8. Comparison With Related Work

Various types of trust building frameworks have been described in the literature for composite web services. In this chapter, we compare our framework for privacy-enabled composite web services with other similar frameworks proposed in the literature. For this comparison, we have selected those frameworks/mechanisms that are representative of research in the area of concern in this dissertation – privacy of consumer’s private information in composite web services.

8.1 FRAMEWORK PROPOSED BY Wei Xu et al.

Wei Xu et al. [40] proposed a mechanism to address consumer privacy concerns. It provides techniques for checking the models at a consumer’s site for compliance with the consumer privacy policies. If there is policy violation, the framework generates obligations for the composite web service. The composite web service is requested to provide alternate attributes, if the consumer does not agree to disclose some of his/her personal information attributes. However, in our framework, checking the privacy preferences of the consumer and privacy policy of the composite web service to find the differences between them is done first, and in case of non-compliance, negotiation with both the consumer and the service provider happens to arrive at an agreement. Our framework also provides policy
tracking and registration of WS-transactions. A consumer can track all WS-transactions that happened for his/her personal information by date, time, and target service providers.

8.2 SEMANTIC-BASED PRIVACY FRAMEWORK

Tumer et al. [41] proposed a semantic-based privacy framework for web services that allows user agents to automatically negotiate with web services on the amount of personal information they will disclose. In this framework, key privacy is considered from two aspects: relieving of minimal information about a user and limited user interaction. The framework also lets web services declare their input parameters related to user’s personal information in two ways: mandatory or optional. If a user does not want to give some mandatory input to a web service, the web service declares alternate data elements. The framework uses DAML-S, which defines an upper ontology for describing semantic web services. However, it does not provide flexibility to a consumer to track all WS-transactions that happened for his/her personal information [41]. In addition to providing complete flexibility of negotiation with both consumer and service provider for arriving at an agreement, our framework also provides the flexibility to a consumer to track all WS-transactions that happened for his/her personal information.

8.3 INFORMATION TRANSFER REGISTRY

Liam and Max [43] proposed the concept of an “information transfer registry” as a mechanism to track compliance in business-to-business network. This registry keeps a record of all information transfers enabling a consumer to track his/her personal information. However, the mechanism does not check compatibility between consumer privacy preferences and service provider privacy policy before executing transfer of personal information. Also, it does not provide flexibility of negotiation with consumer and/or service provider for arriving at an agreement.