

Policy Overlay Networks

Christopher C. Lamb

November 2, 2011

Abstract

Abstract - TBD

Chapter 1

Introduction

1.1 Introduction

Current enterprise computing systems are facing a troubling future. As things stand today, they are too expensive, unreliable, and information dissemination procedures are just too slow.

Generally, such systems still do not use current commercial resources as well as they could and use costly data partitioning schemes. Most of these kinds of systems use some combination of systems managed in house by the enterprise itself rather than exploiting lower cost cloud-enabled services. Furthermore, many of these systems have large maintenance loads imposed on them as a result of internal infrastructural requirements like data and database management or systems administration. In many cases networks containing sensitive data are separated from other internal networks

to enhance data security at the expense of productivity, leading to decreased working efficiencies and increased costs.

These kinds of large distributed systems suffer from a lack of stability and reliability as a direct result of their inflated provisioning and support costs. Simply put, the large cost and effort burden of these systems precludes the ability to implement the appropriate redundancy and fault tolerance in any but the absolutely most critical systems. Justifying the costs associated with standard reliability practices like diverse entry or geographically separated hot spares is more and more difficult to do unless forced by draconian legal policy or similarly dire business conditions.

Finally, the length of time between when a sensitive document or other type of data artifact is requested and when it can be delivered to a requester with acceptable need to view that artifact is prohibitively long. These kinds of sensitive artifacts, usually maintained on partitioned networks or systems, require large amounts of review by specially trained reviewers prior to release to data requesters. In cases where acquisition of this data is under heavy time constraints like sudden market shifts or other unexpected conditional changes this long review time can result in consequences ranging from financial losses to loss of life.

Federal computer systems are prime examples of these kinds of problematic distributed systems, and demonstrate the difficulty inherent in implementing new technical solutions. They, like other similar systems, need to be re-imagined to take advantage of radical market shifts in computational

provisioning.

1.2 Motivation

Current policy-centric systems are being forced to move to cloud environments and build much more open systems. Some of these environments will be private or hybrid cloud systems, where private clouds are infrastructure that is completely run and operated by an organization for wider use and provisioning, while hybrid clouds are combinations of private and public cloud systems. Driven by both cost savings and efficiency requirements, this migration will result in a loss of control of computing resources by involved organizations as they attempt to exploit economies of scale and utility computing.

Robust usage management will become an even more important issue in these environments. Federal organizations poised to benefit from this migration include agencies like the National Security Agency (NSA) and the Department of Defense (DoD), both of whom have large installed bases of compartmentalized and classified data. The DoD realizes the scope of this effort, understanding that such technical change must incorporate effectively sharing needed data with other federal agencies, foreign governments, and international organizations [1]. Likewise, the NSA is focused on exploiting cloud-centric systems to facilitate information dissemination and sharing [2].

Cloud systems certainly exhibit economic incentives for use, providing

cost savings and flexibility but they also have distinct disadvantages as well. Specifically, they are not intrinsically as private as some current systems, generally can be less secure than department-level solutions, and have the kind of trust issues that therapists cannot adequately address [3].

To begin with, cloud technology is not currently as private as some organizations would like:

- *User Data Control* —
- *Secondary Use* —
- *Offshore Development* —
- *Data Routing* —
- *Secondary Storage* —
- *Bankruptcy and Data Ownership* —

Security issues also emerge from utility computing infrastructures:

- *Data Access* —
- *Data Deletion* —
- *Backup Data Storage* —
- *Intercloud Standardization* —
- *Multi-tenancy and Side-Channels* —

- *Logging and Auditing* —

Finally, such systems suffer from internal and external trust issues:

- *Trust Relationships* —
- *Consumer Trust* —

1.3 Related Work

1.4 System Architecture

1.5 Conclusions

Bibliography

- [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.