RECOGNIZE TRUSTWORTHY WEB SERVICES VIA INSTITUTIONS

Han Jiao, Jixue Liu and Jiuyong Li
School of Computer and Information Science, University of South Australia, Adelaide, Australia

Keywords: Trust, Trustworthiness, Web service, Institution.

Abstract: The emergence of web services, which provides flexible but standard methods for heterogeneous entities interacting with each other, has tremendously revolutionized the communication mode on the Web. However, due to large scalability and anonymity, it is difficult for web service users to determine the trustworthiness of web services. This paper introduces a new concept, web service institution, based on which we proposes a web service trust determination framework. We discuss the necessity of web service institutions that leads to a win-win situation for all. We devise the core trust computation logic which takes both institution-level and service-level factors into account. We also discuss several typical use cases.

1 INTRODUCTION

The way people communicate on the web has evolved rapidly in the past decade. Nowadays, web services have been proved to be a promising technology for exchanging information among distributed sources in a flexible but standard manner.

In such open, distributed environment, trust is recognized as an important factor to impact the communication (Gefen et al., 2008). Significant effort has been spent to address the trust issues. At present, there are two major types of methods for determining trust, policy-based methods and reputation-based methods. A good survey can be found in (Bonatti et al., 2005). However, both of the methods cannot solve the problem perfectly. Policy-based methods required unified methods (languages and protocols) for different web service to communicate. The shortage is that it is difficult to devise such a unified method that most web users are willing to accept. Reputation-based methods, because of their fixed reputation calculation logic, can be easily damaged by malicious behaviours such as collusion and whitewashing. Those behaviours will mislead users to dishonest web services who seem to have good reputation.

In this paper, we propose an institution-based solution to fulfil the gap. The contributions can be summarized as follows: (1) we define web service institution and its function; (2) we identify several institution-level and service-level trust factors and devise a framework based on them; and (3) we design a trustworthiness determination logic which integrates both service-level and institution-level trust factors.

The rest of the paper is structured as follows. In Section 2, we introduce some trust-related concepts. In Section 3, we describe the overall architecture and several key processes. In Section 4, we present trust impact factors and the trustworthiness computation logic. Several typical use cases are discussed in Section 5. Section 6 gives the conclusion and looks at future work.

2 RELATED CONCEPTS

The key part in our proposal is the so-called web service institution defined as follows:

Web Service Institution (WSI) is a kind of on-line platform for web services and their users to communicate in an easy, efficient and trust manner.

WSIs act as a conjunction role between web services and their users. Their major functionality is to make the two parties communicate smoothly. To achieve this goal, on the one hand, WSIs provide administrative support to web services, which include but do not limit to service registration, service monitoring and trust calculation. On the other hand, WSIs also provide search interfaces to web service users. The searching function does not simply return a web service address string with a brief service description.

Jiao H., Liu J. and Li J..
RECOGNIZE TRUSTWORTHY WEB SERVICES VIA INSTITUTIONS.
DOI: 10.5220/0003432701870190
In *Proceedings of the 13th International Conference on Enterprise Information Systems* (ICEIS-2011), pages 187-190
ISBN: 978-989-8425-56-0

It contains more information which can reflect the trust status of target web services. Web services registered in a WSI are not required to be physically stored together. They are virtually tied up and just need to register in WSIs.

The existence of WSIs would benefit all the involved parties. It is a good platform for web services to exhibit and advertise themselves. It also provides convenient ways to search ideal web services and conveys more information to users. Finally, WSIs themselves also benefit from linking web services and users. Usually the provided features of advertisement and service registration are not free. Therefore, we can safely conclude that the existence of WSIs brings win-win situation for all the involved parties.

The advant of WSIs also reflects a kind of inevitability in the evolution of the web service environment. If we view the whole web as a society, as the amount of resources increasing rapidly, there must be some effort carved from the whole labours to play as support roles. This makes parts of the social resources concentrate on collecting service information and provide searching features. Our proposed WSI structure is one of them. Therefore, WSIs is also a natural outcome during the evolution of the web service environment.

In general, WSIs build the bridge between web services and their users. They are virtual organizations that provide more comprehensive information of web services to their users.

3 FRAMEWORK ARCHITECTURE

Our research focus is on facilitating users to determine trustworthiness of web services via WSIs. In doing so, our framework architecture must accomplish the following two tasks: (1) enable WSIs to gain information on web services registered in WSIs; (2) enable user to determine the trustworthiness of WSIs. Bearing these two purposes in mind, we design the architecture depicted in Figure 1.

The above figure shows the framework architecture of a WSI and how the whole structure interact with the current web service environment. To participate in a WSI, web services are required to register via the interface for web services. Registration Manager will pass the information to WSI Database and Service Status Monitor starts to watch the registered web services and to record the status information. When a query comes via the Interface for Web Service Users, it first goes into WS Search Engine, which sends request to Service Trust Analyser. Service Trust

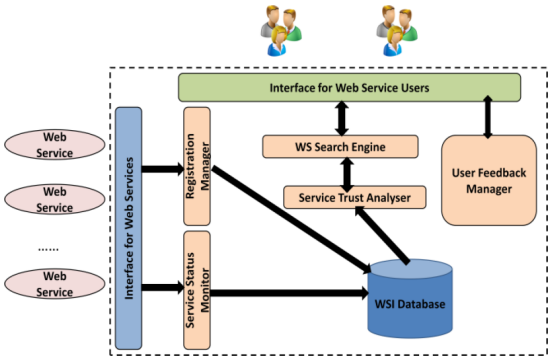


Figure 1: Architecture of Web Service Institution.

Analyser will use trust determination logic and the service status information in the database to calculate the trustworthiness which will be posted back to the user interface. There is another component called User Feedback Manager for accumulating user feedbacks and processing them to form institution-level trust value.

A user query gets a result with two parts: web services information, which includes web service URLs and trust values for both the web service and the. The calculation logic of service-level and institution-level trust will be specified in the next section.

4 TRUST FACTORS AND CALCULATION

The trustworthiness of a web service in a WSI consists of two dimensions: the trustworthiness of the WSI and the web service. Our trust determination logic uses weighted sum to integrate the two dimensions as below:

$$T = w_i(\sum W_i^{in} C_i^{in}) + w_s(\sum W_i^{ws} C_i^{ws}) \qquad (1)$$

$\sum W_i^{in} C_i^{in}$ and $\sum W_i^{ws} C_i^{ws}$ are the sum of the weights multiplied by the contribution of every trust factor for the corresponding dimension and satisfy $\sum W_i^{in} = 1$ and $\sum W_i^{ws} = 1$. w_i and w_s are the weights of the two dimensions and their sum also equals to 1. All the weight values are in [0,1]. Users of our framework can decide them based on their own knowledge and perference. In the following parts, we will go through institution-level factors and service-level factors and discuss their calculation logics in detail.

4.1 Institution-level Trust Factors

For a WSI, four institution-level factors are discussed. They are: (1)Processing Efficiency, (2) Per-

ception Deviation, (3)Information Transparency, and (4) Monitor Effectiveness.

Processing Efficiency (PE). PE is defined as the proportion of the number of on-time returns over the number of total returns for a WSI. Here we assume that each WSI has a promised response time, which, if exceeds, should be regarded as "fail to complete jobs in its promised efficiency". If a WSI does not claim its promised response time, users can define a threshold value based on their expectation or actual situation. We use the formula, $C_{PE} = \frac{\delta_o}{\delta_f}$ to calculate PE, in which δ_o is the number of user feedback on PE saying that a WSI completes its job on time and δ_f is the total number of user feedback on PE.

Perception Deviation (PD). PD reflects the difference between a WSI's opinion and users' opinions towards a specific web service. Suppose that there are n web services registered in a WSI. Given two vectors $(\varepsilon_1^u, \varepsilon_2^u, ..., \varepsilon_n^u)$ and $(\varepsilon_1^w, \varepsilon_2^w, ..., \varepsilon_n^w)$, ε_i^u is the summed score given by all the users to Web Service i. ε_i^w is the total number of times of the users who score Web Service i. One user can only score 1 or 0 for a web service at one time to indicate whether the trust value given by the WSI complies with its own experience. Users have the same opinion with the WSI if $\sum \varepsilon_i^u = \varepsilon_i^w$. Otherwise, $\varepsilon_i^u \leq \varepsilon_i^w$. At beginning of a WSI's formation, all the elements in the two vectors equal to 0. When a user gives feedback to Web Service i, ε_i^u will increase 1 or 0 depending on the user feedback. ε_i^w will always increase 1. PD is calculated as $C_{PD} = \frac{1}{n}\sum_{i=1}^{n} \frac{\varepsilon_i^u}{\varepsilon_i^w}$.

Information Transparency (IT). IT indicates the extent of publicity and reliability of the information released by a WSI. To calculate IT, We first classify information publicity into four different levels: (1) Absolutely transparent; (2) Key-step transparent; (3) Key-step partially transparent; and (4) Not transparent. Level i deserves a score of λ_i and follow the condition such that $\lambda_i > \lambda_{i+1}$. The levels and their scores are configurable. Meanwhile, we define another configurable parameter denoted as γ, ranging in $[0, 1]$, to represent information reliability. Information transparency, then, can be calculated as $C_{IT} = \frac{\sum_{j=1}^{N} \gamma^j \times \lambda^j}{N \times \lambda_{min(i)}}$, where γ^j and λ^j represents the reliability and publicity given by the jth user and N is the total number of times of user feedback.

Monitoring Effectiveness (ME). ME represents how effective web services are monitored, which can be divided into two parts: monitoring frequency (MF) and Monitoring Coverage (MC). MF stands for the reasonableness of current monitoring frequency. MC represents the percentage of web services covered by the monitoring mechanism. Supposet that N users have given their feedback. Each user can score 0 or 1 to both sub factors. The total score are denoted by κ_{mf} and κ_{mc}. ME is calculated as $C_{ME} = \frac{\kappa_{mf} + \kappa_{mc}}{2N}$.

To integrate the above four institution-level factors, the trustworthiness of a WSI is calculated as $T_{in} = w_{PE}C_{PE} + w_{PD}C_{PD} + w_{IT}C_{IT} + w_{ME}C_{ME}$, in which $w_{PE} + w_{PD} + w_{IT} + w_{ME} = 1$. Users can add other factors or replace some of them. However, the newly added factors have to satisfy that the contribution of the factor C_* must be scaled to [0, 1] and the sum of all the weight values must be 1.

4.2 Service-level Trust Factors

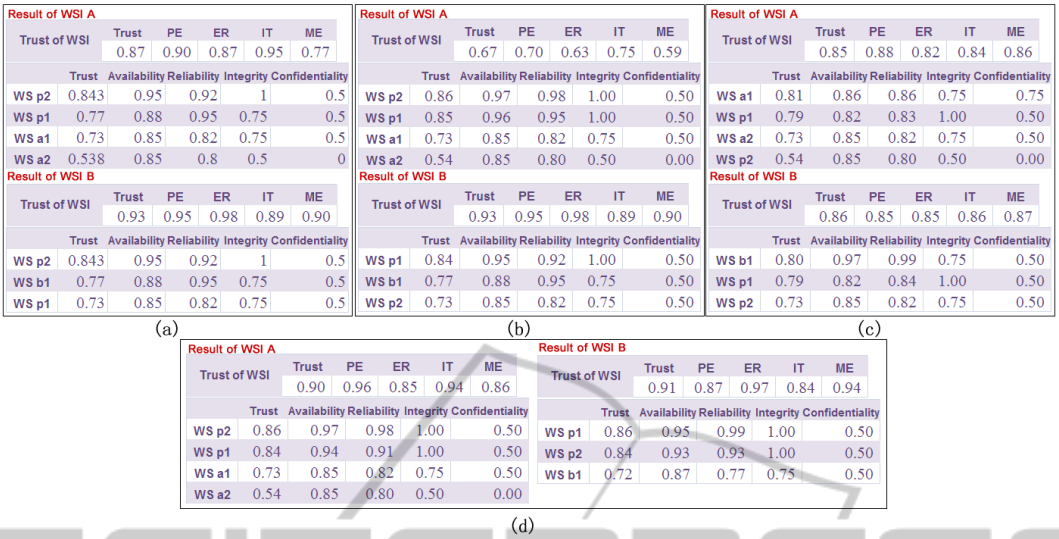
Same as institution-level factors, we captured four factors at service level. They are availability, reliability, integrity and confidentiality.

Availability. Availability of a web service is the ratio of the period in which the service is accessible over the total test period. It was listed as a QoS factor in many literatures (Ran, 2003) (Wang and Vassileva, 2007). Given a certain duration D and a checking frequency f, if we denote the total accessible times in D_a as ρ, calculation of availability is $C_{av} = \frac{\rho}{D_a \times f}$. Given different D and f, the availability of a certain web service at a certain time point may vary. In our framework, these two variables are configurable.

Reliability. Reliability is defined as the ability of a web service to perform its functions under promised conditions and restrictions. We use failure rate to calculate reliability. In duration D_r, denote the number of failed transactions as φ_f and the number of total transaction as φ_t, the reliability can be calculated as $C_{re} = \frac{\varphi_f}{\varphi_t}$. The cycle duration D_r is a configurable variabile in our framework.

Integrity. Integrity of a web service is the correctness, compatibility and completeness of transactions and data processed by the web service. In (Ran, 2003), it is described by the ACID properties (atomicity, consistency, isolation and durability). We use the following formula, $C_{in} = W_a V_a + W_c V_c + W_i V_i + W_d V_d$ to calculate integrity, where all the weights are configurable and satisfy $W_a + W_c + W_i + W_d = 1$ and V_a, V_c, V_i, and V_d are boolean values to indicate whehter the web service supports the corresponding feature.

Confidentiality. International Organization for Standardization (ISO) define confidentiality as "ensuring that information is accessible only to those authorized to have access". Our calculation is based on whether the web service support cryptography and "A-A" (Authentication and Authorization). We use



Result of WSI A

Trust of WSI	Trust	PE	ER	IT	ME
	0.87	0.90	0.87	0.95	0.77

	Trust	Availability	Reliability	Integrity	Confidentiality
WS p2	0.843	0.95	0.92	1	0.5
WS p1	0.77	0.88	0.95	0.75	0.5
WS a1	0.73	0.85	0.82	0.75	0.5
WS a2	0.538	0.85	0.8	0.5	0

Result of WSI B

Trust of WSI	Trust	PE	ER	IT	ME
	0.93	0.95	0.98	0.89	0.90

	Trust	Availability	Reliability	Integrity	Confidentiality
WS p2	0.843	0.95	0.92	1	0.5
WS b1	0.77	0.88	0.95	0.75	0.5
WS p1	0.73	0.85	0.82	0.75	0.5

(a)

Result of WSI A

Trust of WSI	Trust	PE	ER	IT	ME
	0.67	0.70	0.63	0.75	0.59

	Trust	Availability	Reliability	Integrity	Confidentiality
WS p2	0.86	0.97	0.98	1.00	0.50
WS p1	0.85	0.96	0.95	1.00	0.50
WS a1	0.73	0.85	0.82	0.75	0.50
WS a2	0.54	0.85	0.80	0.50	0.00

Result of WSI B

Trust of WSI	Trust	PE	ER	IT	ME
	0.93	0.95	0.98	0.89	0.90

	Trust	Availability	Reliability	Integrity	Confidentiality
WS p1	0.84	0.95	0.92	1.00	0.50
WS b1	0.77	0.88	0.95	0.75	0.50
WS p2	0.73	0.85	0.82	0.75	0.50

(b)

Result of WSI A

Trust of WSI	Trust	PE	ER	IT	ME
	0.85	0.88	0.82	0.84	0.86

	Trust	Availability	Reliability	Integrity	Confidentiality
WS a1	0.81	0.86	0.86	0.75	0.75
WS p1	0.79	0.82	0.83	1.00	0.50
WS a2	0.73	0.85	0.82	0.75	0.50
WS p2	0.54	0.85	0.80	0.50	0.00

Result of WSI B

Trust of WSI	Trust	PE	ER	IT	ME
	0.86	0.85	0.85	0.86	0.87

	Trust	Availability	Reliability	Integrity	Confidentiality
WS b1	0.80	0.97	0.99	0.75	0.50
WS p1	0.79	0.82	0.84	1.00	0.50
WS p2	0.73	0.85	0.82	0.75	0.50

(c)

Result of WSI A

Trust of WSI	Trust	PE	ER	IT	ME
	0.90	0.96	0.85	0.94	0.86

	Trust	Availability	Reliability	Integrity	Confidentiality
WS p2	0.86	0.97	0.98	1.00	0.50
WS p1	0.84	0.94	0.91	1.00	0.50
WS a1	0.73	0.85	0.82	0.75	0.50
WS a2	0.54	0.85	0.80	0.50	0.00

Result of WSI B

Trust of WSI	Trust	PE	ER	IT	ME
	0.91	0.87	0.97	0.84	0.94

	Trust	Availability	Reliability	Integrity	Confidentiality
WS p1	0.86	0.95	0.99	1.00	0.50
WS p2	0.84	0.93	0.93	1.00	0.50
WS b1	0.72	0.87	0.77	0.75	0.50

(d)

Figure 2: Mock data of the Use Cases.

the formula $C_{conf} = W_{cryp}V_{cryp} + W_{AA}V_{AA}$ to calculate confidentiality, where W_{cryp} and W_{AA} are the two configurable weight numbers of cryptography and A-A and satisfy $W_{cryp} + W_{AA} = 1$. V_{cryp} and V_{AA} are boolean values to indicate whether the web service supports corresponding feature.

The following formula is for integrating the service-level factors: $T_{ws} = W_{avai}C_{avai} + W_{reli}C_{reli} + W_{inte}C_{inte} + W_{conf}C_{conf}$ with the sum of all weights is equal to 1. This formula combined to the institution-level formula gives the whole logic for calculating trustworthiness of a web service in a WSI.

5 TYPICAL USE CASES

Four typical situations are given to guide users on how to use the proposed framework. An ideal situation is shown in Figure 2 (a), in which WS p2 gains the highest trust score in both of the WSIs. The trust values of the two WSIs are also relatively high. The user can easily recognize WS p2 is the good choice. In the situation of Figure 2 (b), the data provided by WSI B is more trustworthy than that in WSI A. WS p1 is the rational choice for users since it gains high scores in both WSIs. In this case of (c), users have two options. If the user is conservative, they can directly choose WS p1. Users can also choose WS b1 to gain better stability, if they do not provide very sensitive information. In Figure 2 (d), WS p1 and WS p2 are top 2 in both WSIs but with different order. In this case, we suggest users can reset the weights of institution-level trust factors and put more weights on the factors that are important in their opinions and re-calculate the trustworthiness.

6 CONCLUSIONS

In this paper, we present framework architecture of web service institution to facilitate users determining trust of web services.We identify several service-level and institution-level trust factors and create a computational structure to calculate each of the factors and aggregate the result. Our next step is to do experiments with real data to determine the reasonable weights under different situations.

REFERENCES

Bonatti, P., Duma, C., Olmedilla, D., and Shahmehri, N. (2005). An integration of reputation-based and policy-based trust management. In *In Semantic Web Policy Workshop*.

Gefen, D., Benbasat, I., and Pavlou, P. (2008). A Research Agenda for Trust in Online Environments. *J. Manage. Inf. Syst.*, 24(4):275–286.

Ran, S. (2003). A model for web services discovery with qos. *ACM SIGecom Exchanges*, 4:1–10.

Wang, Y. and Vassileva, J. (2007). A review on trust and reputation for web service selection. In *Proceedings of the 27th International Conference on Distributed Computing Systems Workshops*, pages 25–, Washington, DC, USA. IEEE Computer Society.