Privacy-Enhanced Web Service Composition

Dr. Mohammed Abdul Waheed¹, Sheeba Shabnam²

¹Associate Professor, Department of Computer Science and Engg, VTU Regional Center, Kalaburagi, Karnataka, India
²P G Student, Department of Computer Science and Engg, VTU Regional Center, Kalaburagi, Karnataka, India

Abstract: Data as a Service (DaaS) builds on service-oriented technologies to enable fast access to data resources on the Web. However, this paradigm raises several new privacy concerns that traditional privacy models do not handle. In addition, DaaS composition may reveal privacy-sensitive information. In this paper, we propose a formal privacy model in order to extend DaaS specifications with privacy capabilities. The privacy model allows a service to define a privacy policy and a set of privacy requirements. We also propose a privacy-preserving DaaS composition approach allowing to verify the compatibility between privacy requirements and policies in DaaS composition. We propose a negotiation mechanism that makes it possible to dynamically reconcile the privacy capabilities of services when incompatibilities arise in a composition. We validate the applicability of our proposal through a prototype implementation and a set of experiments.

Keywords: Service Composition, DaaS Services, Privacy, Negotiation.

1. Introduction

Web services have recently emerged as a popular medium for data publishing and sharing on the Web [18]. Modern enterprises across all spectra are moving towards a service-oriented architecture by putting their databases behind Web services, thereby providing a well-documented, platform independent and interoperable method of interacting with their data. This new type of services is known as DaaS (Data-as-a-Service) services [33] where services correspond to calls over the data sources. DaaS sits between services-based applications (i.e. SOA-based business process) and an enterprise’s heterogeneous data sources. They shield applications developers from having to directly interact with the various data sources that give access to business objects, thus enabling them to focus on the business logic only. While individual services may provide interesting information/functionality alone, in most cases, users’ queries require the combination of several Web services through service composition. In spite of the large body of research devoted to service composition over the last years [24], service composition remains a challenging task in particular regarding privacy. In a nutshell, privacy is the right of an entity to determine when, how, and to what extent it will release private information [16]. Privacy relates to numerous domains of life and has raised particular concerns in the medical field, where personal data, increasingly being released for research, can be or have been, subject to several abuses, compromising the privacy of individuals [3].

<table>
<thead>
<tr>
<th>Table 1: A subset of DaaS services</th>
</tr>
</thead>
<tbody>
<tr>
<td>DaaS services</td>
</tr>
<tr>
<td>S1,H(Sx, ?, ?)</td>
</tr>
<tr>
<td>S2,(Sx, ?, d, ?, g)</td>
</tr>
<tr>
<td>S3,(Sx, ?, s)</td>
</tr>
<tr>
<td>S4,(Sx, ?, ?)</td>
</tr>
<tr>
<td>S5,(Sx, ?, n)</td>
</tr>
<tr>
<td>S6,(Sx, ?, ?)</td>
</tr>
</tbody>
</table>

1.1 e-Epidemiological Scenario

Let us consider the services in Table 1 and the following epidemiologist’s query Q “What are the ages, genders, address, DNA, salaries of patients infected with H1N1; and what are the global weather conditions of the area where these patients reside?”. We proposed in [2] a mediator-based approach to compose DaaS. The mediator selects, combines and orchestrates the DaaS services (i.e., gets input from one service and uses it to call another one) to answer received queries. It also carries out all the interactions between the composed services (i.e., relays exchanged data among interconnected services in the composition). The result of the composition process is a composition plan which consists of DaaS that must be executed in a particular order depending on their access patterns (i.e., the ordering of their input and output parameters). Thus, Q can be answered by composing the following services S1,H • S1,4 • S2,2 • S1,1 • S1,1. It means that S1,1 is first invoked with H1N1, then for each obtained patient, S1,4 is invoked to obtain their DNA, S2,2 and S1,1 to obtain date of birth, zip code and salary of obtained patients. Finally, S1,1 is invoked with the patients’ zip code to get information about the weather conditions.

1.2 Challenges

Two factors exacerbate the problem of privacy in DaaS. First, DaaS services collect and store a large amount of private information about users. Second, DaaS services are able to share this information with other entities. Besides, the emergence of analysis tools makes it easier to analyze and synthesize huge volumes of information, hence increasing the risk of privacy violation [21]. In the following, we use our epidemiological scenario to illustrate the privacy challenges during service composition.

Challenge 1: Privacy Specification. Let us consider services S4,1 and S5,1 in Table 1. The scientist considers both input and output parameters of S4,1 (i.e., SSN and DNA) as sensitive data. Let us now assume that this scientist states the following hypothesis: ”weather conditions” has an impact on H1N1 infection.” For that purpose, he/she invokes S5,1. The
scientist may want to keep $S_{31}$ invocation as private (independently of what $S_{31}$ takes and returns as data) since this may disclose sensitive information to competitors. The aforementioned first challenge puts in evidence the need for a formal model to specify private data is and how it will be defined.

**Challenge 2: Privacy within compositions.** Component services (that participate in a composition) may require input data that cannot be disclosed by other services because of privacy concerns. They may also have conflicting privacy concerns regarding their ex-changed data. For instance, let us assume that $S_{11}$ states to disclose its data (SSN) to a third-party service for use in limited time. $S_{11}$ meanwhile attests that it uses collected data (SSN) for an unlimited time use. Then, $S_{11}$ and $S_{31}$ have different privacy constraints regarding the SSN. This will invalidate the composition in terms of privacy concerns.

**Challenge 3: Dealing with incompatible privacy policies in compositions.** The role of the mediator is to return composite services with compatible component services with respect to privacy. The simplest way to deal with compositions with incompatible privacy policies is to reject those composition. However, a more interesting, yet challenging approach would be to try to reach a consensus among component services to solve their privacy incompatibilities, hence increasing the number of composition plans returned by the mediator.

### 1.3 Contributions

**Privacy Model.** We describe a formal privacy model for Web Services that goes beyond traditional data-oriented models. It deals with privacy not only at the data level (i.e., inputs and outputs) but also service level (i.e., service invocation). In this paper, we build upon this model two extensions to address privacy issues during DaaS composition. The privacy model described in this paper is based on the model initially proposed in [30] and [28].

**Privacy-aware Service Composition.** We propose a compatibility matching algorithm to check privacy compatibility between component services within a composition. The compatibility matching is based on the notion of privacy subsumption and on a cost model. A matching threshold is set up by services to cater for partial and total privacy compatibility.

**Negotiating Privacy in Service Composition.** In the case when any composition plan will be incompatible in terms of privacy, we introduce a novel approach based on negotiation to reach compatibility of concerned services (i.e., services that participate in a composition which are incompatible). We aim at avoiding the empty set response for user queries by allowing a service to adapt its privacy policy without any damaging impact on privacy. Negotiation strategies are specified via state diagrams and negotiation protocol is proposed to reach compatible policy for composition.

### 1.4 Paper Organization

The rest of this paper is organized as follows: In Section 2 we review the composition approach proposed in [2] as part of the PAIRSE project. We present our privacy model in Section 3. We introduce the notion of compatibility between privacy policies and requirements in Section 4. In Section 5 we show how our DaaS com-position approach is extended within privacy-preserving mechanism. We present our negotiation model in Section 6 to deal with the issue of privacy incompatibility. In Section 7 we describe our prototype implementation and evaluate the performance of the proposed approach. We overview related work in Section 8. We provide concluding remarks in Section 9.

### 2. The Pairse Project: Background

The approach presented in this paper is implemented as a part of PAIRSE project which deals with the privacy preservation issue in P2P data sharing environments, particularly in epidemiological research where the need of data sharing is apparent for making better a health environment of people. To support the decision process, epidemiological researchers should consider multiple data sources such as the patient data, his social conditions, the geographical factors, etc. The data sources are provided by DaaS services, and are organized with peers. DaaS services differ from traditional Web services, in that they are stateless; i.e. they only provide information about the current state of the world but do not change that state. When such a service is executed, it accepts from a user an input data of a specified format (“typed data”) and returns back to the user some information as an output. DaaS services are modeled by RDF views.

Figure 1 summarizes the architecture of this project. The Multi-Peer Query Processing component is in charge of being stolen by a competing company. We give below the definition of the privacy level.

**Privacy level on resource:** rs1ofSis defined as follows: (i) $L=\text{“data”}$ if rs is an input/output of $S$

---

**Figure 1:** PAIRSE global architecture

---

**Volume 4 Issue 6, June 2015**

[www.ijsr.net](http://www.ijsr.net)  
Licensed Under Creative Commons Attribution CC BY

132

---

Paper ID: SUB155209
local query using an RDF a query rewriting algorithm [2]. Then, it carries out all the interactions between the composed services and generates a set of composition plans to provide the requested data.

3. Privacy Model

In this section, we describe our privacy model for DaaS services. Each service S has a privacy policy (noted as PP) specifying the set of privacy practices applicable on any collected data and privacy requirements (noted as PR) specifying the set of privacy conditions that a third-party service T must meet to consume S’s data. A preliminary version of the model described in this section was proposed in [28].

3.1 Privacy Level

We define two privacy levels: data and operation. The data level deals with data privacy. Resources refer to input and output parameters of a service (e.g., defined in WSDL). The operation level copes with the privacy about operation’s invocation. Information about operation invocation may be perceived as private independently on whether their input/output parameters are confidential or not [10]. For instance, let us consider a scientist that has found an invention about the causes of some infectious diseases, he invokes a service operation to search if such an invention is new before he files for a patent. When conducting the query, the scientist may want to keep the invocation of this operation private, perhaps to avoid part of his idea

3.2 Privacy Rule

The sensitivity of a resource may be defined according to several dimensions called privacy rules. We call the set of privacy rules RulesSet(RS). We define a privacy rule by a topic, domain, level and scope.

The topic gives the privacy facet represented by the rule and may include for instance: the resource recipient, the purpose and the resource retention time. The “purpose” topic states the intent for which a resource collected by a service will be used; the “recipient” topic specifies to whom the collected resource can be revealed. The level represents the privacy level on which the rule is applicable. The domain of a rule depends on its level. Indeed, each rule has one single level: “data” or “operation”. The domain is a finite set that enumerates the possible values that can be taken by resources according to the rule’s topic. For instance, a subset of domain for a rule dealing with the right topic is (“no-retention”, “limited-use”). The scope of a rule defines the granularity of the resource that is subject to privacy constraints. Two rules at most are created for each topic: one for data and another for operations.

A privacy Rule \( R_i \) is defined by a tuple \( (T_i, L_i, D_i, S_i) \) where:

- \( T_i \) is the topic of \( R_i \)
- \( L_i \in \{"data","operation"\} \) is the level of the rule.
- \( D_i \) is the domain of \( R_i \); it enumerates the possible values that can be taken by \( T_i \) with respect to \( r_i \).
- \( S_i \) is the scope of \( R_i \) where \( S_i = \{"total","partial"\} \) if \( L_i = \"operation\" \) and \( S_i = \{"total"\} \) if \( L_i = \"data\". \)

Example 1. We give two examples of rules \( R_1 \) and \( R_3 \) in RS, where: \( R_1=(T_1, L_1, D_1, S_1) \) where \( T_1=\"recipient\" \), \( D_1=\{public, research, lab, government, hospital, university\} \) and \( L_1=\"data\" \) and \( S_1=\"total\" \). \( R_3=(T_3, L_3, D_3, S_3) \) where \( T_3=\"retention\" \), \( D_3=[0,1,...,Unlimited] \) (defining retention in day), \( L_3=\"data\" \) and \( S_3=\"total\". \)

3.3 Privacy Annotation for WSDL-based DaaS

In our previous work detailed in [22], we have defined a mechanism to annotate WSDL 2.0 descriptions under the interface element that describes the abstract part of the service with privacy specification of service. We choose to annotate WSDL descriptions at the three following places: interface, operation, input and output. Furthermore, we note that services are located in Peer-to Peer environment which is controlled and managed by a super-peer. A service S wanting to adhere to this environment, has to undertake to respect its PR and PP by the signing of an e-contract with the responsible peer.

4. The Privacy Compatibility Checking

In this section, we introduce the notion of compatibility between privacy policies and requirements. Then, we define the notion of privacy subsumption and present our cost model-based privacy matching mechanism.

4.1 Privacy Subsumption

Let us consider a rule \( R=(T, L, D, S) \). Defining an assertion \( A(R, rs)=(p, g) \) for \( rs \) involving assigning value(s) from \( D \) to the propositional formula \( pf \) of \( A \). The values in \( D \) are related to each other. For instance, let us consider the domain /public, government, federal tax, research/ for a rule dealing with topic \( T=\"recipient\" \). The value public is more general than the other values in \( D \). Indeed, if the recipient of \( rs \) is declared public (i.e., shared with any entity), then the recipient is also government and research. Likewise, the value government is more general than the other values in \( D \). To capture the semantic relationship among domain values, we introduce the notion of privacy subsumption (noted \( \_\_ \)). For instance, the following subsumptions can be stated: government/public; research _ government. Note that privacy subsumption can be different from the typical subsumption of domain concepts represented with the notation \( Cp \).
5. Existing System

A typical example of modeling privacy is the Platform for Privacy Preferences (P3P). However, the major focus of P3P is to enable only Web sites to convey their privacy policies. In privacy only takes into account a limited set of data fields and rights. Data providers specify how to use the service (mandatory and optional data for querying the service), while individuals specify the type of access for each part of their personal data contained in the service: free, limited, or not given using a DAML-S ontology.

Disadvantages of Existing System

Two factors exacerbate the problem of privacy in DaaS. First, DaaS services collect and store a large amount of private information about users. Second, DaaS services are also service level (i.e., service invocation). In this paper, we use our model two other extensions to address the risk of privacy violation. In the following, we use our epidemiological scenario to illustrate the privacy challenges during service composition.

Challenge 1: Privacy Specification.
Challenge 2: Privacy within compositions.
Challenge 3: Dealing with incompatible privacy policies in compositions.

6. Proposed System

We describe a formal privacy model for Web Services that goes beyond traditional data-oriented models. It deals with privacy not only at the data level (i.e., inputs and outputs) but also service level (i.e., service invocation). In this paper, we build upon this model two other extensions to address privacy issues during DaaS composition. The privacy model described in this paper is based on the model initially proposed.

Advantages of Proposed System

1. Privacy-aware Service Composition: We propose a compatibility matching algorithm to check privacy compatibility between component services within a composition.
2. Negotiating Privacy in Service Composition: In the case when any composition plan will be incompatible in terms of privacy, we introduce a novel approach based on negotiation to reach compatibility of concerned services (i.e., services that participate in a composition which are incompatible).

Algorithm Used:

```
1 foreach rs_j = rs_k do
  2 for i = 1, |i, RS| do
  3 for j = 1, |j, PR^k| do
  4   for j = 1, |j, PP^i| do
  5     if (A_j, (R_s, rs_k), i, j, PR^k) then
  6       A_j, (R_s, rs_k) is compatible with
  7       A_j, (R_s, rs_k)
  8       else Inc = (A_j, (R_s, rs_k), A_j, (R_s, rs_k))
```

7. Conclusion and Future Work

In this paper, we proposed a dynamic privacy model for Web services. The model deals with privacy at the data and operation levels. We also proposed a negotiation approach to tackle the incompatibilities between privacy policies and requirements. Although privacy cannot be carelessly negotiated as typical data, it is still possible to negotiate a part of privacy policy for specific pur-poses. In any case, privacy policies always reflect the usage of private data as specified or agreed upon by service providers. As a future work, we aim at designing techniques for protecting the composition results from privacy attacks before the final result is returned by the mediator.

References


