Towards a Trustworthy Federated Hybrid Cloud and Container-based Platform

Danilo Ardagna
Dipartimento di Elettronica,
Informazione e Bioingegneria,
Politecnico di Milano
Milano, Italy
danilo.ardagna@polimi.it

Ignacio Blanquer
Instituto de Instrumentación para
Imagen Molecular, Universitat
Politècnica de València
Valencia, Spain
iblanque@i3m.upv.es

Francisco Brasileiro
Departamento de Sistemas e
Computação, Universidade Federal de
Campina Grande
Campina Grande, Brazil
fubica@dsc.ufcg.edu.br

Amanda Calatrava[*]
Instituto de Instrumentación para
Imagen Molecular, Universitat
Politècnica de València
Valencia, Spain
amcaar@i3m.upv.es

Wagner Meira Jr.
Departamento de Ciência da
Computação, Universidade Federal de
Minas Gerais
Belo Horizonte, Brazil
meira@dcc.ufmg.br

Marco Vieira
Departamento de Engenharia
Informática, Universidade de Coimbra
Coimbra, Portugal
mvieira@dei.uc.pt

Abstract

Cloud computing has brought many opportunities to scientists, enterprises, industries and individuals in today's competitive environment, by offering a range of services using highly scalable technologies. However, it has also opened up a new challenging space regarding trust. Trust is a choice that is based on past experience. Trust takes time to build, but trust can disappear in a second. Trusting cloud services is as complicated as trusting people. You need a way to measure it and pieces of evidence to build trust. Trust needs a priori certification and continuous verification and assurance. Evaluating trust comprises a broad range of properties. Dimensions such as Security, Privacy protection, Quality of Services, Reliability, and Fairness impose tackling a set of challenges at different layers. However, there is currently a lack of technologies and frameworks to build trust on cloud and Big Data applications, both from the self-evaluation and the dynamic adaptation perspectives.

ATMOSPHERE (Adaptive, Trustworthy, Manageable, Orchestrated, Secure Privacy-assuring Hybrid, Ecosystem for REsilient Cloud Computing) - [1] is a European-Brazilian collaboration aiming at measuring and improving the different trustworthiness dimensions of data analytics applications running on the cloud. ATMOSPHERE has designed a software architecture to provide performance simulation, dynamic Quality of Service (QoS) adaptation, vulnerability assessment, privacy leakage risk estimation and model neutrality evaluation on top of a federated cloud infrastructure. The platform supports composing data analytics workflows, defining QoS and privacy restrictions (such as using enclaves), ethical targets (for evaluating potential discrimination bias of models) and executing such workflows on top of a self-managed cloud platform.

To achieve cloud computing trust services, ATMOSPHERE focuses on providing four different components, that will consider each of the trustworthiness properties identified in the project: (i) a dynamically reconfigurable federated cloud infrastructure that ensures isolation, high-availability, stability and Quality of Service for hybrid resources, including virtual machines and containers; (ii) Trustworthy Data Management services that maximise privacy in the processing of sensitive data by proprietary algorithms on enclaves, guaranteeing that neither the application developer sees the data nor the data owner sees the processing code; (iii) Trustworthy Data Processing services to deploy adaptive applications for Data Analytics, providing high-level trustworthiness metrics for computing fairness and explainability of such models, maximising transparency; and (iv) a trustworthiness monitoring and assessment framework, to compute quantitative scores of the trustworthiness of an application running on the ATMOSPHERE platform, and able to trigger adaptation measures when needed.

The main use case of the project is the characterization of echocardio images obtained from rural areas to identify early surrogates for Rheumatic Heart Disease (RHD). Thus, the nature of the data handled in the project, gives special importance to trustworthiness. This work presents the main goals and research opportunities of the project. Also, it presents the analysis of the use case and user stories of the main actor profiles interacting with the platform.

Acknowledgment

The work in this article has been co-funded by project ATMOSPHERE, funded jointly by the European Commission under the Cooperation Programme, Horizon 2020 grant agreement No 777154 and the Brazilian Ministério de Ciência, Tecnologia e Inovação (MCTI), number 51119.

[*] The author will present the poster.

[1] www.atmosphere-eubrazil.eu