

A Survey on Trust in Semantic Web Services

V.Mareeswari, Dr. E. Sathiyamoorthy

Abstract— In the past many researchers worked in developing trust management models in various disciplines such as E-Business, Multi-Agent Systems, Web Services, Grid Computing, P2P networks, Adhoc networks etc. These trust models are lacking in accurate computation and evaluation of trustworthiness for the Semantic web services. The trust level is measured with respect to the service, service provider, service consumer, trust evaluator and the agents that are relaying services. This survey discusses the various definitions, categories, sources and relationship of trust identified in the literature. Moreover this paper focuses in depth on various trust management models and its issues for semantic web services. This paper will provide a footstep for future researchers to develop new trust model taking in to account the limitations of the models identified here.

Index Terms— Trust, Semantic, Web Service, Trust Model, Survey in Semantic Web Service, Survey on Trusted Web Service

1 INTRODUCTION

Service Oriented Architecture (SOA) is used to shape modern societies in the form of providing interoperable services in vital areas such as business, science, health and government. Web service is the realization of SOA. In heterogeneous environment, web service is a web resource which provides the communication between application-application and application-user through loosely coupled reusable software components. The key factor of web service is interoperability. Syntactic and semantic are the two levels of interoperability [25]. The Semantic Web is the new formation of World Wide Web. Web Service provides syntactic interoperability through XML technologies, but not provides the semantics. The Semantics is used to enables web service automation to understand and integrate with other web service.

Semantic representation plays a major role in web process life cycle. The wrapping of ontology and web service is known as Semantic Web Service (SWS). It is developed around ubiquitous standards for the exchange of semantic data. It is used by programmers to collect the data and services from various resources for combining together to a new one without altering the meaning. SWS can be invoked or executed even not using the browser. Functional, Data, QOS and Execution Semantics are the variation of semantics.

Ontology is the basic building block of Semantic Web that describes the concepts and relationship between information in particular domain. A set of web services can share the ontology to work with a similar domain. The semantic web languages are Ontology Inference Layer (OIL), DARPA Agent Markup Language (DAML), and combination of DAML and OIL, Web Ontology Language (OWL), Resource Description Framework (RDF), Web Service Modeling Language (WSML), Web Services Semantics (WSDL-S) and Semantic Annotations for WSDL and XML Schema

(SAWSDL). These languages allow data and semantically describe the service resources by service provider.

The semantic web process has six layers of activities [1] such as Semantic Web Service Annotation, Semantic Web service Advertisement, Semantic Web Service Discovery, Semantic Web Service Selection, Semantic Process Composition and Execution Web Process which includes traditional model like Process Algebra, Petri Nets, state machines and simulation techniques.

Service composition is a challenging task that uses other existing services. Service selection plays an important role and it is difficult to find the best services from millions of services. There are many different factors are to be considered while selecting the web services like functional and non-functional attributes. Mostly the minimum requirements as functional attributes are satisfied by many services, but some services are not furnished with non-functional requirements like trust.

XML Encryption, XML Signature and P3P (Platform for Privacy Preferences) projects was developed by W3C. Besides, Microsoft and IBM have developed WS-Privacy, WS-Policy, WS-Security and WS-Trust. These security mechanisms have limitations such as susceptibility to attacks, more dependent on Certificate Authority, poor extensibility and lack of concentration on individual view [21].

Trust refers factors such as quality, reputation, cost, availability and experience. Trust is like a vase between communicators once it's broken, though you can fix it the vase that will never be the same again. Therefore, trust factor must be specified in service description, it is useful to find the trusted services by matching factors in service discovery phase.

2. RELATED WORK

2.1 Definitions and Types of Trust

Trust is the essential part of E-Commerce, P2P Networks and Semantic Web because each relation begins with trust. Trust is a complex factor it has many forms like belief, honesty, truthfulness, competence, reliability, confidence or faith, etc., of the service provider, consumer,

- Mrs.V. Mareeswari, Ph.D Research Scholar & Assistant Professor, VIT University, Vellore, India, E-mail:vmareeswari@vit.ac.in
- Dr.E.Sathiyamoorthy, Research Guide & Associate Professor, VIT University, Vellore, India, E-mail:esathiyamoorthy@vit.ac.in

agents, or service.

It is dynamic, multi-directional quantitative value. It is specific to the relationship between X and Y in the relation R1 but not in other relation R2 at a time T. It has played a significant role in web service interactions therefore it is necessary to know how to evaluate trust value for a business partner to respond to a service request.

Trust can be categorized into two like soft trust or reputation based trust and hard trust or certificate based trust. First, soft trust is community dependent, i.e. participants in a business collaboration exchange information about the known other participants or services. The malicious users can be easily identified based on the exchanged information and quarantine it. The main issue of this category is that no one takes the risk to invoke a new unknown service initially before deciding the trustworthiness of the new services for invocation. Second, hard trust is not dependent on the social context. Semantics of security behaviour can be specified in service description hence the trustworthiness of a web services can be derived from the policy or contract. The main issue here is anyone can provide the fake or wrong policy or contract.

Trust can also be categorized like Global Trust, Personalized Trust. Global Trust means consumer can ask the query without the knowledge about service. For example, Top 5 Restaurants in India. Personalized Trust means consumer can specify the attribute with specific constraint in the query. For example, need a Top 5 Restaurants in India with less expensive.

2.2 Trust Sources

The two broad classification of trust [24] is direct trust and indirect trust. The direct trust can be defined as an entity that is experienced directly from the past interactions. The Indirect trust can be defined as an entity that is experienced through other entities experiences indirectly. There are three different subcategories of indirect trust such as reputations, recommendations and referrals. A reputation can be seen as the general feedback about the character or behaviour of an entity. A recommendation is that a user trusts a service because of some suggestion got from a trusted central authority. A referral means a service consumer trusts a service because of some distributed referrals got from known trusted third party software agent.

2.3 Trust Relationship

Trust relationship between the service consumers, providers, agents or services is varying in different domains over the time period. The trust relations satisfy some of the mathematical properties like reflexive, not symmetric and not transitive. Moreover, a trust can be determined by direct experience in successful relations ($A \leftrightarrow B$) and transitivity based recommendation ($A \rightarrow B$ and $B \rightarrow C$ then $A \rightarrow C$) and similarity based recommendation trust in [21]. Furthermore, relation may be categorized as trusted, partially trusted, undecided, partially distrusted and distrusted values lying

between -1 to 1. Similarly the degree of trust also differs depending on the participants of the relation. Trust value can be represented as matrix format in socio-cognitive manner and relationship can be represented by directed acyclic graph. In case of centralized approach as in [[8], [7]], trust computation depends on reputation and centralized evaluation system. The decentralized approach provides better scalability and protection from deficiency that is difficult to implement.

2.4 Trust Models

2.4.1 Trust Computation Related With Services

In the web service interactions, the participants can establish trust based on 1) Peer-To-Peer trust model 2) Trust Chain Model (TC) and 3) Trusted Third Party Model (TTP). In P2P Model, participants should share their trust relations on a one-by-one basis which is not scalable. In TC Model, each participant stabilizes their trust relation with its direct ancestor, which is not flexible for dynamic service integrations. In the TTP model, all participants get the credentials from a trusted third party.

Mangling Zhu et al. [2] designed the social rules on describing the trust relationship between the provider and consumer in the open environments. First, Self Confidence Rule means an agent or service provider is having self-confident about their providing services. Secondly, Persistence Rule means a service agent should be persistent to their goals to achieve better performance. Third, Honest Rule means to analyze whether an agent is trustworthy in their commitments. Fourth, Motivation Rule checks for motivation in providing services. Fifth, Reliance Rule estimates the trust from the reliability of an agent. If an agent was unreliable at previous transactions with a consumer, its trustworthiness will be decreased. Sixth, Reputation Rule finds whether it has positive or negative feedback about providing services from the other agents in the open environment. If an agent always performed the committed service, then its reliability will increase, consequently reputation will improve. Trust value of an agent will increase based on their reputation and other dimension and also it automatically updates their reputation. Finally, they defined a trust is based on performance, commitments, social attitude and relations of particulars.

Trust and reputation model for web service selection based on Bayesian network presented in [3]. This approach considered three sources for trust calculation such as useful reputation, QOS monitoring and direct experience of consumer. This model is trying to overcome some earlier limitations by integrating the mentioned sources to find the trust value. The user can specify their expectations of services based on QoS, rating mechanism based on consumer feedback on each quality attribute after each transaction, checking whether the feedback is reliable or not and to match the services by finding the similarity of trust rater value and requestor expectation value using Euclidean method. Finally it shows the conformance trust value for consumer view. There is no complete implementation can be found for

characterizing web services based on transaction time. For example, if the functionality of services is critical then it's more weighted than light services and if the consumer uses massive transactions on services, then it has more reputation. Moreover, they are not focused on such limitations such as bootstrapping problem, unfair ratings, incentive for ratings and some issues in implementation.

Some of the service provider has highest trust value initially and then maintains it for short duration, later performing malicious activity. These malicious service providers can be found [9] using the result of subtraction of penalty vector from trust vector. Penalty vector represents the misbehavior in past transactions which has been derived from inconsistency and misuse of trust measure by peers.

Priority based trust(PB) model presented in [4] for service selection in general service oriented environments. It follows Reputation based and Trusted Third Party approach. It overcomes the limitations of Certified Reputation Model. In PBTrust, trust is calculated as follows: first, service is described as matrix (2, n) format. The first row indicates the parameter (e.g. cost, speed) of the service. The second row indicates the priority value (e.g.0.3, 0.5) of the corresponding parameter. Second step, find the similarity between the required service for the consumer and the available service based on the priority of the individual parameter of the service. Third, check the reputation level of provided services which is calculated from the Trusted Third Party and history information of the service provider on general performance of a particular service. If a service is having higher similarity and getting more reputation then it will be considered as the trusted service. Hence, Consumer uses this trusted service then sends the service report to service provider. Service experience of the provider is updated based on the consumer opinions. It maintains the timestamp for each service report that will be useful to reduce the out-of-date reference. The PBTrust model finds the success and failure rate of the particular service provided and dynamically updates the service record without using a central system.

Many of the trust models are developed based on reputation of service provider. But a trust model does not take into account the reputation of consumer. It focuses in developing trust model according to the behaviours of consumer and provider at dynamic environment in [5]. Consumer behaviour is framed in two ways: First, it is derived from the experience from the same community. For example, feedback is getting from the same hotel users or other hotel users. Secondly, it is derived from the other community. For example, consumer behaviour may be varied when the information about the service is published in TV or News Paper, etc... Service provider should satisfy their consumer preference. Obviously, service provider behaviour depends on their consumer behaviour and self constraints. It bootstrapped uses the information of consumer behaviour. Similarly, service behaviour should be evaluated from the reputation of the same or other community. Trust model is defined from the service provider behaviour and consumer behaviour over time using Boltzmann equation.

The concepts of service behaviour and evaluation procedure are defined in [6]. Here, there are split trustworthy domains into two categories as objective and subjective characteristics. The objective characteristics are customer requirement, capability of implementing functionalities, commitment to complete work, performance and existence. Reliable, Honest and Expectation are the subjective characteristics. The programming language OWL-S is used to structure the ontology schemas. Eight reasoning rules are developed from trusted ontology through the relationship of subjective and objective characteristics. This model is useful in finding the trustworthiness of the semantic web service discovery, selection and composition. Furthermore, the service behaviour can derived from conversations between the participants in [17].

2.4.2 Trust Computation on Consumer View

The service consumer provide the feedback in the scale from 1 to 10 or desired value or range between 0 and 1 or choosing linguistic terms from the set (e.g. more availability, availability, not availability, not more availability). Furthermore the QoS attributes are considered to be different value for various domains. Galizia et.al. [16] presents a trust methodology for selection of web service. It follows Policy based/Trusted Third Party based approach for the classification of the web services with the help of IRS-III (Internet Reasoning Service) tool. Consumer can send their requirements like the pair {feature, condition} (e.g.{Country Name, Asia Continent} AND {encryption algorithm, any symmetric algorithm}). Web service provider should maintain the guarantees like the pair {feature, value}. According to this methodology, the classifier determined the exact match of services based on quantitative/qualitative value provided by the customer. There are no clear methods to compute trust value.

Surya Nepal et.al. [5] have implemented the fuzzy based trust management framework for web service. Initially, they developed a data model based on consumer views on QoS attributes that evaluates the reputation of services. Secondly, they proposed the fuzzy based linguistic query model to parse the requested query to evaluate by different query processing algorithm. Hence the consumer can express their view with (quantitative value e.g. 1 to 10) and without (qualitative value e.g. low, medium, large and high) their knowledge about data model. For example, using linguistic term, consumer can request the query like q (Privacy is very important AND Cost is not important AND Reliability is important) in implicit or explicit or hybrid mode. This will work on both global trust (e.g. top 5 airline services) and personalized trust(e.g. top 5 airline services with reliability > 0.9) entities. They have not addressed some issues such as trust bootstrapping, propagation, retaliation, reciprocation and dishonest or biased ratings. PBTrust model [4] is also getting consumer expectation on trust for individual service attribute.

Honest agent can give the feedback or opinion and can ask other participants in same domain about the services. The reliability of the service is calculated as average of all the feedbacks from participants [14]. The consumer may give the dishonest or meaningless feedback about the service to make the reputation value to be decreased. When the trust management center found this dishonest feedback, punishment can be given to the consumer [13].

2.4.3 Trust Computation for Content and Context

More research has been focused on certification or reputation based approach for finding trusted service provider. Besides, provider trust level can be measured based on their web content and meta-data. The content and context based approach is useful to analyze the semantic data which are published in the web [19],[15]. The context based approach uses meta-data information which answers the question like who, what, why and when. For example, low trust considering for a product rating which will be older than a year. A Role based trust evaluation is a part of context based approach. Content based approach does not consider the meta-data information but it uses content itself with rules, axiom of content and the views of other authors. For example, higher trust rate for information stated by different ten sources. Fewer trust rates for product amount less than 10% of average. Bizer et al [20] uses the TriQL.P browser to filter the semantic web content based on several trust policies.

Content trust is a perception to determine the trustworthiness of data based on the features of content or resources. The web page content can be trusted based on these factors in [18] such as Authority, Currency (up-to-date information), Accuracy and Relevance of web site information. This model uses RDF graph to represent data sets of semantic web. For example, hasPrice(<http://www.findbookprices.com/search/?isbn=9781420876390>, "\$19.00"), where hasPrice as an attribute, URL is an object and amount is the value of that object. This RDF information is used as criteria for AHP (Analytical Hierarchy Procedure) technique [10] which is used in group decision making to establish the content trust.

The initial trust value has derived from the reputation or policy system. The next level trust value can be calculated from the context of each interaction between two entities. Trust value will be increased depending on the confidence level of information, task, process and external attack context. Moreover, it will be decreased based on negative suspects in each context. Furthermore, the usage of deontic logic, [11] found whether an entity is permissible or impermissible or obligatory.

2.4.3 Trust Computation on Trust Management Center

Consider service requestor and service providers are trusted entity. They request Trust Management Center (TMC) to evaluate the trust for an entity. TMC may be not trusted. Trust value of TMC can be calculated based on the reliability of the service which have previously evaluated by itself.

Similarly, Trust Requestor (TR) can be evaluated depending on the reliability of the service which has been used. Changying and Wentao [12] developed a trust model based on Fuzzy Theory to evaluate the trust value of trust requestor and TMC. They have considered the uncertainty factors that arise in trust evaluation. For example, the factors are distrust, low trust, not clear enough, likely trust and absolute trust. These can be represented as float values from 0 to 1. The service access control follows based on the weight of evaluation of TMC and TR.

3 CONCLUSION

Trust management is an adaptable and never ending research focus. The concept of trust is applied in all the entities like data's, services, and consumers, providers, and agents, community and data resources. Trust value can be changed dynamically in a virtual environment. Trust module is little, but it is more important in our any practical concepts. These existing trust models are developed based on reputations, policies and implemented based on centralized or decentralized approach. These trust models are not focused on some limitations such as Risk value, biased ratings, unfair ratings, incentive for rating, retaliation, reciprocation and reputation milking. Trust model should deal issues more on trust relationship, bootstrapping, updating trust values, penalty the dishonest behaviour and ontology based implementation. Now this is not the end. But it is, perhaps, the end of the beginning of the research on trust models.

REFERENCES

- [1] J. Cardoso and A. Sheth, Introduction to Semantic Web Services and Web Process Composition, in *Semantic Web Process: powering next generation of processes with Semantics and Web Services*, Lecture Notes in Computer Science, Springer, 2005 (in print).
- [2] Manling Zhu, Lin Liu, Zhi Jin, A Social Trust Model for Services, AWRE 2006 Adelaide, Australia.
- [3] Hien Trang Nguyen, Weiliang Zhao, Jian Yang, A Trust and Reputation Model Based on Bayesian Network for Web Services, 2010 IEEE International Conference on Web Services.
- [4] Xing Su, Minjie Zhang, Yi Mu, Kwang Mong Sim, PBTrust: A Priority-Based Trust Model for Service Selection in General Service-Oriented Environments, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.
- [5] Surya Nepal, Wanita Sherchan and Athman Bouguettaya, A Behaviour-Based Trust Model for Service Web, IEEE International Conference on Service Oriented Computing and Applications, 2010.
- [6] Ming Qu, Shufen Liu, Tie Bao, On the Trusted Ontology Model for Evaluating the Semantic web Services, 14th International Conference on Computer Supported Cooperative Work in Design, 2010.
- [7] Srividya K Bansal, Ajay Bansal, M. Brian Blake, Trust-based Dynamic Web Service Composition using Social Network Analysis, IEEE Workshop on Business Applications of Social Network, 13th December 2010.
- [8] Damjan Kovac, Denis Trcek, Qualitative trust modeling in SOA, *Journal of Systems Architecture* 55 (2009) 255-263.
- [9] S. Park, L. Liu, C. Pu, M. Srivatsa, and J. Zhang, Resilient Trust Management

- for Web Service Integration, IEEE International Conference on Web Services, 2005.
- [10] Bagher Rahimpour Cam, Amin Khodabandeh Amiri, AHP Techniques for Trust Evaluation in Semantic Web, Journal of Advances in Computer Research, March 2011.
- [11] Chandrasekaran Subramaniam, Vinod Duraivelu, Rajalakshmi BhavaniShankar, Menaka Mischella F, Mahendra Kumar M, A Predictable Context Aware Trust Model For Organization Management, pp. 151-158, 4th International Conference on Trust Management, June 14-18, 2010, Morioka, Iwate, Japan.
- [12] Changying Dai, Wentao Gong, Model of Services Trust Threshold Assess Based on Fuzzy Theory, IEEE 2nd International on e-Business and Information System Security (EBISS), 2010.
- [13] Yijiao Zhu a, Junhao Wen a, Mingwen Qin a, Guoli Zhou, Web Service Selection Mechanism with QoS and Trust Management, Journal of Information & Computational Science 8: 12 (2011) 2327-2334.
- [14] Javier Carbo, Jose Manuel Molina-Lopez, An extension of a fuzzy reputation agent trust model (AFRAS) in the ART testbed, Soft Computing A Fusion of Foundations, Methodologies and Applications, © Springer-Verlag 2009, Volume 14, Number 8, 821-831, DOI: 10.1007/s00500-009-0470-9
- [15] Ian Jacobi, Lalana Kagal and Ankesh Khandelwal, , Rule-Based Trust Assessment on the Semantic Web, 5th International Symposium on Rule, RuleML-2011 Europe Springer LNCS Proceedings, July 19-21, 2011.
- [16] Stefania Galizia, Alessio Gugliotta and John Domingue, A Trust Based Methodology for Web Service Selection, International Conferences on Semantic Computing, 2007.
- [17] Fahima Cheikh, Giuseppe De Giacomo, Massimo Mecella, Automatic web services composition in trust aware communities, Proceedings of the 3rd ACM workshop on Secure web services, 2006
- [18] Pattanaphanchai, J., O'Hara, K. and Hall, W. (2011) DC Proposal: Evaluating Trustworthiness of Web Content using Semantic Web Technologies, The 10th International Semantic Web Conference, October 23-27, 2011, Bonn, Germany.
- [19] Christian Bizer and Radoslaw Oldakowski, Using context- and content-based trust policies on the semantic web, Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters, ACM New York, USA ©2004
- [20] Christian Bizer, Richard Cyganiak, Tobias Gauss, and Oliver Maresch, The TriQLP Browser: Filtering Information using Context-, Content- and Rating-Based Trust Policies, Proceedings Of The Semantic Web And Policy Workshop, Held In Conjunction With The 4th International Semantic Web Conference, 7 November, 2005
- [21] Ping Sun, Service Composition and Optimal Selection with Trust Constraints, IEEE Asia-Pacific Services Computing Conference, 2010.
- [22] Yang Yu, Jeff Heflin, Survey of trust algorithms on the semantic web, Journal of Web Semantics, 5th Volume, 2nd Issue, Pages: 58-71, JUN 2007.
- [23] Yao Wang, Julita Vassileva, Toward Trust and Reputation Based Web Service Selection: A Survey, International Transactions on Systems Science and Applications, Volume: 3, Issue: 2, Publisher: Citeseer, Pages: 118-132, 2007
- [24] Nicola Dragoni, A Survey on Trust-Based Web Service Provision Approaches, IEEE Third International Conference on Dependability, 2010
- [25] B. Medjahed and A. Bouguettaya, Service Composition for the Semantic Web, 0.1007/978-1-4419-8465-4_1, © Springer Science+Business Media, 2011