Privacy-Enhanced Web Service Composition

Ajjumpudi Venkata Vamsi Krishna , Dr.I.R.Krishnam Raju , Sri.V.Bhaskara Murthy
MCA Student, Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

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 descriptions 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.

I.INTRODUCTION

Web services have recently emerged as a popular medium for data publishing and sharing on the Web. 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 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. 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

II. **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.

Problems on 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.

ADVANTAGE

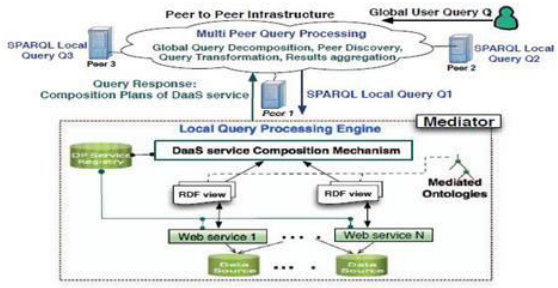
1. Negotiating Privacy in Service Composition :

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).

2. Privacy-aware Service Composition:

We propose a compatibility matching algorithm to check privacy compatibility between component services within a composition.

IV.SYSYEM ARCHITECTURE



V. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Main Modules:-

1. User Module

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

2. 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.

3. Privacy Compatibility Evaluation:

In the PAIRSE prototype, we developed more than 100 real Web services. The developed services include services providing medical information about patients, their hospital visits, diagnosed diseases, lab tests, prescribed medications, etc. In the following, we evaluate the efficiency and scalability of our compatibility algorithm. For each service deployed in our architecture, we randomly generated PR and PP files regarding its manipulated resources (i.e., inputs and outputs). Assertions in PR and PP were generated randomly and stored in XML files. All services were deployed over an Apache Tomcat 6 server on the Internet. We implemented our PCM algorithm in Java and run the composition system with and without checking compatibility. To evaluate the impact of PCM on the composition processing, we performed two sets of experiments.

4. Privacy And Negotiation:

The proposal of is based on privacy policy lattice which is created for mining privacy preference-service item correlations. Using this lattice, privacy policies can be visualized and privacy negotiation rules can then be generated. The Privacy Advocate approach consists of three main units: the privacy policy evaluation, the signature and the entities preferences unit. The negotiation focuses on data recipients and purpose only. An extension of P3P is proposed in . It aims at adjusting a pervasive P3P-based negotiation mechanism for a privacy control. It implements a multi-agent negotiation mechanism on top of a pervasive P3P system. The approach proposed in aims at accomplishing privacyaware access control by adding negotiation protocol and encrypting data under the classified level.

VI.CONCLUSION

In this project, 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 purposes. 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

[1] M. Alrifai, D. Skoutas, and T. Risse. Selecting skyline services for qos-based web service composition. In Proceedings of the 19th international 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 Rewriting Approach for Web Service Composition. IEEE Transactions on Services Computing (TSC), 3(3):206–222, 2010.

[3] G. T. Duncan, T. B. Jabine, and V. A. de Wolf, editors. Private lives 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. Kagal, and D. Olmedilla, editors, Proceedings of the Workshop on Privacy 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 Information Privacy Management, Papers from the AAAI Spring Symposium, pages 69–74, March 2010.

[7] B. Hore, S. Mehrotra, and G. Tsudik. A privacy-preserving index for range queries. In Proceedings of the Thirtieth international conference on Very large data bases - Volume 30, VLDB '04, pages 720–731. VLDB Endowment, 2004.

[8] M. K¨ahmer, M. Gilliot, and G. M¨ uller. Automating privacy compliance with expdt. In Proceedings of the 2008 10th IEEE Conference 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, privacy-preserving 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/ICDT Workshops, 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 context-aware service. In Proceedings 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 SOAbased workflow environment. Journal of Korean Society for Internet Information, 10(149), 09/2009 2009.

[14] M. Maaser, S. Ortmann, and P. Langend¨orfer. The privacy advocate: 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. G¨
otz. Data publishing against realistic adversaries.
PVLDB, 2(1):790–801, 2009.