Privacy-Enhanced Web Service Composition for IJETTCS

C. GangaBhanu,
Department of Computer science of Engineering
SREC College, Karakambadi Road, Tirupathi.

N. JayKrishna
(Assistant Professor),
Department of Computer science of Engineering
SREC College, Karakambadi Road, Tirupathi

M. Harish,
Department of MCA
,SITAMS College, chittoor.

***Abstract*—The (DaaS) Data as a Service, builds on service-oriented technologies to permit fast access to data resources on the Web. However, this pattern raises several new privacy concerns where traditional privacy prototypes do not handle. Additionally DaaS composition may disclose privacy-sensitive information. In this paper, we state a formal privacy model to extend DaaS descriptions with privacy capabilities. The privacy model provide a service to define a privacy policy and a set of privacy requisites. We also suggest a privacy-preserving DaaS composition that sound out allowing to verify the compatibility between privacy requisites and policies in DaaS composition. We proffer a negotiation mechanism that makes it possible to dynamically reconcile the privacy capabilities of services when incompatibilities emerge in a composition. We substantiate the applicability of our proposal via a prototype implementation and a set of experiments.**

Key Terms—Service Composition, DaaS Services, Privacy, Negotiation

I. INTRODUCTION

The Data as a Service (DaaS) builds on service-oriented technologies to facilitate fast access to data resources on the Web. Conversely, this prototype raises several new privacy concerns that traditional privacy models do not handle. On top, DaaS composition may reveal privacy-sensitive information. In this paper, we intend a formal privacy model in order to expand DaaS descriptions with privacy capabilities. The privacy model allows a service to illustrate a privacy policy and a set of privacy requirements. We also recommend 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 merge the privacy capabilities of services when incompatibilities arise in a composition. We authenticate the applicability of our proposal through a prototype implementation and a set of experiments.

When you present the paper print it in two-column format, including figures and tables. Additionally, choose one author as the "corresponding author". This is the author to whom proof of the paper will be sent.

1.1 PURPOSE OF THE PROJECT

- In the present system web based collaborations and processes are distinctive.
- The present system didn't solve the potential problems distributed collaboration environments.
- Flexibility in composition models is inadequate since unpredicted changes require remodeling of the process. Such changes may cause exceptions troublesome the normal execution of the process.

1.2 PROBLEM IN EXISTING SYSTEM

Web services have recently emerged as a popular medium for data publishing and distributing on the Web. Modern enterprises across all spectra are moving towards a service-oriented architecture by putting their databases behind Web services, in this manner providing a well-documented, platform independent and interoperable method of interacting with their facts. This new type of services is known as DaaS (Data-as-a-Service) services where services' communicate 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 protect application developers having an directly interact with the various data sources that give access to business objects, thus enable them to focus on the business logic only. While individual services may provide interesting information/functionality alone, in most cases, users' query require the combination of several Web services through service composition. In spite of the large body of research dedicated to service composition over the last years), 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 discharge private information.

II. Problem Statement

Two factors aggravate the problem of confidentiality in DaaS. The First, DaaS services collect and store a huge amount of private information about users. Second, DaaS services are proficient to share this information with other entities. Further, the emergence of analysis tools makes it easier to analyze and amalgamate huge volumes of information, hence increasing the threat of privacy destruction. The following, we use our epidemiological scenario to demonstrate the privacy challenges through service composition.

Problem 1: Privacy pattern.

Let us consider services S4.1 and S5.1 in. The scientist considers both input and output parameter of S4.1 (i.e., SSN and DNA) as sensitive data. Let us presume that scientist states the following hypothesis:"weather conditions" has an impact on H1N1 infection." For that rationale, he/she invoke S5.1. The scientist may keep S5.1 invocation as private since this may reveal sensitive information to competitors. The aforesaid first challenge put in substantiation the need for a formal model to specify private data is and how it will be distinct.

Problem 2: Privacy within composition

Component services (that participate in a composition) may necessitate input data that cannot be disclosed by other services because of privacy concerns. They may also have conflicting privacy apprehension regarding their exchanged data. For instance, let us imagine that S1.1 states to reveal its data (SSN) to a third-party service for use in inadequate time. S3.1 meanwhile attest that it uses collected data (SSN) for an indefinite time use. Then, S1.1 and S3.1 have dissimilar privacy constraints regarding the SSN. This will nullify the composition in terms of privacy concerns.

2. *Key Idea*

Inputs:

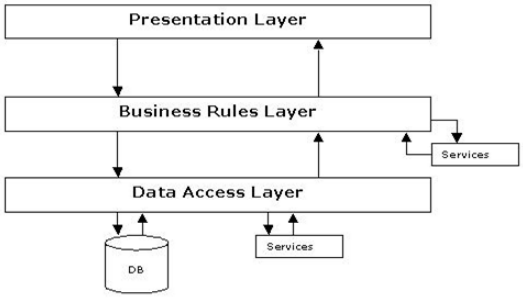
- Administrator enters his or her user id and password.
- Administrator enters weather information.
- User enters his or her user id and password.
- General User enters his or her user id and password.
- User requests the report.
- Users request the search.
- Admin can revise the personal details and so on.

Outputs:

- Administrator receives personal details.
- Administrator views weather report.
- User receive weather alerts information.
- Display search result.

III. PROPOSED SYSTEM

Let us consider the services in Table 1 and the following epidemiologist's query Q "What are the age, gender, address, DNA, salaries of patients contaminated with H1N1; and what are the global weather condition of the area where patients reside?" We predicate in a mediator-based approach to compose DaaS. The mediator selects, combine and assemble the DaaS services (i.e., gets input from one service and uses it to call another one) to answer traditional queries. It also carry out all the exchanges 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 answer by composing the following services S1.1 • S4.1 • S2.2 • S3.1 • S5.1. It means that S1.1 firstly is invoked with H1N1, then for each obtained patient, S4.1 is invoked to obtain their DNA, S2.2 and S3.1 to obtain date-of-birth, zip-code and wages of patient. Finally, S5.1 is invoked with the patients 'zip−code to get information about the weather−conditions. Two factors intensify the problem of privacy in DaaS. First, DaaS services collect and store a huge amount of private information about users. Second, DaaS services are able to exchange this information with other entities. Further, the appearance of analysis tools makes it easier to analyze and combine huge volumes of information, hence escalating the risk of privacy violation. In the following, we use our epidemiological scenario to reveal the privacy challenges during service composition.



The Presentation Layer:

In other words, it is known as the client layer comprise of components that are dedicated to presenting the data to the user. For example: Windows/Web Forms and buttons, edit boxes, Text boxes, labels, List boxes, grids, etc.

The Business Rules Layer:

The Business rules or the business logic are encapsulated in this layer. To have a separate layer for business logic is of a grand advantage. This is because any certainty/uncertainty changes in Business Rules can be easily handled in this layer. On condition that, the interface between the layers leftovers the same, any changes to the functionality/processing logic in this layer can be made without disturbing the other layers. A lot of client-server applications failed to implement successfully as altering the business logic was a painful process.

The Data Access Layer:

Components that help in accessing the Database are in this layer. If used in the accurate way, this layer provides a level of abstraction for the database structures. Simply update changes made to the database, tables, views, Lists, etc do not distress the rest of the application because of the Data Access layer. The unlike application layers send the data requests to

and receive the response from this layer, by this way effective interaction exists between different layers.

The Database Layer:
This layer consists of the Database Components such as Database Files, Tables, Views, Lists etc. The authentic database could be designed using SQL Server, Oracle, Flat files, Tables etc. In an n-tier application, the whole application can be implemented in such a way that it is independent of the actual Database. For instance, you could change/alter the Database position/location with minimal changes to Data Access Layer. The rest of the Application should stay unaffected.

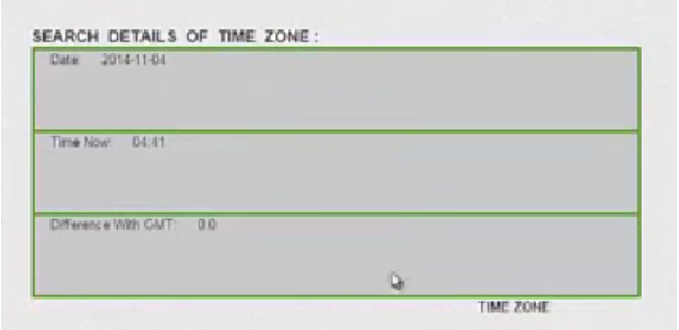
NUMBER OF MODULES:
The system after careful study has been identified to be accessible with the following modules:

Modules:-
- Confidential stage.
- Confidential regulation.

Confidential stage:
We define two confidential stages: data and operation. The data level deals with data privacy/security. Resources/operations refer to input and output parameter 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 hypothetical as private independently on whether their input/output parameters are off the record or not . For instance, let us consider a scientist that has found an innovation about the causes of some infectious diseases; invoke a service operation to search if such an invention is new before he/she files for an infectent. When conducting the query, the scientist may want to keep the invocation of this operation private, perhaps to avoid part of his idea being thief by a competing company.

Confidential Regulation:
The sensitivity of a resource may be defined according to several dimensions called privacy rules. We call the set of privacy rules, Rules Set (RS). We define a privacy/confidential rule by a topic, domain, level and scope. The topic gives the confidential fact represented by the rule and may include for instance: the resource recipient, the purpose and the resource preservation 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 composed resource can be revealed. The level/stage represents the privacy level on which the rule is appropriate. The specific area domain of a rule depends on its level. Indeed, each rule has only one single level: "data" or "operation". The domain is a finite set that enumerate the possible values that can be taken by resources according to the rule's topic. For instance, a division of domain for a rule dealing with the right topic is {"no-withholding", "limited-access"}. The scope of a rule defines the granularity of the resource that is focus to privacy constraints. Two rules majorly are created for each topic: one for data and another for operations.

3. *Simulation Results (Graphs, Tables)*



Equations

If you are using *Word*, use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). "Float over text" should not be selected.

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). First use the equation editor to create the equation. Then select the "Equation" markup style. Press the tab key and write the equation number in parentheses.

$$E = \sum_{p=1}^{P} \sum_{k=1}^{K} (\delta_{pk}^{o})^2 \qquad (1)$$

REFERENCES

1. Salah-Eddine Tbahriti, Chirine Ghedira, Brahim Medjahed and Michael Mrissa, "Privacy-Enhanced Web Service Composition." IEEE Transactions on Services Computing, March 2013
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. B. C. M. Fung, T. Trojer, P. C. K. Hung, L. Xiong,K. Al - Hussaen, and R. Dssouli. "Service-oriented architecture for high-dimensional private data mashup." IEEE Transactions on Services Computing,99 (PrePrints), 2011.
4. Zibin Zheng, Lyu, M.R, "Collaborative reliability prediction of service-oriented systems." IEEE International Conference on Software Engineering, 35-44, 2010.
5. L. Cranor, M. Langheinrich, M. Marchiori, and J. Reagle, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification," W3C Recommendation, Apr. 2002. [Online]. Available: http://www.w3.org/TR/P3P/

6. S. Ran, ‘‘A model for Web services discovery with QoS,’’SIGecom Exchanges, vol. 4, no. 1, pp. 1-10, 2003.
7. Oasis. Extensible Access Control Markup Language (XACML). Identity, (v1.1):134, 2006.
8. M. Kahmer, M. Gilliot, and G. Muller. Automating privacy compliance with expdt.In Proceedings of the 2008 10th IEEE C onference 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. N. Mohammed, B.C.M. Fung, K. Wang, and P.C.K. Hung, ‘‘Privacy-Preserving Data Mashup,’’ in Proc. 12th Int’l Conf. EDBT, 2009, pp. 228-239.
10. M. Mrissa, S.-E. Tbahriti, and H.-L. Truong,‘‘Privacy Model and Annotation for DaaS,’’inProc. ECOWS, G.A.P. Antonio Brogi and C. Pautasso, Eds., Dec. 2010, pp. 3-10., Inc.