Trust Metrics for Services and Service Providers

Zainab M. Aljazzaf, Mark Perry
Department of Computer Science
University of Western Ontario
London, Canada
{zaljazza, mperry}@uwo.ca

Miriam A. M. Capretz
Department of Electrical and
Computer Engineering
University of Western Ontario
London, Canada
mcapretz@uwo.ca

***Abstract*—Trust is as significant a factor for successful online interactions as it is in offline communities. Trust is an important factor that is used as a criterion for service selection. There is a need to know information about services and service providers to establish trust and identify their trustworthiness. Most trust studies focus on trust establishment for services without clearly identifying trust information for services and service providers. Services and service providers traverse many domains with different properties and requirements. Identifying a unified trust information (trust metrics) for such an open environment is a challenge. This paper proposes a unified trust metrics classification for services and service providers. The proposed trust metrics can be extended and used in an open environment or within specific domains to establish trust for services and service providers.**

Keywords - Trust; trust metrics; service; service provider.

I. Introduction

In human communities, there is uncertainty about the behaviour of strangers. People avoid interacting with others who they do not trust. Trust plays a significant role in facilitating the interaction in such uncertain environments. A *Trustor* is the subject that trusts a target trusted entity known as a *Trustee*. We define trust as *the willingness of the trustor to rely on a trustee to do what is promised in a given context, irrespective of the ability to monitor or control the trustee, even though negative consequences may occur* [1].

Building a distributed software system requires the interaction and use of resources from diverse organisations throughout the Web. In such diverse systems, different entities spread around different domains and organizations, and pass the boundary of a particular physical community, which may have clear security and trust preferences. Service Oriented Architecture (SOA) is "an architectural style for building enterprise solutions based on services" [2]. There are three roles in SOA as shown in Figure 1 [3]: *service provider*, an organization or platform that owns, implements, and controls access to the services; *service requestor*, an application, services, or the client who is looking for and invoking a service; and *service registry*, a searchable directory where the description of the services is published by the providers and searched by the requestors.

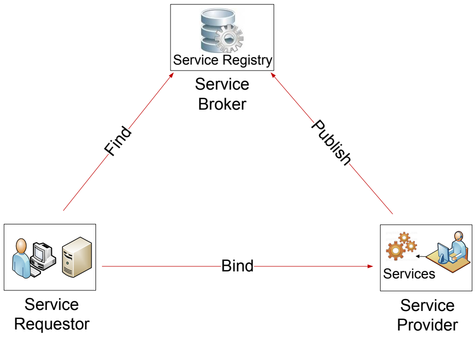

Fig. 1. Services roles and operations in SOA [3].

There are many services with similar functionalities. The non-functional properties of a service can be a differentiating factor between the similar services and as a criteria for service selection. Quality of Service (QoS) is the quality aspect of a service [4], and is considered as a non-functional property of a service. Trust has been used as a criteria for service selection [5][6][7][8]. The trustworthiness of a service is considered as a non-functional property of a service. Service requestor (trustor) may select a service/provider (trustee) based on its trustworthiness.

The trustworthiness of a service provider can enhance the requestor's trust in its services [9]. A requestor can select a service from providers of the highest level of trust [10]. Considering trustworthiness of service providers supports trust bootstrapping (rating new comers) the providers' new services. For example, if a provider is known to be a trustworthy, requestors will trust the provider's services and encourage to select its new services. Therefore, it is important to establish trust for service providers and select a service based on its provider's trustworthiness in addition to the service's own trustworthiness.

Trust is based on information [1], but it is difficult to determine the information that should be used. In the offline world, traditional forms of communication allow people to assess a wider range of cues related to trustworthiness than is currently possible through online communication. The Internet gives little evidence about the solidity of the entity behind it. The challenge is to find sufficient online substitutes for the traditional cues to trust, which are obvious in the physical world and identify new information elements, which are appropriate for deriving measures of trust [11].

ISBN: 978-1-61208-124-3

Trust Metrics (TM) is a new term and is defined in this paper as *the information of an entity that is required and used to evaluate the trustworthiness of the entity*. An entity, in this work, can be a service or service provider. TM is the first party (i.e., a service or provider) information provided by a service or service provider to evaluate its trustworthiness [1]. For example, a service can present its reliability as a trust metric for the requestors to trust the service based on the reliability trust metric. To identify trust metrics, it is important to explore what information is required to build trust for services and service providers.

Information has many dimensions and each service/provider sets its own information. In SOA, transaction may span a range of domains and organization. Services and service providers may traverse many domains with different properties and requirements. For example, a requestor of a service has many requirements and each seeks for different services' properties. Therefore, a domain may need to support a range of trust metrics and this requires to identify a unified trust metrics for such an open environment. Some studies try to overcome this problem by defining a notion of community [12] or address trust in specific domains [5][13][14]. This paper proposes a unified trust metrics classification for services and service providers that is suitable for SOA environment.

The rest of the paper is organised as follows: Section II presents related work. Trust metrics and trust principles is presented in Section III. Section IV presents trust metrics and QoS. The proposed trust metrics for services and service providers is presented in Section V. Section VI concludes the paper.

II. Related Work

In the literature, there is no clear identification of trust metrics for services. In addition, there is no defined trust metrics for service providers.

A. Trust Services

Zhengping et al. [15] defined domain specific trust information that is limited. The work monitors the behaviour of a trusted Web Service in case it has bugs during operation, which will drop the trust degree of the Web Service. The authors define properties to establish trust for services such as functions and run time environment, and for recommender who recommend a service such as popularity and authenticity of the description. Different domain characteristics defined by the system analyst. Kim and Doh [16] propose the selection of the optimal path to compose a number of Web Services based on QoS information and trust type (the computed trust level based on aggregated ratings from the consumer of the services, which indicate the estimation of the reliability of the service provider). The authors assume that trust type is associated with each service where the assignment of trust types performed by the clients themselves or trust authority. Trust metrics are not specified and trust is based on assumed trust type.

Maximilian and Singh [10] made a distinction between trust and QoS and presented the selection of a Web Service based on non-functional attributes such as QoS and trust. Wang and Vassileva [9] stated the importance to define information needed for trust and reputation mechanism. They stated the use of QoS to build trust where trust and reputation are built for each quality property of a service and the overall trust and reputation depend on the combination of trust and reputation for each property.

Other researchers address trust as a QoS [5][6][8][17], build trust based on a set of QoS [8][17][18][19], or build trust based on a set of QoS related to specific system, application, or domain [5][17][18][19]. Dragoni [5] mentioned that evaluation of trust is a key QoS aspect of Web Service selection. The author used security features of the service to establish trust (satisfying the provider's trust security requirements). Ying-Feng and Pei-Ji [6] specify trust or reputation as one of the QoS of Web Service. Kalepu et al. [8] identified a new QoS attribute, *verity*, as an important contributor to the quality driven selection and composition of Web Services and to be a measure of trustworthiness of a Web Service. Verity refers to the degree of variance in the compliance levels of the services and assesses the reputation of the provider based on local and global rating. They identify verity for Web Services and verity for Web Services providers. However, trust is not a QoS and there is a clear distinction between the two terms.

In [18], reputation is modelled as a vector of QoS attributes such as performance and reliability. Jin-dian et al. [19] establish trust based on whether it is secure enough to access a service or how to choose a more reliable provider. They measure the possibilities of providing cheating or malicious behaviour and satisfaction values to measure how satisfied a user feels about a given interaction (both are real numbers in [0,1] and a high rate reflects a high interaction quality). The trust evaluation can take many aspects (QoS requirements) into account such as process time and access speed. Vu et al. [17] rank services according to its prospective level of satisfying user's QoS requirements. However, building trust should consider other properties beside QoS.

B. Trust Service Provider

In Web Services and SOA, the idea of trusting a service based on its provider is neglected [9]. Trust in the Internet has a clear distinction between the two and has identified quality requirements for providers to assist their trustworthiness and help users in their decision to use providers' services [20][21].

Jin-Dian et al. [19] presented the idea of assigning trust provider rate to its new Web Services. They mentioned that assigning trust rate to the provider is an interesting research problem. They stated that a registry that has past experiences with the Web Service's provider initializes the rate of the new Web Service to be equal to its provider's rate.

The work in [18] assesses the trustworthiness of a Web Service provider by measuring its reputation based on the rate given by the user. However, identifying trust information supports the trust bootstrapping process (i.e., rating new services and service providers). Maximilien and Singh [10] mentioned that if service provider is already determined to be trustworthy, then the selection of services will be based on their provider's rating. The authors stated that determining the trust level to be assigned to providers is a nontrivial process. However, identifying trust metrics helps to establish trust.

III. Trust Metrics and Trust Principles

In our previous work [1], we identified the trust principles. This work follows the trust principles to identify TM. The TM addresses the following trust principles :

- Trust and risk: Requestors have no control over services that advertise only their interface. Less perception of control increases the risk. Under a risky exchange situation it is important to include penalties, rewards, insurance, and other risk remedies in case something goes wrong. Risk remedies can be identified as a TM.
- Trust development phases: Trust goes through three development phases: trust building, stabilising trust, and dissolution [21]. Most studies assume a system where trust and reputations already exist (i.e., stabilising trust phase). In trust building phase, it is important to initialize a trust rate for a new service or a new service provider. Identifying TM is important in the initialization process, where the TM are rated and the overall trust for a service and service provider can be the average of trust for each TM.
- Trust relationship properties: Trust is usually specified in terms of a relationship between a trustor and a trustee. Trust relationship can be one-to-one between a requestor and a service and one-to-many between a requestor and a group of services (i.e., a provider who provides a group of services). By identifying trust metrics the system can support the context specific characteristic of trust (trust a service to perform a specific action within a specific context), where a requestor can select a service based on a set of trust metrics.
- Trust is based on information. There is a need to know information about the services and service providers to establish trust.
- First party information: First parties (i.e., services/service providers) should provide the information to develop trust. For example, QoS properties and other information (e.g., delivery methods, insurance, privacy, security, pricing, and availability) can be considered as important information on which to build trust.
- The distinction between trust and QoS: Trust is not a QoS aspect of a service or a service provider. There is a clear distinction between the two terms' definitions as presented in the introduction. QoS properties can be identified as TM to establish trust.
- Security and privacy: Security and privacy are important factors to consider in the trust establishment process. Security and privacy can be considered as important TM.
- Provider's trustworthiness: Trust ratings of a service and its provider are related and each one affects the other. Therefore, it is important to identify providers' trustworthiness and define TM for service providers.

IV. Trust Metrics and QoS

QoS can be identified as an important TM to establish trust. This work defines QoS as TM. To identify TM for an open system, it is important to generalize a list of TM applicable for most services. As a part of generalization process, it is required to generalize QoS for diverse services and service providers. To define a unified TM classification, we need to extract diverse QoS from the literature. Some QoS can be measured and some are not. It is important to include and quantify the non-measurable QoS to be used in trust rating algorithm and calculation.

There are many research efforts to define and categorize QoS and how to express, quantify, and model them [4][16][22][23]. In [4][8][9][22][24][25][26][27][28][29] generic and business QoS requirements for services are presented. Lee and Shin [26] define a set of major Web Services' QoS attributes. Menasce [28] presents the QoS issues in web services. Yu et al. [23] present a list of QoS and how to calculate each. They specify that security is not quantifiable QoS but they present a formula to test the security of Web Services based on the number of attacks detections. Rahman and Meziane [27] present five essential QoS requirements based on the most used QoS from the literature. These are: readiness, transaction, reliability, speedy, and security.

O'Brien et al. [24] define other QoS requirements for SOA such as: modifiability, testability, and usability. Ran [22] identified other QoS, which are: supported standard, stability/change cycle, and completeness. In addition, there are a domain or application specific QoS. Hoyle [29] identifies other quality characteristics for services such as courtesy, comfort, competence, credibility, dependability, efficiency, effectiveness, flexibility, honesty, promptness, responsiveness. Larson [30] identified serviceability and user satisfaction as performance measurement of service delivery.

Moorsel [25] discusses quantitative metrics and a framework for evaluating internet services. Three metrics are defined that should be emerged to evaluate Business to Consumer (B2C), Business to Business (B2B) and service provider systems. The metrics are: QoS, Quality of Experience (QoE), and Quality of Business (QoBiz). QoE and QoBiz are claimed to quantify the user experience and business return, respectively.

Based on the aggregated QoS in the literature, we propose a classification of QoS into objective QoS and subjective QoS, as shown in Figure 2. Objective QoS are the QoS that can be measured. Subjective QoS are the QoS that cannot be measured. This classification helps to define and classify TM.

V. Trust Metrics

In this work, TM overcome other trust information in the literature to include information of diverse domains (government, online marketing, bank, etc), QoS, and different possible services and service providers' information and properties. Some TM may not be applied to all services and it is possible to add other TM. Figure 3 shows the proposed TM for services and service providers which is classified into Services Trust Metrics (STM) and service Providers Trust Metrics(PTM).

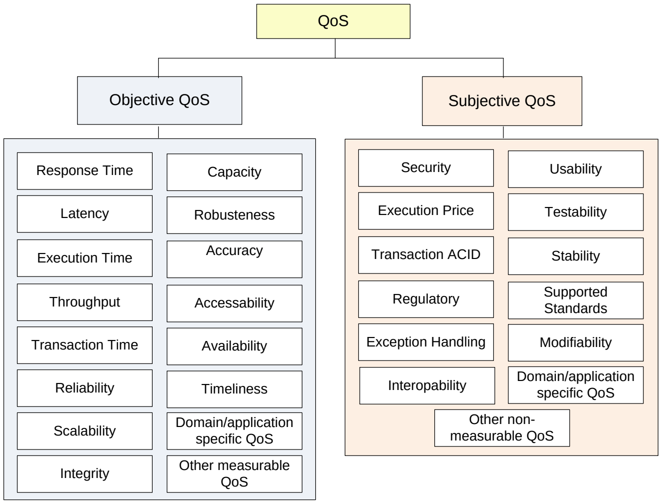

Fig. 2. A classification of QoS.

A. Trust Metrics for services (STM)

STM is classified into Objective STM (OSTM) and Subjective STM (SSTM) as follows:

1) Objective Services' Trust Metrics (OSTM): OSTM are the TM that can be measured. OSTM for services are their objective QoS properties such as response time, latency, execution time, throughput, reliability, domain specific measurable properties, and other services' measurable properties. In the following, a number of OSTM is presented:

- Execution Time OSTM, $OSTM_e(s)$: Is the time taken by a service to execute and process its sequence of activities.
- Latency OSTM, $OSTM_l(s)$: Is the delay time between sending a request and receiving the response, i.e., the time the message needs to reach its destination.
- Response Time OSTM, $OSTM_r(s)$: Is the time required to process and complete a service request.
- Throughput OSTM, $OSTM_{thp}(s)$: Refers to the number of requests a service can process per unit of time.
- Availability OSTM, $OSTM_{Av}(s)$: Is the probability that a service is up and accessible to use.
- Reliability OSTM, $OSTM_R(s)$: Refers to the ability of a service to perform its function correctly with either 'no fail' or 'response failure to the user'. It is related to $OSTM_{Av}(s)$.

2) Subjective Services' Trust Metrics (SSTM): SSTM are the TM that are hard to measure directly. SSTM include functional properties, subjective QoS properties, and other properties of services such as remedies, payment satisfaction, output/item satisfaction, delivery satisfaction, domain specific non-measurable properties, and other non-measurable services properties. The following presents some SSTM. Because SSTM are not measurable TM, it is important to quantify them.

- Remedies SSTM, $SSTM_{rem}$: Is the most important metric that should be provided by a service provider for each of its services. Services should provide remedies in case any thing goes wrong. Each service has different remedies. For example, if the service is shipment service and there was a delay in shipment, lower the shipment price can be offered as a remedy. Another example is that if a service provides a video and the video was slow referred to the subscribed level of a customer, the service should increase the bandwidth for that customer.
- Security SSTM, $SSTM_{sec}$: A requestor can trust a service or service provider based on security. Security is an important factor to be considered in trust establishment.
- Privacy SSTM, $SSTM_{prv}$: A requestor can trust a service or service provider based on privacy. Privacy is an important factor to be considered in trust establishment.
- Payment Satisfaction SSTM, $SSTM_{pym}$: Refers to the degree of the user satisfaction on the offered service based on the payment, if any. For example, do the service charge the user the same or extra amount, do users pay extra unexpected fees, etc.
- Output/Item satisfaction SSTM, $SSTM_{out}$: Refers to the degree of the user satisfaction on the offered service based on the output/item provided. For example, do they get the same output/item they ordered/expected, are they satisfied with the output/item, the quality of the output/item they received, etc.
- Delivery satisfaction SSTM, $SSTM_{delv}$: Refers to the degree of the user satisfaction on the offered service based on the delivery of the item. For example, do they deliver the item on time, do they return the item in case of dissatisfaction, etc.

3) Trust Metrics Collection for services: OSTM and SSTM are rated for each service and can be stored in a registry to be used for rating services and service providers. The following is the collected STM in a matrix format. Each row represents a service and each column represents one of the STM (m:s and n:STM). $STM = OSTM + SSTM$

$$\mathbf{STM} = \begin{bmatrix} STM_{11} & STM_{12} & \dots & STM_{1n} \\ STM_{21} & STM_{22} & \dots & STM_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ STM_{m1} & STM_{m2} & \dots & STM_{mn} \end{bmatrix}$$

Trustworthy services support remedies, security and privacy; provide high throughput, fast response time, high availability and reliability; provide lower execution, response and latency times. In addition, trustworthy services get high rates for the execution cost, output, payment, and delivery STM.

B. Trust Metrics for service Providers (PTM)

A good provider rate can enhance the requestor's trust in the provider and its services. If a requestor has an alternative to choose between many services from different providers, he can select a provider with a higher trust rate. Rating providers help to encourage providers to behave well, increases the opportunities of the providers to be selected by consumers, encourage competition between providers, influence the economic growth of the providers positively, increase the usage of the Internet technologies such as e-markets, and evolve commerce online.

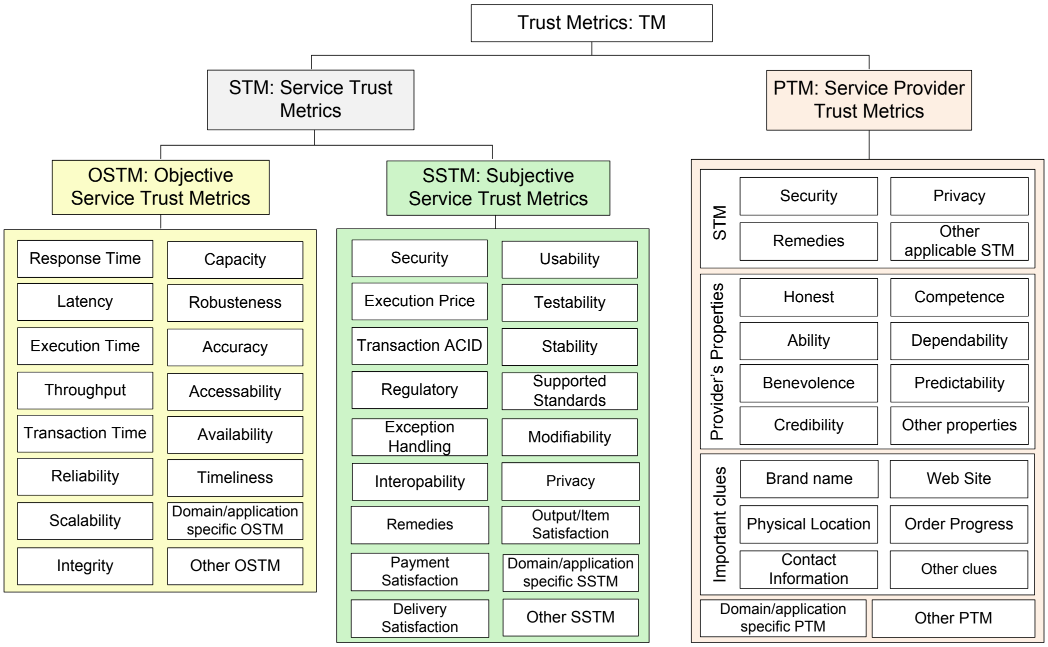

Fig. 3. Trust Metrics.

Trustworthiness of a service provider is based on the *trustworthiness of its services* and the rates of its *properties*. Service providers have many properties that can be considered as useful PTM to build trust. A trustworthy service provider should behave upon its advertised properties and its services advertised properties (i.e., STM). In addition to providers' properties, a provider can provide important clues for requestors to assess its trustworthiness. In the following, a number of important PTM are presented.

1) Providers' services' properties: A service provider trustworthiness is based on the trustworthiness of its services. Therefore, STM are implicitly included as metrics to evaluate providers. Any STM can explicitly be identified as PTM to emphasize its importance and can be used as PTM such as security PTM, PTM_{sec}; privacy PTM, PTM_{prv}; remedies PTM, PTM_{rem}; and other applicable STM such as reliability, integrity, robustness, accessibility, availability, timeliness, payment satisfaction, output/item satisfaction, delivery satisfaction, transaction ACID, supported standards, interoperability, and stability.

2) Provider's properties: Competence, honesty, ability, benevolence, predictability, credibility, dependability, courtesy, comfort, efficiency, effectiveness, flexibility, promptness, and responsiveness are properties to be considered as PTM. These properties can be evaluated by long term interactions with a provider based on other TM. In the following, competence and honest PTM will be presented.

- Competence PTM, PTM_{comp}: Shows a provider's ability and capability to provide a service and perform the function expected from it (i.e., compliance). Competence is more relevant term for the environment related to services and computing system [31].
- Honest PTM, PTM_{hons}: The provider that continuously shows its competence will be honest.

3) Important clues: Service providers can provide important clues to support their trustworthiness. The more clues a provider provides, the more the provider can support its trustworthiness, and the more is the opportunity for its services to be selected by the requestors. Some clue information may suit some requestors but not others especially if the requestor is an application which dynamically bind to services. The following presents some important providers' clue information, as follows:

- Brand name PTM, PTM_{brand}: A service provider who has a brand name, popular name that is established by a long term interactions with consumers, may encourage the requestors to use its services. A brand name can help in the assessment of service providers' trustworthiness, and this will influence the economic growth of the service providers positively. Trust-based systems can play an important role on the establishment of brand names for service providers. A service provider can provide a name and the system can brand the name based on the level of the trustworthiness of the service provider.
- Web site PTM, PTM_{wsite}: A service provider who has a web site may give an important clue for the requestor to trust the provider and use their services. Web sites may contain information that can assess the trustworthiness of a service provider.
- Contact information PTM, PTM_{inf}: Contact information such as telephone number and e-mail has a great impact in the assessment of the trustworthiness of a service

provider. Having contact information allow the requestors to contact providers to, for example, resolve any issues.

- Retail location PTM, PTM_{loc}: Having physical location, such as physical store, may increase a provider's trustworthiness.
- Order progress PTM, PTM_{ord}: While order progress is more clear offline, it should be provided online, and this may increase a provider's trustworthiness.

4) Trust Metrics Collection for service Providers: The evaluated PTM rates for each service provider are stored in a registry to be used for rating purposes. The following is the collected PTM in a matrix format. Each row represents a service provider and each column represents one of the PTM (m:provider and n:PTM).

$$\mathbf{PTM} = \begin{bmatrix} PTM_{11} & PTM_{12} & \dots & PTM_{1n} \\ PTM_{21} & PTM_{22} & \dots & PTM_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ PTM_{m1} & PTM_{m2} & \dots & PTM_{mn} \end{bmatrix}$$

Trustworthy service providers support remedies, security, and privacy and provide trustworthy services. In addition, trustworthy service providers provide important clues to support its trustworthiness. By the time, a service provider will become competence and then honest by acting as a trustworthy provider.

VI. Conclusion

This paper presents a unified trust metrics classification for services and service providers. Trust metrics cover different information and properties of services and service providers. The trust metrics are extendible and can support domain specific properties. Trust metrics support the trust principles. Each trust metric may require different techniques to gather and evaluate its trust rates. As a next step, trust models to rate the trust metrics, services, and service providers will be established. In addition, there is a need to build a trust framework that establish trust for services and service providers and supports trust-based service selection in SOA.

References

[1] Z. M. Aljazzaf, M. Perry, and M. A. Capretz, "Trust online: Definition and principles," *ICCGI 2010: The Fifth International Multi-Conference on Computing in the Global Information Technology*, 2010.

[2] M. Rosen, B. Lublinsky, K. T. Smith, and M. J. Balcer, *Applied SOA: Service-Oriented Architecture and Design Strategies*. Wiley Publishing, 2008.

[3] M. Papazoglou, *Web Services: Principles and Technology*. Prentice Hall, 2008.

[4] K. Lee, J. Jeon, W. Lee, S. Jeong, and S. Park, "QoS for web services: Requirements and possible approaches," W3C, Web Services Architecture Working Group, Tech. Rep., November 2003. [Online]. Available: http://www.w3c.or.kr/kr-office/TR/2003/ws-qos/, last accessed Jan, 2011

[5] N. Dragoni, "Toward trustworthy web services - approaches, weaknesses and trust-by-contract framework," *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, vol. 3, pp. 599–606, 2009.

[6] Z. Ying-Feng and S. Pei-Ji, "The model for consumer trust in C2C online auction," *ICMSE '06 International Conference on Management Science and Engineering*, pp. 125 –129, Oct. 2006.

[7] M. N. Huhns and M. P. Singh, "Service-oriented computing: Key concepts and principles," *IEEE Internet Computing*, vol. 9, pp. 75–81, 2005.

[8] S. Kalepu, S. Krishnaswamy, and S. Loke, "Verity: a QoS metric for selecting web services and providers," *Proceedings Fourth WISEW*, pp. 131 – 139, Dec. 2003.

[9] Y. Wang and J. Vassileva, "A review on trust and reputation for web service selection," in *ICDCSW '07: Proceedings of the 27th International Conference on Distributed Computing Systems Workshops*. Washington, DC, USA: IEEE Computer Society, 2007, p. 25.

[10] E. Maximilien and M. Singh, "Toward autonomic web services trust and selection," in *ICSOC*, M. Aiello, M. Aoyama, F. Curbera, and M. P. Papazoglou, Eds. ACM, 2004, pp. 212–221.

[11] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.*, vol. 43, no. 2, pp. 618–644, 2007.

[12] Z. Malik and A. Bouguettaya, "Reputation bootstrapping for trust establishment among web services," *IEEE Internet Computing*, vol. 13, no. 1, pp. 40–47, 2009.

[13] T. A. Khopkar, "Provision, interpretation and effects of feedback in reputation systems," Ph.D. dissertation, School of Information, The University of Michigan, 2008.

[14] G. Zacharia, A. Moukas, and P. Maes, "Collaborative reputation mechanisms for electronic marketplaces," *Decision Support Systems*, vol. 29, no. 4, pp. 371–388, 2000.

[15] L. Zhengping, L. Xiaoli, W. Guoqing, Y. Min, and Z. Fan, "A formal framework for trust management of service-oriented systems," in *SOCA '07: Proceedings of the IEEE International Conference on Service-Oriented Computing and Applications*. Washington, DC, USA: IEEE Computer Society, 2007, pp. 241–248.

[16] Y. Kim and D. Doh, "A trust type based model for managing QoS in web services composition," *International Conference on Convergence Information Technology*, vol. 0, pp. 438–443, 2007.

[17] L.-H. Vu, M. Hauswirth, and K. Aberer, "Qos-based service selection and ranking with trust and reputation management," vol. 3760 LNCS, Agia Napa, Cyprus, 2005, pp. 466 – 483.

[18] E. Maximilien and M. Singh, "Reputation and endorsement for web services," *SIGecom Exchanges*, vol. 3, no. 1, pp. 24–31, 2002.

[19] S. Jin-Dian, G. He-Qing, and G. Yin, "An adaptive trust model of web services," *Journal Wuhan University Journal of Natural Sciences*, 2005.

[20] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *The Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.

[21] T. Kautonen and H. Karjaluoto, Eds., *Trust and New Technologies: Marketing and Management on the Internet and Mobile Media*. Edward Elgar, 2008.

[22] S. Ran, "A model for web services discovery with QoS," *ACM SIGecom Exchanges*, vol. 4, no. 1, pp. 1–10, 2003.

[23] W. D. Yu, R. B. Radhakrishna, S. Pingali, and V. Kolluri, "Modeling the measurements of qoS requirements in web service systems," *Simulation*, vol. 83, no. 1, pp. 75–91, 2007.

[24] L. O'Brien, P. Merson, and L. Bass, "Quality attributes for service-oriented architectures," in *SDSOA '07: Proceedings of the International Workshop on Systems Development in SOA Environments*. Washington, DC, USA: IEEE Computer Society, 2007, p. 3.

[25] A. Moorsel, "Metrics for the internet age: Quality of experience and quality of business," 5th Performability Workshop, 2001.

[26] S. Lee and D. Shin, "Web service QoS in multi-domain," vol. 3, feb. 2008, pp. 1759 –1762.

[27] W. Rahman and F. Meziane, "Challenges to describe QoS requirements for web services quality prediction to support web services interoperability in electronic commerce," in *Proceedings of the 10th IBIMA Conference on Innovation and Knowledge Management in Business Globalization, Kuala Lumpur, Malaysia, 30 June - 2 July 2008, 4 (6) , pp. 50-58.*

[28] D. Menasce, "QoS issues in web services," *Internet Computing, IEEE*, vol. 6, no. 6, pp. 72 – 75, Nov/Dec 2002.

[29] D. Hoyle, *Automotive Quality Systems Handbook*, 2nd ed. Elsevier Ltd, 2005.

[30] K. Larson, "The role of service level agreements in it service delivery," *Information Management and amp; Computer Security*, vol. 6, no. 3, pp. 128 – 32, 1998.

[31] T. Grandison and S. Sloman, "A survey of trust in Internet applications." *IEEE Communications Surveys and Tutorials*, vol. 3, no. 4, 2000.