4. The Framework for Privacy-enabled Composite Web Services

Having realized the need to develop a better mechanism for privacy of private information in composite web services, we initiated research for building a framework for privacy-enabled composite web services. The resulting framework is described in this chapter.

4.1 FRAMEWORK OVERVIEW

Figure 4.1 shows the architecture of our proposed framework for privacy-enabled composite web services. It consists of the following major components:

1. Consumer
2. Composite Service Provider (CSP) interface
3. Composite Service Provider (CSP): It consists of CSP Proxy and CSP Privacy Components. CSP Privacy Components, in turn, contain modules for Composite Web Service Management, Transaction Tracking and Registration, Consumer Privacy Preferences, Service Provider Privacy Policies, Privacy Policy Control, Consumer Enforcement, and Service Provider Enforcement.
Roles of the various components of the proposed framework are as follows:

1. **Consumer.** A consumer (or customer or client) is a user of services offered by composite web services. In our framework, Composite Service Provider (CSP) offers the services to consumers.

2. **CSP interface.** All interactions between a consumer and the CSP take place through this interface. It supports commands for various functionalities such as transaction tracking and registration, composite web service management, consumer privacy preferences, service provider privacy policies, privacy policy control, consumer enforcement, and service provider enforcement.
as login, service request, service response, specification of consumer privacy preferences, negotiation for privacy agreements, transaction tracking information request, etc.

3. **CSP proxy.** CSP proxy serves as an interface between web services on the Internet and consumers. To service a consumer’s request (a web service transaction or WS-transaction) it identifies the appropriate web services from those available on the Internet and combines them to form a composite web service for servicing the request.

4. **Composite web service management.** This module manages the multiple web services of a composite web service to complete a WS-transaction’s goal. Each web service of a composite web service takes care of its own part of the total service required by the WS-transaction. Hence, this module includes business logic for interaction among the various web services of a composite web service.

5. **Consumer privacy preferences.** This module maintains consumers’ privacy preferences. While registering with the CSP and/or making a service request to the CSP, a consumer specifies his/her privacy preferences, which indicate which information is he/she willing to share with whom and in what manner. It also includes which of the submitted information the consumer is not willing to share with third parties.

6. **Service provider privacy policies.** This module maintains privacy policies of web service providers identified for becoming part of a composite web service. While agreeing to offer its services as part of a composite web service, a web service provider specifies its privacy policies, which deal with issues such as:
   - What information will the service provider collect from a consumer
   - How will the service provider use consumer’s information
   - With whom will the service provider share the consumer’s information
   - How can the consumer access his/her information
   - For how much time will the service provider save the information
• How will the service provider protect the consumer’s information

7. **Privacy policy control.** This module validates a consumer’s privacy preferences and a service provider’s privacy policy for compatibility. If compatible, the consumer is allowed to use the service, else this module interacts with consumer enforcement module and/or service provider enforcement module for negotiating consumer’s privacy preferences and/or service provider’s privacy policy to enable compatibility.

8. **Consumer enforcement.** When a consumer’s privacy preferences and the service provider’s privacy policy do not comply fully, the privacy policy control module first interacts with consumer enforcement module to check if the consumer is willing to relax its privacy preferences to match the service provider’s privacy policy. For this, the consumer enforcement module, in turn, interacts with the consumer and the consumer privacy preferences module.

9. **Service provider enforcement.** When a consumer’s privacy preferences and the service provider’s privacy policy do not comply even after the privacy policy control module has negotiated with the consumer enforcement module, the privacy policy control module then interacts with service provider enforcement module to check if the service provider is willing to change its policy and/or accept alternate attributes. For example, the service provider of an airline ticket booking service requests mobile no. from the consumer, but if he/she does not agree, then an alternate choice can be provided to the consumer (e.g. email-ID instead of mobile no.). For this, the service provider enforcement module, in turn, interacts with the service provider and the service provider privacy policies module.

10. **Transaction tracking & registration.** It records and tracks all WS-transactions between a consumer and a service provider, and gives alert to the consumer’s email-ID when a WS-transaction happens, including the agreement done between the consumer and the service provider. For example, when the composite service submits some personal information
of a consumer that is required by a service provider of airline ticket booking service, then one copy of that WS-transaction is sent to Transaction Tracking & Registration unit. Later, if a third party requests some personal information from the web service (second party), same recording will happen for the WS-transaction.

11. **Web services.** These are the web sites, which offer various types of web services and are registered web service providers for composite service provisioning. Services are grouped together using composition code to form a composite web service. The services grouped together perform different functions to help consumers meet their multiple associated requirements. For example, multiple associated requirements of a travel arrangement, such as Air ticket booking, Hotel reservation, and Car rental can be part of a composite web service.

12. **Database.** It stores various types of information (such as login information of consumers, privacy preferences of consumers, and privacy policies of service providers) collected from consumers and service providers. It also stores information related to all WS-transactions (which information is shared with whom all and for what duration), including negotiations and agreements done between various consumers and service providers.

### 4.2 FRAMEWORK'S SERVICE PROCESS

Key operations in the proposed framework for service request and provisioning process are described below.

#### 4.2.1 Consumer Registration

Only registered clients are granted access to composite service provider’s services. Hence, every client (or consumer) must first register with the CSP to avail its services.
The registration process allows clients to choose their service-login credentials, consisting of a unique username and a password. Clients then need to specify their privacy preferences according to information categories (described later in this chapter). Since a username is used to identify a client, no duplicates are allowed. The interface for this registration process is provided through a web site.

Client credentials are sensitive piece of information, which need to be kept private. For this purpose, a secured (using MD5 encryption) communication channel is established between a client and the CSP during registration process. This secures the clear text credentials submitted via the registration process and assures the clients of privacy and confidentiality of their private information. Figure 4.2 provides an overview of the registration process and the security steps involved.

![Figure 4.2. Consumer registration.](image)
4.2.2 Consumer Login

A registered consumer has to first login with the CSP to start an interaction session with it. The CSP authenticates the consumer at the time of login. If the consumer is authenticated successfully, he/she can access his/her privacy preferences details, tracking details, agreements and edit details, and can request for web services. Figure 4.3 shows the login screen.

![Login Screen]

Figure 4.3. Login to CSP.

4.2.2 Consumer Service Request

A successfully logged in consumer can make a web service request to the CSP. At the time of making a service request, a consumer can also specify any special privacy preferences for this service request over and above its default privacy preferences specified at the time of registration. Privacy preferences specified with a service request override a consumer’s default privacy preferences specified at the time of consumer’s registration. Other privacy preferences of the consumer hold good as specified at registration time.
When a consumer makes a web service request, the CSP identifies one or more web service providers to service the request. The CSP then asks each identified web service provider to specify its privacy policies. Assuming that a single web service provider is identified for this request, the CSP then checks privacy compliance of the consumer and the selected service provider as per the privacy compliance algorithm described below.

### 4.2.3 Privacy Compliance

Privacy compliance deals with checking for compliance between a consumer's privacy preferences and the privacy policy of a service provider, which has been identified for providing service to the consumer. If the two do not comply fully, it also deals with negotiating with the consumer and/or the service provider for relaxation of their privacy preferences and/or privacy policy for privacy agreement.

Figure 4.4 shows the pseudocode for the algorithm for privacy compliance. In Lines 1 and 2, two arrays are read, which include privacy policy of service provider (e.g. credit card number, email-ID, date of birth, and mobile number) and privacy preferences of consumer (e.g. credit card number, date of birth, mobile number, and email-ID). In Lines 4 and 5, privacy policy of service provider and privacy preferences of the consumer are compared for privacy compliance. If they are compatible, then in Line 6 privacy compliance is recorded and in Line 7 the request is forwarded to the service provider. Otherwise, in Line 10, consumer enforcement is initiated to check if consumer is willing to relax its privacy preferences for compliance. If the consumer agrees for relaxation, then in Line 12 privacy compliance with consumer enforcement is recorded (relaxations agreed by consumer are also recorded and in Line 13 the request is forwarded to the service provider. Otherwise, in Line 16 service provider enforcement is initiated to check if service provider is willing to change its policy and/or accept alternate attributes. If the service provider agrees for relaxation, then in Line 18 privacy compliance with service provider enforcement is recorded (relaxations agreed by service provider are also recorded), and in Line 19 the request is forwarded to the service provider.
Input: = list of privacy policy of service provider (PPOSP)
Input: = list of privacy preferences of consumer (PPOC)

Begin

Select (PPOSP) & (PPOC) from list

If (PPOSP = PPOC) then

Record it as privacy compliance

Forward the request to service provider

Go to End

Else

Initiate consumer enforcement to check if consumer is willing to relax its privacy preferences for compliance

If (Consumer agrees for relaxation) then

Record it as privacy compliance with consumer enforcement (records relaxations agreed by consumer)

Forward the request to service provider

Go to End

Else

Initiate service provider enforcement to check if service provider is willing to change its policy and/or accept alternate attributes

If (Service provider agrees for relaxation) then

Record it as privacy compliance with service provider enforcement (records relaxations agreed by service provider)

Forward the request to service provider

Go to End

End if

End if

End

Figure 4.4. Privacy compliance algorithm.
Note that in our pilot implementation (privacy compliance algorithm of Figure 4.4), we have shown that privacy agreement is reached either by consumer enforcement (consumer relaxes its privacy preferences) or by service provider enforcement (service provider relaxes its privacy policy). However, in real implementation of the framework, privacy agreement could also be reached by partial consumer enforcement (consumer relaxes some attributes of its privacy preferences) and partial service provider enforcement (service provider relaxes some attributes of its privacy policy).

### 4.2.4 Transaction Tracking and Registration

Transaction tracking and registration deals with keeping track of and informing a consumer whenever the CSP shares consumer’s private information with a service provider, or a service provider that has received consumer’s private information needs to share it with another service provider (third party).

Figure 4.5 shows the pseudocode for the algorithm for transaction tracking and registration. In Line 1, consumer’s request is read (for example, airline ticket booking request). In Line 3, CSP selects a suitable service provider for providing the requested web service. If the service provider requires consumer’s private information (for example, Social Security Number (SSN), telephone number, and address) for offering its service, the same is sent to the service provider in Line 5 and the consumer is intimated about it in Line 6. At the same time, in Line 7 CSP records one copy of that information, including the WS-transaction ID, contact number, date and time. Transaction tracking and registration process ends with the CSP sending a response to the consumer when the service is completed (Lines 8 and 9).

A similar process is carried out in Lines 11-13, if a service provider having consumer’s private information needs to share this information with another service provider (third party).
1: **Input**: = consumer’s request
2: **Begin**
3: Select suitable service provider for servicing consumer’s request
4: **If** (service provider requires consumer’s private information) **then**
5: Send the private information to the service provider
6: Send alert to consumer intimating private information has been sent to the service provider
7: Record this information with WS-transaction ID, contact number, date and time
8: Send response to consumer when the service is completed
9: **End if**
10: **If** (service provider needs to share consumer’s private information with third party) **then**
11: Send consumer’s private information to third party
12: Send alert to consumer intimating private information has been sent to third party
13: Record this information with WS-transaction ID, contact number, date, time and third party’s ID
14: **End if**
15: **End**

---

**Figure 4.5.** Transaction tracking and registration algorithm.

### 4.2.5 Edit Privacy Preferences

It is a part of the interface between consumer and CSP. It enables a consumer to display his/her privacy preferences and update it suitably from time-to-time. Figure 4.6 shows a snapshot of edit privacy preferences screen. If a privacy preferences
attribute is “public”, it can be shared with service providers without consumer’s permission during service provisioning. One the other hand, if an attribute is “private” it can be shared with a service provider only after negotiation for relaxation with the consumer during consumer enforcement.

![Privacy Component Interface](image)

**Figure 4.6. Privacy preferences details.**

### 4.2.6 Display Transaction Tracking Information

This is also a part of the interface between consumer and CSP. It enables a consumer to display the details of a WS-transaction. For a WS-transaction, the details include information about which attributes of consumer’s private information have been shared with which service providers and when. It also tells policy status indicating whether there was a direct match between consumer’s privacy preferences and service provider’s privacy policy for sharing this attribute or an obligation (relaxation) was required for agreement to share the attribute. Figure 4.7 shows a snapshot of screen displaying transaction tracking information.
### 4.3 INFORMATION CATEGORIES AND SENSITIVITY OF INFORMATION

We use two attributes, information categories and sensitive information, to classify user's data to ease policy specification and management. Information categories can be of various types such as personal information, financial information, health information, and address information. Using the attributes sensitive information and information category, a consumer can specify more expressive privacy policies. Hence, when a consumer decides to release personal information to different web sites or web services, he/she can put his/her desired trust for each one.
of them. Figure 4.8 presents example data based on sensitive information and information categories.

<table>
<thead>
<tr>
<th>Information Categories</th>
<th>Sensitive Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-World Contact Information</td>
<td>Physical-world contact info, address, phone, fax</td>
</tr>
<tr>
<td>Online Contact Information</td>
<td>Email address, screen name, instant messaging identifier</td>
</tr>
<tr>
<td>Financial Information</td>
<td>History of financial accounts, transaction, balances</td>
</tr>
<tr>
<td>Purchase Information</td>
<td>Specific to one transaction, such as payment method</td>
</tr>
<tr>
<td>Non-Financial Identifier</td>
<td>User ID, social security no, other non-financial ID</td>
</tr>
<tr>
<td>Personal Preferences Data</td>
<td>Favorite color, music, hobbies, other interests</td>
</tr>
<tr>
<td>Online Postings and User Content</td>
<td>Display contact, user name</td>
</tr>
<tr>
<td>Political Information</td>
<td>Membership in political parties, trade unions</td>
</tr>
<tr>
<td>Health Information</td>
<td>Physical/mental health history, interests, related purchases</td>
</tr>
<tr>
<td>User Navigation and Click stream Data</td>
<td>Cookies, IP Address</td>
</tr>
</tbody>
</table>

**Figure 4.8.** Information categories and sensitive information.

### 4.4 STANDARDS FOR CONTRACTS AND INFORMATION TRANSFERS

The centralization of control in the Tracking and Agreement units requires some standardization of the manner in which agreements and transfers are recorded to ensure a more consistent approach of information exchange. We propose standard information shown in Figure 4.9 and Figure 4.10.
Matched Policy of Figure 4.9 identifies the relevant agreement. Policy Status identifies the status of policy, which is private or public. If it is private, customer is supposed to create agreement with service provider to get the service. User Type is one of the two types of users: consumer or service provider.

<table>
<thead>
<tr>
<th>Matched Policy</th>
<th>Tracking Date</th>
<th>User Name</th>
<th>User Type</th>
<th>Policy Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.9.** Standard for recording agreement between a consumer and a service provider.

In Figure 4.10, User Policy identifies the customer code, Matched Policy identifies the relevant agreement, Sensitive Information lists personal information of the consumer, and Information Categories identifies the category of each sensitive information.

<table>
<thead>
<tr>
<th>User Policy:</th>
<th>Matched Policy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive Information</td>
<td>Information Categories</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.10.** Standard for recording an information transfer between a consumer and a service provider as per an agreed agreement.

Standardization of information in this fashion enables the Tracking and Agreement units to provide a consistent interface and summary across all agreements and transfers for a given consumer. This makes it easy for the consumer to follow the flow of his/her personal information in a business process network.