

Accepted Manuscript

Improving security in cloud by formal modeling of IaaS resources

Flora Amato, Francesco Moscato, Vincenzo Moscato, Francesco Colace

PII: S0167-739X(17)30596-4

DOI: <http://dx.doi.org/10.1016/j.future.2017.08.016>

Reference: FUTURE 3611

To appear in: *Future Generation Computer Systems*

Received date: 8 April 2017

Revised date: 2 August 2017

Accepted date: 8 August 2017

Please cite this article as: F. Amato, F. Moscato, V. Moscato, F. Colace, Improving security in cloud by formal modeling of IaaS resources, *Future Generation Computer Systems* (2017), <http://dx.doi.org/10.1016/j.future.2017.08.016>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Improving Security in Cloud by Formal Modeling of IaaS Resources

Flora Amato^a, Francesco Moscato^b, Vincenzo Moscato^a, Francesco Colace^c

^aDIETI, University of Naples Federico II, Italy

^bDiSciPol, University of Campania Luigi Vanvitelli, Italy

^cDIIN, Università degli Studi di Salerno, Italy

Abstract

Nowadays, it is a matter of fact that Cloud is a “must” for all complex services requiring great amount of resources. Big-Data Services are a striking example: they actually perform many kind of analysis (like analytics) on very *big* repositories. Many File Systems and middlewares exist for efficient distribution and management of data and they usually use Cloud Resources. Anyway Several problems arose about Security of data: Virtualization is the base of Cloud resources and, even if we consider data storage as *virtually* separated elements, security issues exist if privilege escalation allows for gaining control on any data on *physical* hosts. In this paper we show how it is possible to cope Model Driven Engineering techniques to security analysis and monitoring of Cloud infrastructures. For reducing overhead, we provide a formal profile of hosts thermal behaviors. Depending on services input workloads, we detect and forecast malicious actions by comparisons with real thermal data.

Keywords: Cloud services, Verification, Big-Data, Security

1. Introduction

In the age of Big-Data, Cloud Computing is the best solution to the problem of acquiring enough computational, network and storage resources in order to

Email addresses: flora.amato@unina.it (Flora Amato), francesco.moscato@unina2.it (Francesco Moscato), vmoscato@unina.it (Vincenzo Moscato), francesco.colace@unisa.it (Francesco Colace)

Download English Version:

<https://daneshyari.com/en/article/6872960>

Download Persian Version:

<https://daneshyari.com/article/6872960>

[Daneshyari.com](https://daneshyari.com)