Dynamic, Secure Resource Control in the Cloud

Edward J. Nava, Viswanath Nandina, José Marcio Luna, Christopher C. Lamb,
Gregory L. Heileman, Chaouki T. Abdallah
University of New Mexico
Department of Electrical and Computer Engineering
Albuquerque, NM 87131-0001
{ejnava, vishu, jmarcio, cclamb, heileman, chaouki}@ece.unm.edu

ABSTRACT

In this paper we describe the development of a system that provides security and performance controls over content in a cloud environment. Using artifacts that are classed at different sensitivity levels associated with service level agreements (SLAs) describing how and where they can be used, we are able to successfully provision resources in a hybrid cloud environment. These provisioned resources are created to match both performance characteristics as well as specific sensitivity restrictions specified within associated SLAs.

Categories and Subject Descriptors

D.2.11 [**Software**]: Software Architectures—*Domain-specific Architectures*

General Terms

Design, Performance, Security

Keywords

Access Control, Interoperability, DRM, Usage Management

1. INTRODUCTION

With the advent and widespread use of cloud computing, those responsible for a given usage managed resource are almost never those responsible for the computing systems, except at edge devices like mobile phones or other small profile computing devices. Resources are regularly moved across national boundaries and regional areas without either the content owner's or creator's knowledge. Furthermore, this kind of transfer is generally according to pre-established algorithms or data routing protocols over which users have no control. Managing these issues requires new usage management capabilities that can run on platforms ranging from small, hand-held devices to nodes in large data centers.

Herein, we define usage management as the ability to control actions over resources and data across and within computing environments. More than access control or digital rights management, usage management addresses with fine-grained control of all aspects of how a given digital resource is used. As digital environments become more open over time, the need for usage management for resources that span utility computational environments (e.g. cloud provider systems) will become increasingly important [14, 15].

One of the central problems with respect to usage management application in cloud environments is the ability to specify and enforce specific levels of usage management over resources. The essential mobility of information within private, public, and hybrid cloud environments makes this management virtually impossible currently, leaving system developers left with the sole option of designing proprietary information management capabilities. These capabilities become more and more expensive to develop as computational environments become increasingly distributed, and are generally a nightmare to manage, both due to the proliferation of disparate technology throughout the available public and private cloudosphere.

Furthermore, cloud computing is emerging as the future of utility systems hosting for consumer-facing applications. In these kinds of systems, components, applications, and hardware are provided as utilities over the Internet with associated pricing schemes pegged by system demand. Users accept specific Quality-of-Service (QoS) guidelines that providers use to provision and eventually allocate resources. These guidelines become the basis over which providers charge for services.

This work focuses on developing integrated SLAs that address both traditional performance measures as well as security and usage management directives. We feel that cloud monitoring capabilities have over the past year reached the point at which commercial providers supply enough performance monitoring and system management primitives to begin to implement cloud-scale automatic management systems addressing data processing suitability from both performance and security perspectives. For example, Amazon now supplies information through their CloudWatch product and provides a robust control interface via their Elastic Compute Cloud (EC2). Likewise, private cloud infrastructure-as-a-service (Iaas) offerings like OpenStack and Eucalyptus provide similar control interfaces, simplifying control of hybrid systems.

In this paper we first develop the mechanisms to enable

CCSW' 12, October 19, 2012, Raleigh, NC, USA.

control based on SLA established performance and security measures. Then, we introduce a prototypical system architecture based on widely used open-source tooling to establish a simple proof of concept. Finally we discuss preliminary observations from running our prototypical system in a hybrid cloud enfvironment.

2. CONTRIBUTING WORK

Current policy-centric systems are being forced to move to cloud environments and incorporate much more open 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 using cloud-centric systems to facilitate information dissemination and sharing [3].

Cloud systems certainly exhibit economic incentives for use, providing cost savings and flexibility, but they also have distinct disadvantages as well. Specifically, the are not intrinsically as private as some current systems, generally can be less secure than department-level solutions, and have extensive trust and privacy issues [16].

How to address these issues is an open research question. Organizations ranging from cloud service providers to governments are exploring how to engineer solutions to these problems, and to more clearly understand the trade-offs required between selected system architectures [2]. The problems themselves are wide ranging, appearing in a variety of different systems. Healtcare and government systems are clearly impacted by these kinds of trust and security issues, and they also have clear information sensitivity problems. This, coupled with the fact that these organizations have been dealing with these issues in one form or another for decades make them very well suited for prototypical implementation and study.

Over the past few years multiple service-based paradigms such as web services, cluster computing and grid computing have contributed to the development of what we now call cloud computing [8]. Cloud computing distinctly differentiates itself from other service-based computing paradigms via a collective set of distinguishing characteristics: market orientation, virtualization, dynamic provisioning of resources, and service composition via multiple service providers [9]. This implies that in cloud computing, a cloud-service consumer's data and applications reside inside that cloud provider's infrastructure for a finite amount of time. Partitions of this data can in fact be handled by multiple cloud services, and these partitions may be stored, processed and routed through geographically distributed cloud infrastructures. These activities occur within a cloud, giving the cloud consumer an impression of a single virtual system. These operational characteristics of cloud computing can raise concerns regarding the manner in which cloud consumer's data and applications are managed within a given cloud. Unlike other computing paradigms with a specific computing task focus, cloud systems enable cloud consumers to host entire applications on the cloud (i.e. software as a service) or to compose services from different providers to build a single system. As consumers aggressively start exploiting these advantages to transition IT services to external utility computing systems, the manner in which data and applications are handled within those systems by various cloud services will become a matter of serious concern [12].

A growing body of research has begun to appear over the past two years applying control theory to tuning computer systems. These range from controlling network infrastructure [6] to controlling virtualized infrastructure and specific computer systems [17], [13] to exploring feedforward solutions based on predictive modeling [4]. Significant open questions remain within this field [18], [11].

To address these issues, we first applied the principles of system design to develop a framework for usage management in open, distributed environments that supports interoperability. These principles have been used by researchers in large network design to create a balance between interoperability and open, flexible architectures [5, 7, 10], without sacrificing innovation. Initially we standardized certain features of the framework operational semantics, and left free of standards features that necessitate choice and innovation.

Usage management incorporates specific characteristics of traditional access control and digital rights management incorporating encryption mechanisms, trust management, and trusted computing platforms [12]. In order to be effective, it must be flexible enough to provide users with opportunities for differentiation and extension, but interoperable enough to provide services across widely diverging computational environments.

3. CONCLUSIONS AND FUTURE WORKS

Usage management is a common problem set with features embodied in domains ranging from security systems to video games to music production and retail. The ability to provide management of resources with regard to authorized subjects is being addressed in multiple different forums, many of which are taking remarkably different approaches. Common features however generally include the need for either ubiquitous rights expression language acceptance or for extensive translation between all supported rights languages.

In this paper, we first described the primitives and approaches currently available that use used to enable simple SLA-centric control over information distribution and processing based on performance and security sensitivity attributes. Thereafter, we described in some detail a system architecture currently realizable with modern open-source tools that enables this kind of dynamic information control. Finally, we discussed our experiences with a prototypical implementation of our proposed system architecture.

In the future, we currently plan to move away from our current web-centric model, examining more data-centric tooling, though we expect to remain committed to open source tools. We will also incorporate more standards, like the eXtensible Access Control Markup Language (XACML), to describe policies and controls, and work to establish a clear model behind our work in order to more deeply understand the intrinsic limitations of this problem domain.

4. REFERENCES

[1] DoD Information Sharing Strategy. http://cio-nii.defense.gov/docs/InfoSharingStrategy.pdf, May 2007.

[2] Assured Information Sharing in Clouds. http://www.zyn.com/sbir/sbres/sttr/dod/af/af11-bt30.htm, August 2011.

[3] NSA Pursues Intelligence-Sharing Architecture. http://www.informationweek.com/news/government/cloud-saas/229401646, April 2011.

[4] S. Abdelwahed, J. Bai, R. Su, and N. Kandasamy. On the application of predictive control techniques for adaptive performance management of computing systems. *Network and Service Management, IEEE Transactions on*, 6(4):212 –225, 2009.

[5] H. Alverstrand. The role of the standards process in shaping the internet. *Proceeding of the IEEE*, 92(9):1371–1374, 2004.

[6] Y. Ariba, F. Gouaisbaut, and Y. Labit. Feedback control for router management and tcp/ip network stability. *Network and Service Management, IEEE Transactions on*, 6(4):255 –266, 2009.

[7] M. S. Blumenthal and D. D. Clark. Rethinking the design of the Internet: The end-to-end arguments vs. the brave new world. *ACM Transactions on Internet Technology*, 1(1):70–109, Aug. 2001.

[8] R. Buyya. Market-oriented cloud computing: Vision, hype, and reality of delivering computing as the 5th utility. In *Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, CCGRID '09, pages 1–, Washington, DC, USA, 2009. IEEE Computer Society.

[9] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6):599–616, 2009.

[10] D. D. Clark, J. Wroclawski, K. R. Sollins, and R. Braden. Tussle in cyberspace: Defining tomorrow's internet. In *SIGCOMM*, pages 347–356, Pittsburg, Pennsylvania, USA, Aug. 2002.

[11] J. Hellerstein, S. Singhal, and Q. Wang. Research challenges in control engineering of computing systems. *Network and Service Management, IEEE Transactions on*, 6(4):206 –211, 2009.

[12] P. A. Jamkhedkar, G. L. Heileman, and C. C. Lamb. An interoperable usage management framework. In *Proceedings of the tenth annual ACM workshop on Digital rights management*, DRM '10, pages 73–88, New York, NY, USA, 2010. ACM.

[13] M. Kjaer, M. Kihl, and A. Robertsson. Resource allocation and disturbance rejection in web servers using slas and virtualized servers. *Network and Service Management, IEEE Transactions on*, 6(4):226 –239, 2009.

[14] C. C. Lamb, P. A. Jamkhedkar, G. L. Heileman, and C. T. Abdallah. Managed control of composite cloud systems. In *6th IEEE International Conference on System of Systems Engineering (SOSE)*. IEEE.

[15] C. C. Lamb, P. A. Jamkhedkar, G. L. Heileman, and C. T. Abdallah. Managed control of composite cloud systems. In *System of Systems Engineering (SoSE), 2011 6th International Conference on*, pages 167 –172, june 2011.

[16] 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.

[17] Z. Wang, Y. Chen, D. Gmach, S. Singhal, B. Watson, W. Rivera, X. Zhu, and C. Hyser. Appraise: application-level performance management in virtualized server environments. *Network and Service Management, IEEE Transactions on*, 6(4):240 –254, 2009.

[18] X. Zhu, M. Uysal, Z. Wang, S. Singhal, A. Merchant, P. Padala, and K. Shin. What does control theory bring to systems research? *SIGOPS Oper. Syst. Rev.*, 43:62–69, January 2009.