A semi-automatic and trustworthy scheme for continuous cloud service certification

Abstract:

Traditional assurance solutions for software-based systems rely on static verification techniques and assume continuous availability of trusted third parties. With the advent of cloud computing, these solutions become ineffective since services/applications are flexible, dynamic, and change at run time, at high rates. Although several assurance approaches have been defined, cloud requires a step-change moving current assurance techniques to fully embrace the cloud peculiarities. In this paper, we provide a rigorous and adaptive assurance technique based on certification, towards the definition of a transparent and trusted cloud ecosystem. It aims to increase the confidence of cloud customers that every piece of the cloud (from its infrastructure to hosted applications) behaves as expected and according to their requirements. We first present a test-based certification scheme proving non-functional properties of cloud-based services. The scheme is driven by non-functional requirements defined by the certification authority and by a model of the service under certification. We then define an automatic approach to verification of consistency between requirements and models, which is at the basis of the chain of trust supported by the certification scheme.

Introduction:

Cloud computing paradigm supports a new vision of IT where software and computational resources are released as services over a virtualized ICT infrastructure accessible through the Internet. The convenience introduced by cloud computing in terms of flexibility, and reduced costs of owning, operating, and maintaining the computational infrastructures, comes at a price of increased risks and concerns. Users deploying a service in the cloud in fact lose full control over their data and applications, which are fully or partially in the hands of cloud providers.

Assurance and verification techniques (e.g., audit, certification, and compliance) need to be adapted to fit the dynamics of the cloud ecosystem .The advent of cloud in fact makes traditional techniques inappropriate, because assurance claims and information were assumed to be all available a priori at the time of evaluation and before service deployment. Cloud assurance aims to increase cloud trust and transparency, and therefore needs to manage claim verification and evidence collection in a post-deployment environment. Moreover, due to the fact that cloud assurance should manage the complete cloud service/application life cycle, it should

i) depart from the assumption of a single trusted third party that is available during the whole process and takes responsibility over different claims done on a target object ,

 ii) implement (semi-)automatic approaches that adapt to changes in the service and/or its environment,

iii) target multiple cloud layers at the same time.

we focus on certification techniques, which aim to implement a secure, trusted, and transparent cloud by specifying a dynamic delegation mechanism supporting multiple signatures of artifacts in a cloud environment. A certification process in the cloud must follow a multi-step process that certifies the support of a given set of non-functional properties by a cloud-based system.

Technofist,

YES Complex, 19/3&4, 2nd Floor, Dinnur Main Road, R.T.Nagar, Bangalore-560032Ph:080-40969981,Website:www.technofist.com.E-mail:technofist.projects@gmail.com