Preface

Rose F. Gamble*

Tandy School of Computer Science,
University of Tulsa,
Tulsa, OK 74104, USA
Email: gamble@utulsa.edu
*Corresponding author

Indrakshi Ray

Department of Computer Science,
Colorado State University,
Fort Collins, CO 80523, USA
Email: iray@cs.colostate.edu

Cloud computing plays a major role in how IT is conducted within organisations today, having emerged as a highly sought after distributed platform of services and information resources. It offers services and storage on demand to a wide range of clients and consumers. Cloud computing services are on the rise and are making their way in various critical application domains, including the financial sector, healthcare, and military. However, before these services can be widely deployed, it must be ensured that they are secure and reliable. Quality of Services (QoS) is extremely important for cloud providers and consumers requiring well-crafted service level agreements. QoS in a cloud includes parameters such as response time, energy consumption, and level of security. Failure to meet the QoS needs has important financial consequences.

Cloud service offerings can create service-oriented architectures (SOAs) that include distinct services composed to respond to complex queries. Data may traverse the service compositions and even extend to other services external to the original cloud. The absence of a well-defined perimeter in a cloud environment introduces new challenges with respect to QoS parameters. Brokering services increase the likelihood of parameter and expectation matching among services used within the cloud. The papers in this special issue make important contributions in this regard. The first two papers focus on issues with respect to QoS modelling and prediction. The middle two papers examine different brokering strategies with respect to event distribution and sensor configuration. The last three papers focus on security as a QoS, which is becoming increasingly important in cloud computing as security breaches for critical applications can have severe consequences including loss of life. All of the seven papers in this issue present research results relevant to advances in cloud computing.

The first four papers are extensions of selected papers from the 10th IEEE International Conference on Services Computing. In the first paper 'Graph reduction for QoS prediction of cloud-service compositions', Ngoko et al. argue that deterministic techniques of graph-reduction for QoS prediction when deciding how to compose services do not work in a cloud environment for reasons of variability and propose a probabilistic approach. Next, Zheng et al. in 'Cloud service negotiation: a research report' focus on how cloud consumers can negotiate with cloud providers in the context of QoS requirements. The authors present a model to quantify the QoS services, to provide a negotiation strategy for consumers and providers to interact, and to describe a technique from which consumers can get the minimum resources that fulfil their needs. In Casola et al.'s 'An SLA-based brokering platform to provide sensor networks as-a-service', the authors describe a Cloud Sensing Brokering Platform that negotiates end user selection of sensor network providers. In the fourth paper, 'PAPas: peer assisted publish and subscribe', Ahmed et al. discuss a different form of secure brokering that determines efficient event dissemination for peer-to-peer sharing.

The last three papers are extensions of selected papers from the 1st IEEE International Cloud Security Auditing Workshop held as part of the 9th IEEE World Congress on Services. In the fifth paper of the special issue, 'Cloud security auditing based on behavioural modelling', Dolgikh et al. capture and create graphical patterns of legitimate system call streams based on previous system behaviour. Anomalies collected from an intrusion detection system are formulated in the same graphical approach. Databases of legitimate and anomalous patterns are compared with new system calls to determine when new anomalies occur. Referring to the sixth paper 'Auditing and analysis of network traffic in a cloud environment', Shetty et al. focus on how the data on the network between a cloud provider and its users can be captured for security analysis. This results in two techniques to allow the user to verify certain aspects of outsourced data. In the last paper 'Enforcing the Chinese wall model for tenant conflict of interest in the service cloud', Alqahtani et al. devise a methodology using a Security Management Database, which houses service

vectors that embed the conflict of interest classes that a tenant service accesses to impose a Chinese wall model preventing information leakage among competing tenants. The vectors are used during the cloud's provisioning of a composite set of services to complete a user request and then again at the execution of the service chain in case an access causes a vector to violate the Chinese wall model.

As a result, all seven papers depict various challenges in cloud computing and offer directions for additional research.