Accepted Manuscript

Context-Aware Multifaceted Trust Framework For evaluating trustworthiness of cloud providers

Mohannad Alhanahnah, Peter Bertok, Zahir Tari, Sahel Alouneh
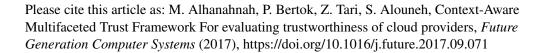
Please cite this article as: M. Alhanahnah, P. Bertok, Z. Tari, S. Alouneh, Context-Aware Multifaceted Trust Framework For evaluating trustworthiness of cloud providers, *Future Generation Computer Systems* (2017), https://doi.org/10.1016/j.future.2017.09.071

Context-Aware Multifaceted Trust Framework For Evaluating Trustworthiness Of Cloud Providers

Mohannad Alhanahnah[a,*], Peter Bertok[b], Zahir Tari[b], Sahel Alouneh[c]

[a]unaffiliated
[b]School of Science, RMIT University
[c]School of Electrical Engineering and Information Technology, German Jordanian University

Abstract

With the rapidly increasing number of cloud-based services, selecting a service provider is becoming more and more difficult. Among the many factors to be considered, trust in a given service and in a service provider is often critical. Appraisal of trust is a complex process, information about the offered service's quality needs to be collected from a number of sources, while user requirements may place different emphasis on the various quality indicators. Several frameworks have been proposed to facilitate service provider selection, however, only very few of them are built on existing cloud standards, and adaptability to different contexts is still a challenge. This paper proposes a new trust framework, called *Context-Aware Multifaceted Trust Framework* (CAMFT), to assist in evaluating trust in cloud service providers. CAMTF is flexible and context aware: it considers trust factors, users and services. When making recommendations, CAMFT employs a combination of mathematical methods that depend on the type of trust factors, and it takes both service characteristics and user perspective into account. A case study is also presented to demonstrate CAMFT's applicability to practical cases.

Keywords: Analytic Hierarchy Process, Cloud Computing, Trust, Fuzzy Simple Additive Weighting, Multifaceted

1. Introduction

In recent years, we have witnessed the rapid growth of cloud computing. Among its major benefits are the ease of provisioning and management of computing resources, and reduction of running costs. At the same time, cloud computing faces several challenges, including the related issues of security, privacy and trust [1, 2, 3, 4, 5]. In particular, building trust between users and service providers in the cloud is a major challenge. Customers have little control over the way their data is stored and handled at the Cloud Service Providers' (CSPs) premises, hence, they need guarantees that the data will be managed securely and reliably. This is related to *trust* and is based on a number of factors, some of which are expressed explicitly e.g. in service level agreements (SLAs), while others are implicit or based on user perceptions.

Selecting an appropriate CSP for a particular task is a complex process, and several frameworks have been proposed to help it. Those frameworks usually consider trust from a single perspective, e.g security [6, 7]; only few of them have a broader view and include multiple aspects, such as competence, reputation and potential risk [8], or privacy, availability and response time [9]. As different users may have different requirements, some frameworks allow the inclusion of new, additional factors and parameters [9, 7]. However, some aspects still present a challenge, notably the adaptation to different application contexts [8] or the catering for the cloud's dynamic nature [2].

---

*Corresponding author
Email addresses: ma481@kent.ac.uk (Mohannad Alhanahnah), peter.bertok@rmit.edu.au (Peter Bertok),
zahir.tari@rmit.edu.au (Zahir Tari), sahel.alouneh@gju.edu.jo (Sahel Alouneh)