Privacy-Enhanced Web Service Composition

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.

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.

PROBLEM DEFINITION:

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.

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

MICANS INFOTECH, NO: 8, 100 FEET ROAD, PONDICHERRY.
WWW.MICANSINFOTECH.COM; MICANSINFOTECH@GMAIL.COM
+91 90036 28940; +91 94435 11725
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).
SYSTEM ARCHITECTURE:

HARDWARE CONFIGURATION:-

- Processor - Pentium –IV
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA
SOFTWARE CONFIGURATION:-

✔ Operating System : Windows XP
✔ Programming Language : JAVA
✔ Java Version : JDK 1.6 & above.