Trust and Privacy Enabled Service Composition Using Social Experience

Shahab Mokarizadeh, Nima Dokoohaki, Mihhail Matskin, Peep Küngas

Trust and Privacy Enabled Service Composition using Social Experience

Shahab Mokarizadeh[1], Nima Dokoohaki[1], Mihhail Matskin[1,2], Peep Küngas[3]

[1] ICT School, Royal Institute Of Technology (KTH), Stockholm Sweden
[2] Norwegian University of Science and Technology (NTNU), Trondheim, Norway
[3] University of Tartu, Tartu, Estonia
[1]{shahabm, nimad, misha}@kth.se, [3] peep.kungas@ut.ee

Abstract—In this paper, we present a framework for automatic selection and composition of services which exploits trustworthiness of services as a metric for measuring the quality of service composition. Trustworthiness is defined in terms of service reputation extracted from user profiles. The profiles are, in particular, extracted and inferred from a social network which accumulates users past experience with corresponding services. Using our privacy inference model we, first, prune social network to hide privacy sensitive contents and, then, utilize a trust inference based algorithm to measure reputation score of each individual service, and subsequently trustworthiness of their composition

Keywords- Social Network; Privacy; Trust; Web-service; Web-service Composition

1 Introduction

Emergence of Internet of Services (IoS)[3] as convergence of Web 2.0 and SOA, has promoted the role of human users in IT supported business models. The aim of IoS is to empower (non professional) human users with ability to discover and utilize resources (e.g. services) through supporting them with flexible, human centric Web 2.0 features which provide tagging resources (to indicate their evaluation) or mashing up resources according to their requirements [9].

In the open and redundant service environment of IoS, service consumers will face a problem of selecting the most appropriate services among bunch of services providing similar functionality. In fact, recent studies [14] have shown high degree of functional equivalence in available services. In this light, Quality of Service (QoS) features has been leveraged as a reasonable metric for evaluation of services. As the current Web service technology does not support enough QoS or other non functional aspects of Web services, service selection mechanisms have been dependant on QoS information advertised by service providers, or on collected data on service consumers' side. The problem in this case is that reliability of the information advertised by service suppliers cannot be verified and collected experience on the consumer side is quite limited. This is why exploiting WEB 2.0 for capturing end-user experience and learning the quality of services from collective user experience are promising solutions [4][16]. User's experience can be aggregated through ratings, tags or even textual reviews on different aspects of utilized resources (e.g. services). Because user feedback is vulnerable to malicious user's manipulation, only experience which is provided by

trusted users should be taken into account. Social Networks, as a Web 2.0 trend, are repositories of resources capable of documenting and revealing trust relationships among other nodes on the network. The ultimate goal here is finding highly trusted atomic or composite services based on reputation of users. Although this approach may support Web service discovery and composition, currently, it is mainly focused on clarifying some specific steps in trustworthy service selection and composition rather than on proposing generic yet comprehensive architecture accommodating Web 2.0 components with SOA requirements. In addition, the increasingly important aspects of privacy of user information in Social Networks need to be taken into account for practical solutions.

In this paper, we present our ongoing work in Web 2.0 enabled Web service composition framework. A goal of this work is providing an ordinary service consumer with tools allowing finding the most appropriate composition of services based on his/her past experience as well as on experience of other trusted users. The distinguishing feature of this work is our privacy inference model which protects visibility of user profile information from low trusted users. Notion of service trustworthiness [1] is employed to measure the quality of service composition. Trustworthiness of services is defined in terms of service reputation from service consumers' perspective which is extracted from user profiles. A semantic Web enabled structure is proposed to aggregate personal user information and its past experience.

The rest of the paper is organized as follows. Section 2 gives an outline of our approach to computing trustworthiness of services including population of profiles, trust and privacy inference models and social network pruning algorithms. The architecture of trustworthy service composition framework is presented in Section 3. Section 4 reviews some important relevant work. Finally, concluding remarks and directions for future work are presented in Section 5.

2 Solution outline

Our solution targets IoS and combines Web 2.0 trends with SOA paradigm by pursuing reputation based approach for service selection. We consider Web 2.0 as a platform for a trustworthy service selection and composition framework. The solution relies on user feedback, profiling and information extracted from social network as the major resources for computing reputation of Web services. We extend Kuter and Golbeck's formalism [1] for computing Web service trustworthiness by taking into account privacy of users in a social network.

The cycle of service selection, composition, rating and profiling in our solution is initiated by the end-user through submitting the request for service(s) which might not be implemented yet. Due to the fact that we are underlining service composition issue in this work, we refer to the end-user as a "composer user". The composer user's request is decomposed into a bunch of candidate services which should potentially satisfy the request. Next, a set of alternative composite services, which comply with the request, is generated. The composite services, in this set, need to be ranked to allow execution of only highly ranked services. In order to do that we delve into a (social) network of users who already exploited the candidate services. During the social network exploration process the privacy concerns of users and trustworthiness of users are taken into account. Based on the information from the network, reputation of each individual service constituting composite services is computed according to the given

user ratings, trust and privacy measures. Having in hand reputation of each individual service, trustworthiness of their composition is measured and the most trusted composite service is selected. After invocation (consuming) the service, the composer user may provide his/her experience with the composite service (and, possibly, with each component service) as a rating which may be published in the social network for future utilization.

We consider a scenario where a third party application provides recommendations for selecting appropriate services (e.g. hotel, flight or trip online booking services). This selection is made amongst a set of alternatives by exploiting the past experience of inter-related trusted users while preserving their privacy concerns over their profiles. As the third party applications do not have direct access to profile contents, they are obliged to obey inferred privacy assertions of profiles, which are computed by the system which is handling the profiles (e.g. the online social networking website). Issues related to technical application or legal enforcement of such privacy policies remains outside of the scope of this work. In the next sections we describe the approach in details and provide algorithms for collecting the required information and computing metrics in different steps of the aforementioned process. We also would like to underline that in this paper we are focusing on models and algorithms proposed and developed in the framework while leaving the experimental results for the future work.

2.1 User Profiles

Profiling of users' personal information and capturing users' past experience have shown to be reliable approaches for predicting user models [6][13] .We specifically emphasize active involvement of user in the process of enriching its experience through supplying explicit feedback. User profile consists of two segments: 1) Basic personal information including pieces revealing connections to social network(s) and 2) User past experiences with services.

The first segment is grounded to well known FOAF (Friend Of A Friend) ontology [5] which is extended to capture trust relationships and privacy concerns [6]. Both *Trust* and *Privacy* assertions take values ranging from 0 to 1. In case of *Trust* assertions, 0 implies complete distrust and 1 implies absolute trust towards the individuals for whom the assertion has been issued. *Privacy* assertion, unlike *Trust* assertion, takes discrete values where value 0 makes profile content visible for everyone and, in contrary, no one will be able to access the content if its *Privacy* value is set to 1. Tuning *Privacy* level of profile with values in range [0, 1] allows more control on the visibility of profile content by vast number of loosely defined acquaintances. We consider a single *Privacy* assertion over second segment of the profile (past experiences).

The second segment accumulates user experience with services (i.e. ratings). Ratings reflect user's overall satisfaction over the utilized services. For the sake of simplicity we only

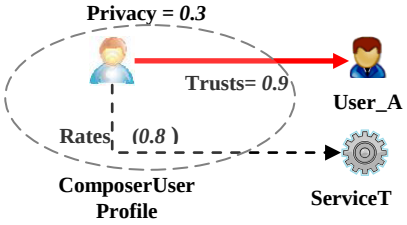

Fig. 1. Structure and Content of User Profile

consider numerical ratings in range [0, 1]. Fig.1 presents sample profile content for *ComposerUser*, where *User_A* is a highly trusted friend of *ComposerUser* (trust value = 0.9). *ComposerUser* had utilized *ServiceT* and was satisfied by assigning it high (0.8) rating value. Finally, *ComposerUser* is willing to expose her profile content to certain individuals due to low privacy value (0.3) assigned to profile content.

2.2 Populating User Profile Content

Basically, there are two scenarios to populate the user profile content which differ due to the availability of resources:

1) In the first scenario, we are employing a social network application (e.g. a *Facebook*[23] *Application*) which allows us to exploit certain user profile information, specifically friend list, quality of friendship (e.g. best friend , friend, acquaintance, etc), privacy values defined over profile items, and ratings provided over utilized services or applications. This all together provides ready to use ingredients for populating both segments of the user profiles. In a social network, the quality of a trust relationship between every two friends is not necessarily symmetric. For example, two friends may label each other in two different friend category lists (e.g."close friend" and "acquaintance"). This case raises the privacy concern over profile content, especially when the certain profile information is a subject to abuse by less trusted users.

2) In the second scenario, we do not have any social network available; hence we have to preliminary harvest user ratings (feedbacks, textual reviews, etc) from some resources; for example *Apple App. Store*, where such information is publicly available. Then we approximate trust relationship between users based on similarity measures over provided ratings. In fact, several researches have denoted a strong correlation between trust and overall similarity [13][20]. Based on calculated trust relationship, we can build a trust network between users. If we don't have any explicit privacy policy in the harvested user information, we assign a default privacy value to all constructed user profiles.

After populating the user profiles, they are mined in order to extract social network of composer user by exploring FOAF segment of profiles and chaining those profiles embodying past experiences about interested services.

2.3 Trust and Privacy Inference Models

As we follow reputation based approach, we make use of a centralized trust and privacy inference server to compute global trusts for all users in the system. Having some trust and privacy relations between neighbor users in the social network (see Section 2.3) we might need inference models for calculation of trust and privacy for users having indirect relations in the network. In this paper we propose usage of the following inference models.

Trust Inference Model: As there has been outstanding research on trust inference in Web based social networks, instead of proposing a new inference model, we exploit off-the shelf trust-inference algorithms. The only restriction we have is that the selected trust inference model should not be dependent on privacy value of the user profile because of our privacy inference model is computed based on the inferred trust value. If we presume availability of a social network, any trust-inference algorithms such as TidalTrust[7], Appleseed [8], or even probabilistic trust inference model [21]

can be employed to compute trust between two individuals. While in the case of second scenario, we can recruit, for example, nuanced profile similarity approach [20] or T-Index method [13] to compute inferred trust. In both cases, we refer to the inferred trust value of user *s* towards user *u* by *trust(s,u)*. In particular, in our previous experiments T-index method was successfully used [13].

Privacy Inference Model: To the best of our knowledge, there is no privacy inference model in the context of social networks. As a matter of fact, we consider privacy as an inverse function of trust towards the individuals for whom privacy assertion is issued. In other words, decreasing confidence in someone leads to strength of privacy level towards him or her, as presented in following formula:

$$\begin{cases} privacy \propto (1 - trust) \\ trust \rightarrow [0,1], \quad privacy \rightarrow \{0, 0.1, \dots, 1\} \end{cases} \tag{1}$$

Unlike trust values, privacy level takes a discrete value from range of {0, 0.1… 0.9, 1}. The reason for utilization of such coarse grained privacy values is that privacy can be associated to different visibility level of information in the profile. The idea behind formula (1) intuitively makes sense: people consider more relaxed privacy concerns for their highly trusted friends, while they are not willing to expose so much (if any) information to less trusted friends or strangers. As an evidence supporting this observation, we point out to the fuzzy approaches proposed by [12] to compute privacy values from user trust values. Based on this observation, we justify our privacy inference model. Let's presume availability of two nodes (individuals) *s* and *u* in our target social network and consider p_s as given privacy value to profile of individual *s*. Thus, inferred privacy rating of node *s* from perspective of node *u* can be computed by formula (2).

$$privacy(s,u) = \begin{cases} \alpha(1 - trust(s,u)) + \beta\, p_s & ,if \;\; trust(s,u) \geq Min_{trust} \\ \gamma(1 - trust(s,u)) + p_s & ,else \end{cases} \tag{2}$$
$$0 < \gamma < 1,\ 0 \leq \alpha, \beta < 1,\ \alpha + \beta = 1,$$

where Min_{trust} denotes the trust threshold for considering user *u* as trusted individual and *trust(s,u)* represents inferred trust value from node *s* to node *u* to be computed using any of the algorithms pointed out in the previous section. According to formula (2), less trusted nodes are always ignored by shrinking their visibility (i.e. higher privacy level). In fact, the amount of ignorance is partially tuned by parameter γ .This is quite compatible with aforementioned observations for increasing privacy level for non-trusted neighbors. If the result is higher than maximum privacy level then the maximum privacy value (equal to 1) will be considered. In contrast, formula (2) can be generous towards highly trusted nodes by enforcing $\alpha \gg \beta$ as a constraint on the weights. In this case, highly trusted nodes are rewarded by decreasing the privacy level they face to access the content. The granted visibility volume is tuned through weights assigned to initial privacy and inferred trust.

2.4 Social Network Pruning Algorithm

Before moving to utilization of ratings provided by the composer user's social network, privacy concerns of content owners need to be preserved. In other words, we need to identify those individuals who are not willing to expose their past experience

to the composer user and then mark them as empty nodes (a node with empty profile which is preserved only for the sake of network connectivity). Fig. 2.a shows the outline of our network pruning algorithm. The input to the procedure consists of: *src* referring to the composer user node, *network* presenting the network to be pruned, Min_{trust} denoting the trust threshold and $Max_{privacy}$ which is the maximum tolerable privacy value to make content of a profile accessible. The algorithm computes inferred privacy of every node in the network from perspective of node *src*. For every node *sink* in the network, first, the inferred trust towards *src* is computed using *TrustInference* procedure which could implement any of the aforementioned trust inference models. Then the respective inferred privacy of node sink towards *src* is measured by *PrivacyInference* procedure that implements the privacy model presented in formula (2). If the inferred privacy value is greater than maximum tolerable privacy threshold, then the profile content is not visible and the node will be marked as intermediate node.

As an illustrative example we consider a fragment of social network showing the network's trust relationship towards *ComposerUser* presented in Fig. 2.b. The edges show trust relationships between users and labels over directed edges denote the trust values. Let us assume the following simple probabilistic interpretation of trust [21] where two trust links (e.g. (*D* ,*B*) and (*B, ComposerUser*) in the graph in Fig. 2.b) correspond to two independent trust measures; the trust that *D* has for *ComposerUser* corresponds to the intersection of those two events:

trust(D, ComposerUser) = trust (D, B). trust(B, ComposerUser)

Accordingly, we will have the following inferred trust values: *t(D)=0.45, t(E)=0.64.* Having the trust values, observed privacy level of nodes by *ComposerUser* can be calculated using formula (2). Inferred privacy values, for $\alpha = 0.15$, $\beta = 0.85$, $\gamma = 0.15$, $Treshold_{trust} = 0.5$, are as follows: *p(D)=0.5825, p(E)=0.479, p(C)=0.455 ,p(B)=0.44*

Applying network pruning algorithm leads us to removal of node *D* because of its inferred privacy level exceeds the maximum threshold ($Max_{privacy}$=0.55) assumed to make the content (i.e. profile) of a node visible to *ComposerUser*, despite to the fact

```
PruneNetwork(src,network,Min_trust,Max_privacy)

For each node sink in network

Trust_sink,src=TrustInference(sink,src,Min_trust)
V_sink=privacy of node sink
Privacy_sink,src=PrivacyInference(v_sink,Trust_sink,src)
If (Privacy_sink,src > Max_privacy)
        mark node sink for removal
End For
```

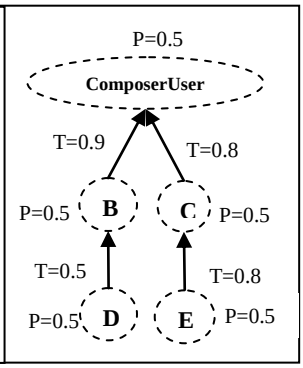

Fig. 2 (a) Left; Social Network Prunning Algorithm (b) Right; Sample Social Network showing Network's Trust towards ComposerUser

that its (not inferred) privacy level (*0.5)* meets the designated threshold. This simple example shows how the inferred privacy value can be personalized (the privacy may decrease or increase) to each individual user in a social network by taking into account the inferred trust value. The optimal values for respective parameters in formula (2), i.e. α, β, γ, $Max_{privacy,}$ and $Min_{trust,}$ will be determined after we perform extensive experiments with real world datasets (these experiments are in progress now).

2.5 Web-service Trustworthiness

We adopt Kuter and Golbeck's[1] formalism for Web service trustworthiness in our work. Web service trustworthiness is defined as a function of user ratings over QoS characteristics of Web services. As the ingredients for computing trustworthiness can be harvested from user profiles and the respective social network, we continue with formalism and computation steps. If *w* represents a Web service then rating of composer user *u* over service *w* is denoted by $\rho_u(w)$. Let us U be a set of all individuals in the social network who rated service *w*. Consequently, the reputation of service *w* from the user *c* perspective can be computed as follows:

$$t_c(w) = \frac{\sum_{u \in U} \rho_u(w)\, trust(c,u)}{|U|} \qquad (3)$$

In formula (3), $t_c(w)$ indicates the reputation of service *w* with respect to user *c* and *trust(c,u)* denotes trust of composer user *c* to individual user *u* in set *U* of users who has provided ratings over service *w* in their profile and their inferred privacy level allows exploitation of their ratings by user *c*. The final trustworthiness of service *w* is considered as the average of its reputation across all users in set *U*.

2.6 Composite Web Service Trustworthiness

Trustworthiness of a composite service is computed via propagating the trust values of atomic services, computed by formula (3), upward in the composition. Here three strategies can be utilized according to Kuter and Golbeck [1]: *Overly-Cautious, Overly- Optimistic* and *Average*. All these strategies aim in finding a composition with highest trust value. The goal of the first strategy is maximizing the minimum expected trust value that the composer user has in atomic services of the composite service. In other words, it assumes that if something bad could happen it would definitely happen, thus it avoids incorporating low trusted services. In contrast to the first strategy, *Overly Optimistic* strategy promotes the influence of highly trusted atomic services into trust of the composite service because of it believes that nothing bad happens if low trusted services are taken into account for composition. The last strategy is an intermediate approach looking for compositions with maximum average trust.

3 Service Composition Architecture

Taking into account the above-mentioned methods and algorithms we develop a framework for trust and privacy enabled service composition. The proposed framework is an extension of our previous work [2] by incorporating components

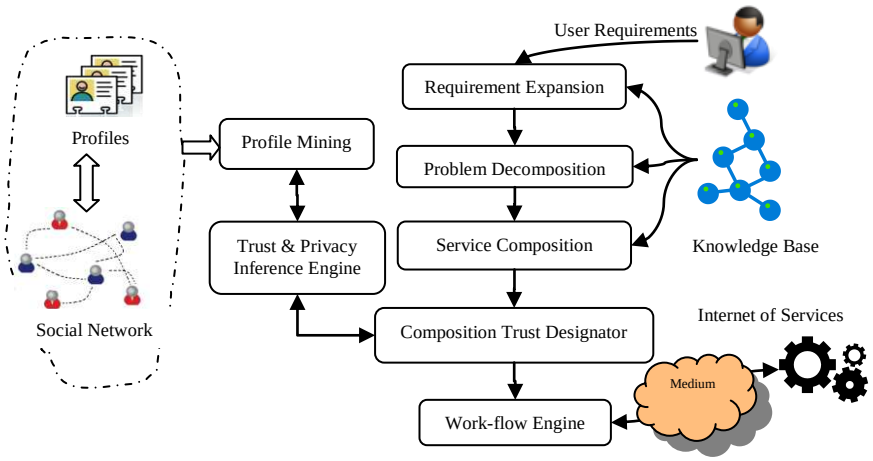

Fig. 3. Trustworthy Service Composition Architecture

dealing with trustworthiness of services and profiling of user experience with service. The architecture of the framework is depicted in Fig.3. For newly introduced layers, we point out relevant sections in this paper while for some other layers references to our previous works are provided: ***A)*** **Requirement Expansion Layer**: It expands user requirement statement, specified in terms of available input and expected output parameters of services, with relevant concepts in order to increase service discovery efficiency. We obtain these terms and concepts from our pre-populated knowledge base which is built based on our ontology learning methodology [22]. The requirement expansion is performed according to the method proposed by Kungas and Dumas [11]. ***B)*** **Problem Decomposition Layer:** The objective of this layer is discovery of potential services in the problem domain that could realize end-user expanded requirement [2]. ***C)*** **Service Composition Engine Layer:** The goal of this layer is generation of a plan (plans) to fulfill the user requirement through composition of discovered services [2]. ***D)*** **Trust & Privacy Inference Engine:** It accommodates the trust and privacy inference algorithms and implements network pruning algorithm to compute the trustworthiness of a service from a specific user's perspective (Sections 2.3, and 2.4). ***E)*** **Composition Trust Designator Layer:** This layer receives the inferred trust for each individual service in the generated compositions and utilizes any of the three strategies mentioned in section 2.5 to compute trustworthiness of each alternative composition. The highest trusted composition is delivered to Work-flow engine for execution. ***F)*** **Work-flow Engine Layer:** This layer provides components for orchestration and execution of atomic services in composite services [2]. It manages the control flow, performs data mediation and invokes the services. ***G)*** **Profile Mining Layer:** The profiler component manages a profile repository and implements mechanisms for collecting and archiving user experience and also mining the content of user profiles to build a social network of users (Section 2.2). While the individual layers of the framework are developed their integration and experiments with real data at the time of writing the paper are under construction.

4 Related Works

Pursuing a feedback based service selection approach (see [4][16]) exploited user feedback to measure Web service trustworthiness and social trust to receive feedback only from trusted users. This work is similar to our solution in the sense that we both are employing Web 2.0 social and technology trends. However, unlike our approach which aims to find highly trusted service composition, this solution solely tackled only the service selection issue.

Trust aware approaches for Web service composition have been investigated widely in the literature [1][10][15][17]. While Galizia et al. [10] presented a policy based approach (WSTO) for selection of WSMO semantic Web services, Kuter and Golbeck [1] targeted OWL-S upper ontology and followed a reputation based approach for selecting highly trusted composite web service. Paradesi et al. [15] adopted a multi-agent based reputation model to define trustworthiness of services. Moreover, they developed a trust framework to derive trust for a composite service from trust model of component services. Nepal et al. [17] tackled the problem of fair reputation propagation of a composite service into its component services. Unlike our work, none of the aforementioned trust aware approaches considered privacy of users when they infer trust relationships or exploit their profile content.

Banks and Wu [18] proposed a hypothesis on possible relationship between interaction intensity and privacy preference for online social network users. However, their proposal remained on abstract level as they didn't provide the detailed model for computing privacy. Liu and Trezi [19] developed mathematical models to estimate the privacy score of the disclosed information by online social network users based on visibility and sensitivity of the individual items in user profile. In quite opposite direction but aiming the same goal, our approach exploits the default privacy and inferred privacy values for providing a personalized visibility of the profile information for users in the social network. Unlike our model, their approach do not support personalized privacy view over profile content for each individual in the social network.

5 Conclusion and Future work

In this paper, we propose a framework for trustworthy service composition which utilizes privacy and trust inference models. The models permit measuring trustworthiness of services through exploiting other trusted users past experience (accumulated in their profile) while respecting the privacy of users. Our future work includes analyzing the efficiency of the proposed privacy model using real world dataset and the effect of privacy on quality of composition. Results will reveal appropriate values to be assigned to each privacy inference parameters. Finally we need to develop a fair algorithm for propagation of composite service rating into the ratings of component web services.

Acknowledgement. This work was partially supported by the Grant 621-2007-6565 from the Swedish Research Council.

6 References

[1] Kuter,U. Golbeck,J.:Semantic Web Service Composition in Social Environments. In Proceedings of the 8th international Semantic Web Conference, (2009)

[2] Mokarizadeh,S., Grosso, A., Matskin, M., Kungas, P., Haseeb, A.: Applying Semantic Web Service Composition for Action Planning in Multi-robot Systems. In Proc. of Fourth international Conference on internet and Web Applications and Services. IEEE Computer Society, 370-376. (2009)

[3] Schroth,C. Janner, T.: Web 2.0 and SOA: Converging Concepts Enabling the Internet of Services. IT Professional 9, 3, 36-41. (2007)

[4] Leitner, P., Michlmayr, A., Rosenberg, F., Dustdar, S.: Selecting Web Services Based on Past User Experiences,In Proc. of 4th IEEE Asia-Pacific Services Computing Conference, (2009)

[5] http://www.foaf-project.org

[6] Dokoohaki,N., Matskin, M.: Personalizing human interaction through hybrid ontological profiling: Cultural heritage case study, In 1st Workshop on Semantic Web Applications and Human Aspects, M. Ronchetti, Ed., In conjunction with Asian Semantic Web Conference (2008)

[7] Katz, Y., Golbeck,J.: Social network-based trust in prioritized default logic. In Proceedings of the 21st National Conference on Artificial intelligence – Vol. 2 , 1345-1350. (2006)

[8] Ziegler, C., Lausen, G.: Spreading Activation Models for Trust Propagation. In Proceedings of the 2004 IEEE international Conference on E-Technology, E-Commerce and E-Service, 83-97, (2004)

[9] O'reilly, T.: What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. Communications & Strategies, No. 1, p. 17, (2007)

[10] Galizia, S., Gugliotta, A., Domingue,J.: A Trust Based Methodology for Web Service Selection. In Proc. of the international Conference on Semantic Computing , 193-200. (2007)

[11] Kungas, P., Dumas, M.: Cost-Effective Semantic Annotation of XML Schemas and Web Service Interfaces. InProceedings of the 2009 IEEE international Conference on Services Computing . Symposium on Compiler Construction. IEEE Computer Society, 372-379. (2009)

[12] Zhang, Q., Qi, Y., Zhao, J., Hou, D., Niu, Y.: Fuzzy Privacy Decision for Context-Aware Access personal Information. University Journal of Natural Sciences, V. 12; No 5, 941-945 (2007)

[13] Zarghami, A., Fazeli, S., Dokoohaki, N., Matskin, M. : Social Trust-Aware Recommendation System: A T-Index Approach. In Proceedings of the 2009 IEEE /WIC /ACM international Joint Conference on Web intelligence and intelligent Agent Technology. Vol.3 .IEEE Computer Society, 85-90 (2009)

[14] Kahan, D.R., Nowlan, M.F. , Blake, M.B.: Taming Web Services in the Wild. In Proceedings of the IEEE international Conference on Web Services. ICWS. IEEE Computer Society, 957-958 (2006)

[15] Paradesi, S., Doshi, P., Swaika, S.: Integrating Behavioral Trust in Web Service Compositions. In Proceedings of the 2009 IEEE international Conference on Web Services . I453-460. (2009)

[16] Cai, S., Zou, Y., Xie, B., Shao, W.: Mining the Web of Trust for Web Services Selection. In Proc. of 2008 IEEE international Conference on Web Services . IEEE Computer Society, 809-810 (2008)

[17] Nepal, S., Malik, Z., Bouguettaya, A.: Reputation Propagation in Composite Services. In Proc. of the 2009 IEEE international Conference on Web Services.IEEE Computer Society, 295-302 (2009)

[18] Banks, L., Wu, S.F.: All Friends Are Not Created Equal: An Interaction Intensity Based Approach to Privacy in Online Social Networks, International Conference on Computational Science and Engineering, Vol. 4, 970-974 (2009)

[19] Liu, K., Terzi, E.: A Framework for Computing the Privacy Scores of Users in Online Social Networks, In Proc. of 9th IEEE International Conference on Data Mining, 288-297(2009)

[20] Golbeck, J.: Trust and nuanced profile similarity in online social networks. ACM Trans. Web 3, 4, 1-33. (2009)

[21] Bonnati, P.A. et al.: Rule-based Policy Specification: State of the Art and Future Work, Reasoning on the Web with Rules and Semantics,61-62 (2004) online: http://rewerse.net/deliverables/i2-d1.pdf

[22] Mokarizadeh, S., Kungas, P., Matskin, M.: Ontology Learning for Cost-Effective Large-scale Semantic Annotation of XML Schemas and Web Service Interfaces, In Proc. of 17th Int. Conf. on Knowledge Engineering and Knowledge Management (EKAW-2010) (To Appear), (2010)

[23] http://www.facebook.com