Preface

Cloud computing is gaining a considerable momentum as a new computing paradigm for providing flexible and on-demand infrastructures, platforms and software as services. The trust management of services issues attracted many researchers in the past years. However, in cloud computing, with the highly dynamic, distributed and non-transparent nature of cloud services, this research area has gained a considerable significance. Robust trust management approaches will be essential in establishing trust between cloud service consumers and providers and will significantly contribute to the adoption and growth of cloud computing.

In this book, we present a novel approach for credibility-based trust management and automatic discovery of cloud services in distributed and highly dynamic environments. We first propose a *Zero-Knowledge Credibility Proof Protocol* to prove the credibility of consumers' feedback without breaching consumers' privacy. We then propose an adaptive and robust *Credibility Model* for assessing the consumers' credibility in giving feedback to cloud services. To measure how experienced a consumer would be, we use the concepts of *Consumer Capability* and *Majority Consensus*. We further introduce the concepts of *Feedback Density* and *Occasional Feedback Collusion* to detect strategic and occasional behaviors of collusion attacks. To detect Sybil attacks, we introduce the concepts of *Multi-Identity Recognition* and *Occasional Sybil Attacks*. To adjust trust results for cloud services that have been affected by malicious behaviors, we introduce the concept of *Change Rate of Trust*. We then propose a scalable *Availability Model* to manage the availability of the decentralized implementation of the trust management service. To share the workload between the trust management service nodes, we use the concept of *load balancing* thereby always maintaining a desired availability level. We introduce the concept of *operational power* to determine the optimal number of nodes and exploit particle filtering to precisely predict the availability of each node and determine the optimal number of replicas for each node.

The techniques presented in this book are implemented in *Cloud Armor*, a prototype that provides a set of functionalities to deliver Trust as a Service (TaaS). Finally, we conduct an exhaustive series of experimental and performance studies of the proposed techniques using a collection of real-world trust feedbacks on cloud services. We particularly develop a Cloud Service Crawler Engine for cloud services

collection. The collected datasets include meta-data of nearly 6000 real-world cloud services (1.06 GB). The experimental results shows that our system (i) is able to effectively distinguish between feedbacks from experienced and amateur consumers; (ii) is more adaptive and robust in trust calculations by effectively detecting collusion and Sybil attacks without breaching consumers' privacy no matter attacks occur in a strategic or occasional behavior; (iii) is more scalable and maintains a desired availability level in highly dynamic environments and (iv) provides an efficient support for identifying, collecting, validating, categorizing and recommending cloud services based on trust.

Talal H. Noor
Quan Z. Sheng
Athman Bouguettaya

http://www.springer.com/978-3-319-12249-6

Trust Management in Cloud Services

Noor, T.H.; Sheng, Q.Z.; Bouguettaya, A.
2014, XIX, 119 p. 39 illus., Hardcover
ISBN: 978-3-319-12249-6