International Journal of Science Engineering and Advance Technology

Privacy enhanced and web based service composition

Bandaru Swamy Sri [1], U.Vinod Kumar[2]
[1]PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: udayswamysri@gmail.com.
[2]Assistant Professor, Pydah College of Engineering, Kakinada, AP, India.

Abstract— Service selection is a key issue in the Future Internet ,where applications are built by composing services and content service providers. The Most existing service selection of schemas only focus on the functional QoS By contrast, the risk of privacy breaches arising properties of the services such as throughput, latency and response time, or on their trust and reputation level. From selection different of component services whose privacy policy is not offered by compliant with customers 'privacy preferences is largely ignored. We propose the novel privacy-preserving Web service composition and selection approach which (i) makes it the possible to verify the compliance between users' privacy the requirements and providers' privacy policies and (ii) ranks the composite Web services with respect to their privacy level they offer. We demonstrate our approach using a travel agency Web service as an example of service composition.

Key words: Service composition, DaaS services, privacy, negotiation

I. Introduction

The Future Internet will be characterized by a new generation of applications services and data from different providers and organizations built by composing in order to provide users with added-value services tailored to their needs. Web services play a key, and composed over the Internet using standards like WSDL, UDDI and BPEL, respectively. Typically, role in realizing this vision because they can be advertised, located Web service composition is represented by a plan consistingto the actual services of tasks that, at run-time, are instantiated satisfying users' requirements. Due to the increasing numberof services available offering similar functionalities, it hard forusers to select a composition among optimal service a list ofcandidate services that satisfy their needs. Therefore, serviceselection is a key challenge in the Future Internet.The literature offers of work on Web servicecomposition and selection. Most of the existing approachesfocus on the identification of optimal a large amount Web services among aset of candidates based on constraints on the Quality of Service(QoS) performance of the To the bestof our knowledge, only few works have investigated privacyissues in service selection Theorchestrator usually collects a large amount of personal dataabout their clients and eventually shares these data with theservice providers providing the orchestrated services. This, however, may lead to risks of data misuse. For instance, aservice provider may use client data for unlawful purposes. Asa consequence, more and more users are considering privacypractices adopted by Web service providers as an importantfactor for service selection: users will the service provision based on users'privacy preferences.In this paper, we propose an approach more likely use Web services that customize to assist both users and Web service providers in composing and selecting optimal services with respect to their privacy preferences. We use AND/OR tree to represent the orchestration schema, component services and their privacy policies. Based on this representation, we present an algorithm that determines the Web service compositions compliant with user privacy preferences. To help them to select the best Web service composition, our approach ranks admissible composite Web services (i.e., composite services whose privacy policy satisfy user preferences)with respect to their privacy level. The privacy level quantifies the risk of misuse of personal data based on three dimensions: the sensitivity, visibility and retention period of information. The contribution of this paper is three-fold. First, we propose a fine grained model to express Web service providers privacy policies and users' privacy preferences based on several privacy dimensions – sensitivity, purpose, retention period, and visibility while other approaches to privacy-aware service composition only consider one dimension, e.g. sensitivity or visibility. Second, we propose Web service composition algorithm which merges into a single step the selection of services that satisfy users' functional requirements and the selection of services compliant with users' privacy requirements, while most existing approaches execute these two steps separately.

II. Related Work

Our work is related to the fields of service composition modelling, service composition, and service selection.

a) Service composition modelling: To model service compositionand verify whether it satisfies properties like safetyand liveness, several languages, such as WS-BPEL, orapproaches, such as process algebra Petri nets, model checking, and finite state machines, have beenproposed. Contributions to service composition modelling alsocome from the requirement engineering community, where goal-oriented approaches, are used to representstrategic business goals. Similarly, we adopt a goal-orientedapproach to model service composition. The advantage of suchan approach is that it provides the abstraction necessary torepresent privacy policies without getting bogged down intothe functioning of Web services.

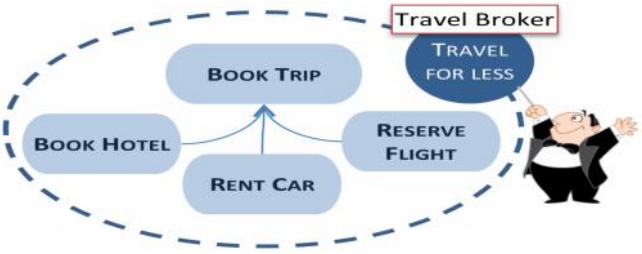
b) Service composition: Service composition is the problemof aggregating services in such a way that given (functionaland not functional) requirements are satisfied. The roleof privacy in service composition has been investigated in [13],where only services requiring the disclosure of less sensitiveinformation and offered by trusted providers are selected inthe composition. Users' privacy concerns are often addressedby providing automated techniques for matching provider'sprivacy policies with customer's preferences. The most prominent solution for policy matching isP3P (Platform for Privacy

Preferences Project). P3P aims to assist service providers in specifying their privacy practices on the web, and users in matching such practices a gains ttheir preferences. To automate the matching process, P3P hasbeen complemented with privacy service composition is the result of a negotiation phase between user privacy preferences (describing the type of access to each piece of personal information) and the web service policy statement(specifying which information is mandatory and which is optional to use a service). Here, the outcome of the negotiation indicates what personal information the user should disclose to the service provider. However, these techniques only focus on the relation between a server and a client. In contrast, our work uses a privacy policy matching approach to build the model ofadmissible service compositions. In addition, our work goes

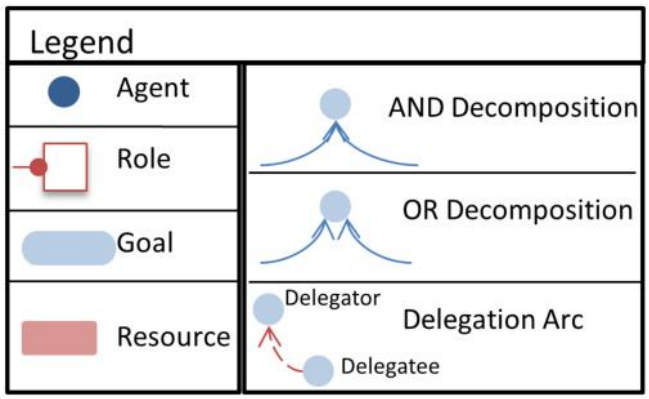
Beyond pure service composition: we also identify the mostprivacy preserving composition.

III. Modeling Service Composition And Privacy

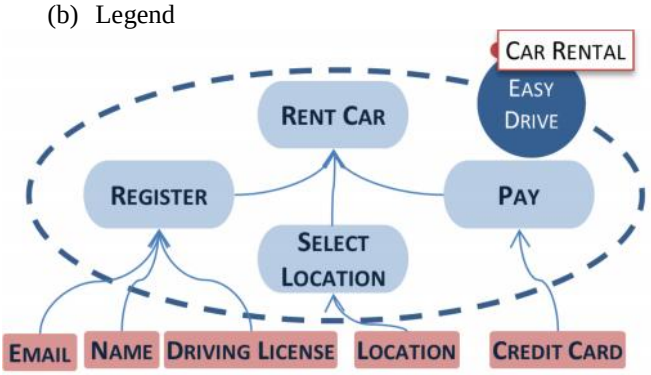
In this section we introduce the models to represent webservice orchestration, privacy policies and user privacy preferenceson which our approach is based.A. Modelling Service OrchestrationIn Web services composition typically there is an orchestratorwhich combines the functionalities provided by otherservices usually denoted as component services to satisfyusers' requests. Several services may be able to providethe same functionality requested by the user. The serviceresulting from the orchestration is called composite service.We model the composition schema as an orchestrator model,each component service as a component service model, and allpossible alternative instantiations of the schema as a serviceorchestration model.We represent these models as AND/OR trees where theemploys the notions of actor,goal, resource, decomposition and delegation. Actors are activeentities that have strategic goals and perform actions to achievethem. Actors can be agents or roles: agents are used torepresent the orchestrator and component services, and rolesto represent the types of services. respectively. Decomposition is used to refine a goal:AND decomposition refines a goal into subgoals and resourcesneeded to achieve the goal, while OR decomposition definesalternatives to achieve a goal. Delegation marks a formalpassage of responsibility or authority from an actor (delegator)to another actor (delegate) to achieve a goal. We use theseconcepts to define the notion of service model and Specific component services.



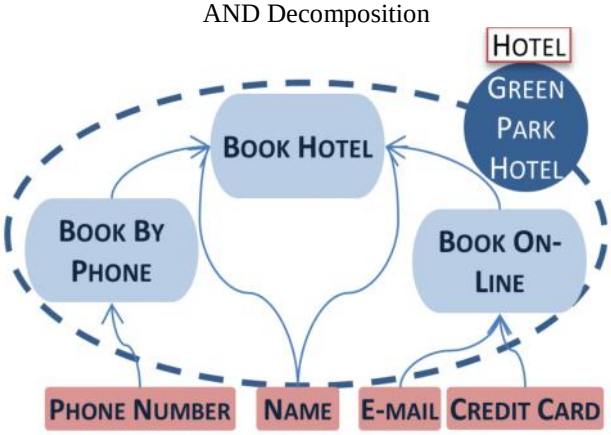
(a) Orchestrator Model



(b) Legend



(c) Component Service Model with AND Decomposition



(d) Component Service Model with OR Decomposition

Fig 1: Examples of our Modeling

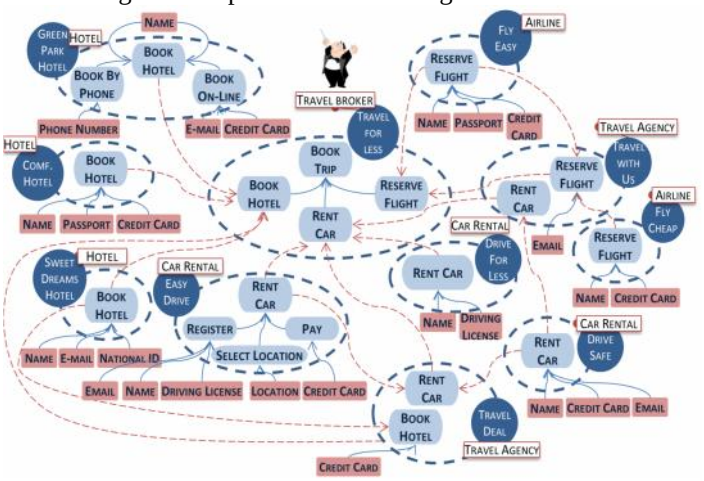


Fig 2: Example of Orchestration Model

In addition, the user may decideto not disclose a certain data item. Finally, the user shoulddefine the sensitivity of each data item, which may vary frompurpose to purpose. Users, however, are not allowed to changethe delegation depth and retention period. This is becausethese attributes are often constrained by the business modelof the orchestrator as well as by the requirements imposedby the legal framework in force (e.g., telecommunicationsdata have to be stored for six to 24 months according to theEU Directive on data retention). The result of this refinementprocess represents the privacy preferences of the user.We formally specify users' privacy preferences as follows.

Definition 6 (Privacy preferences): The privacypreferences of a user are a set of tuples hd; piwhere: d 2 R denotes a data item; p 2 G is the purpose for which d can be collected; 2 [1; 10] is the sensitivity of d;A[T is the visibility of d for achieving p; _ 2 N [f_gis the (re)delegation depth which limits the sharing of d forachieving p; _ 2 < is the retention period of d.Example 5: Let Bob be a new customer of TravelForLess.He wants to book a trip to Barcelona but, since he is afraidto fly, he only wants to book a hotel and rent a car. Basedon the privacy policy of TravelForLess (Table I), he specifiesconstraints on the collection and processing of his data. Bob'sprivacy preferences are presented in Table II. Since name andemail are usually required by service providers, Bob leavestheir visibility to all. In contrast, he prefers that his credit cardis only disclosed to agents he trusts, i.e. Travel with Us, TravelDeal and GreenParkHotel. Bob also restricts the accessto his driving license only for the purpose of renting a car, andthe national ID only for booking a hotel. Finally, Bob prefersto be contacted by email and thus he is not willing to disclosehis phone number.

IV. Privacy-Aware Service Selection

Figure 4 shows the architecture of our approach for privacy aware service composition and selection, which consists of two main components: a) the Privacy-Aware Orchestrator queries the Service Repository to select Web services that match users 'functional and privacy requirements for the composition;

b)the Privacy Aware Ranker prioritizes the admissible composite services based on their privacy level.

In what follows we describe in details the operations performedby the architectural components.

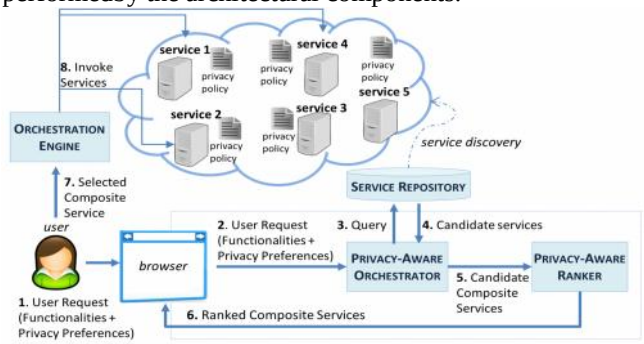


Fig.4. Privacy-Aware Service Composition and Ranking Architecture

A. Service Composition

Service orchestrators usually do not provide the functionalitiesrequired by a client directly but they outsource theprovision to specialized services. Nonetheless, according to theEU privacy regulation, they are liable for the actions performedby the subcontractors. Therefore, an orchestrator is willing toselect a component service only if the privacy policy of thecomponent service complies with its policy and user privacypreferences. The aim of the service orchestration compositionstep is to identify admissible composite services, i.e. thosecomposite services that comply with the user preferences andlegal requirements.After a user has defined her privacy preferences throughthe refinement of the orchestrator's privacy policy (see Example5), the orchestrator uses those preferences to identifyadmissible composite services. Admissible composite servicesare determined using Algorithm 1. The algorithm builds theprivacy model of the service orchestration that includes onlythose component services whose privacy policy complies withthe privacy preferences of the user (for the sake of simplicity,here we omit sensitivity in the user preferences, and representthem using the notation for privacy policies; sensitivity is usedin the next step). The algorithm first identifies the portion ofthe policy model of the orchestrator related to the functionalitiesrequired by the user (lines 5-20). The policy associatedwith a purpose is propagated to sub-purposes (lines 16-17).Intuitively, a purpose inherits the constraints from the higherlevel purpose. This makes it possible to check the consistencyof policies along the service orchestration model.When the policy of the orchestrator is fully analyzed, thealgorithm identifies the component services which offer thefunctionalities required by the user and whose privacy policyis compliant with the privacy policy of the service delegatingthe service to them (lines 21-41). If the node to be analyzedis not a leaf node of the policy (line 24), the algorithmchecks whether the policy associated with the subnodes ofthat node complies with the policy associated with the leafnode in the policy of the service delegating the provisioningof the functionality.

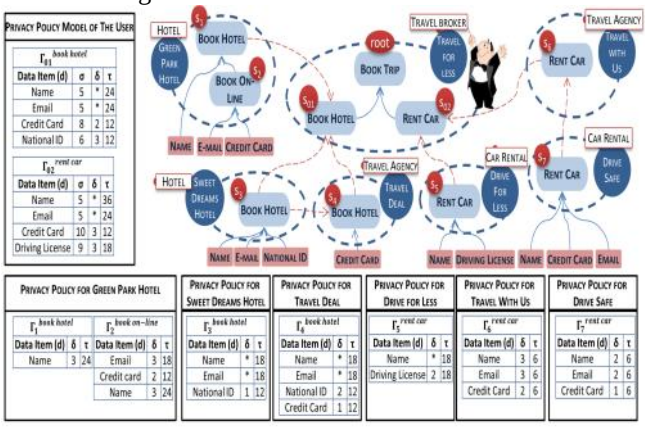
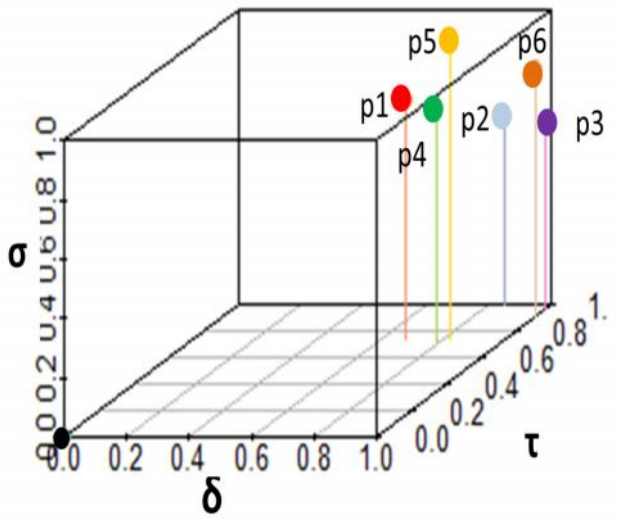


Fig 5: Example of Service Composition

The dimensions obtained above range in different scales.To make them comparable, they need to be normalized. If the normalized vector corresponding to a compositeservice is optimal with respect to all dimensions, such acomposite service is the most privacy-preserving compositeservice. Otherwise, the most privacy-preserving compositeservice should be determined by analyzing the componentsforming

the privacy level. However, end-users often are notable to understand the consequences of their privacy preferences.In addition, requiring the user to specify additional



(a) Graph Representation

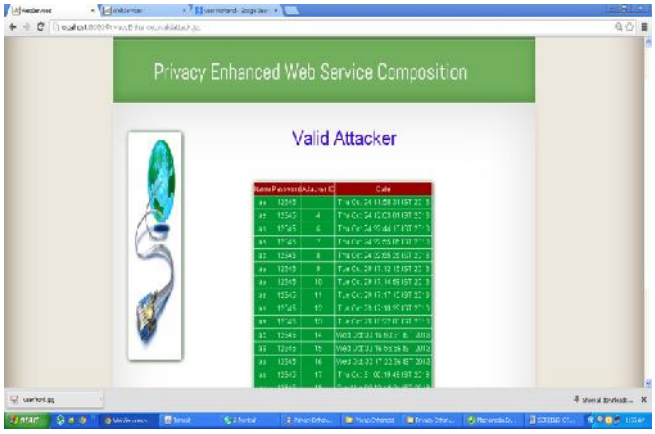
CS	Description	σ	δ	τ	Norm
P1	$S_{01}, S_1, S_2, S_{02}, S_6, S_7$	0.80	0.67	0.75	1.29
P2	$S_{01}, S_1, S_2, S_{02}, S_5$	0.64	0.85	1.00	1.46
P3	S_{01}, S_3, S_{02}, S_5	0.63	1.00	0.96	1.52
P4	$S_{01}, S_3, S_{02}, S_6, S_7$	0.79	0.79	0.72	1.33
P5	$S_{01}, S_4, S_3, S_{02}, S_6, S_7$	1.00	0.82	0.74	1.49
P6	$S_{01}, S_4, S_3, S_{02}, S_5$	0.84	0.99	0.93	1.59

(b) Admissible Composite Services

Fig 6: Privacy-preserving Composite Service Rankinginformation makes the level of her involvement too high and, thus, the selection process cannot be automated. Decision making should be simple and intuitive as well easy to review. Therefore, instead of asking the user toset her priorities over the privacy dimensions, we aggregatethem using an approach based on the norm. Intuitively, theprivacy of a composite service is computed as the average ofthe criteria forming the privacy level. The dimensionsand as well the norm for each The height of a point representsits aggregated sensitivity, whereas the most right points are those with higher depths, and those more in the back have alonger retention period. Intuitively, we prefer those compositeservices represented by the lowest, left-most, front-most pointson the graph. The norm gives a precise measure of the privacylevel of composite services and, thus, makes it possible todistinguish the most privacy-preserving composite service,represented by p1 in our example. Notice, however, that the framework is flexible enoughto allow users to account more a particular dimension byspecifying weights for the dimensions. These weights can beused to calculate the (weighted) average of the privacy level.For instance, a user can select the composite service thatrequires the less sensitive data release by setting the weightfor the first two components.

Results

Screen Shots



V. Conclusions

We have presented a novel approach to assist users and Web service providers in the composition and selection ofcomposite services that are more privacy preserving. Withrespect to other proposals for privacy-preserving Web servicecomposition, our approach supports the specification of finegrainedprivacy policies and preferences based on differentprivacy dimensions, i.e. purpose, visibility, retention periodand sensitivity. In addition, our approach ranks the generatedcomposite Web services with respect to

their privacy level,which quantifies the risk of unauthorized disclosure of userinformation based on three dimensions: sensitivity, visibilityand retention period.As future work, we are planning to implement our approachas a Web service, and to test its performance with respectto the number of candidate Web services the complexityof the privacy policies of the orchestrator and componentservices.

REFERENCES

[1] M. Alrifai, T. Risse, and W. Nejdl, "A hybrid approach for efficient webservice composition with end-to-end qos constraints," TWEB, vol. 6,no. 2, pp. 7:1–7:31, 2012.

[2] K.-M. Chao, M. Younas, C.-C. Lo, and T.-H. Tan, "Fuzzy matchmakingfor web services," in Proc. of AINA. IEEE, 2005, pp. 721–726.

[3] B. Jeong, H. Cho, and C. Lee, "On the functional quality of service(fqos) to discover and compose interoperable web services," Expert Syst.Appl., vol. 36, no. 3, pp. 5411–5418, 2009.

[4] V. X. Tran and H. Tsuji, "QoS Based Ranking for Web Services: FuzzyApproaches," in Proc. of NWeSP, 2008, pp. 77–82.

[5] P. Wang, K.-M. Chao, C.-C. Lo, C.-L. Huang, and Y. Li, "A FuzzyModel for Selection of QoS-Aware Web Services," in Proc. of ICEBE.IEEE, 2006, pp. 585–593.

[6] E. M. Maximilien and M. P. Singh, "Toward autonomic web servicestrust and selection," in Proc. of SOC. ACM, 2004, pp. 212–221.

[7] S. Paradesi, P. Doshi, and S. Swaika, "Integrating behavioral trust in webservice compositions," in Proc. of ICWS. IEEE, 2009, pp. 453–460.

[8] P. Wang, K.-M. Chao, C.-C. Lo, R. Farmer, and P.-T. Kuo, "A reputationbasedservice selection scheme," in Proc. of ICEBE. IEEE, 2009, pp.501–506.

[9] Z. Xu, P. Martin, W. Powley, and F. Zulkernine, "Reputation-Enhanced QoS-based Web Services Discovery," in Proc. of ICWS. IEEE, 2007,pp. 249–256.

[10] F. Massacci, J. Mylopoulos, and N. Zannone, "Hierarchical Hippocratic databases with minimal disclosure for virtual organizations," VLDB J.,vol. 15, no. 4, pp. 370–387, 2006.

[11] A. Squicciarini, B. Carminati, and S. Karumanchi, "A privacy-preservingapproach for web service selection and provisioning," in Proc. of ICWS.IEEE, 2011, pp. 33–40.

[12] S.-E. Tbahriti, M. Mrissa, B. Medjahed, C. Ghedira, M. Barhamgi, andJ. Fayn, "Privacy-Aware DaaS Services Composition," in Database andExpert Systems Applications, ser. LNCS 6860. Springer, 2011, pp.202–216.

[13] R. Hewett and P. Kijsanayothin, "Privacy and recovery in compositeweb service transactions," International Journal for Infonomics, vol. 3,no. 2, pp. 240–248, 2010.

[14] W. Xu, V. N. Venkatakrishnan, R. Sekar, and I. V. Ramakrishnan, "Aframework for building privacy-conscious composite web services," inProc. of ICWS. IEEE, 2006, pp. 655–662.

[15] OASIS, "Web Services Business Process Execution Language Version2.0," OASIS Standard, 2007.

[16] H. Foster, S. Uchitel, J. Magee, and J. Kramer, "Ws-engineer: Amodel-based approach to engineering web service compositions andchoreography," in Test and Analysis of Web Services. Springer, 2007,pp. 87–119.

[17] R. Hamadi and B. Benatallah, "A Petri net-based model for web servicecomposition," in Proc. of ADC. Australian Computer Society, Inc.,2003, pp. 191–200.

[18] X. Fu, T. Bultan, and J. Su, "Formal verification of e-services andworkflows," in Web Services, E-Business, and the Semantic Web, ser.LNCS 2512. Springer, 2002, pp. 188–202.