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.

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.

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.

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.

Main Modules:
1. User Module:

In this module, Users are having authentication and security to access the detail which is presented in the 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 privacy-aware access control by adding negotiation protocol and encrypting data under the classified level.

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.

BIBLIOGRAPHY:

Good Teachers are worth more than thousand books, we have them in Our Department.
References Made From:


