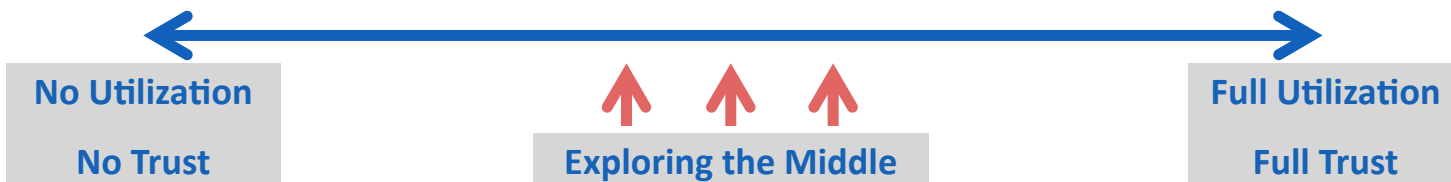


# The HybrEx Model for Confidentiality and Privacy in Cloud Computing

Steven Y. Ko<sup>1</sup>, Kyungho Jeon<sup>1</sup> and Ramsés Morales<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, University at Buffalo and <sup>2</sup>Xerox Research Center Webster

## How Much Can We Utilize Clouds without Sacrificing Confidentiality and Privacy?

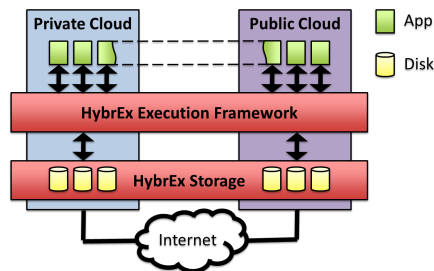


### Research Motivation

- Some just don't trust the clouds.
  - Confidentiality and privacy concerns
  - Threats do exist.
- However, cloud computing offers benefits.
  - Elasticity
  - Pay-as-you-go
  - Availability & maintenance

### Our Approach of Hybrid Execution

- Our approach: integration with safety

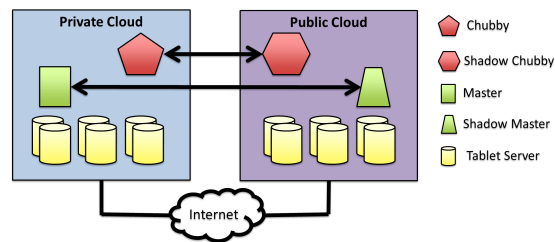


- HybrEx (*Hybrid Execution*)
  - Partitions data, computation and system
  - Utilizes public clouds only for public data and computation

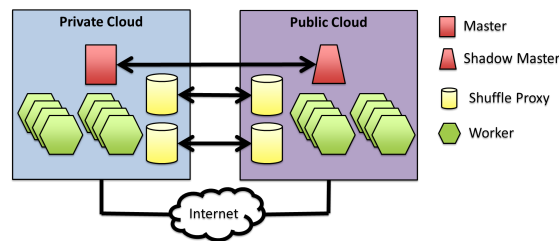
### How Much Do We Trust the Clouds?

	Computation Code	Data	Execution Environment
Private Cloud	Trusted	Trusted	Trusted
Public Cloud	Untrusted	Untrusted	Untrusted

### HybrEx MapReduce and HybrEx Bigtable



The Architecture of HybrEx Bigtable

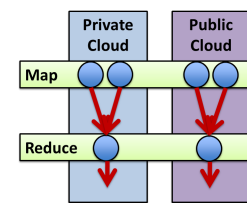


The Architecture of HybrEx MapReduce

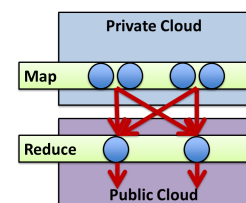
### Integrity

- Data integrity
  - Keep the hashes of the public data in the private cloud
- Computation integrity
  - Re-execute every task: only for accounting
  - Selectively check the results from the public cloud

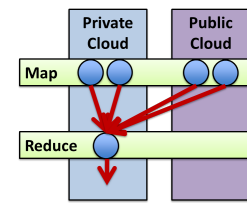
### New Execution Categories



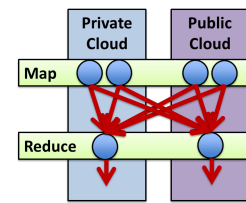
(a) Vertical Partitioning



(b) Horizontal Partitioning



(c) Map Hybrid



(d) Hybrid