

Detection of Malicious Feedback Rating for Measuring Cloud Service Reputation

Dr. Maya Rathore

Associate professor, Christian Eminent College, Indore
mayarathore114@gmail.com

Prof. Y. S Chouhan

Professor, Christian Eminent College, Indore
yschouhan05@gmail.com

Abstract

In the field of cloud computing, reputation of a service is usually calculated using feedback ratings provided by cloud service users. However, the existing malicious ratings and the changing preferences of different service users often lead to a bias towards positive or negative ratings. A reputation computation approach is proposed along with an algorithm for accurately measuring the reputation of Cloud services. We first detect malicious feedback ratings using similarity computation and then adjust the malicious rating with the average rating for computing the actual service reputation. It can also enhance the reliability of service selection.

Keywords- Cloud service; Feedback rating; Reputation; Similarity computation.

1. Introduction

Cloud services are widely accepted to facilitate various stockholders to use the cloud as a portal for trade their own services and overwhelming in built services of others. The unpredictable expansion of cloud services increases the complexity for users to choose among a large number of Cloud services. Therefore, selecting and ranking Cloud services effectively becomes a key challenge for the Cloud service community. Traditional Cloud service selection approaches are usually based on the promised qualities offered by the service providers. However, service providers promises on the quality of published services but be unsuccessful partially or fully to deliver on these promises at runtime [1]. It is a tedious task for some service providers who may not perform what they guarantee. Reputation of the providers needs to be considered when making selection. Hence, accurate reputation measure of Cloud services is crucial for business applications. The discovered services can be evaluated and ranked according to the feedbacks from service users.

Several research works have recognized the importance of reputation measure of Cloud services. Existing work has explored the efficacy and robustness of reputation measure approaches and many among them suffer from the certain weaknesses. Firstly, it is tricky to make sure the transparency of feedback ratings because of existing malicious service users. Malicious service users might provide some malicious feedbacks to affect the measure results for commercial benefits. Hence, malevolent service users can account hateful feedback ratings for a Cloud service. There is a large variety of service users on the Internet. Service users can articulate their preferences over Quality of Service (QoS) attributes of services [1]. The user ratings are often subject to service users' preferences. As some service users provide near to the ground ratings on various Cloud services, whereas some others may provide higher ratings [7]. Hence, different service users often give different ratings to the same used service. To address the aforementioned weaknesses, an approach is proposed to detect the malicious feedback rating and determine the accurate service reputation for reliable service selection. An algorithm is also presented to show the overall working of proposed mechanism.

This paper is organized as follows Section II describes literature survey carried out. Section III describes proposed approach for feedback rating detection and reputation computation, which contains malicious rating detection and adjustment. Section IV presents an algorithm for the proposed approach. Section V presents the implementation and experimental evaluation of proposed work. Finally section VI concludes the paper.

2. Literature survey

Reputation is one of the primary issues among the various business communities. The service users select the provider or services based on their reputation. Many researchers have worked on trust and reputation using various mechanisms, incentive based, association based, previous invocation based etc. In this section, various reputation computation approaches are identified.

A popularity based service search method is adopted, which consists of tracking all kind of services. It stores important information into database related to discovered, invoked or published services which is helpful in finding frequency of used cloud services, their availability, usage history etc [3]. A unique approach is proposed that energetically recommends cloud services that fit users' interest [4]. It is a hybrid approach used to combines collaborative filtering and content-based recommendation. Trust-based recommender system is proposed to solve the problem of traditional recommender system which is often ineffective and is not able to compute a user similarity weight for many of the users [5]. It accepts trust metrics and rating matrix as input and generates neighbors using trust metrics and user similarity respectively. In this approach, trust-based issues are discussed to solve the problem of traditional recommender system such as, data sparsity, cold-start users, malicious attacks on recommender systems and centralized architectures. A semantic enhanced personaliser (SEP) framework of hybrid recommender system is proposed for cloud personalization [6]. A novel Cloud service recommendation approach is proposed which incorporates user's potential QoS preferences and diversity feature of user interests on Cloud services [8].

A QoS prediction framework, called WSPred, is proposed to pro-vide time-aware personalized QoS value prediction for different service users [9]. QoS performance of services is highly related to the service status and network environments which are variable against time. A neighborhood based collaborative filtering approach is presented to predict unknown values for QoS-based service selection [10]. A hybrid service recommendation approach is presented by combining collaborative filtering with content-based features of Cloud services [11]. This approach exploited both rating data and content data of services using a three-way aspect model. Although previous work on existing solutions has explored the efficacy and robustness of measure approaches, most of them suffer from the certain weaknesses. Firstly, it is difficult to ensure the purity of feedback ratings because of existing malicious service users. Malicious service users might provide some malicious feedbacks to affect the measure results for commercial benefits. Secondly, previous approaches fail to ensure the accuracy of feedback ratings. There is a large variety of service users on the Internet. Service users can express their preferences over Quality of Service (QoS) attributes of services [10]. The user ratings are often subject to service users' preferences. As some service users are conservative (tend to provide low ratings on various Cloud services), whereas some others may be aggressive or neutral [7]. Hence, different service users often give different ratings to the same used service.

In order to address aforesaid issues, in this paper an approach is proposed for detecting the malicious users' feedback rating and computing the service reputation. An algorithm is also presented for the proposed approach. The proposed approach detects malicious feedback ratings by using cumulative sum method and reduces the effect of user feedback preferences by Pearson correlation coefficient. The limitation with this approach is that only negative feedback ratings are dropped because they cause malicious ratings.

3. User Rating Based Reputation Computation Approach

Reputation of a service can also be evaluated according to feedback ratings provided by service users. A collaborative filtering approach in which user feedback plays vital role in the assessment of reputation prediction accuracy of cloud services is proposed. Therefore, user feedback ratings as provided by service users can not be totally avoided. But the major issue with user feedback rating is the trustworthiness and accuracy of their feedback. This issue can be solved by providing an automatic mechanism for detecting malicious user feedback which assesses the service reputation by discarding the malicious users. Here, manual user feedback is collected from group of consumers for their usage experience with the service. A log file is maintained for user feedback data, with columns user_id and user_feedback rating. Feedback rating is any numeric value between 1 to 5, in which 1 means poor service, 2 means average, 3 means good, 4 means very good and 5 means excellent. Here, feedback data from 15 consumers are collected and analyzed to determine whether it contains any malicious user rating or not. It is necessary to consider only that users rating, which are accurately provided in order to improve the accuracy of reputation of a service.

Detecting nasty user rating, the feedback data is analyzed to know the frequency of positive or negative malicious rating provider. For example, if a service user provides the feedback of a service as excellent and majority of users provide the ratings as poor, then the malicious positive rating is discarded for further computation of reputation of a service to predict and improve reputation accuracy. This phase works in two steps, first step identifies the list of non malicious users by performing similarity computation of previous users feedback and second step compares the percentage of non malicious users with the specified threshold value.

Similar feedback ratings are identified with similarity computation of previous user's feedback using Pearson correlation coefficient (PCC). Similar feedback ratings are stored in similarity coefficient variable. We assume that there are m users and n cloud services, and the relationship between users and cloud services is denoted with an $m \times n$ matrix. Then each entry $r_{x,i}$ in the matrix denotes the feedback rating of the cloud service I rated by the user x where $r_{x,i}$ is a normal feedback rating. It uses following equation to compute the similarity between user x and user y based on their commonly rated cloud services:

$$\text{Sim}(x,y) = \frac{\sum_{i \in I_x \cap I_y} (r_{x,i} - \bar{r}_x)(r_{y,i} - \bar{r}_y)}{\sqrt{\sum_{i \in I_x \cap I_y} (r_{x,i} - \bar{r}_x)^2} * \sqrt{\sum_{i \in I_x \cap I_y} (r_{y,i} - \bar{r}_y)^2}}$$

Where, $\text{Sim}(x,y) \in [-1,1]$ represents the similarity of two users.

$I_x \cap I_y$ is a set of commonly rated cloud services by both users a and u .

$r_{x,i}$ and $r_{y,i}$ are the two feedback ratings of cloud service i rated by user a and u .

\bar{r}_x represents the average feedback rating of all of the cloud services that are rated by user x

$s(x) = \{y | \text{sim}(x,y) \geq \text{sim}_k, \text{sim}(x,y) > 0, x \neq y\}$

After calculating and ranking the PCC similarity values between the current user and the other users, a set of similar users $S(x)$ can be identified, as follows:

Where, Sim_k is the k th largest PCC value with the current user y .

k represents the number of the similar users (i.e., they have larger PCC values than others), and

$\text{Sim}(x,y) > 0$ is to exclude the dissimilar users (dissimilar users, e.g., those with negative PCC value, will influence the reputation measurement accuracy).

After obtaining the set of similar users, according to a set of community cloud services $SS^k = \{s_1^k, s_2^k, \dots, s_l^k\}$ which contains l services used by the K users, we can calculate the feedback similarity between user a and user u as:

$$\text{FS}^k(x,y) = \begin{cases} 1 - \sqrt{\frac{\sum_{y \in S(x)} (r_{x,i}^k - r_{y,i}^k)}{|SS^k|}}, & \text{if } |SS^k| \neq 0 \\ 0, & \text{if } |SS^k| = 0 \end{cases}$$

4. Proposed Algorithm

This algorithm detects the malicious user rating and evaluates the service reputation based on positive feedback rating. Here, R is the user feedback rating, R_l is the lowest rating level. R_{avg} is the average of all rating given by user for particular service; R_{th} is the maximum no. of user given that rating called threshold rating. List1 and list2 are the list for storing feedback ratings for actual and malicious users.

Begin

Step 1: Input:

R_l = Input given by user for Qualify for rating of services. i.e lower rating

R = User rating for particular service.

Calculate:

R_{avg} = Average of all rating given by user for particular service i.e $R_{avg}(R)$.

R_{th} = Maximum no. of user given that rating called threshold rating.

$NoOfPersonAboveR_{th}$ = Total no. of people which has given the rating equal and above to R_{th} .

NoOfPersonBelowR_{th}=Total No. Of People Which Has Given Below The R_{th}.

Step 2:

```

If (R >= Rth) then
    NoOfPersonAboveRth++
Else
    NoOfPersonBelowRth++

```

Step 3 :

```

If (NoOfPersonAboveRth >= 80%) And (Rth >= RL) Then
    IF (R >= Rth)
        List1[] = No. Of Positive User .
    Else
        List2[] = No. Of Malicious User.
Else
    If (Ravg > RL) Then
        Final Rating = Ravg. (It is Avg Rating)
    Else
        Final Rating = RL (Below Your Expectation)

```

Step 4 : Separate the List1[] for Positive User

Separate the List2[] for Malicious User

Step 5:

[Reputation Computation]

Calculate Average Of Positive User List1.eAvg[List1].

End.

5. Conclusion

Reputation is one of the major concerns among the online as well as offline business community. User feedback rating plays vital role in assessing the cloud service reputation. We have addressed the issue of purity of user feedback rating which may be maliciously provided by some users in order to provide bad reputation of a cloud service. In this paper, we have proposed an approach for assessing cloud service reputation to address the limitations of existing reputation computation approaches which uses malicious feedback ratings. An algorithm is also presented for the proposed approach. The approach is able to detect the malicious feedback rating and assess the accurate cloud service reputation for reliable cloud service discovery.

References

1. Shangguang Wang et al., "Evaluating Feedback Ratings for Measuring Reputation of Cloud Services," IEEE International Conference on Services Computing, 2011.
2. Kang, G., Liu, J., Tang, M., Liu, X., Cao, B. and Xu, Y., "AWSR: active cloud service recommendation based on usage history," Proceeding of 19th IEEE International Conference on Cloud Services (ICWS), 24-29 June, pp.186-193, 2012.
3. Elfirdoussi, S., Jarir, Z. and Quafafou, M., "Popularity Based Cloud Service Search," Proceeding of 19th IEEE International Conference on Cloud Services (ICWS), 24-29 June, pp. 683-689, 2012.
4. Yao, Lina, Sheng, Q. Z., Segev, A. and Yu, J., "Recommending Cloud Services via Combining Collaborative Filtering with Content-based Features," Proceeding of IEEE 20th International Conference on Cloud Services(ICWS), Santa Clara, CA,28 June-3 July, pp. 42-49, 2013.
5. Sharma S. K. and Suman U., "A trust-based architectural framework for collaborative filtering recommender system," International Journal of Business Information Systems, Vol. 16, No.2, pp. 134-153, 2014.
6. Sharma S. K. and Suman U., "A framework of hybrid recommender system for cloud personalization," International Journal of Business Information Systems (IJBIS), Vol. 13, No.3 pp. 284 - 316, 2013.
7. Maya Rathore and Ugrasen Suman, "A Mixed Opinion based Reputation Prediction Approach for Reliable Cloud Service Discovery," International Journal of Business Information System (IJBIS), Vol. 22, No. 2, pp. 143-165, 2016.

8. G. Kang et al., "Diversifying cloud service recommendation results via exploring service usage history," *IEEE Trans. Serv. Comput.*, Vol. 6, No. 1, pp. 35–47, 2015.
9. W. Lo, J. Yin, S. Deng, Y. Li, Z. Wu., "Collaborative cloud service qos prediction with location-based regularization," *Proceedings of 2012 IEEE 19th International Conference on Cloud Services (ICWS)*. IEEE, pp. 464-471, 2012.
10. J. Wu, L. Chen, Y. Feng, Z. Zheng, M. C. Zhou, Z. Wu., "Predicting quality of service for selection by neighborhood-based collaborative filtering," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 43, No. 2, pp. 428-439, 2013.
11. Y. Xu, J. Yin, W. Lo, Z. Wu., "Personalized Location-Aware QoS Prediction for Cloud Services Using Probabilistic Matrix Factorization," *Proceedings of Cloud Information Systems Engineering–WISE 2013*. Springer, pp. 229-242, 2013.

