Pak. J. Biotechnol. Vol. 13 (special issue on Innovations in information Embedded and Communication Systems) Pp. 274- 278 (2016)

SECURE TRUST WORTHY SERVICE DISCOVERY (STSD) MODEL BASED ON USER PREFERENCES

N.Anithadevi[1] and M.Sundarambal[2]

[1]Department of Computer Science & Engineering,, Coimbatore Institute of Technology, Coimbatore, Tamilnadu, India , [2]Department of Electrical & Electronics Engineering,,Coimbatore Institute of Technology,Coimbatore, Tamilnadu, India E-mail: [1]anitha.cit@gmail.com; [2]msundarambal@cit.edu.in

ABSTRAC

The need for filtering authentic web services from the rest has become quite hectic seeing as the malicious ones seem to more and more legitimate by the day. The loss of proprietary information to such web services is becoming increasingly common and as such the paper suggests an idea in which a third party authenticating web service evaluate web service providers and facilitates the user with credible list of providers based on its "Trust filter". The filter takes into account many factors including the various customer preferences and prepares its itinerary trusted candidates in order to satisfy the customized needs of the individual. The idea is to mine user's preferences from the requirements specification provided by the user and the preferences are used to determine the weights of each Quality of Service QoS attribute. The local trust on a service for the user is derived by combining the trust on QoS attributes and the trust on user's ratings. In order to classify the web services based on the user's opinion the user must first be legitimate. The global trustworthiness of a service for the users group, the dishonest user are removed based on the results of Local honesty evaluation process. The simulation results indicate that the model works well on personalized evaluation of trust, and it can effectively dilute the influence of malicious ratings.

***Index Terms*—Trust Filter, Authentication, QoS Attributes, Malicious Rating, Local Trust, Global Trust.**

I. INTRODUCTION

The primary objective of the research is to enhance the web service Quality of Service QOS which focuses on eliminating un-reliability and improve trustworthiness. Here we define the concepts of trustworthiness through Local trust, Global trust and honesty Assessment [1]. Local trust is calculated based on the user's ratings of the (previous) services, and the degree that the quality of the services meets the requirements of users.

The idea is such that the system must automatically mine user's preferences from their requirements. Following local trust and Global trust [3] is established by eliminating the dishonest users who post false ratings to promote or "bad mouth" a web service. Both these factors contribute to the calculation of honesty assessment.

Honesty Assessment is arrived as an average objective trust of the user group.

The Procedure is the following:

- Compare each user's rating with the calculated average objective trust.
- If the difference is in a reasonable range, the user would be regarded as an honest one. Else the user is regarded as dishonest user.
- Count up the number of honest users, and derive the ratio of honest users.

This Model provides both personalized trust evaluation for users and overall trust worthiness [4] assessment of newly published web services. To assign Initial trust value for newly published services the following protocol was suggested. Based on the feedback from the risk unit if the network does not have any information about the new service, then initial trust value is assigned for the new service. This value is chosen carefully, to allow this to get services that require high security and build a trust relationship with other services [3]. Another feature of our trust model is that the trust value is service specific. It is dynamic and changes depending on the behavior of the web service thus providing with accurate results rather than results that dull over time.

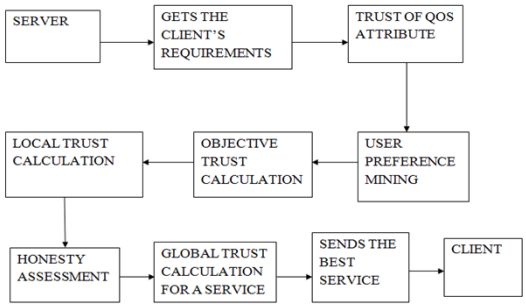

Figure 1. System Architecture

This model concentrates on users requirements and their satisfaction of requirements as shown in Figure 1.Initially the server inputs the client's requirement .Based on QoS attribute objective trust [9,19] is evaluated depends on user preferences. Then that output unit gives the input to Honesty assessment unit [7,20] , their calculates global trust and send the best service to the client. This approach is suitable for already excising services [10,11]. If the service is new then it leads to STSD model which has Risk evaluation unit to manage the risk when the model is trying to compose a new unknown service [3,21-26]. Focus is given to the elimination of false ratings before calculation of objectives. The objective trust is calculated by combining the monitored QOS with the users preference. Subjective trust is calculated by collecting the user's ratings, which tells if the user satisfied with the received QoS [6]. Finally the legitimate user's contribution of objective and subjective trust is used to consolidate the global trust [1]. The aim of the input design is to ensure the maximum possible levels of accuracy and also ensures that the input is accessible that understood by the user [7]. The input design is the part of overall system design where if the data going into the system is incorrect then the processing and output will result in multiplying errors rather than remove them. Input design features can ensure the reliability of the system and produce result from accurate data or they can result in the production of erroneous information. User requirements can be classified into many categories such as availability and response time [5].

In this model the output of each phase is displayed to the user. After the user enters their transaction details they can see the output of the transaction whether it is a successful transaction or a failure transaction and rate the web service accordingly.The output of positive event, negative event, trust of each QoS attributes [8], preference mining, objective trust calculation of the web service, honesty assessment and global trust of web service is displayed at the server side for reference.

II. Back Ground

This section describes the different ideologies of Secure Trust worthy Service discovery (STSD) model in distributed environment.

A. Trust Model Deign

Trust is closely related to the users' requirements, and the meeting of said requirement is met in one of two ways: The first way is to compare the monitored QoS with the user's requirements which is deemed as objective trust [9]. The second way is to collect the user's ratings, which tells the satisfaction with the function of the service and the received QoS. This kind of trust evidence is called subjective trust here. The architecture of Web services should be extended first as shown in Figure 2. The UDDI is enhanced with a Trust Management Module (TMM), which is responsible for collecting trust report from Trust Proxy (TP), dividing users into different groups and calculating the overall trust worthiness of Web services for user groups. The purpose of TMM is to seggregate the the dishonest users and forward said user info to the UDDI [1]. TP is an extra component deployed on client side machines.

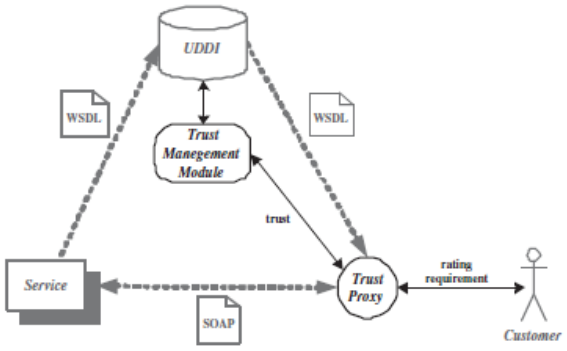

Figure 2. Extended web service architecture

User's requirements are fed to the TP and it in turn requests TMM for the most trustworthy service. The TP plays a role of monitoring component, recording the real time quality of service when a user is interacting with the service. Then it evaluates the local trust value after the user submits his or her rating on the service[11]. To build up a practical trust evaluating platform, there are many other things that should be taken into consideration. However, here main focus is on the process of trust assessment to derive local trust evaluation value and trustworthiness of Web services combining two kinds of trust evidences.

Then it calculates the average trust value using formula (1) and assigns this value in the corresponding table position. Depending on this newly calculated value, it decides whether to accept the request or not.

$$\tau(WP,B) = \frac{\sum_{i=1}^{n} Wi * \tau(WPi,B,y)}{\sum_{i=1}^{n} Wi.} \quad (1)$$

Here, WP is the service provider, (WP,B) the average trust value of service B for service WP, Wi the security level of ith service, (WPi,B,y) the trust value of B for ith service and n is the number of services that links WP and service B. Equation (2) is used by the service manager to calculate the trust value for any new service [11]. If the new service requests a service, the service providing service generates a multicast message to all services that it has involvement and asks for their recommendation about this service.

$$\tau(WP,Bnew) = ((\sum_{i=1}^{n} \tau(WP,i) \times \tau(i,Bnew))/n \quad (2)$$

Here, WP is the service provider, Bnew the new service requesting service, τ(WP,Bnew) the average trust value of Bnew for service WP, (i,Bnew) the average trust value of service i for Bnew and n is the number of services that are link with both WP and Bnew. The above model allows a service to get services from a provider never before interacted with, and build a trust relationship gradually [12]. If the service provider fails to get any recommendations from the services, it communicates with the risk assessment unit for risk analysis. Based on the feedback from the risk unit [14] if any service of the network does not have any information about the new service, then it assigned some initial trust value.

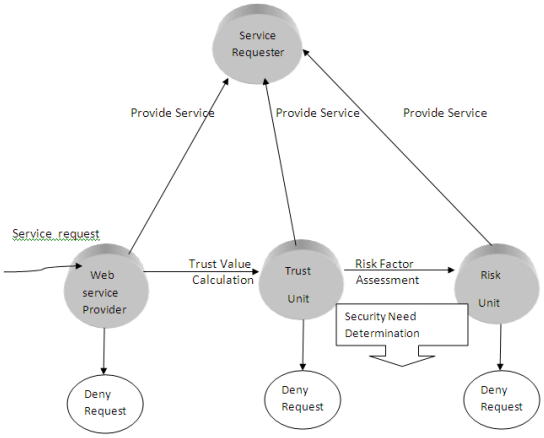

Figure 3. STSD Conceptual Diagram

B. QoS Attributes Trust Factor

Trust of QOS attribute is the degree to which the received quality fulfills the requirement. Positive evidence is the sum of all positive events (events where the user's specs are met) and negative evidence (where the user's are let down) is the sum of all negative events[13]. Positive evidence mi and negative evidence ni can be calculated using the following formula:

$$^{j}_{i'} \text{ if } n \le nt \quad (3)$$

The existing system considers only the trust values which was given during the initial experience of the user with the web service. But the quality of web service may degrade with respect to time so this model considers only the latest trust values given by the user and not the trust value which was given during the initial experience. Thus, the trust evaluation can comply with the fact that trust will increase slowly after positive event but decrease quickly after negative event[15]. Finally, the trust of QoS attributes such as availability and response time is found.

C. User Preference Mining

The project predicts the user's preference level based on their requirement provided by the user. Each QoS attribute of the web service is divided into five levels namely worst, bad, normal, good and best[1][17]. This is achieved by sorting web services based on each QOS attribute. Then from the users requirement level ,the preference of every user to each QoS attribute is found. This preference can be used to find the objective trust of the user.

III. System Design

This section gives details about the system design and the underlying modules.

A. Local Trust Calculation

Before calculating the local trust of the web service, the objective trust is calculated by combining the users preference and the trust of each QoS attribute for a web service.

$$T_{obj} = \sum_{i=1}^{nq} p_i . tq_i \quad (4)$$

According to the trust evaluation process defined, the next step is to combine objective trust with subjective trust. The subjective trust here refers to the users' ratings for the Web service. The users update their ratings, which is a real number between 0 and 1. The combined subjective and objective trust now forms the local trust of the web service.

B. Honesty Assessment

Average method is applied first to estimate the approximate ratio of honest users in a user group and the following steps are done:

- User group average objective trust Calculation
- Calculated average Objective trust is compared with each user's ating, if the difference is in a reasonable range, the user would be regarded as an honest one. Else the user is regarded as dishonest user.
- Depends on the Count of number of honest users, ratio of honest users is derived.

The figure below explains the honesty assessment procedure:

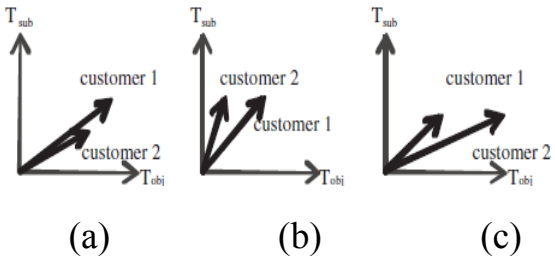

Figure 4. Honesty Assessment

In the figure 4 (a) the subjective trust of customer 1 and customer 2 relies with the average objective trust hence they are honest users. In the figure (b) the subjective trust of both the customers is more than the average objective trust which means that the user has rated falsely to promote the web service so he/she is regarded as dishonest user and is eliminated from the user group. In the the figure (c) the subjective trust of the customer 1 is less than the average objective trust which means that the user has rated falsely to badmouth the web service so he/she is regarded as dishonest user and is eliminated from the user group.

C. Global Trust Calculation

In this module a global subjective trust is calculated by eliminating the dishonest users who post false ratings to distort the true nature of a web service. Finally the overall trust of web service is calculated as:

Global trust = (ratio of honest users of a web service)*
(average subjective trust)*
(average objective trust).

Web service ranking is done based on the global trust which

Web service Id	Number of request (ø)	Number of accept (γ)	Average trust value (τ)	Average service time (σ) in ms
5	3	1	0.75	21
9	7	6	0.6	15
13	17	13	0.83	40

is calculated as mentioned above. In this model four banking services are created. These four web services are ranked in the descending order based on their global trust. Then the web service which has highest global trust value is composed with the user request.

D. Risk Assessment

A risk model is essential during the sharing services in distributed environment. Risk evaluation becomes significant when a service request comes from an unknown service or when there is not enough recommendation information.

TABLE I .Risk Value Table

When a service request arrives, we calculate the trust value of the requesting service (if the providing service has information about the requester or by collecting recommend-dation from other services). Then based on the security level of the requested service, we accept or deny the request. When the requester is unknown to all the neighboring services, the service is assigned an initial trust value of 0.5 which would allow it to receive lower security-intensive services and build a trust relationship with others [21]. However, if that service requires a higher security level service, it is denied. To address this issue, we have added the risk assessment along with our trust model. In this each service has a risk evaluator. This evaluator stores information about high security services and calculates the risk value when a request comes for one of these services [3,22]. Each time a service request arrives along with an accepted or rejected event, it updates the risk value associated with that service. It collects information about the service that includes number of accepts (γ), total number of requests (ø), average trust values of the services who request this service, service time (σ), etc. To calculate, the risk factor following formula is used:

Here, ρ is the risk factor, γ the number of accepts, ø the number of request and τ is the average trust value for this service.The range of the risk factor, ρ is 0 to ρ 1.0. This is a weighted average with respect to average trust value. A value of 0.5 indicates around 50% acceptance rate for this particular service. If the risk factor value is high (>0.5), then the request is rejected. In the case of a low risk factor, the service is provided. Based on this value, the service assigns a risk factor with the service. As this information is collected every time a service is requested or shared, a historical database is created for services of a particular service. Each service has its own database that allows it to decide the risk factor for its services. Based on this allows a service to decide whether to accept a request or not when there is little or no information available about a requester. Table 1 shows some sample data stored in a service. Each time a service request is made, the

risk value table is updated to include the modified number of requests, number of accepts, average trust value of services for which the request is accepted, and average service time to offer. The updated data is used to calculate the risk factor when composing a service with unknown services. We are currently using statistical distributions to find out optimal percentage rate and trust value pair that lowers the risk of service sharing. The average service time is compared with the service-sharing time to evaluate the behavior of the requesting service. This value is used for dynamic modification of trust value.

IV. Performance Analysis

In order to evaluate the performance of our Model, we compare Exciting system in terms of availability and response time with our proposed model Secure Trust Worthy Service Discovery(STSD). The proposed algorithm is more secured based on user's preferences such as (availability and response time) which yields a better performance than the earlier models. STSD model provides much more high performance in the Trustworthy web service evaluation process than others and also it is more secured because of the Risk assessment model. In order to evaluate our trust model, we build a prototype of trust estimation platform for Web service. The platform mainly simulates two kinds of entities: Web services and users.

• To simulate a Web service, we need to set up its function and QoS attributes. The function is represented by a string of characters such as Bank transactions,calculator etc. The dynamic changes of each QoS attribute obey the normal distributionN(μ,σ), where μ is the average performance of the service and σ means the deviation between the quality value of a specific interaction with the expectation.

TABLE.2 Simulated Services Configuration

Services	Availability		Response Time	
	μ	Σ	μ	Σ
Ws1	84	1	537	10
Ws2	88	2	773	60
Ws3	78	3	629	50
Ws4	83	1	561	35
Ws5	80	5	652	10
Ws6	76	2	851	25
Ws7	79	2	516	15
Ws8	86	1	918	20
Ws9	82	5	815	70
Ws10	90	4	695	65

A user is simulated by setting up their requirements and honesty. Each user has personalized requirements for every QoS attribute. The honesty is a Boolean variable: true means the user is an honest one, who submits ratings according to actual performance of services, while false represents a dishonest one. There are two kinds of dishonest users: some of them want to bad-mouth the service by giving quite low rating, and the others submit much high ratings in order to advertise the service. Three experiments are carried out to show the effectiveness of the model on evaluating the trust of QoS attributes, expressing user's preference to trust assessment and reducing the influence of malicious users. Ten functional equivalent Banking services are shared by these experiments, and the detailed configurations of each service is shown in Table

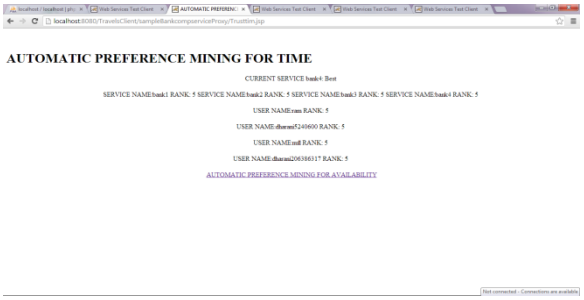

Figure 5. Automatic Preference Mining

Figure 6. User Preference Mining

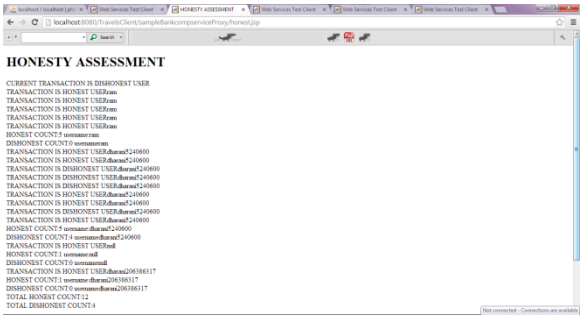

Figure 7. Honesty Assessment

V. CONCLUSION

In this model, the issue of evaluating trust in Web services and highlighting the gaps of existing trust models is discussed. In the existing trust models user's preferences are not considered and false ratings are not eliminated and also the new web service is not handled properly. So this model aims to fill these gaps, and it introduced a user-oriented trust evaluation model which integrates preference and honesty aware for Web services with risk assessment. The model combines objective trust with subjective trust, which makes it more comprehensive than existing models. An automatic preference mining approach is adopted in the model which can not only save the user's time, but also prevent potential inconsistency. The hybrid honesty assessment mechanism proposed in this method which makes use of the connection and consistency between two user's subjective and objective trust, providing a novel way to classify honesty and cheating users. And also a distinction is made between the local and global trust, providing both personalized trust evaluation for users and overall trustworthiness assessment of web services. If the web service is new then risk assessment will handle that web service with proper security measures. Results show that this model can effectively support different preferences of users, dilute the influence of malicious ratings and compose the secured newly arrived web services properly.

REFERENCES

[1] Li, Bixin, Li Liao, Henry Leung and Rui Song, PHAT: A preference and honesty aware trust model for web services. Network and Service Management, IEEE Transl. **11**: 363-375 (2014).

[2] Ahamed, Sheikh, I., and Moushumi Sharmin, A trust - based secure service discovery (TSSD) model for pervasive computing. Computer Communications **31**: 4281-4293 (2008).

[3] Su, Xing, et al., A robust trust model for service-oriented systems. Journal of Computer and System Sciences **79**: 596-608 (2013).

[4] Wang, S., Huang, L., Hsu, C. H. and Yang, F., Collaboration reputation for trustworthy Web service selection in social networks. Journal of Computer and System Sciences **82**: 130-143 (2016).

[5] Bhatia, Rekha and Manpreet Singh, Minimizing Privacy Disclosure in Web Services Paradigm. Procedia Computer Science **48**: 782-789 (2015).

[6] Gupta, Reena, Raj Kamal and Ugrasen Suman. A QoS-aware optimal selection scheme for web services with a trusted environment. CSI Transactions on ICT **3**: 13-21 (2015).

[7] Malik, Zaki and Athman Bouguettaya, Rateweb: Reputation assessment for trust establishment among web services. The VLDB Journal—The International Journal on Very Large Data Bases **18**: 885-911 (2009).

[8] Ye, B., et al., A trust-based model for quality of web service. International Conference on Advanced Service Computing, Valencia Spain, Pp 39-45 (2013).

[9] Deng, Shuiguang, Longtao Huang and Guandong Xu, Social network-based service recommendation with trust enhancement. Expert Systems with Applications **41**: 8075-8084 (2014).

[10] Li, Lei and Yan Wang, The study of trust vector based trust rating aggregation in service-oriented environments. World Wide Web,**15**: 547-579 (2012).

[11] Sanadhya, Shashvat and Shailendra Sing, Trust Calculation with Ant Colony Optimization in Online Social Networks. Procedia Computer Science **54**: 186-195 (2015).

[12] Park, J. S., Kwiat, K. A., Kamhoua, C. A., White, J. and Kim, S., Trusted Online Social Network (OSN) services with optimal data management. Computers & Security **42**: 116-136,(2014).

[13] Li, M., Sun, X., Wang, H., Zhang, Y., and Zhang, J., Privacy-aware access control with trust management in web service. World Wide Web **14**: 407-430 (2011).

[14] El-Kafrawy, Passent, Emad Elabd and Hanaa Fathi, A Trustworthy Reputation Approach for Web Service Discovery. Procedia Computer Science **65**: 572-581 (2015).

[15] Haydar, Charif, Azim Roussanaly and Anne Boyer, Comparing Local, Collective, and Global Trust Models. International Journal On Advances in Life Sciences **6** (1&2): 30-40 (2014).

[16] Liu, Min, and Ying Li, Global trust value grading calculation method in P2P network. Journal of Networks **9**(1): 216-222 (2014).

[17] Das, Anupam, and Mohammad Mahfuzul Islam, SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems. Dependable and Secure Computing IEEE Tranl **9**: 261-274 (2012).

[18] Bhatti, Rafae, Elisa Bertino and Arif Ghafoor, A trust-based context-aware access control model for web-services. Distributed and Parallel Databases **18**: 83-105 (2005).

[19] Liu, F., Wang, L., Gao, L., Li, H., Zhao, H. and Men, S. K., A Web Service trust evaluation model based on small-world networks. Knowledge-Based Systems **57**: 161-167 (2014).

[20] Han, S., Dillon, T., Chang, E. and Tian, B., Secure web services using two-way authentication and three-party key establishment for service delivery. Journal of Systems Architecture **55**: 233-242 (2009).

[21] She, W., Yen, I. L., Thuraisingham, B. and Bertino, E., Security-aware service composition with fine-grained information flow control. Services Computing, IEEE Transl **6**: 330-343 (2013).

[22] Na Shi, The study of web services selection based on QoS, International Conference on Computer Application and System Modeling, Pp. 13-112 (2010).

[23] Zainab M. Aljazzaf, Mark Perry and Miriam A. M. Capretz, Trust in Web services. 6th IEEE Congress on Services, Pp189-190 (2010).

[24] Hien Trang Nguyen, Weiliang Zhao and Jian Yang, A trust and reputation model based on Bayesian Network for web services, IEEE International Conference on Web Services, Pp 251-258 (2010).

[25] Cai, S., Zou, Y., Xie, B., Shao, W., Mining the Web of Trust for Web Services Selection. IEEE international Conference on Web Services, Pp 809-810 (2008).

[26] Paradesi, S., Doshi, P. and Swaika, S, Integrating Behavioral Trust in Web Service Compositions. IEEE international Conference on Web Services, Pp.453-460 (2009).