A Review on Trust and Reputation for Web Service Selection

Yao Wang, Julita Vassileva
Department of Computer Science
University of Saskatchewan
{yaw181, jiv}@cs.usask.ca

Abstract
A trust and reputation mechanism is a mechanism using consumers' feedbacks to identify good services from bad ones. Compared with other approaches, it has more advantages in solving the selection problem for web services. The paper proposes a typology to classify trust and reputation systems using the three criteria, centralized or decentralized, person or resource, global or personalized. Inspired by the criteria, some potential research directions for web service selection are pointed out.

Key words
Trust, reputation, web service selection

1. Introduction

The Service Oriented Architecture (SOA) is “an architecture that represents software functionality as discoverable services on the network” [9]. As an implementation of SOA, web services are defined as a set of standards, SOAP, UDDI, WSDL, which enable a flexible way for applications to interact with each other over networks. SOAP (Simple Object Access Protocol) is the protocol for applications to communicate with each other. UDDI (Universal Description Discovery Integration) defines a registry for service providers to publish their services. WSDL (Web Services Description Language) is used to describe a web service’s capabilities and the interface to invoke it. A WSDL document is self-describing so that a service consumer can examine the functionality of the web service at runtime and generate corresponding code to automatically invoke the service. All these standards are XML-based (EXtensible Markup Language), which allows applications to interact with each other over networks, no matter what languages and platforms they are using. The two features, self-description and language-/platform-independence, distinguish web services from other distributed computing technologies, like CORBA (Common Object Request Broker Architecture) and DCOM (Distributed Component Object Model). Web services have won an increasing popularity.

Although the future of web services looks very promising, there are still some challenging problems. Web service selection is one of them. The focus of current web service techniques is on the functional aspects of services. A service provider publishes its service function description by which a service consumer can find the service. But in a redundant open system, a service consumer faces a dilemma in having to make a choice from a bunch of services offering the same function. At this time, a service consumer needs to know not only what a service can do, but also how well a service can do, evaluated according to some quality of service (QoS) metrics. Current web service technology cannot support QoS or other non-functional aspects of a service. A service consumer is forced to either make a selection manually at design time depending on some external information resources or it has to make a random choice, which is a blind choice. In an open environment where anyone can publish services, a consumer may select a poor quality, time-consuming, expensive, or even harmful service. Therefore, mechanisms are needed to help consumers to distinguish good from bad services. Various trust and reputation mechanisms have been proposed and implemented to guide choice in many other open systems, like e-commerce, peer-to-peer, and multi-agent systems. Recently, trust and reputation mechanisms have also been applied to web service systems [13, 16, 18-21]. Since trust and reputation mechanisms have several advantages over other web service selection methods (see Section 2), they are getting more attention from web service researchers. In this review paper, we are going to discuss current trust and reputation solutions for web service selection and explore further opportunities for developing trust and reputation mechanisms for web services by examining systematically trust and reputation mechanisms proposed for other open systems. Two web service selection scenarios and the currently used web service selection methods are presented in the next section. Section 3 discusses the existing trust and
reputation mechanisms for web service selection. Section 4 introduces a typology to classify trust and reputation systems proposed for other open systems. Section 5 discusses future directions for using trust and reputation in web service selection.

2 Web service usage scenarios and current approaches for web service selection

![Figure 1. Two web service usage scenarios](image1)

The main application of web services is in business-to-business interactions. The scenarios where a business uses a web service can be classified into two types: direct selection and mediated selection. Direct selection means that the client gets directly the result of the service, i.e. a computation result, for example, a weather report from the web service provider, as shown in Figure 1 A. In this scenario, the selection of web service is mainly determined by the properties of the web service itself. The mediated scenario is to use a web service to get (indirectly) a result from another service, called “general service” in Figure 1 B to differentiate it from the intermediary web service. For example, a consumer uses a flight booking web service like Expedia.com to get a flight service (the general service) from an airline company like Air Canada. For the scenario B, the major part of selecting a web service is decided by the general service properties, for example, the quality of the flight service. The properties of the intermediary web service (the flight booking service in the example) only play a small part in the web service selection since the web service is just a tool to acquire the general service.

![Figure 2. Activities model](image2)

Figure 2 shows activities of different parties in the process of web service selection. It relates to different solutions for automatic WS selection from a high level. The central QoS registry in Figure 2 is a central node used to collect and store QoS information in a web service system.

A provider may advertise a service with a QoS description. Therefore the most common solution for service selection depends on the QoS information from service providers [16]. Although the provider is supposed to deliver the service with the described quality, it is not an agreement or obligation. A provider can deliver a service not according to its published QoS description. A provider may also exaggerate its capability of providing good QoS on purpose to attract consumers to get more benefits, such as money. A consumer is vulnerable to inaccurate QoS information. Therefore, in order to get a service with a guaranteed quality, a consumer can negotiate with a provider to make an agreement, called a Service Level Agreement (SLA) which specifies the quality that a service should meet. A SLA may also include the methods of how to measure different QoS metrics. A third party may be involved to supervise the service and do the justice. The SLA expresses an obligation of a service provider, who may have to pay a penalty when the service is not delivered according to SLA. However, making a SLA comes with a cost, such as time, expenses. This method relies on the establishing of a common ontology so that providers and consumers have the same understanding of various QoS metrics.

No matter whether a service advertisement comes with QoS information or not, a central node or a third party can be used to provide a service’s QoS information. They can either actively monitor QoS, or collect consumers’ QoS feedback, or use both ways. Sensors can be deployed to monitor web services and constantly report QoS data to the central node or third party [27]. This method is very costly since each web service needs a sensor to monitor it.
It is only suitable for a small system. In a large open system, there may be hundreds and thousands of web services. It is very hard to deploy each sensor for each service since the cost will be huge. In addition, in a dynamic environment where new services may often come in and old services may disappear, it also creates a lot of overhead to install or remove sensors. Even though the central node/third party can actively monitor each web service by itself to collect QoS information, this method is still not suitable for large systems since it puts too much burden on the central node/third party. Maximilien and Singh proposed a method where the central node just takes part of the responsibility of monitoring web services [19]. In their method, agents are used to interact with each other on behalf of their users providing or consuming services. The central node can actively create consumer agents, called explorer agents, to consume services that have a negative reputation for their quality. Once the explorer agents find that the service quality has been improved, they can help the services gain positive reputation so that they have a chance to be selected by other consumer agents. Therefore the purpose for the central node to monitor services with a negative reputation is just to give the services a chance to be selected when they improve their service quality.

Another way that the central node/third party acquires QoS information is to collect feedback from consumers who actually consume the services [16, 19]. The feedback from consumers may have two kinds of information. One is quality information collected from actual execution monitoring, such as response time and execution time. The other is ratings about the quality of the service, especially the QoS aspects like accuracy that can not be acquired through execution monitoring. This method has three advantages over the method using a central QoS registry/third party to do the monitoring. First, it can greatly lower the burden of the central node. The central node does not need to check the QoS of each service constantly. Secondly, it is much easier to implement. Thirdly, and most importantly, it allows capturing QoS information directly from consumers that can not be obtained by a central monitor. Because of these advantages, researchers are showing more and more interest in applying trust and reputation mechanisms for web service selection since they are exactly the mechanisms relying on consumers’ feedbacks to identify services (good or bad).

3. Trust and Reputation

Trust and reputation mechanisms are used for large open systems. In general, reputation is the public’s opinion about the character or standing (such as honesty, capability, reliability) of an entity, which could be a person, an agent, a product or a service. It is objective and represents a collective evaluation of a group of people/agents, while trust is personalized and subjective reflecting an individual’s opinion. Trust can be transitive [10]. For example, Alice trusts her doctor and her doctor trusts an eye specialist. Then Alice can trust the eye specialist. The notions “trust” and “reputation” are closely related. Trust can be gained from a person/agent’s own experiences with an entity or the reputation of the entity, while an entity’s reputation relies on the aggregation of each individual person/agent’s experiences with it. Trust and reputation are both used to evaluate an entity’s trustworthiness. They also share some common characteristics.

- **Context specific.**
  Trust and reputation both depend on some context. For example, Mike trusts John as his doctor, but he does not trust John as a mechanic to fix his car. So in the context of seeing a doctor, John is trustworthy, but in the context of fixing a car, John is untrustworthy.

- **Multi-faceted.**
  Even in the same context, there is a need to develop differentiated trust in different aspects of a service. The same applies for reputation. For instance, a user might evaluate a web service from different QoS aspects, such as response time, accuracy, execution time. For each aspect, she develops a kind of trust. The overall trust depends on the combination of the trusts in each aspect. While the context-specificity accentuates that trust or reputation can be different in different situations, the characteristic, multi-faceted, emphasizes that trust has multiple aspects, which can play a role in deciding whether a service is trustworthy to use.

- **Dynamic.**
  Trust and reputation can increase or decrease with further experiences (interactions or observation). They also decay with time. New experiences are more important than old ones since old experiences may become obsolete or irrelevant with time passing by.

3.1 Questions about trust and reputation mechanisms for web service systems

In a web service system, a trust and reputation mechanism is a mechanism of making a web service selection using trust, reputation and other information. There are some key questions to consider when designing a trust and reputation mechanism for a web service system.

1) When should a trust and reputation mechanism be used?

A trust and reputation mechanism is used for web service selection. The major way currently used is
selecting a service manually at design time by software developers and/or the members of the community that software developers are serving, according to their requirements and the service information from a web service system [6]. But this task becomes very tedious and time-consuming when people have to examine lots of various services that have different features and varying levels of QoS. The alternative way is to do the selection automatically at run time by the system. It can make the fulfillment of a task much easier and faster, but also raise higher the requirements for a trust and reputation mechanism. In a selection system requiring human participation, human knowledge (e.g. common knowledge) and preferences will play a role in the selection process. For example, for a web service that offers a mathematical computation service, a common knowledge can be “everyone prefers a short execution time and a low price”. A trust and reputation mechanism could be very simple in this case, just providing some statistic data from users’ feedbacks on the service’s execution time. However, in an automatic selection system, a trust and reputation mechanism has to be able to not only provide statistic data, but also capture and use the common knowledge and people’s preferences in the selection process.

2) What kind of information is needed for a trust and reputation mechanism?

QoS has been discussed a lot in the literature and seen as the major criteria for selecting web services. It is defined in various ways and measured by different metrics, which causes confusion sometimes. After examining existing research efforts in the area of web services, the W3C group gives a summarized guide about defining QoS and its metrics. They clarify that QoS refers to the quality aspects of a web service [15], which include the metrics as shown in Figure 3. These metrics are used to select a web service for the first scenario A (direct selection) mentioned in Figure 1, where the web service selection is decided by the quality of web services. Trust and reputation are built for each quality aspect of a web service (i.e. each metric). The overall trust and reputation depend on the combination of trust and reputation in each aspect.

In the second scenario (B, the mediated selection scenario mentioned in Figure 1), a web service selection depends on the quality aspects of a general service, which could be a hotel service, a flight service, or any other kind of service. Trust and reputation system should use the quality information of the general service. Since a general service is so diverse that it is very hard to generalize a list of common QoS metrics applicable for most services. Each domain has its own related QoS metrics.

Other information may be needed for a web service selection, such as cost of a web service, common knowledge, user preferences and others.

3) How can dishonest feedbacks or unfair ratings be detected?

A trust and reputation mechanism largely relies on users’ feedbacks or ratings to judge a service as good or not. However, it is inevitable that some users may provide false feedback to badmouth or raise the reputation of a service on purposes. Some methods have been proposed to combat this problem, such as the cluster filtering approach [5], the approach of using the majority opinion [26], and the approach of combining the reputation mechanism with the approach of cluster filtering [38].

3.2 Trust and reputation mechanisms for web services

Several trust and reputation approaches have been proposed for web service selection. Most of these approaches depend on a central QoS registry to collect
and store feedbacks from consumers. The general idea of these methods is that consumers report the data acquired from executing a web service (e.g. execution time, response time) and/or their ratings on other QoS metrics as shown in Figure 3 to the central QoS registry. According to the QoS information and a consumer’s profile that shows the consumer’s preference over different QoS metrics (i.e. how these QoS metrics are important to a consumer), the QoS registry will calculate an overall rating for each web service that matches the consumer’s search request. Then the consumer will select the web service with the highest rating. Although these approaches share the same idea, they are different in their focuses and calculation algorithms. Maximilien and Singh [18, 20, 21] put a lot of effort on building a QoS ontology, the basis for service providers to advertise their services and for consumers to express their preferences and provide ratings. Liu, Ng and Zeng [16] proposed an algorithm about how to combine different QoS metrics to get a fair overall rating for a web service. Manikrao and Prabhakar [17] use the collaborative filtering technology in their web service selection method. Karta [13] also proposed to apply collaborative filtering techniques to web service selection. He concentrated on the technical details of the collaborative filtering method, for example the selection of similarity calculation algorithm (Pearson correlation algorithm vs. Vector Similarity algorithm). In Day’s thesis [5], he suggested two algorithms for web service selection, a rule-based expert system and naïve Bayesian networks. As far as we know, the only trust and reputation approach for decentralized web service system is proposed by Vu, Hauswirth and Aberer [29]. They use some dedicated QoS registries to collect QoS feedbacks from consumers. Although these QoS registries are organized in a P2P way, they are based on a specially designed P-Grid structure. Each registry is responsible for managing reputation for a part of service providers. An algorithm is introduced to detect and deal with dishonest feedbacks by comparing the QoS data from dedicated monitoring agents with the data from consumers to filter out dishonest feedbacks. This approach is much more complicated than the centralized trust and reputation methods and involves a lot of communication and calculation because of the use of the complicated P-Grid structure.

Although these trust and reputation methods are proposed for web services, the research on trust and reputation in the area of web services is still new and limited. In other areas, like eCommerce, multi-agent systems, peer to peer systems, trust and reputation mechanisms have been studied for a long time. These studies can provide valuable observations and theories for the studies in web services. A topology is introduced in the next section that presents an overview of various trust and reputation systems and used to explore further opportunities for developing trust and reputation mechanisms for web services.

4. Typology of trust and reputation approaches

Various trust and reputation systems have been proposed or implemented in different open systems, e.g. P2P, multi-agent or e-commerce systems. In attempt to systematically compare the various approaches, several classifications of trust and reputation mechanisms have been proposed [11, 22, 25]. They use the application areas, the algorithms, or some other characteristics (e.g. a mathematical approach vs a cognitive approach, different information sources) as criteria. But none of them allows comparing trust and reputation systems from the perspective we mention below, which is nontrivial in determining the underlying trust and reputation mechanisms.

Instead of using a flat structure, we use three criteria to analyze existing trust and reputation systems, resulting in a classification as a three-level hierarchy as shown in Figure 4. The leaf-level represents examples of various trust and reputation systems. More details on each system can be found in [32]. Each upper level in the tree is associated with one criterion used for classifying reputation systems. The three criteria are explained below.

- **Centralized vs. decentralized.** Whether a trust and reputation system is centralized or decentralized determines the feasibility and complexity of a trust and reputation mechanism. In a centralized system, a central node will take all the responsibilities of managing reputations for all the members. In a decentralized system, e.g. a peer-to-peer system, there is no central node. The members in the system have to cooperate and share the responsibilities to manage reputation. Generally speaking, the mechanisms in centralized systems are less complex and easier to implement than those in decentralized systems. But they need powerful and reliable central servers and a lot of bandwidth for computing, data storage, and communication.

Almost all of the current trust and reputation mechanisms proposed for web services [13, 16, 18-21] are centralized where a central QoS registry is deployed to collect and store QoS data from web service consumers. It is based on a classical web service framework where a central UDDI server is used to publish and search services for web service providers and consumers. It is inevitable that this server-centric framework will suffer a single point of failure. Moreover, the information stored in the UDDI server may become outdated in a dynamic networking environment where a service may fail or
become unreachable. Therefore, peer to peer web services have been proposed [9, 14, 28], which leads to the need to learn decentralized trust and reputation techniques.

- **Person/agent vs. resource.** Trust and reputation systems can be classified as person/agent systems or resource systems. In person/agent systems, the focus is modeling the reputation of people or agents, acting on behalf of people. In resource systems, the focus is modeling reputation of resources, which could be products or services. Many resource systems also involve dealing with the reputation of people/agents, but it serves for the purpose of building representation of the reputation of resources. This criterion draws the line between the eBay-like reputation systems and the reputation systems, such as Amazon, Epinions.

In a trust and reputation web service system, it is obvious that trust and reputation need to be established for web services themselves. There is also a need to build trust and reputation for service providers, which has been neglected in current trust and reputation approaches for web services. A good reputation of a service provider can enhance a consumer’s confidence in its services. For example, a provider may provide several services at the same time. If the provider has a good reputation for providing good quality services, it is easy for a consumer to believe that a new service offered by this provider has a good quality too. If a service provider has a good reputation for her honesty, consumers would like to believe what she says about her new service.

- **Global vs. personalized.** In global reputation systems, the reputation of an entity (i.e., a person/agent/product/service) is based on the opinions from the general population, which is public and visible to all the members, while in personalized reputation systems, for a particular member, the reputation of an entity is built on the opinions from a group of other members selected by the particular member. Therefore, for the particular member, the reputation of the entity is personalized. The reputation of an entity is influenced by many factors, such as the particular member’s social network, environmental uncertainties, priorities, interests, preferences etc. It is much harder and more complicated to design a global reputation mechanism in a decentralized system than in a centralized system.

In web service systems, for some kinds of web services (e.g., weather forecast services), personalization is not important, so a global reputation system is sufficient. However, if the selection includes subjective factors, which have to do with a consumer’s special needs or interests, the problem of web-service selection becomes similar to the problem of generating personalized recommendations and personalized reputation systems are required.

![Figure 4. Trust and reputation system classification](image-url)
5 Future directions for using trust and reputation in web service selection

As Figure 4 shows, most of the current trust and reputation mechanisms proposed for web services [13, 16, 18-21], written in bold and underlined in Figure 4, belong to one branch in the classification - centralized, resources-based, and personalized trust and reputation mechanisms, which leaves space to research the suitability of many other types of mechanisms for web services.

- Decentralized trust and reputation mechanisms for peer-to-peer based web service systems
  Various peer to peer based web service techniques have been proposed [9, 14, 28], which require decentralized mechanisms for trust and reputation. As far as we know, the only trust and reputation approach for decentralized web service system is proposed by Yu, Haaswirth and Aberer [29]. But their approach is based on the complex P-Grid structure they developed. It is very complicated and hard to implement. Other solutions are still expected.

- Trust and reputation mechanisms for web service providers rather than just for web services
  Building trust and reputation for web service providers is beneficial for web service selection, and has been neglected in current trust and reputation approaches for web services. A good reputation of a service provider can enhance a consumer’s confidence in its services. More importantly, for the service for which the trust and reputation has not been established, e.g. a new service or a service that has not been selected by consumers, the trust and reputation of the service provider, accumulated by the provider from providing other services, can be used for the selection since if a provider has a good reputation for providing good quality services, a consumer would like to believe that its new service has good quality too.

- Application of existing global/personalized trust and reputation techniques to web services
  In a web service system, personalization is important so that the selected service meets the consumer’s special needs. Collaborative filtering is a good example for using the recommender system technology to personalize web service selection in a centralized system. The approach proposed by Zhang and Cohen [38] can also be applied to web service systems to combat the problem of unfair ratings. The decentralized methods proposed by Yu & Singh [35, 36] and Wang & Vassileva [31, 32] can be easily modified to apply to peer-to-peer based web service systems. Since not all web services need personalization, for example, a currency converter or a weather forecast service, some global reputation mechanisms that are simple and effective are also applicable to web service systems, like the one used in eBay. The mechanisms used by Epinions [8] may be suitable, too. There may be possibilities of applying other methods to web service systems. Further studies are needed.

Using trust and reputation mechanisms offers a promising way to solve the web service selection problem. Although this research on trust and reputation is still new in the area of web services, the investigation and application of the existing trust and reputation mechanisms in other areas will definitely accelerate the research process for using trust and reputation in web services. More investigation and studies are still needed.

References

[7] eBay Available online at: http://www.eBay.com
[9] W. Han, Integrating Peer-to-Peer into Web Services, Master thesis, University of Saskatchewan 2006
P2P Networks”. In Proc. of the twelfth International Conference on World Wide Web, 2003


urs-ken.pdf.


