International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763
Issue 12, Volume 3 (December 2016) www.ijirae.com

# Secure Web Service Composition

**Dr.K.B.S.Sastry[1], S.AB.Nehru[2], K.B.S.M.D.S.Sai Prasanth[3]**

*1.Lecturer, Dept. of Computer Science, Andhra Loyola College, Vijayawada*
*2.Head, Dept. of Computer Science, Andhra Loyola College, Vijayawada*
*3.IIIrd year B.Tech(ECE)Student, Andhra Loyola Institute of Engineering and Technology, Vijayawada.*

***Abstract-- Privacy is the word listening frequently from many places. In every application privacy is the most widely used technique to secure the data in the application. Data as a Service (DaaS) is the latest service oriented technology which is used to enable fast access in the web. In this Daas there are many privacy issues are arises. In this paper, a new enhanced privacy model is implemented in the Daas. This model verifies the compatibility of privacy requirements and policies in Daas. To improve the privacy we adopted and enhanced negotiation mechanism. The performance is showed in the implementation and execution of the proposed work.***

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

## I. 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 to-wards 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 (Dataas-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].

## II. EXISTING SYSTEM

A typical example of modelling 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 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. 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.*


 

## III. 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:

**Privacy-aware Service Composition**: We propose a compatibility matching algorithm to check privacy compatibility between component services within a composition.

**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)

## IV. MODULES

- *e-Epidemiological Scenario*
- *Privacy Level*
- *Privacy Rule*
- *Privacy-aware Service Composition*
- *Negotiating Privacy in Service Composition*

### 4.1 MODULE DESCRIPTION:

#### E-EPIDEMIOLOGICAL SCENARIO

The first module is E-epidemiology scenario module. We develop the scenario of E-epidemiology. E-epidemiology is the science underlying the acquisition, maintenance and application of epidemiological knowledge and information using digital media such as the internet, mobile phones, digital paper, digital TV. E-epidemiology also refers to the large-scale epidemiological studies that are increasingly conducted through distributed global collaborations enabled by the Internet.The traditional approach in performing epidemiological trials by using paper questionnaires is both costly and time consuming. The questionnaires have to be transformed to analyzable data and a large number of personnel are needed throughout the procedure. Modern communication tools, such as the web, cell phones and other current and future communication devices, allow rapidly and cost-efficient assembly of data on determinants for lifestyle and health for broad segments of the population. 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).

#### PRIVACY LEVEL

In this module 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. 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 being stolen by a competing company. We give below the definition of the privacy level.

#### 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.

#### 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.In this module we also propose an algorithm called PCM (Privacy Compatibility Matching). The first option is to require full matching and the second is partial matching.


 

### 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.

## V. CONCLUSION

In this paper, we proposed a new Enhanced privacy model for Web services. The model deals with privacy at the data and operation stages. We also proposed a Advanced 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.

## VI. REFERENCES

[1]. M. Alrifai, D. Skoutas, and T. Risse.Selecting skyline services for qos-based web service composition. In Proceedings of the 19thinternational conference on World wide web, WWW '10, pages 11–20,New York, NY, USA, 2010. ACM.
[2]. M. Barhamgi, D. Benslimane, and B. Medjahed. A Query Rewrit-ing Approach for Web Service Composition. IEEE Transactions onServices Computing (TSC), 3(3):206–222, 2010.
[3]. G. T. Duncan, T. B. Jabine, and V. A. de Wolf, editors. Privatelives and public policies: confidentiality and accessibility of government statistics. National Academy Press, Washington, DC, USA, 1993.
[4]. B. C. M. Fung, T. Trojer, P. C. K. Hung, L. Xiong, K. Al-Hussaeni, and R. Dssouli. Service-oriented architecture for high-dimensional private data mashup.IEEE Transactions on Services Computing, 99(PrePrints), 2011.
[5]. Y. Gil, W. Cheung, V. Ratnakar, and K. kin Chan. Privacy enforcement in data analysis workflows. In T. Finin, L. Ka-gal, and D. Olmedilla, editors, Proceedings of the Workshop onPrivacy Enforcement and Accountability with Semantics (PEAS2007) at ISWC/ASWC2007, Busan, South Korea, volume 320 of CEUR Workshop Proceedings. CEUR-WS.org, November 2007.
[6]. Y. Gil and C. Fritz. Reasoning about the appropriate use of private data through computational workflows. In Intelligent InformationPrivacy Management, Papers from the AAAI Spring Symposium,pages 69–74, March 2010.
[7]. B. Hore, S. Mehrotra, and G. Tsudik.A privacypreserving index for range queries.In Proceedings of the Thirtieth internationalconference on Very large data bases - Volume 30, VLDB '04, pages720–731.VLDB Endowment, 2004.
[8]. M. Kahmer,¨ M. Gilliot, and G. Muller¨. Automating privacy compliance with expdt. In Proceedings of the 2008 10th IEEEConference on E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services, pages 87– 94,Washington, DC, USA, 2008. IEEE Computer Society.
[9]. H. Kargupta, K. Das, and K. Liu. Multi-party, privacypreserving distributed data mining using a game theoretic framework. In Proceedings of the 11th European conference on Principles and Practice of Knowledge Discovery in Databases, PKDD 2007, pages 523–531,Berlin, Heidelberg, 2007. Springer-Verlag.
[10]. J. Kawamoto and M. Yoshikawa. Security of social information from query analysis in daas. In Proceedings of the 2009 EDBT/ICDTWorkshops, EDBT/ICDT '09, pages 148–152, New York, NY, USA,2009. ACM.
[11]. O. Kwon. A pervasive p3p-based negotiation mechanism for privacy-aware pervasive e-commerce.Decis. Support Syst., 50:213– 221, December 2010.
[12]. Y. Lee, D. Sarangi, O. Kwon, and M.-Y. Kim. Lattice based privacy negotiation rule generation for contextaware service. In Pro-ceedings of the 6th International Conference on Ubiquitous Intelligence and Computing, UIC '09, pages 340–352, Berlin, Heidelberg, 2009.Springer-Verlag.
[13]. Y. Lee, J. Werner, and J. Sztipanovits. Integration and verification of privacy policies using DSML's structural semantics in a SOA-based workflow environment.Journal of Korean Society for InternetInformation, 10(149), 09/2009 2009.
[14]. M. Maaser, S. Ortmann, and P. Langendorfer¨. The privacy advo-cate: Assertion of privacy by personalised contracts. In J. Filipe and J. A. M. Cordeiro, editors, WEBIST (Selected Papers), volume 8 of Lecture Notes in Business Information Processing, pages 85–97. Springer, 2007.
[15]. A. Machanavajjhala, J. Gehrke, and M. Gotz¨. Data publishing against realistic adversaries. PVLDB, 2(1):790–801, 2009.
[16]. A. Machanavajjhala, D. Kifer, J. M. Abowd, J. Gehrke, and L. Vil-huber. Privacy: Theory meets practice on the map. In ICDE, pages 277–286. IEEE, 2008.
[17]. A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubra-maniam. L-diversity: Privacy beyond kanonymity. ACM Trans.Knowl.Discov. Data, 1(1):3, 2007.
[18]. B. Medjahed, B. Benatallah, A. Bouguettaya, A. H. H. Ngu, and A. K. Elmagarmid. Business-to-business interactions: issues and enabling technologies. The VLDB Journal, 12:59–85, May 2003.


 