2014 47th Hawaii International Conference on System Science

Introduction to Secure Cloud Computing mini-track

William J. Yeager
Semi-retired
Formerly of Stanford University and Sun Microsystems, Inc.
byeager@fastmail.fm

Jean-Henry Morin
Institute of Services Science
University of Geneva, Switzerland
Jean-Henry.Morin@unige.ch

Cloud Computing offers SaaS, PaaS, and IaaS as cost effective ways of doing computation. The recent rapid deployment of Cloud Computing comes with a cost that can leave users open to vulnerabilities such as: Disruptions that may shutdown 24x7 computation availability of essential services since the concentration of government and or multiple businesses resources at a single site is a convenient target for effective cyber-terrorist attacks; Possible theft of Cloud resident software Intellectual Property and confidential Personal Information; and the unwarranted invasions of user data privacy. While this mini-track cannot adequately cover all of the issues with respect to "Secure Cloud Computing," the following six papers open for discussion several significant issues in this area.

The first paper, "Analysis of Monolithic and Microkernel Architectures: Towards Secure Hypervisor Design," by Jordan Shropshire of Georgia Southern University, focuses on hypervisor architecture, and the vulnerability of its subsystems.

The second paper, "SLA Information Management Through Dependency digraphs: The Case of Cloud Data Services," by Katerina Stamou, et al., of the University of Geneva, and Michael Georgio of the University of Cyprus, addresses the issue of SLA data management.

The third paper, "A Policy-based Security Framework for Storage and Computation on Enterprise Data in the Cloud," by Sourya Joyee De and Asim K. Pal, of the Indian Institute of Management Calcutta, West Bengal, India, discusses methods for establishing trust with an outsourced CSP.

The forth paper, "Securing KVM-based Cloud Systems via Virtualization Introspection," by Sheng-Wei Lee, and Fang Yu of National Chengchi University, Taipei, Taiwan, and Ken Tang of National Chiao Tung University, HsinChu, Taiwan, proposes a new virtualization introspection system to protect the hosts as well as VMs on a KVN-based cloud structure from malicious attacks.

The fifth paper, "A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification (CSC) Criteria," by Stephan Schneider, Jens Lansing, Fangjian Gao, and Ali Suyaev of the University of Cologne, delineates the results of expert interviews in a taxonomy that can be used in future research to improve CSC's.

The sixth paper, "Cloud Computing Data Protection, A literature Review and Analysis," by Florian Pfaff, Thomas Buckel and Axel Winkelmann of the University of Wuerzburg, aims to provide an overview of privacy issues and legal frameworks for data protection in Cloud environments discussed in recent scientific literature.

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.612