Towards a trust-manager service for hybrid clouds.

Fatma Ghachem, Nadia Bennani, Chirine Ghedira, Parisa Ghodous

Towards a trust-manager service for hybrid clouds

Fatma Ghachem*, Nadia Bennani*, Chirine Ghedira**, Parisa Ghoddous*
*Université de Lyon, CNRS, LIRIS, Lyon, France
{firstname.lastname@liris.cnrs.fr}
**Université de Lyon, MAGELLAN, MODEM, Lyon, France
Chirine.ghedira-guegan@univ-lyon3.fr

Abstract
Cloud computing changed recently business view regarding their Information System through an on-demand provisioning of computing resources. Recent discussions about data security requirements in cloud computing environment tend to conflict with other requirement including usability and economic. In hybrid clouds that combine private and public clouds usage, private clouds are able both to externalize resources and invoke services from public cloud when needed. However, in such specific inter-cloud environment risks arise. Indeed, private clouds aren't sufficiently assured about how credible is the data computed by these resources they entrusted. This is due to clouds autonomy preservation, difference in control policy definitions and lack of transparency in clouds. In this position paper, we tend to propose an approach to help private cloud selecting a trustworthy public cloud service. The idea consists in a trust manager as a service that bases the decision-making on the private cloud past invocation analysis

Keywords-component: Cloud computing, data credibility, trust management, hybrid cloud, SLA

1 Introduction

Cloud computing changed recently business view regarding their Information System through an on-demand provisioning of computing resources. Recent discussions about data security requirements in cloud computing environment tend to conflict with other requirement including usability and economic. In our opinion, these discussions are too undifferentiated and neglect the real-world security reasoning and concerns. In the context of cloud, security problems increase tenfold. Indeed, the invoking schema is both horizontal as many cloud services use other cloud services not necessarily deployed on the same cloud, and vertical, as most cloud offering are deployed over several layers (IaaS, PaaS and SaaS) with different security requirements.

This observation is accentuated in the context of hybrid cloud computing where data security problems can be classified into two categories: security problems due to data externalization towards services deployed on the public cloud to ensure systems responsiveness; and security problems coming from data issued by public cloud ser-

vices and that require to be trusted by the invoking private cloud. In the first case, the problems encountered are mainly privacy and integrity problems due to data externalization. Many solutions have been proposed such as [10]. In the second case, private cloud services often interact with cloud providers for services provisioning such as infrastructure, platforms and software. However, they aren't sufficiently assured about how trustable and credible the data computed by these resources are. The lack of trust in a data produced by a service deployed on a public cloud, can impact private cloud services security. Indeed, a data misuse by a private cloud service (which is generally kept inside due to its sensitivity) can lead to produce bad data or to make inappropriate decisions. In this position paper we concentrate on the last case. The case of hybrid cloud is slightly more complex as the private cloud service has to base its decision on a set of aspects such as the trust level of the invoked service, the public cloud service execution environment (the reliability of the physical or the virtual machine (if machine virtualization stands) and so on). Solutions to the trust challenge are hence to be crucial ingredient to a more wide spread deployment of hybrid cloud computing.

Solving this problem is not an obvious task due to clouds autonomy preservation, differences in control policy definitions, and lack of transparency in clouds.

One way of coping with the problem is to identify how to determine data credibility through evaluation of service trustworthiness in hybrid cloud computing environments? In other words, proposing a methodology that enables private cloud to determine the trustworthiness of public cloud entities based on past service invocation information inference. Selection of a particular service could be motivated by information such as services provider's reputation in terms of performance, security and quality of service.

The rest of the paper is organized as follows. Section 2 briefly mentions recent work on trusting public cloud entities. Section 3 presents our current research. At the end, we summarize conclusions and challenges for future work.