloud services to potential cloud consumers for helping them select the most suitable cloud services. To the best of our knowledge, there are no prior approaches in the literature, which can effectively evaluate the credibility of both types of cloud users in cloud service evaluation.

In this paper, we propose a novel model for evaluating cloud users' credibility of providing subjective assessment or objective assessment, where subjective assessment is from ordinary cloud consumers (called Ordinary Consumers, $OC$ for short), and objective assessment is from professional cloud performance monitoring and testing parties (called Testing Parties, $TP$ for short). The credibility of $OC$s and $TP$s providing subjective assessment or objective assessment is respectively represented by *trustworthiness* of $OC$s and *reputations* of $TP$s. For an $OC$, an authority center computes the *relative trustworthiness* of the other $OC$s who consume the same cloud services as the $OC$. Relative trustworthiness represents other $OC$s' trustworthiness from the $OC$'s prospect. The relative trustworthiness can also be affected by the difference of variation trend between the other $OC$'s subjective assessments and $TP$s' objective assessments over time. Then, the authority center selects the $OC$s who are considered trustworthy enough by the $OC$ as his/her virtual neighbors according to all the relative trustworthiness values. The neighborhood relationships of all the $OC$s form a social network. The global trustworthiness of an $OC$ on how truthful he/she provides subjective assessment is computed based on the number of $OC$s who select him/her as their virtual neighbor.

In the meantime, the reputation of a $TP$ on providing truthful objective assessment is modeled in a different way based on the difference among the $TP$'s objective assessments, the majority of objective assessments from other $TP$s and the majority of subjective assessments from $OC$s. That implies that the trustworthiness of $OC$s and the reputations of $TP$s can be influenced by each other. For this reason, our model can resist collusion among cloud users providing untruthful assessments to some extent. Through our model, a successful collusion attack would become very difficult in practice since a large number of cloud users would have to be involved in such collusion. In contrast to the existing user credibility evaluation model which is based on subjective ratings only, our experimental results show that our model can significantly improve the accuracy of evaluating user credibility, and enhance the resistance capability of user collusion in cloud environments.

## 2 The Proposed Model

In this section, we first introduce the framework of our proposed model for evaluating cloud users' credibility, and then present the details of our model.

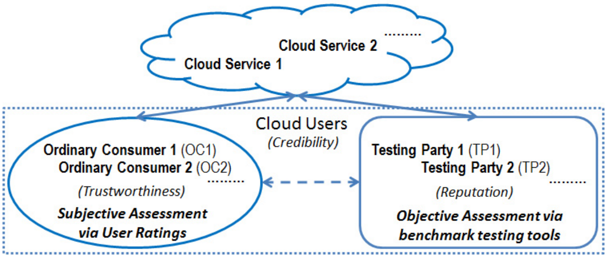


**Fig. 1.** The Framework of Our Model

### 2.1 The Framework

Fig. 1 illustrates the framework of our model consisting of two sub models, each of which targets one class of cloud users, i.e., $OC$s or $TP$s, respectively. In our framework, subjective assessments for cloud services are extracted from ratings submitted by ordinary consumers, and objective assessments are offered by testing parties using their own benchmark testing tools. After that, subjective assessments and objective assessments will be aggregated in the further cloud service selection process, e.g., the process specified in [7]. In our framework, there is an authority center which is in charge of managing assessments of cloud services and evaluating the trustworthiness and reputation of every $OC$ and $TP$. Without loss of generality, we focus on the situation, where both subjective assessments and objective assessments evaluate one performance aspect of cloud services. For example, the *response time* of a cloud service can be quantitatively tested by $TP$s. Meanwhile, an $OC$ consuming the same cloud service can also give his/her subjective ratings for the service response time by sensing how long the cloud responds to his/her requests. The situation of considering multiple performance aspects can be modeled based on multi-criteria decision-making, which will be the object in our future work. In addition, we assume that all assessments are given in similar circumstances.

### 2.2 The Sub Model for Computing Trustworthiness of $OC$s

The basic idea of evaluating trustworthiness of $OC$s in this sub model is that, an $OC$ is considered trustworthy to provide truthful subjective assessments if there are many other $OC$s or $TP$s whose subjective assessments or objective assessments are similar to his/hers. To this end, we improve Zhang *et al.*'s work [9], in which, an incentive mechanism is proposed based on modeling the credibility of both buyers and sellers for eliciting truthful ratings of sellers from buyers. Firstly, a series of multiple ratings commonly employed by most rating systems for cloud services are employed instead of binary ratings (i.e., "0" and "1") in Zhang *et al.*'s work to express $OC$s' subjective assessments. Secondly, in our model, the trustworthiness of an $OC$ can also be influenced by the reputations of $TP$s. If the variation trend of an $OC$'s subjective assessments over time is more similar to those of objective assessments from $TP$s having high reputations, the $OC$'s subjective assessments are considered more trustworthy. Finally, in our model, we apply the PageRank algorithm [6] to compute *global trustworthiness* of $OC$s

**Table 1.** A Multiple Fuzzy Rating System [7]

| Linguistic Ratings | Fuzzy Ratings | Crisp Ratings | Normalized Ratings ($r_i$) |
|---|---|---|---|
| Very low (VL) | $(0, 0, 0, 3)$ | 0.75 | 0 |
| Low (L) | $(0, 3, 3, 5)$ | 2.75 | 0.235 |
| Medium (M) | $(2, 5, 5, 8)$ | 5 | 0.5 |
| High (H) | $(5, 7, 7, 10)$ | 7.25 | 0.765 |
| Very High (VH) | $(7, 10, 10, 10)$ | 9.25 | 1 |

instead of Zhang *et al.*'s method. The experimental results demonstrate that our method is fairer than Zhang *et al.*'s.

**Distance Measurement between Multiple Ratings:** In this sub model, we apply the rating system defined in Table 1, which is frequently used in prior literature, such as [1,7], to express *OC*s' subjective assessments. In order to compare two ratings, we adopt the approach proposed by Li and Wang [2], which maps the *rating space* into a *trust space*, to measure the distance between two ratings. As shown in Table 1, fuzzy ratings are first converted into crisp ratings through the signed distance defuzzification method [1]. Then, the crisp ratings are normalized into the interval $[0, 1]$ according to their values. Due to space limitations, we omit the detailed procedure of mapping the rating space into the trust space. In short, a trust space for a service is defined as a triple $T = \{(t, d, u) | t \geqslant 0, d \geqslant 0, u \geqslant 0, t + d + u = 1\}$. Through Bayesian Inference and the calculation of *certainty* and *expected probability* based on a number of sample ratings, normalized ratings can be put into three intervals, i.e., for a normalized rating $r_i \in [0, 1]$, we have

$$r_i \text{ is } \begin{cases} \textit{distrust}, & \text{if } 0 \leqslant r_i \leqslant d; \\ \textit{uncertainty}, & \text{if } d < r_i < d + u; \\ \textit{trust}, & \text{if } d + u \leqslant r_i \leqslant 1. \end{cases}$$

A rating in the *distrust* range means the consumer who gave this rating deems that the service provider did not provide the service with committed quality, and we have a contrary conclusion when a rating is in the *trust* range. A rating in the *uncertainty* range means the consumer is not sure whether the service is provided with committed quality. Here, we call such a range a ***trust level***.

**The Trustworthiness of *OC*s:** The computation of the trustworthiness of an ordinary consumer $OC_A$ consists of two steps: in Step 1, the authority center computes all the other *OC*s' *relative trustworthiness* based on $OC_A$'s own experience, and selects a fixed number of top *OC*s according to the descending order of all their relative trustworthiness values, where these top *OC*s are considered as $OC_A$'s virtual neighbors. Here, relative trustworthiness represents other *OC*s' trustworthiness from $OC_A$'s prospect. In Step 2, all these neighborhood relationships form a virtual social network, based on which, the *global trustworthiness* of all *OC*s are computed.

The details of these two steps are provided below:

***Step 1. Computing Relative Trustworthiness of OCs:*** Suppose there are two ordinary consumers denoted as $OC$ and $OC'$, both of whom consume a group of cloud services, denoted as $\{s_1, s_2, \cdots, s_i, \cdots, s_l\}$. The relative trustworthiness of $OC'$ based on $OC$ is denoted as $RTr(OC \sim OC')$, where $OC \neq OC'$, and computed as follows:

$$\begin{aligned} RTr(OC \sim OC') = \overline{R_{TP}(OC')} \times \\ [\omega \times S_{pri}(OC \sim OC') + (1-\omega) \times S_{pub}(OC' \sim ALL)]. \end{aligned} \tag{1}$$

The details in Eq. (1) are introduced below:

**1.** $S_{pri}(OC \sim OC')$ **(private similarity between *OC* and *OC'*)**: All ratings for a service $s_i$ rated by $OC$ and $OC'$ are ordered into two rating sequences, denoted as $\overrightarrow{r_{OC,s_i}}$ and $\overrightarrow{r_{OC',s_i}}$ respectively, according to the time when the ratings are provided. The rating sequences are then partitioned in mutually exclusive time windows. The length of each time window may be fixed or determined by the frequency of the submitted ratings for $s_i$. Moreover, it should be considerably small so that the performance of $s_i$ can hardly change in a time window. After that, a pair of ratings $(r_{OC,s_i}, r_{OC',s_i})$, each of which is from its own rating sequence, is said *correspondent* only if they are given in the same time window. If there are more than one correspondent rating pairs in a time window, the most recent $r_{OC,s_i}$ and $r_{OC',s_i}$ are put together as the correspondent rating pair for this time window.

Let $N_{s_i}$ denote the total number of correspondent rating pairs for $s_i$ in all the time windows, then the total number of such pairs for all cloud services is computed as $N_{all} = \sum_{i=1}^{l} N_{s_i}$. If the two ratings of a correspondent rating pair are in the same trust level, such a pair is said *positive*, otherwise *negative*. Thus, if there are $N_p$ positive pairs, then the number of negative pairs is $N_{all} - N_p$. a positive correspondent rating pair means the ratings submitted by $OC$ and $OC'$ respectively in this time window are similar; A negative pair means quite different. In Eq. (1), $S_{pri}(OC \sim OC')$ is called the *private similarity* of $OC'$ which presents the similarity between the ratings provided by $OC$ and $OC'$, and computed as follows:

$$S_{pri}(OC \sim OC') = \frac{N_p}{N_{all}}. \tag{2}$$

**2.** $S_{pub}(OC' \sim ALL)$ **(public similarity between *OC'* and all other *OC*s)**: If there are insufficient correspondent rating pairs between $OC$ and $OC'$, $OC'$'s *public similarity*, denoted as $S_{pub}(OC' \sim ALL)$ in Eq. (1), should be calculated. The public similarity of $OC'$ depends on the similarity between his/her ratings and the majority of ratings submitted by the other $OC$s. In each time window, the most recent $r_{OC',s_i}$ and the average of the other ratings submitted by the other $OC$s for $s_i$ are put together as a correspondent rating pair, denoted as $(\overline{r_{s_i}}, r_{OC',s_i})$. Suppose the total number of such correspondent rating pairs for all cloud services is $N'_{all}$, where there are $N'_p$ positive pairs. The public similarity of $OC'$ is computed as follows:

$$S_{pub}(OC' \sim ALL) = \frac{N'_p}{N'_{all}}. \tag{3}$$

**3.** $\omega$ **(weight for private similarity)**: $\omega$ is the weight for how much the private similarity and the public similarity of $OC'$ can be trusted if there are insufficient correspondent rating pairs between $OC$ and $OC'$. Such a weight can be calculated based on the Chernoff Bound [4] as follows:

$$N_{min} = -\frac{1}{2\varepsilon^2} ln \frac{1-\gamma}{2}, \qquad \omega = \begin{cases} \frac{N_{all}}{N_{min}}, & \text{if } N_{all} < N_{min}; \\ 1, & \text{otherwise,} \end{cases} \tag{4}$$

where $\varepsilon$ is a small value (e.g., 0.1) representing a fixed maximal error bound which $OC$ can accept, and $\gamma \in (0, 1)$ is $OC$'s confidence level about his/her own subjective assessments.

**4.** $\overline{R_{TP}(OC')}$ **(average reputation of similar** ***TP*****s with** ***OC'*****)**: $\overline{R_{TP}(OC')}$ represents the weighted average of reputations of $TP$s, the variation trends of whose objective assessments over time are similar to that of $OC'$'s subjective assessments. Suppose there are $m$ $TP$s, denoted as $\{TP_1, TP_2, \cdots, TP_j, \cdots, TP_m\}$, providing objective assessments for the $l$ cloud services mentioned above. Following the time window partition method introduced above, we build *correspondent* assessment pairs between $OC'$'s subjective assessments and $TP_j$'s objective assessments for each cloud service, denoted as $(r_{OC',s_i}, oa_{TP_j,s_i})$, where $oa$ denotes the value of objective assessments. All $r_{OC',s_i}$ and $oa_{TP_j,s_i}$ are then put together to build two assessment sequences ordered by the time of every time window, denoted as $\overrightarrow{r_{OC',s_i}}$ and $\overrightarrow{oa_{TP_j,s_i}}$ respectively. After that, each assessment sequence is converted into a ranking sequence according to the assessment values. Suppose the converted ranking sequences for $\overrightarrow{r_{OC',s_i}}$ and $\overrightarrow{oa_{TP_j,s_i}}$ are $\overrightarrow{x_{OC',s_i}}$ and $\overrightarrow{y_{TP_j,s_i}}$ respectively. Then, the similarity, denoted as $\rho(OC' \sim TP_j, s_i)$, between these two ranking sequences are computed via Spearman's rank correlation coefficient [3] which is a common method to compute ranking similarity. Hence, the average similarity of assessment variation trends between $OC'$ and $TP_j$ for all cloud services can be computed as follows:

$$\rho(OC' \sim TP_j) = \frac{1}{l} \sum_{i=1}^{l} \rho(OC' \sim TP_j, s_i). \tag{5}$$

All the $TP$s with $\rho(OC' \sim TP_j) > 0$ are then selected as the $TP$s whose objective assessments are similar to $OC'$'s subjective assessments. Suppose there are $p$ such $TP$s for $OC'$, then the weighted average reputation of these $TP$s in Eq. (1) is computed as follows:

$$\overline{R_{TP}(OC')} = \frac{1}{p} (\sum_{q=1}^{p} \rho(OC' \sim TP_q) \times R_{TP_q}), \tag{6}$$

where $R_{TP_q}$ represents $TP_q$'s reputation on how truthfully its objective assessments are offered. The details of such reputations will be introduced later.

***Step 2. Computing Global Trustworthiness of OCs:*** Through Eq. (1), the authority center selects a fixed number of virtual neighbors for an $OC$ according to the descending order of all other $OC$s' relative trustworthiness values, and maintains a virtual social network according to all these neighborhood relationships. Then, we apply the PageRank algorithm [6] in our model. Given a directed graph of neighborhood relationship $G$, and an $OC$ is a vertex in $G$, then the *global trustworthiness* of the $OC$ denoted as $Tr(OC)$ is computed as follows:

$$Tr(OC) = \frac{1-d}{N} + d \sum_{OC_i \in G(OC)}^{G(OC)} Tr(OC_i), \tag{7}$$

where $G(OC)$ is the set of all vertices who select the $OC$ as their neighbor, $N$ is the total number of vertexes in $G$ and $d$ is a damping factor which is commonly set to 0.85 in the PageRank algorithm. In our model, $Tr(OC)$ is equivalent to the probability that a random $OC'$ selects the $OC$ as his/her neighbor.

### 2.3 The Sub-model for Computing Reputations of $TP$s

In the sub model for computing reputations of $TP$s, every $TP$ offers objective assessments for the same cloud performance aspect assessed by $OC$s. The reputation of a $TP$ depends on comparing its objective assessments to the majority of subjective assessments from $OC$s and the majority of objective assessments from other $TP$s. We assume that there exists a conversion function [7], through which the values of objective assessments can be converted into normalized ratings introduced in Table 1. Suppose that, for a cloud service $s_i$, there is a sequence of normalized ratings, which is ordered by time and denoted as $\overrightarrow{r_{TP_j,s_i}}$, corresponding to the sequence of objective assessment values provided by a testing party $TP_j$. Then, $\overrightarrow{r_{TP_j,s_i}}$ is partitioned in the same way of time window partition introduced in Section 2.2. In a time window, for $s_i$, there is one normalized objective rating $r_{TP_j,s_i}$ from $\overrightarrow{r_{TP_j,s_i}}$, some subjective normalized ratings from $OC$s and some objective normalized ratings from other $TP$s. Let $r_{\overline{TP},s_i}$ denote the average of the objective ratings for $s_i$ provided by all $TP$s except $TP_j$ in a time window, and $r_{\overline{OC},s_i}$ denote the average of the subjective ratings provided by all $OC$s of $s_i$ in a time window. In each time window, the authority center gives $TP_j$ a reputation payoff to judge its behaviors in the time window. The reputation payoff matrix is illustrated in Table 2, where "1" means that the two corresponding ratings in a rating pair are in the same trust level, "0" means in different trust levels, and $\varepsilon_a$, $\varepsilon_b$, $\varepsilon_c$ and $\varepsilon_d$ are the reputation payoffs.

In a time window, the reputation payoff that $TP_j$ can obtain depends on four cases as shown in Table 2:

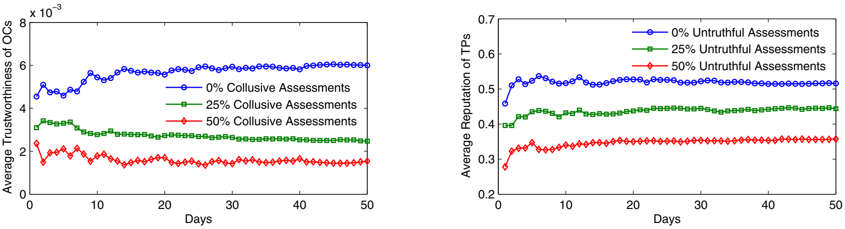
**Table 2.** Reputation Payoff Matrix

| Cases | Payoffs ($TP_j$) | $(r_{TP_j,s_i}, r_{\overline{TP},s_i})$ | $(r_{TP_j,s_i}, r_{\overline{OC},s_i})$ |
|---|---|---|---|
| 1 | $\varepsilon_a$ | 1 | 1 |
| 2 | $\varepsilon_b$ | 1 | 0 |
| 3 | $\varepsilon_c$ | 0 | 1 |
| 4 | $\varepsilon_d$ | 0 | 0 |

**Case** 1: If $r_{TP_j,s_i}$, $r_{\overline{TP},s_i}$ and $r_{\overline{OC},s_i}$ are all in the same trust level, which means a high probability of $TP_j$ providing truthful objective assessments of $s_i$.

**Cases** 2&3: If $(r_{TP_j,s_i}, r_{\overline{TP},s_i})$ or $(r_{TP_j,s_i}, r_{\overline{OC},s_i})$ is in the same trust level, but $(r_{TP_j,s_i}, r_{\overline{OC},s_i})$ or $(r_{TP_j,s_i}, r_{\overline{TP},s_i})$ is not, the probability of $TP_j$ providing truthful objective assessments should be lower than that in Case 1. Because objective assessments are usually considered more reliable than subjective assessments, the payoff in Case 2 should be higher than that in Case 3.

**Case** 4: If both $(r_{TP_j,s_i}, r_{\overline{TP},s_i})$ and $(r_{TP_j,s_i}, r_{\overline{OC},s_i})$ are all in the different trust levels, then $TP_j$ is penalized by giving the least reputation payoff. The reputation payoffs can be defined in the inequality: $\varepsilon_a > \varepsilon_b > \varepsilon_c > \varepsilon_d > 0$.



(a) The Trustworthiness of $OC$s (b) The Reputations of $TP$s

**Fig. 2.** Experimental Results with Collusion

Suppose that the total reputation payoffs that $TP_j$ obtains by assessing $s_i$ in the total $t$ time windows are denoted as $\xi_{TP_j,s_i}$, then the reputation of $TP_j$ based on $s_i$ and the reputation of $TP_j$ for all cloud services are computed as follows:

$$R_{TP_j,s_i} = \frac{\xi_{TP_j,s_i}}{t\varepsilon_a}, \qquad R_{TP_j} = \frac{1}{l}\sum_{i=1}^{l} R_{TP_j,s_i}. \tag{8}$$

## 3 Experimental Results

Because no suitable testing environment exists to evaluate our model, we simulate a cloud service environment based on our proposed framework. We collect the data of *response time* from CloudSleuth for 59 real cloud services. To the best of our knowledge, there is no data set of subjective assessments published for those 59 cloud services. Hence, we select 8 similar cloud services from these cloud services, and then simulate subjective assessments from 300 $OC$s and objective assessments from 36 $TP$s for the 8 cloud services. We simulate the assessment behavior of all the participants in the cloud environment for a period of 50 simulated days. The trustworthiness of every $OC$ and the reputation of every $TP$ are computed and recorded at the end of each day. In our model, a collusion attack refer to that some users colluding to provide similar untruthful (too high or too low) assessments for a cloud service in order to manipulate the cloud service's reputation, and collusive assessments refers to such similar untruthful assessments. We require that each $OC$ or $TP$ has his/her/its own percentage of providing randomly untruthful or collusive assessments.

In our experiments, all the $OC$s or $TP$s are divided into three groups. The $OC$s or $TP$s in each group provide different percentages of randomly untruthful or collusive assessments. We have conducted experiments in many different settings. The experimental results demonstrate that our model can effectively detect the $OC$s or $TP$s who/which provide randomly untruthful or collusive assessments. Due to space limitations, we only present the experimental results in Fig. 2 when some $OC$s provide collusive subjective assessments and some $TP$s provide randomly untruthful objective assessments. Fig. 2 demonstrates that the more collusive assessments/randomly untruthful assessments the $OC$s/$TP$s provide, the lower the trustworthiness of the $OC$s/the reputations of the $TP$s.

Next, we test the *tolerance* of our model, i.e, the maximum percentages of randomly untruthful or collusive assessments that our model can withstand to stay effective. We compare our model with Zhang *et al.*'s work [9] and the version of our model without $TP$s, i.e., only $OC$s' subjective assessments are used to compute their trustworthiness. The experimental results of *tolerance* in Table 3 shows that our model with/without $TP$s can achieve approximately 83%/43% improvement compared to Zhang *et al.*'s model in the case of providing randomly untruthful assessments, and 38%/14% in the case of providing collusive assessments.

**Table 3.** Randomly Untruthful or Collusive Assessment Tolerance of Different Models

| Models<br>Subjective Assessments | Zhang *et al.*'s model [9] | Our model without $TP$s | Our model with $TP$s |
|---|---|---|---|
| Untruthful Assessments | 30% | 43% | 55% |
| Collusive Assessments | 21% | 24% | 29% |

## 4 Conclusion

We propose a novel model for evaluating cloud users' credibility of providing subjective assessment or objective assessment for cloud services. Our model considers two different classes of cloud users (i.e., ordinary users and testing parties). The trustworthiness of *OC*s and the reputation of *TP*s are computed respectively to reflect how truthfully they provide subjective or objective assessments. Moreover, our model have the ability to resist user collusion to some extent. The experimental results demonstrate that our proposed model considering both subjective assessment and objective assessment significantly outperform the exist work considering users' subjective assessment only.

## References

1. Chou, S.Y., Chang, Y.H., Shen, C.Y.: A fuzzy simple additive weighting system under group decision-making for facility location selection with objective/subjective attributes. EJOR 189(1), 132–145 (2008)
2. Li, L., Wang, Y.: Subjective trust inference in composite services. In: AAAI Conference on Artificial Intelligence (2010)
3. Marden, J.I.: Analyzing and Modeling Ranking Data. Chapman & Hall (1995)
4. Mui, L., Mohtashemi, M., Halberstadt, A.: A computational model of trust and reputation for e-businesses. In: HICSS, p. 188 (2002)
5. Noor, T.H., Sheng, Q.Z.: Trust as a service: A framework for trust management in cloud environments. In: Bouguettaya, A., Hauswirth, M., Liu, L. (eds.) WISE 2011. LNCS, vol. 6997, pp. 314–321. Springer, Heidelberg (2011)
6. Page, L., Brin, S., Motwani, R., Winograd, T.: The pagerank citation ranking: Bringing order to the web. Technical Report 1999-66 (November 1999)
7. Qu, L., Wang, Y., Orgun, M.A.: Cloud service selection based on the aggregation of user feedback and quantitative performance assessment. In: IEEE International Conference on Services Computing (SCC), pp. 152–159 (2013)
8. Qu, L., Wang, Y., Orgun, M.A., Liu, L., Bouguettaya, A.: Cloud service selection based on contextual subjective assessment and objective assessment. In: AAMAS 2014, pp. 1483–1484 (2014)
9. Zhang, J., Cohen, R., Larson, K.: A trust-based incentive mechanism for E-marketplaces. In: Falcone, R., Barber, S.K., Sabater-Mir, J., Singh, M.P. (eds.) Trust 2008. LNCS (LNAI), vol. 5396, pp. 135–161. Springer, Heidelberg (2008)
10. Zheng, Z., Wu, X., Zhang, Y., Lyu, M.R., Wang, J.: QoS ranking prediction for cloud services. IEEE Trans. Parallel Distrib. Syst. 24(6), 1213–1222 (2013)