

Managed Control of Composite Cloud Systems

Christopher C. Lamb, Pramod A. Jamkhedkar, Gregory L. Heileman,
and Chaouki T. Abdallah

Department of Electrical and Computer Engineering
University of New Mexico

June 10, 2011



THE UNIVERSITY *of*
NEW MEXICO

Outline

- ① Introduction
- ② Motivation — Cloud-centric Usage Management
- ③ Introduction

Introduction

The Problem

Current policy-centric systems are being forced to move to cloud environments and build much more open systems:

"...It is imperative to effectively exchange information among components, Federal agencies, coalition partners, foreign governments and international organizations as a critical element of our efforts to defend the nation and execute national strategy..."[1]

— *DoD Information Sharing Strategy*

"...The CIO of the National Security Agency is focusing on IT architecture and a cloud-centric approach to sharing information..."[2]

— *Informationweek*

The Problem

Cloud systems may save money, provide more flexibility, but they also [3]:

- *Are Not Private* —
- *Are Less Secure* —
- *Cannot Be Trusted* —

- [1] DoD Information Sharing Strategy.
<http://cio-nii.defense.gov/docs/InfoSharingStrategy.pdf>, May 2007.
- [2] NSA Pursues Intelligence-Sharing Architecture.
<http://www.informationweek.com/news/government/cloud-saas/229401646>, April 2011.
- [3] S. Pearson and A. Benameur. Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom)*, 2010 IEEE Second International Conference on, pages 693 –702, 30 2010-dec. 3 2010.