

# Chapter 102

## On Developing Fair and Orderly Cloud Markets: QoS- and Security-Aware Optimization of Cloud Collaboration

**Olga Wenge**

*Technische Universität Darmstadt, Germany*

**Dieter Schuller**

*Technische Universität Darmstadt, Germany*

**Christoph Rensing**

*Technische Universität Darmstadt, Germany*

**Ralf Steinmetz**

*Technische Universität Darmstadt, Germany*

### ABSTRACT

*While cloud markets promise virtually unlimited resource supplies, standardized commodities and proper services, some providers may not be able to offer effectual physical capacity to serve large customers. A solution is cloud collaborations, in which multiple providers unite forces in order to conjointly offer capacities in the cloud markets. Supposably, both the Quality of Service and security properties of such collaborations will be determined by “the weakest link in the chain”, therefore resulting in a trade-off between the monetary aggregates, cumulative capacity and the non-functional attributes of a cloud collaboration. Based on previous research, this paper examines efficient composition of cloud collaborations from the broker’s perspective, considering Quality of Service and information security requirements of multiple cloud providers and users and presents an exact approach CCCP-EXA.KOM for building cloud collaborations. Furthermore, it proposes a Mixed Integer Programming-based heuristic optimization approach CCCP-PRIOSORT.KOM and provides its quantitative evaluation in comparison with prior optimal approach.*

DOI: 10.4018/978-1-5225-8176-5.ch102

## 1. INTRODUCTION

Cloud markets promise to supply virtually unlimited capacities and services in a scalable, pay-as-you-go fashion (Buyya, R., Yeo, C., Venugopal, S., Broberg, J., & Brandic, I., 2009). Yet, specifically smaller providers may not be able to satisfy the resource and service demands of large customers on their own due to limited data center capacity and, consequently, limited range of services. A solution lies in cloud collaborations within cloud markets, i.e., the cooperation of multiple providers to aggregate their resources and conjointly satisfy user's demands. Supposably, such cloud collaborations have both Quality of Service (QoS) and information security impacts: as a user may potentially be served by any provider within a collaboration, the aggregated non-functional service attributes - e.g., availability, latency, security protection level, data center location or tiers - will be determined by "the weakest link in the chain", i.e., by a provider with the lowest guarantees.

Take the example of two providers: one provider guarantees 99.5% of availability and another provider guarantees only 99%. If these providers aggregate their capacities and related non-functional guarantees to build collaboration, the availability guarantees will be determined by the worst one - 99%.

Consideration of country-specific and industry-specific data privacy laws and regulations is another concern by building cloud collaborations within cloud markets. Since providers can reside in different jurisdictions (the European Union, Russia, Singapore, or the United States), where data privacy laws and data classification substantially differ (Carroll, M., van der Merwe, A., & Kotzé, P., 2011; Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A., 2010). Also regulatory requirements for banking, medical and healthcare institutions are stricter and harder with respect to confidentiality, integrity and availability of data in comparison with other public enterprises or business areas without confidential data (Ackermann, T., Widjaja, T., Benlian, A., & Buxmann, P., 2012). Therefore, the fulfillment of such requirements may not be achieved once multiple cloud providers enter cloud collaborations.

In our previous research (Wenge, O., Lampe, U., Müller, A., & Schaarschmidt, R., 2014; Wenge, O., Siebenhaar, M., Lampe, U., Schuller, D., & Steinmetz, R., 2012; Wenge, O., Lampe, U., & Steinmetz, R., 2014), we examined security risks and concerns of cloud computing with the focus on multi-clouds and cloud brokerage. We identified that multi-clouds are still very heterogeneous and the lack of security standards between cloud providers still pose obstacles in their cooperation and in cloud services exchange. Therefore, the role of the cloud broker is of growing interest. The broker's function is not trivial - he/she should bring cloud providers and cloud users together in order to satisfy their functional and non-functional requirements. Due to the mentioned lack of standards, cloud brokerage is becoming more complex, especially if very fine-grained security parameters and the entire security landscape must be considered.

Based on this scenario and our previous research, we examine the Cloud Collaboration Composition Problem (CCCP) in the work at hand. Our focus is on a broker within the cloud market, who aims *to maximize his/her profit* through the composition of cloud collaborations from a set of providers and assignment of users to these collaborations. In that assignment, QoS and security requirements, i.e., non-functional attributes, should also be considered and fulfilled. This work extends the previously introduced CCCP problem and its exact optimization solution approach with a heuristic approach that improves the computational time in the context of cloud markets.

The remainder of this paper is structured as follows: In Section 2, we give an overview of cloud markets and related regulations that must be considered by trading with cloud products. Section 3 describes

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/on-developing-fair-and-orderly-cloud-markets/224673](http://www.igi-global.com/chapter/on-developing-fair-and-orderly-cloud-markets/224673)

## Related Content

---

### Overview of Big Data-Intensive Storage and its Technologies for Cloud and Fog Computing

Richard S. Segall, Jeffrey S. Cook and Gao Niu (2019). *International Journal of Fog Computing* (pp. 1-40).

[www.irma-international.org/article/overview-of-big-data-intensive-storage-and-its-technologies-for-cloud-and-fog-computing/219362](http://www.irma-international.org/article/overview-of-big-data-intensive-storage-and-its-technologies-for-cloud-and-fog-computing/219362)

### Privacy Preserving Public Auditing in Cloud: Literature Review

Thangavel M., Varalakshmi P., Sridhar S. and Sindhuja R. (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications* (pp. 2059-2083).

[www.irma-international.org/chapter/privacy-preserving-public-auditing-in-cloud-literature-review/224670](http://www.irma-international.org/chapter/privacy-preserving-public-auditing-in-cloud-literature-review/224670)

### Web 2.0, Social Media, and Mobile Technologies for Connected Government

Zaigham Mahmood (2021). *Web 2.0 and Cloud Technologies for Implementing Connected Government* (pp. 1-18).

[www.irma-international.org/chapter/web-20-social-media-and-mobile-technologies-for-connected-government/259731](http://www.irma-international.org/chapter/web-20-social-media-and-mobile-technologies-for-connected-government/259731)

### FogLearn: Leveraging Fog-Based Machine Learning for Smart System Big Data Analytics

Rabindra K. Barik, Rojalina Priyadarshini, Harishchandra Dubey, Vinay Kumar and Kunal Mankodiya (2018). *International Journal of Fog Computing* (pp. 15-34).

[www.irma-international.org/article/foglearn/198410](http://www.irma-international.org/article/foglearn/198410)

### Development of Community Based Intelligent Modules Using IoT to Make Cities Smarter

Jagadish S. Kallimani, Chekuri Sailusha, Pankaj Lathar and Srinivasa K.G. (2019). *International Journal of Fog Computing* (pp. 1-12).

[www.irma-international.org/article/development-of-community-based-intelligent-modules-using-iot-to-make-cities-smarter/228127](http://www.irma-international.org/article/development-of-community-based-intelligent-modules-using-iot-to-make-cities-smarter/228127)