Privacy enhanced and web based service composition

Bandaru Swamy Sri¹, U.Vinod Kumar²

1PG Scholar, Pydah College of Engineering, Kakinada, AP, India, E-mail: udayswamysri@gmail.com.
2Assistant 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 application 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 consisting to the actual services of tasks that, at run-time, are instantiated satisfying users’ requirements. Due to the increasing number of services available offering similar functionalities, it hard for users to select a composition among optional service a list of candidate services that satisfy their needs. Therefore, service selection is a key challenge in the Future Internet. The literature offers of work on Web service composition and selection. Most of the existing approaches focus 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 best of our knowledge, only few works have investigated privacy issues in service selection. The orchestrator usually collects a large amount of personal data about their clients and eventually shares these data with these service providers providing the orchestrated services. This, however, may lead to risks of data misuse. For instance, a service provider may use client data for unlawful purposes. As a consequence, more and more users are considering privacy practices adopted by Web service providers as an important factor 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 modeling, service composition, and service selection.

a) Service composition modeling: To model service composition and verify whether it satisfies properties like safety and liveness, several languages, such as WS-BPEL, or approaches, such as process algebra Petri nets, model checking, and finite state machines, have been proposed. Contributions to service composition modelling also come from the requirement engineering community, where goal-oriented approaches, are used to represent strategic business goals. Similarly, we adopt a goal-oriented approach to model service composition. The advantage of such an approach is that it provides the abstraction necessary to represent privacy policies without getting bogged down into the functioning of Web services.

b) Service composition: Service composition is the problem of aggregating services in such a way that given (functional and not functional) requirements are satisfied. The role of privacy in service composition has been investigated in [13], where only services requiring the disclosure of less sensitive information and offered by trusted providers are selected in the composition. Users’ privacy concerns are often addressed by providing automated techniques for matching provider’s privacy policies with customer’s preferences. The most prominent solution for policy matching is P3P (Platform for Privacy

www.ij-seat.com
Preferences Project). P3P aims to assist service providers in specifying their privacy practices on the web, and users in matching such practices against their preferences. To automate the matching process, P3P has been complemented with privacy service composition as 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 of admissible service compositions. In addition, our work goes beyond pure service composition: we also identify the most privacy preserving composition.

III. Modeling Service Composition And Privacy

In this section we introduce the models to represent web service orchestration, privacy policies and user privacy preferences on which our approach is based.

A. Modelling Service Orchestration

In Web services composition typically there is an orchestrator which combines the functionalities provided by other services usually denoted as component services to satisfy users' requests. Several services may be able to provide the same functionality requested by the user. The service resulting 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 all possible alternative instantiations of the schema as a service orchestration model. We represent these models as AND/OR trees where the employs the notions of actor, goal, resource, decomposition and delegation. Actors are active entities that have strategic goals and perform actions to achieve them. Actors can be agents or roles: agents are used to represent the orchestrator and component services, and roles to represent the types of services, respectively. Decomposition is used to refine a goal: AND decomposition refines a goal into subgoals and resources needed to achieve the goal, while OR decomposition defines alternatives to achieve a goal. Delegation marks a formal passage of responsibility or authority from an actor (delegator) to another actor (delegate) to achieve a goal. We use these concepts to define the notion of service model and specific component services.

![Orchestrator Model](image1)

![Component Service Model with AND Decomposition](image2)

![Component Service Model with OR Decomposition](image3)

![Legend](image4)
In addition, the user may decide to not disclose a certain data item. Finally, the user should define the sensitivity of each data item, which may vary from purpose to purpose. Users, however, are not allowed to change the delegation depth and retention period. This is because these attributes are often constrained by the business model of the orchestrator as well as by the requirements imposed by the legal framework in force (e.g., telecommunications data have to be stored for six to 24 months according to the EU Directive on data retention). The result of this refinement process represents the privacy preferences of the user. We formally specify users’ privacy preferences as follows.

Definition 6 (Privacy preferences): The privacy preferences of a user are a set of tuples \( (d; f; g; p, T) \). The purpose for which \( d \) can be collected, \( f \) is the visibility of \( d \) for achieving \( p \), \( g \) is the (re)delegation depth which limits the sharing of \( d \) for achieving \( p \), and \( T \) 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 afraid to fly, he only wants to book a hotel and rent a car. Based on the privacy policy of TravelForLess (Table I), he specifies constraints on the collection and processing of his data. Bob’s privacy preferences are presented in Table II. Since name and date of birth are usually required by service providers, Bob leaves their visibility to all. In contrast, he prefers that his credit card details only be disclosed to agents he trusts, i.e. Travel with Us, TravelDeal and GreenParkHotel. Bob also restricts the access to his driver’s license only for the purpose of renting a car, and the national ID only for booking a hotel. Finally, Bob prefers that his phone number not be contactable by email and thus he is not willing to disclose his 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 performed by the architectural components.

A. Service Composition

Service orchestrators usually do not provide the functionalities required by a client directly but they outsource the provision to specialized services. Nonetheless, according to the EU privacy regulation, they are liable for the actions performed by the subcontractors. Therefore, an orchestrator is willing to select a component service only if the privacy policy of the component service complies with its policy and user privacy preferences. The aim of the service orchestration composition step is to identify admissible composite services, i.e. those composite services that comply with the user preferences and legal requirements. After a user has defined her privacy preferences through the refinement of the orchestrator’s privacy policy (see Example 5), the orchestrator uses these preferences to identify admissible composite services. Admissible composite services are determined using Algorithm 1. The algorithm builds the privacy model of the service orchestration that includes only those component services whose privacy policy complies with the user’s privacy preferences for the sake of simplicity, here we omit sensitivity in the user preferences, and represent them using the notation for privacy policies; sensitivity is used in the next step. The algorithm first identifies the portion of the privacy policy model of the orchestrator related to the functionalities required by the user (lines 5-20). The policy associated with a purpose is propagated to sub-purpose (lines 16-17). Intuitively, a purpose inherits the constraints from the higher level purpose. This makes it possible to check the consistency of policies along the service orchestration model. When the policy of the orchestrator is fully analyzed, the algorithm identifies the component services which offer functionalities required by the user and whose privacy policies are compliant with the privacy policy of the service delegating the service to them (lines 21-41). If the node to be analyzed is not a leaf node of the policy (line 24), the algorithm checks whether the policy associated with the subnodes of that node complies with the policy associated with the leaf node in the policy of the service delegating the provision of the functionality.
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

(b) Admissible Composite Services

Fig 6: Privacy-preserving Composite Service Ranking information 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 to set her priorities over the privacy dimensions, we aggregate them using an approach based on the norm. Intuitively, the privacy of a composite service is computed as the average of the criteria forming the privacy level. The dimensions as well the norm for each The height of a point represents its aggregated sensitivity, whereas the most right points are those with higher depths, and those more in the back have a longer retention period. Intuitively, we prefer those compositeservices represented by the lowest, left-most, front-most points on the graph. The norm gives a precise measure of the privacy level of composite services and, thus, makes it possible to distinguish the most privacy-preserving composite service, represented by p1 in our example.

Notice, however, that the framework is flexible enough to allow users to account more a particular dimension by specifying weights for the dimensions. These weights can be used to calculate the (weighted) average of the privacy level. For instance, a user can select the composite service that requires the less sensitive data release by setting the weight for the first two components.

Results

V. Conclusions

We have presented a novel approach to assist users and Web service providers in the composition and selection of composite services that are more privacy preserving. With respect to other proposals for privacy-preserving Web service composition, our approach supports the specification of fine-grained privacy policies and preferences based on different privacy dimensions, i.e., purpose, visibility, retention period, and sensitivity. In addition, our approach ranks the generated composite Web services with respect to...
their privacy level, which quantifies the risk of unauthorized disclosure of user information based on three dimensions: sensitivity, visibility, and retention period. As future work, we are planning to implement our approach as a Web service, and to test its performance with respect to the number of candidate Web services the complexity of the privacy policies of the orchestrator and component services.

REFERENCES


