

# Web Service Discovery Based on Privacy Preferences

Mona Tavakolan, Maryam Zarreh and Mohammad Abdollahi Azgomi

**Abstract**—Today, most Internet users are worried about protecting their personal information, which may be gathered by web services. This concern can have a profound influence on finding a way for applying privacy-aware policies on web services. In this regard, there are just a few accessible web services on the web, which usually provide users with simple operation and are not able to apply the user preferences. In this paper we present a new method for applying the users' preferences within the privacy-aware policies on web services. In this method, an extensible model for describing the users' preferences on discovery of web services is proposed. The model along with general rules can cover the desired criteria according to privacy-aware policies and presents a scenario based on users' preferences for discovering web services.

**Index Terms**— Web service, privacy, privacy-aware policy.

## I. INTRODUCTION

In the past few years, many companies have been forced to reorganize their businesses by using heterogeneous technologies in order to remain competitive in a business world. Current trends in Information and communication technology (ICT) may accelerate the widespread use of web services in business [25]. Web services have become more and more popular in the research community as well. A web service is defined as an autonomous unit of application logic that provides either some business functionalities or information to the other applications through an Internet connection. Web services are based on a set of extensible markup language (XML) standards such as the universal description, discovery and integration (UDDI), web services description language (WSDL), and simple object access protocol (SOAP) [26].

Web services encapsulate the operation and information sources and make them available on the web by the means of standard programming interfaces. Using prepared web services has many advantages for the Internet users. Thus, there is an increasing growth of the web services, which leads to raising the importance of retention of user's personal information by these services [1],[2].

Privacy control is usually not concerned with the individual subjects. The traditional view of access control model should be

extended with an enterprise wide privacy policy for managing and enforcing of individual privacy preferences [27].

As web services are becoming more and more popular for supporting different business applications, there are also increasing demands for web services privacy technologies in the industry and research community. The information exchange in such a web services-based business environment must be protected by privacy-enhancing technologies [28].

In particular, the information privacy relates to an individual's rights to determine how, when, and to what extent the personal information can be released to the other individuals or organizations. The information privacy is usually concerned with the confidentiality of the business sensitive information on Internet. Many studies show that a good privacy protection is an important factor to generate a good business. In general, the privacy policies of an organization describe the information collected from individuals (e.g., consumers) and the purposes of this data collection [5],[20].

The main issue, which should be concerned, is when a web service is found, the application will try to bind to each web service through SOAP messages. From the users' point of view, the privacy concerns mainly raise in the registries and web services. For example, the users may want the registries to protect their privacy such as their identities and what information they have retrieved from the registries. In addition, the users may also want to validate the privacy policies of business entities and services based on their privacy preferences. It means that the web services application may only bind to those web services such that their privacy policies are satisfied [17].

In this paper we present a discovery algorithm based on users' preferences through adding a measure named *privacy of service* (PoS) to the privacy information core of the UDDI structure as well. We present a new method for applying the users' preferences within the privacy-aware policies on web services. In this method, an extensible model for describing the users' preferences on discovery of web services is proposed. The model along with the general rules can cover the desired criteria according to privacy-aware policies and presents a scenario based on users' preferences for discovering web services.

The rest of this paper is organized as follows. In section II, an extensible privacy-aware policy model for web services is presented. In section III, we introduce the processes of a web service using the proposed model. In section IV, we propose a method to evaluate the web service privacy-policies confidence.

Manuscript received March 15, 2009.

Mona Tavakolan. (e-mail : mona\_tavakkolan@yahoo.com)

Maryam Zarreh. (e-mail : maryam\_zarreh@yahoo.com)

Mohammad Abdollahi Azgomi (e-mail: azgomi@iust.ac.ir)

In section V, we present the web service discovery algorithm based on the users' preferences. In section VI, a comparison to the related works is presented. Finally, section VII concludes the paper.

## II. AN EXTENSIBLE PRIVACY-AWARE POLICY MODEL FOR WEB SERVICES

The aim is to specify and apply the user's privacy preferences, such as *collection*, *use*, *disclosure* and *retention*, as a privacy-aware policy for web services. The existing web services ignore the users' preferences on privacy metrics for their personal information. To solve this problem, first an exact and nominal description of the privacy metrics should be introduced. In this section, such a privacy metrics is defined. Then, a model for privacy-aware web service will be presented [15].

### A. Privacy Metrics

The absence of a common definition of privacy metrics may cause that the web services and users have vague interpretations on privacy. For constructing a descriptive model of the general privacy policies, a classification and exact definitions for some metrics is presented in TABLE I.

TABLE I  
CLASSIFICATION OF PRIVACY METRICS [12]

Principle	Brief Description
Collection	Collect information only if needed and in a lawful manner after disclosing its identity.
Disclosure	Not use or disclose personal information for reasons other than the purpose for which the information is collected.
Data quality	Take reasonable steps to make sure that the personal information that it collects uses or discloses is accurate.
Data security	Take reasonable steps to protect the personal information it holds from misuse.
Openness	Set out an easily accessible document that clearly expresses policies.
Access and Correction	Personal information must provide the individual with access to the information on request by the individual as per the rules.
Identifiers	Adopt as its own identifier of an individual that has been assigned by: an agency; or an agent of agency acting in its capacity as agent.
Anonymity	Wherever it is lawful and practicable, individuals must have the option of not identifying themselves.
Transborder data flows	Transfer personal information about an individual to someone who is in a foreign country with individual's consent to transfer.
Sensitive information	Not collect sensitive information about an individual unless the individual has consented or the collection is required by law.

The metrics presented in TABLE I, are useful for constructing a descriptive model of privacy-aware policy on web services. In this regard, the descriptive model of web

services must be changed and enriched through the concept of privacy-aware and should be able to add the privacy metrics. In addition, such a model must be defined to enable the consumers to express their opinion on the requirements of privacy.

Each privacy metrics can be composed of several sub-metrics and it can also be expanded with new metrics. The users of service can have various interests in applying the privacy policies. Therefore, it is necessary to prioritize web services privacy metrics before their evaluation, based on the user interests [18].

### B. A Descriptive Model of Privacy-Aware Policy for Web Services

Now, we propose an expanded model on web services as in Fig. 1, which is based on [13], to present how to categorize the privacy metrics that for example can be composite of obligation, disclosure and collection. Also, in the next level obligation can be aggregated from data retention and data accessibility.

In the proposed model of privacy for web services, the user must be able to select a series of metrics and attribute and then assign some weights to them.

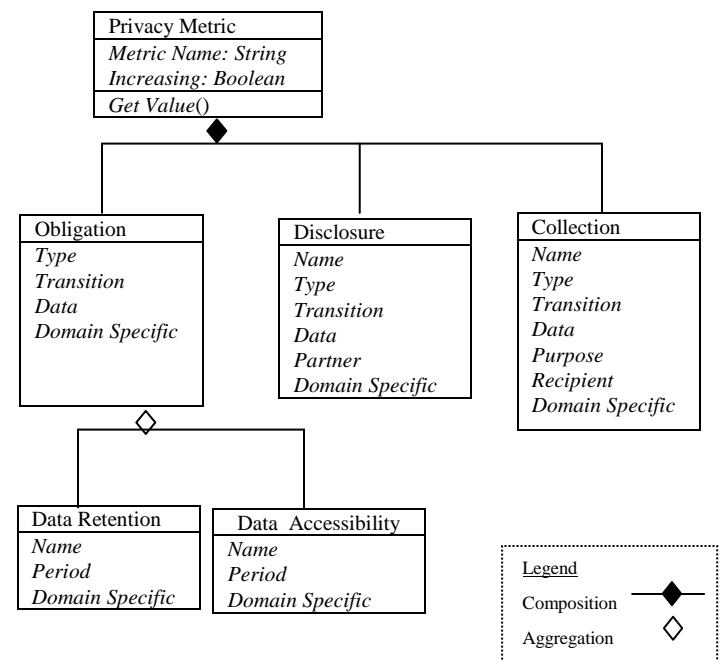


Fig. 1. An expanded model of web services

Based on Fig. 1, each web service is composed of a series of privacy metrics and each privacy metrics must have its own weight. The increasing value can be zero or one. If increasing the privacy is a preferred by the user, the value will be set to one; otherwise the value will be set to zero.

### C. The Model of Privacy-Aware Requirements

The user's requirements for applying the privacy criteria may be different. Indeed, there are two kinds of requirements in the privacy policy requirements. One of them is the necessities and constraints on the privacy policies and the other is the priority of the privacy criteria. The constraints are those privacy policies which must be applied to the users [4]. Prioritizing

privacy policies criteria are ranked based on the user’s interests. In this method the users are able to determine some weights based on their preferences for ranking the criteria.

The model of privacy requirements for a service can be encoded by the XML sections and can be included in the description of the user’s request to the web service [3].

Fig. 2 presents how to evaluate the users' privacy preferences metrics in retention of their personal information in the specific period of time. In addition, by weighting the privacy metrics based on the users' considerations, these metrics will be prioritized.

```

<Privacy Requirement>
  <State Name="Book Selection">
    <Obligation Type "R",
      data ="/user [@cart-data]",      transition,"t3">
      <Retention Name="R2",
        Period="6 months"/>
    </Obligation>
    <Privacy Evaluation System>
      <Weight Item ItemName="time" weight="6"/>
      <Weight Item ItemName="content" weight="4">
    </Privacy Evaluation System>
  </State>
</Privacy Requirement>
    
```

Fig. 2. A sample privacy metrics description [12]

### III. THE PROCESS OF WEB SERVICE USING PRIVACY-AWARE POLICY

There is a simple procedure for applying privacy policies in the proposed process of UDDI to find a desired web service. While the accommodation of the privacy policies with the user preferences is considered as an important factor, the process of applying the privacy-aware policy should change. Fig. 3 shows the proposed process of web service using the privacy-aware policies [23].

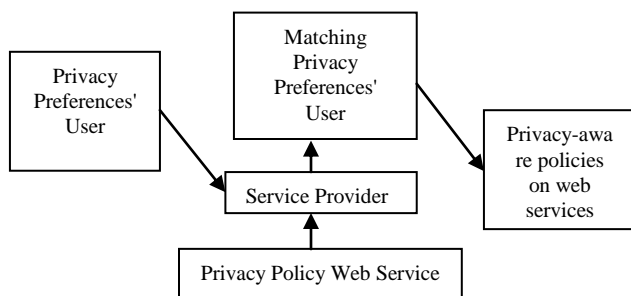


Fig. 3. Web service process using privacy-aware policies

Service providers record the web service information in the UDDI. While the request is being sent to the service, it will be sent to the service provider. The process of applying the privacy-aware policy for the web services are accomplished in some stages. First, the user sends his/her interests on the personal information. Then, a correspondence will be done between the user’s interests and the web service privacy policies. Finally, the degrees of user’s confidence to the privacy-aware policies on web services will be evaluated. These stages will be explained in the next section. Fig. 4 shows this process.

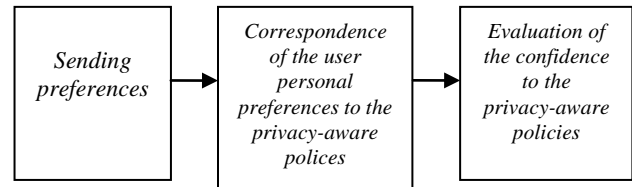


Fig. 4. The stages of applying privacy-aware policies

### IV. EVALUATION OF WEB SERVICE PRIVACY-POLICIES CONFIDENCE

After sending the user preferences and doing a correspondence with the web service privacy policies, the degree of user’s confidence to apply these policies will be calculated. The algorithm must determine that a desired web service *S* how much confidence provides based on the privacy policies and the user preferences. Using *m* parameters for the personal preferences, the following matrix *P* will be obtained:

$$P = \begin{bmatrix} P_{1,1} & P_{1,2} & \dots & P_{1,m} \\ P_{2,1} & P_{2,2} & \dots & P_{2,m} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ P_{n,1} & P_{n,2} & \dots & P_{n,m} \end{bmatrix}$$

where, each line of the matrix *P* shows one privacy metrics and each column presents one of the parameters.

In order to evaluate the web service privacy policies confidence, the matrix *P* should be normalized. Through normalization, we can measure parameters equally without dependence on their measurement units and also construct an equal index for showing the web service privacy confidence. For example, the disclosure of user personal information may be expressed in terms of day or for some special persons. For constructing an equal index, *P* should be normalized.

Before normalization, two arrays should be defined. First,  $N = \{n_1, n_2, \dots, n_m\}$ , which is  $1 < j < n$ . Then,  $n_j$  value is the same increasing field value in the privacy-aware model, which could be 0 or 1 and  $n=1$  is considered when increase of  $P_{i,j}$  value for user is an advantage. The second array is  $C = \{c_1, c_2, \dots, c_m\}$ , where  $c_j$  adjusts the most normalized value and  $\mu = \frac{1}{n} \sum_{i=1}^n P_{i,j}$  is the average privacy-aware confidence metrics value *j* in the matrix *P* and constant *c* value is a premise for metrics *j*. Normalizing each element of the matrix *P* is done using the following formulas [7],[8],[11]:

If  $n_j=1$ , then:

$$P_{i,j} = \begin{cases} \frac{P_{i,j}}{\frac{1}{n} \sum_{i=1}^n P_{i,j}} & \text{if } \frac{1}{n} \sum_{i=1}^n P_{i,j} \neq 0 \\ & \text{and } \frac{P_{i,j}}{\frac{1}{n} \sum_{i=1}^n P_{i,j}} < c_j \\ & \text{and } n_j = 1 \\ c_j & \text{if } \frac{1}{n} \sum_{i=1}^n P_{i,j} = 0 \\ & \text{and } n_j = 1 \\ & \text{and } \frac{P_{i,j}}{\frac{1}{n} \sum_{i=1}^n P_{i,j}} \geq c_j \end{cases}$$

If  $n_j=0$ , then:

$$P_{i,j} = \begin{cases} \frac{P_{i,j}}{\frac{1}{n} \sum_{i=1}^n P_{i,j}} & \text{if } P_{i,j} \neq 0 \\ & \text{and } n_j = 0 \\ & \text{and } \frac{P_{i,j}}{\frac{1}{n} \sum_{i=1}^n P_{i,j}} < c_j \\ c_j & \text{if } P_{i,j} = 0 \\ & \text{and } n_j = 0 \\ & \text{and } \frac{P_{i,j}}{\frac{1}{n} \sum_{i=1}^n P_{i,j}} \geq c_j \end{cases}$$

By using the normalization formulas in the matrix  $P$  we will obtain matrix  $P'$ , which consists the normalized values of the metrics:

$$P' = \begin{bmatrix} P'_{1,1} & P'_{1,2} & \dots & P'_{1,m} \\ P'_{2,1} & P'_{2,2} & \dots & P'_{2,m} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ P'_{n,1} & P'_{n,2} & \dots & P'_{n,m} \end{bmatrix}$$

For applying the user's preferences, we define an array named  $F$ , where  $F=\{f_1, f_2, \dots, f_m\}$ , where each  $f_j$  is a weight for privacy confidence metrics which were analyzed in the descriptive model of privacy requirements. Finally, with applying  $f$  array in  $P'$  matrix we can calculate the degree of privacy-aware confidence on web services.

The following equation shows the way of calculating privacy-aware evaluation index, named *privacy aware confidence* (PAC) for the web service:

$$PAC(S) = \sum_{j=1}^m (P'_{i,j} * f_j)$$

where,  $P'_{i,j}$  are the normalized values of each metrics and  $f_j$  is the related metrics weights. Therefore, we achieve the desired web service privacy-aware confidence index. After calculation of PAC value for web services, we rank the web services and present it to the user. Then, the user makes a decision based on the resulted ranks to select a web service.

### V. WEB SERVICE DISCOVERY BY A CERTIFIER BASED ON USERS' PREFERENCES

After requesting a composite web service by a user, it may be use other web services to provide the requested service. In this case, the web service privacy policies must be accommodated with privacy policies of other web services in use.

Four stages are being discussed to find out a web service. In the first stage, service provider registers the related service in UDDI. In the second stage, service user requests the related service from the discovering agent. And at next stage, the discovering agent accommodates the operational requirements of the service requested by the user using the services registered in UDDI. And finally, the accommodated services are recalled by the user from the service provider. Fig. 5 shows the process of web service discovery.

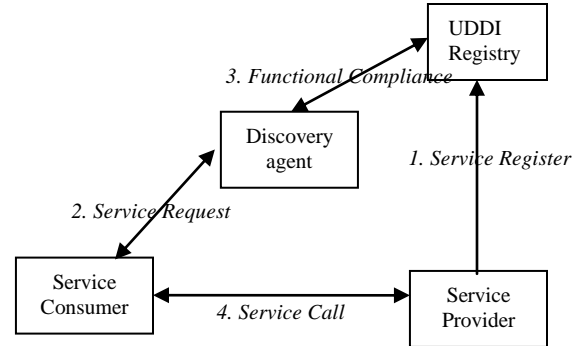


Fig. 5. Web service discovery process [6]

In the proposed method for discovering web services, a *certifier* is used. The certifier considers the non-operational requirements of users. It also accommodates the web services with the user's operational requirements. As appeared in Fig. 6, the certifier examines the distributed non-operational requirements before registering the service. Before service recalling, the user can examine the distributed non-operational information by certifier.

The UDDI standard is the most dominating among the web services discovery mechanisms [14]. A UDDI registry is a directory for storing information about web services. A service provider makes its services available to public users by publishing information about the service in a UDDI registry.

Individuals and businesses can then locate the services by searching public and private registries.

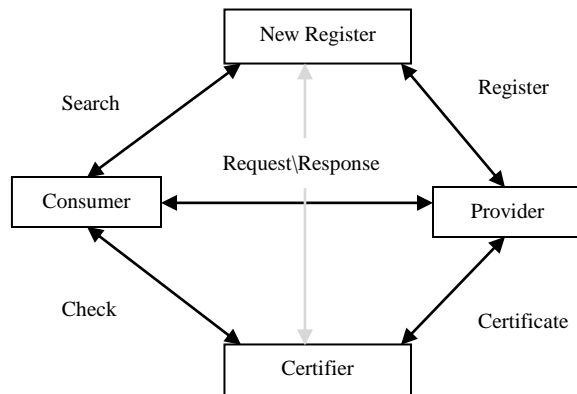


Fig. 6. Web service discovery based on non-operational requirements

The information about web services in a UDDI registry includes a description of the business and organizations that provide the services, a description of a service's business function, and a description of the technical interfaces to access and manage those services [19]. A UDDI registry consists of instances of four core data structures including the *businessEntity*, the *businessService*, the *bindingTemplate* and the *tModel*. This information comprises everything a user required to know to use a particular web service. The *businessService* is a description of a service's business function, *businessEntity* describes the information about the organization that has published the service, *bindingTemplate* describes the service's technical details, including a reference to the service's application programming interface (API), and *tModel* defines other attributes or metadata such as taxonomy and digital signatures [20].

To register non-operational information in this method UDDI data structure is changed according to Fig. 7. As appeared in the figure, a new part to UDDI structure of privacy data has been added. In this section, there is presented professional service data structure accompanying with the model of dependency.

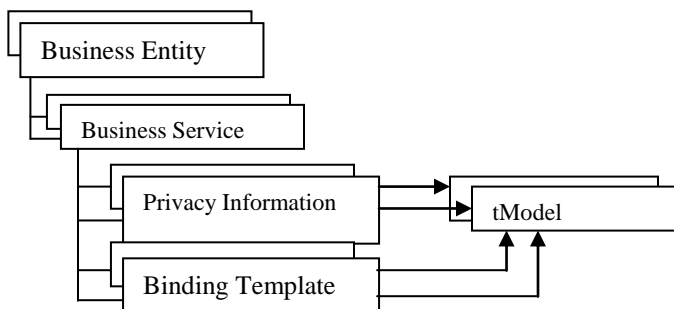


Fig. 7. UDDI structure based on non-operational requirements

#### A. Storage of Privacy of Service Information in the UDDI Registry

As a current feature in the UDDI registry, the *tModel* is used to describe the technical information for services. A *tModel*

consists of a key, a name, an optional description and a uniform resource locator (URL) which points to a place where details about the actual concept represented by the *tModel* can be found [16]. *tModel* plays two roles in the current UDDI registries. The primary role of a *tModel* is to represent a technical specification that is used to describe the web services. The other role of a *tModel* is to register categorizations, which provides an extensible mechanism for adding property information to a UDDI entity. We propose that the categorization *tModel* in UDDI registries can be used to provide *privacy of service* (PoS) on *bindingTemplates* and a *tModel* for privacy of service information for the binding template that represents a web service deployment is generated to represent privacy of service information. Each PoS metric, such as collection, use or disclosure is represented by a *keyedReference* that is a general-purpose structure for a *name-value pair*, on the generated *tModel* [28],[29].

We give an example of the *bindingTemplate* reference to the *tModel* with the PoS attribute categories, and an example of the PoS information *tModel*, which contains a *categoryBag*, which is a list of name-value pairs specifying the PoS metrics. The two examples are shown in Fig. 8 and Fig. 9, respectively. The example used in Fig. 8 is a *stock quote* service. A *tModel* with *tModelKey* "uddi:mycompany.com:

*StockQuoteService:PrimaryBinding:PoSInformation*" containing the PoS attribute categories is referenced in the *bindingTemplate*. In order to retrieve more detailed management information, the location of a WSDL description is stored in a keyed reference with *tModelKey* "uddi:mycompany.com:StockQuoteService:

*PrimaryBinding:PoSDetail*", which is not shown in the Fig. 9 shows the *tModel* that is referenced in the *bindingTemplate* in Fig. 8. This *tModel* contains a *categoryBag* that specifies four PoS metrics of collection, use, disclosure, and data quality. The *tModelKey* in each *keyedReference* is used as a namespace which provides a uniform naming scheme [21].

#### B. Scenario of web Service Discovery

According to PoS value that is added to the privacy information core of UDDI structure, now we present the scenario for discovering web service based on privacy policies. Suppose *A*, *B*, *C* and *D* indicate web service provider, web service user, agent for discovering web service, and SOAP protocol, respectively.

To discover a web service, the following steps are applied and web services are ranked based on their privacy indices:

1. *A*→*C*: *A* requests the privacy policies from a discovering agent (*C*).
2. *A*: the web service provider examines the accommodation between its privacy preferences and the privacy policies of the discovering agent.
3. *A*→*C*: if accommodated, the web service provider distributes service in WSDL and determines the privacy policies as well.
4. *A*→*UDDI*: *A* finds a suitable web service using UDDI.
5. *B*: web service user examines accommodation between privacy policies of provider and the discovering agent and compares them with its privacy policies. If accommodated, the user can use the web service.

```

<businessService>
serviceKey="uddi:mycompany.com:StockQuoteService"
businessKey="uddi:mycompany.com:business">
<name>Stock Quote Service</name>
<bindingTemplates>
<bindingTemplate
bindingKey="uddi:mycompany.com:StockQuoteService:primaryBinding"
serviceKey="uddi:mycompany.com:StockQuoteService">
<accessPoint URLType="http">
http://location/sample
</accessPoint>
<tModelInstanceDetails>
<tModelInstanceInfo
tModelKey="uddi:mycompany.com:StockQuoteService:Primary
Binding:PoSInformation">
<description xml:lang="en">
This is the reference to the tModel that will have all of the
POS related categories attached.
</description>
</tModelInstanceInfo>
<tModelInstanceInfo
tModelKey="uddi:mycompany.com:StockQuoteService:Primary
Binding:PoSDetail">
<description xml:lang="en">
This points to the tModel that has the reference to the
web service endpoint that allows detailed retrieval of
information
</description>
</tModelInstanceInfo>
</tModelInstanceDetails>
</bindingTemplate>
</bindingTemplates>
</businessService>
    
```

Fig. 8. POS Information on BindingTemplates

```

<name>PoS Information for Stock Quote Service</name>
<overviewDoc>
<overviewURL>
http://<URL describing schema of PoS attributes>
<overviewURL>
<overviewDoc>
<categoryBag>
<keyedReference
tModelKey="uddi:uddi.org:PoS: Collection"
keyName=" collect information "
keyValue="necessary" />
<keyedReference
tModelKey="uddi:uddi.org:PoS: Disclosure"
keyName=" disclose personal information "
keyValue=">Purpose" />
<keyedReference
tModelKey="uddi:uddi.org:PoS:Data Quality"
keyName="Data Correction"
keyValue=" accuracy" />
</categoryBag>
</tModel>
<tModel tModelKey="mycompany.com:StockQuoteService: Primary
Binding : PoSInformation">
    
```

Fig. 9. The tModel with the PoS Information

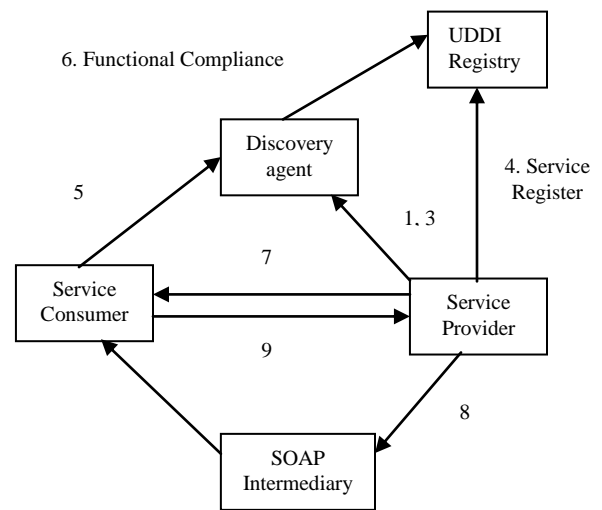


Fig. 10. Steps for discovering web services based on privacy policies

6.  $C \rightarrow UDDI$ : the discovering agent examines the operational accommodation of the related service with the web services registered in UDDI.
7.  $B \rightarrow A$ : If accommodated, the web service user can use the web service through SOAP messages.
8.  $A$ : the web service provider locates the privacy policies in SOAP messages.
9.  $A \rightarrow B$ : the web service provider requests the web service user to declare its satisfaction.

Fig. 10 displays the steps for discovering web services based on privacy policies.

## VI. COMPARISON

In the architecture for describing the way of applying privacy policies proposed in [12], the users are not able to apply their requirements in the way of managing personal information. In this architecture, just a couple of simple performances on the user's registration information, user's profiles, IP address and cookies are accomplished. Same thing is correct for applying the user preferences. However, in the proposed model, the users are able to apply their privacy preferences on the web service privacy metrics.

In [22], a privacy policy checker engine is designed and implemented for automatically verifying and certifying the web service application based on the levels of overall privacy principle compliance, privacy statement compliance and classification of privacy metrics. We use this classification of privacy metrics to evaluate the web service privacy policy confidence by using a normalization algorithm.

In some references, such as [9], a UDDI registry consists of instances of four core data structures including the *businessEntity*, the *businessService*, the *bindingTemplate* and the *tModel*. In the proposed discovery method, a structure is used to augment the UDDI registries with additional privacy information. We have added a new data structure to the UDDI architecture that performs the privacy matching between web service metrics and user preferences.

The users interact with the web service applications via information exchanges. The information exchanges between the users and the web service applications always contain different confidential and sensitive data. Referring to the *publish/find/bind* model in web services [10], one can imagine that web service providers publish their web services descriptions at registries (e.g., UDDI) for public access. The web services are described in WSDL documents. Then, the users (web service requestors) find the appropriate web services at the registries. In many cases, there may have a mediator (i.e., a service locator) that helps to find appropriate web services for requestors [24]. From the users' point of view, applying their privacy preferences in web services discovery is an important issue so in the proposed algorithm, we consider the privacy metrics as well.

## VII. CONCLUSIONS

By increasing the number of web service users, making privacy policies is being more and more important. On the other hand, it simplifies the possibility of applying user preferences on the personal information. Bearing this in mind in the existing process, the possibility of applying user preferences in privacy policies has not been considered, so it is necessary to have a systematic method for describing and applying privacy-aware policies on web services.

In this paper we presented an extensible model for describing and applying privacy-aware policies of a web service with using privacy metrics and shows how can include the user interests in the calculation of web service privacy confidence. The proposed model benefits both flexibility and extensibility. It is possible to add new privacy metrics without any change in the calculation model. This paper also demonstrates a model of web service privacy-aware requirements for expressing the user preferences and proposes an improved process on the web service to enable users to apply their preferences and presents a scenario for discovering web services based users' preferences through adding privacy of service (PoS) information to the privacy information core of the UDDI structure as well.

In future, we can consider presenting a scenario for discovering composite web services based on privacy policies regarding to ontology concepts. In addition, using users' feedback for changing the privacy metrics of web services is an effective solution for improving the flexibility.

## REFERENCES

- [1] A. Tumer, Dogac and H. Toroslu, "A Semantic Based Privacy Framework for Web Services," *Intelligent Techniques for Web Personalization*, Lecture Notes in Computer Science, vol. 3169, Springer, 2005, pp. 289-305.
- [2] M. Walid Bagga, "Privacy-Enabled Application Scenarios for Web Services," Technical Report, Corporate Communications Department, EUROCOM Institute, Sydney, Australia, Sept. 2003.
- [3] L. Kagal and T. Finin, "Authorization and Privacy for Semantic Web Service," *IEEE International Conference on Web Services*, Maryland, USA, 2004, pp. 3-7.
- [4] L. Zeng and B. Benatallah, "Quality Driven Web Services Composition," *Proc. of the 12<sup>th</sup> International Conference on WWW*, Budapest, Hungary, ACM Press, May 2003, pp. 6-10.
- [5] N. Henze and D. Krause, "User Profiling and Privacy Protection for a Web Service oriented Semantic Web", *Proc. of LWA*, 2006, pp. 42-46.
- [6] P. Rajasekaran, J. Miller, K. Verma and A. Sheth, "Enhancing Web Services Description and Discovery to Facilitate Composition," *Lecture Notes in Computer Science*, vol. 3387, Springer, 2005, 55-68.
- [7] J. Karvanen, "The Statistical Basis of Laboratory Data Normalization," *Drug Information Journal*, vol. 37. No. 1, 2003, pp. 101-107.
- [8] Y. T. Yan, "Normalization of the Parameterized Courant-Snyder Matrix for Symplectic Factorization of a Parameterized Taylor Map," the 1991 *IEEE Particle Accelerator Conference*, San Francisco, CA, USA, 1990, pp. 1663-1665.
- [9] S. Luc Clement, I. Andrew Hatley, S. A. Claus von Riegen, and C. A. Tony Rogers, "UDDI version 3. 0. 2," Oct. 2004, UDDI Spec Technical Committee Draft. URL: [http://www.uddi.org/pubs/uddi\\_v3.htm](http://www.uddi.org/pubs/uddi_v3.htm), visited: April 30, 2009.
- [10] C. Mohen, "Tutorial: Application Servers and Associated Technologies," *ACM SIGMOD International Conference on Management of Data (SIGMOD'02)*, Madison, USA, June 2002, pp. 2-7.
- [11] H. Aghdasinia, "Quality Model for Finding Dynamic Web Services," M.Sc. Thesis, Iran University of Science and Technology, Tehran, Iran, 2008 (*in Persian*)
- [12] R. Hamadi, "Conceptual Modeling of Privacy-Aware Web Service Protocol," *Lecture Notes in Computer Science*, vol. 4495, Springer, 2007, pp. 233-248.
- [13] M. Alsaleh and C. Adams, "Enhancing Consumer Privacy in the Liberty Alliance Identify Federation and Web Services Framework," *Lecture Notes in Computer Science*, vol. 4258, 2006, pp. 59-77.
- [14] S. Ran, "A Model for Web Services Discovery with QoS," *SIGECOM Exchanges*, vol. 4, no. 1, ACM, 2004, pp. 1-10.
- [15] P. C. K. Hung, E. Ferrari and B. Carminati, "Towards Standardized Web Services Privacy Technologies," *Proc. of the 2004 IEEE International Conference on Web Services*, Oshawa, Ontario, Canada, 2004, pp. 174-181.
- [16] "UDDI Version 2. 03 Data Structure Reference," URL: <http://www.uddi.org/pubs/DataStructure-V2.03-Published-20020719.htm>, visited: April 30, 2006.
- [17] D. Zuquim, G. Garcia, M. Beatriz and F. de Toledo, "A Web Service Privacy Framework Based on a Policy Approach Enhanced with Ontologies," *Proc. of the 11<sup>th</sup> IEEE International Conference on Computational Science and Engineering - Workshops*, 2008, pp. 209-214.
- [18] Y. Yang and J. Yang, "Towards Unconditional Anonymity: Privacy Enforcement Model in Web Services," *Proc. of the IEEE Congress on Services*, Beijing, 2008, pp. 26-33.
- [19] D. D. Lamanna, J. Skene, and W. Emmerich, "SLAng: A language for defining Service Level Agreements," *Proc. of the Ninth IEEE Workshop on Future Trends of Distributed Computing Systems (FTDCS'03)*, San Juan, Puerto Rico, May 2003.
- [20] G. Yee, "Measuring Privacy Protection in Web Services," *Proc. of the IEEE International Conference on Web Services*, (ICWS'06), pp. 647-654.
- [21] A. Blum, "UDDI as an Extended Web Services Registry," URL: <http://soa.sys-con.com/node/45102>, visited: April 30, 2009.
- [22] S. Benbernou, H. Meziane and Y. Hua Li, "A Privacy Agreement for Web Services," *Proc. of the IEEE International Conference on Services Computing*, Salt Lake City, UT, 2007, pp. 196-203.
- [23] W. D. Yu, Sh. Doddapaneni and S. Murty, "A Privacy Assessment Approach for Serviced Oriented Architecture Applications," *Proc. of the Second IEEE International Workshop Service-Oriented System Engineering (SOSE'06)*, 2006, pp. 67-75.
- [24] Z. Zhang and C. Zhang., "An Improvement to Matchmaking Algorithms for Middle Agents," *Proc. of the First International Joint Conference on*

Autonomous Agents and Multiagent Systems, Bologna, Italy, ACM Press, New York, N. Y. , 2002, pp. 1340-1347.

- [25] L. Aversano, G. De Canfora, A. Lucia and P. Gallucci, "Integrating Document and Workflow Management Tools using XML and Web Technologies: A Case Study," Proc. of Sixth European Conference on Software Maintenance and Reengineering, 2002, pp. 24-33.
- [26] "SOAP Version 1.2 Part 1: Messaging Framework," World Wide Web Consortium (W3C), Proposed Recommendation, 07 May 2003. URL: [www.w3c.org/TR/2003/PR-soap12-part1-20030507/](http://www.w3c.org/TR/2003/PR-soap12-part1-20030507/), visited: April 30, 2009.
- [27] C. S. Powers, P. Ashley and M. Schunter, "Privacy promises, access control, and privacy management - Enforcing privacy throughout an enterprise by extending access control," Proc. of the Third International Symposium on Electronic Commerce, 2002, pp. 13-21.
- [28] V. Senicar, B. Jerman-Blazic and T. Klobucar, "Privacy-Enhancing Technologies -Approaches and Development," Computer Standards and Interfaces, vol. 25, 2003, pp. 147-158.
- [29] G. Yee and L. Korba, "Privacy Policy Compliance for Web Services," Proc. of the IEEE International Conference on Web Services (ICWS'04), San Diego, California, USA, 2004, pp. 128-133.

**Mona Tavakolan** received the B.Sc. degree in Computer engineering (software) from Mazandaran University of Science and Technology (2005) and M.Sc. degree in information technology from Iran University of Science and Technology (March. 2009). Title of her M.Sc. thesis is "Designing a Web Service with Capabilities to Apply User Preferences Based on Privacy," which has been done under supervision of Dr. Mohammad Abdollahi Azgomi. Miss Tavakolan's research interests include web service discovery and web service . She has published several papers in international conferences.

**Maryam Zarreh** received the B.Sc. degree in computer engineering (software) from Tehran Science and Culture University (2005) and M.Sc. degree in Information Technology engineering from Iran University of Science and Technology (Feb. 2009). Title of her M.Sc. thesis is "An Architecture for Privacy-Aware Access Control," which has been done under supervision of Dr. Mohammad Abdollahi Azgomi. Miss Zarreh's research interests include web security, privacy-aware access control and web service. She has published several papers in international conferences.

**Mohammad Abdollahi Azgomi** received the B.Sc., M.Sc. and Ph.D. degrees in computer engineering (software) (1991, 1996 and 2005, respectively) from Sharif University of Technology, Tehran, Iran. His research interests include performance and dependability modelling with high-level modelling formalisms such as stochastic Petri nets, tools for modelling and evaluation, verification and validation, object-oriented modelling, web services, network and web security. He has published several papers in international journals and conferences. Dr. Abdollahi Azgomi is currently an assistant professor at the department of computer engineering, Iran University of Science and Technology, Tehran, Iran.