Abstract

In the recent years, the Web has evolved to a vibrant platform where applications can be automatically invoked by other Web clients. The key contribution in this regard has come from the introduction of Web services. Services are autonomous, platform-independent entities that can be described, published, discovered, and loosely coupled in novel ways. They perform functions that range from answering simple requests to executing sophisticated business processes requiring peer-to-peer relationships among multiple layers of service consumers and providers. Any piece of code and any application component deployed on a system can be reused and transformed into a network-available service. Services reflect a service-oriented approach to programming that is based on the idea of composing applications by discovering and invoking network-available services to accomplish some task. This approach is independent of specific programming languages or operating systems. It lets organizations expose their core competencies programmatically over Internet or various networks.

The potentials of Web services are often challenged by the lack of perfect information about the quality of the services they provide. This is due to the fact that Web services are autonomous (i.e., provided by independent service providers), highly volatile (i.e., low reliability), and apriori unknown (i.e., new or no prior history of performance). So there is always a question to which extent the clients may believe the Web services to provide the required functionality, prior to their accesses. A Web services may make promises about the provided service and its associated quality but fail partially or fully to deliver on these promises causing huge risks on the part of the clients. Thus, the challenge lies in providing a framework for enabling the selection and composition of services based on trust and reputation parameters. Since trust management can be assumed to decrease risk, it can be assumed that trust will

increase security. Using proper trust management for evaluating the trustworthiness of interacting services, particularly those with malicious intensions can be prevented from causing any harm or unwanted incident.

This dissertation reports a study on various issues of trust and reputation modelling for Web services. We proposed a framework for the evaluation of a service provider from the direct experiences of a service user and/or recommendations from the other service users. Central to our framework is a prediction method based on time series principle and Gaussian process regression (GPR). Using the sound principle of clustering and Markov models our techniques can detect the patterns of trusting behaviour of the service provider from the history of interactions. These patterns represent the patterns that may follow the current time. So, prediction methods based on non-parametric GPR using these patterns are proposed. To enhance, the prediction we also proposed an ensemble approach where many competing GPR models will be simultaneously predicting the target value. Using an adaptive controlling technique, the weaker models are suppressed while the stronger models still participate in the prediction. Further, using heteroscedastic GP, we proposed a method of handling reputation feedbacks infected with different noise distribution.