# An Actor-Centric, Asset-Based Monitor Deployment Model for Cloud Computing

Uttam Thakore, Gabriel A. Weaver, and William H. Sanders
*Coordinated Science Laboratory*
*University of Illinois at Urbana-Champaign*
*Urbana, Illinois 61801*
{*thakore1, gweaver, whs*}*@illinois.edu*

***Abstract*—Effective monitoring is essential for the security of cloud systems. Although many monitoring tools exist in the cloud domain, there is little guidance on how to deploy monitors to make the most of collected monitor data and increase the chances of detecting security breaches. We introduce an actor-centric, asset-based cloud monitor deployment model that enables practitioners to reason about monitor deployment in terms of the security of their cloud assets. We define an actor model that consolidates several roles in the literature to three roles motivated by security. We then develop an architectural model that identifies the assets that can be owned by each actor, and use it to drive an asset-based cloud threat model. Using our threat model, we describe how a cloud practitioner can reason about monitor deployment to more efficiently deploy monitors and increase its chances of detecting intrusions.**

***Keywords*-cloud computing; monitor deployment; security; actor model; asset-based; cloud architecture; threat modeling**

## I. Introduction

Cloud computing introduces unique security risks because the cloud is a shared computational resource that is owned and maintained by many actors. Despite continuing progress in cloud security, 57% of respondents to a recent Intel survey of cloud practitioners marked the inability to measure security services as one of their top three security concerns [1]. We claim that effective monitor deployment is necessary to efficiently detect security breaches in a cloud system.

We introduce a monitor deployment model that cloud practitioners can use to reason about monitor deployment. Our intent is to enable practitioners to detect security breaches in cloud assets that span organizational boundaries.

Existing approaches to cloud monitoring deployment are either general but too high-level to give practical advice on how to deploy a monitoring system, or provide practical advice only for very specific scenarios. Furthermore, existing approaches to cloud threat modeling may provide a high-level overview of threats, but do not give practitioners practical insights on which threats are relevant to their assets. See [2] for our analysis of related work.

In contrast, our approach uses a simple actor model to express threats relative to the cloud assets owned by each actor. Our intended contribution is to address gaps in cloud threat modeling to improve cloud monitoring. We also aim to provide a general framework that practitioners can use to analyze their set of cloud assets and deploy monitors (or cooperate with one another) to detect security breaches.

In Section II, we define the three components of our approach (the actor model, architecture model, and threat model) and describe how we used them to develop an approach to monitor deployment in the cloud. We discuss future work and conclude in Section III.

## II. Cloud Monitor Deployment Model

We approach monitor deployment in the cloud from an actor-centric and asset-based perspective.

### A. Cloud Actor Model

We distill the roles defined in the literature into the following three primary roles: Cloud Provider (CP), Cloud Service Provider (CSP), and Cloud Service Consumer (CSC) [3], [4].

The *Cloud Provider (CP)* is the provider and owner of the physical infrastructure. The service provided by the CP may be infrastructure, platform, or even software. The CP does not own the data or computation that is run through its cloud offering. The *Cloud Service Provider (CSP)* is the user of a CP but is also a provider of a service offering to consumers. It does not have control over the cloud infrastructure that it uses. The CSP is not the sole end-user of the cloud software chain; it passes on some risk to its consumers. Finally, a *Cloud Service Consumer (CSC)* is the end-user of a cloud service. This party only consumes the cloud service and has no control over the security of the infrastructure.

The key difference between a CP and a CSP in our model is that the CP owns and provisions use of the cloud infrastructure. The CP has control over monitor deployment within the entire infrastructure of the cloud, whereas the CSP has control over only the set of assets it pays to use and must rely on the CP to monitor lower-level assets.

### B. Cloud Architecture

We identify the cloud assets that can be monitored to gain insight on where to deploy monitors. Based on the work of the Cloud Security Alliance, Spring identifies 7 layers within which cloud assets can exist: facility, network, hardware, operating system, middleware, application, and user [5]. Cloud assets and their ownership by cloud actors are illustrated in Fig. 1. For definitions of each asset and layer, see [2].

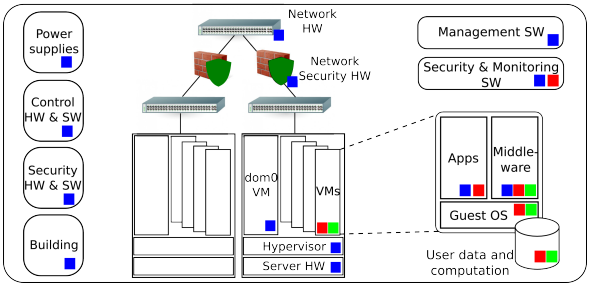


Figure 1. Cloud architecture as reflected in our monitor deployment model. Colored boxes signify ownership. Blue is CP, red is CSP, and green is CSC.

### C. Cloud Threat Model

Monitor deployment can be used to detect security breaches in cloud assets. To aid in detection, we first identify the threats to each actor's assets. Understanding which threats an actor can detect can allow the actor to reason about where to deploy monitors to make best use of collected data.

Table I lists the threats to the assets owned by the CSP. We have developed similar lists for the CP and CSC; for the complete threat model, see [2].

Table I
THREATS TO THE CLOUD SERVICE PROVIDER'S ASSETS.

| Asset | List of threats |
|---|---|
| Client VM | Exploitation of vulnerability in OS code, improper allocation of physical resources by malicious or compromised VMM. |
| Middle-ware | Exploitation of a vulnerability in software code, improper security mechanisms used by developers of software, malicious or deceptive middleware or third-party software. |
| Software and services | Code injection, denial of service, exploitation of a vulnerability in application code, misbehavior or inadvertent damage by insiders, loss of availability due to government confiscation of hardware associated with cotenants' illicit activity, loss of security due to malicious or compromised VMM or OS, loss of availability due to CP's loss of availability. |
| Client data | Improper management of storage hardware by CP, leakage of data during transit between cloud and users, leakage of data during transit within cloud, PATRIOT ACT, government confiscation of storage hardware, leakage of data through covert channels or mismanaged cotenancy, malicious or inadvertently harmful CP or CSP insider. |
| Client computation | Theft of encryption keys stored in memory, leakage of client activity profiles through sidechannels, unauthorized access to client's or own computation information through usurpation of provider's or own resources. |
| Monitoring and security software | Exploitation of predictability in usage of CP infrastructure, unavailability of management software, unavailability of security or auditing software, misinformation provided by malicious or compromised CP management and security software. |

### D. Security-driven Monitor Deployment

We now explain the steps of our approach to monitor deployment using our model. Resources may be limited, so monitors must be selectively deployed to maximize utility.

First, a practitioner should enumerate all assets under their control and identify the versions of each asset. It should also be aware of the versions of assets being used by its providers and consumers. The practitioner should then determine its system architecture (i.e., the relationships between its assets and those of its providers and consumers), as a compromised asset can be used as a platform for further attacks.

Next, the practitioner should examine the list of threats in our threat model and determine which ones are applicable to its assets. For example, if a CP uses network hardware that has known vulnerabilities, then a threat that exploits one of those vulnerabilities may warrant targeted monitoring. Further, if the practitioner offers a service that is known to be subject to a particular type of attack, then more monitors should be deployed to the assets that are directly affected by the attack and can detect the attack early.

Practitioners should also consider the mission-criticality of an asset, the marginal utility of data collected by each monitor, the impact of an intrusion on the data collected by the monitors, and ways of collecting data from assets not under their ownership. See [2] for a more in-depth analysis.

## III. CONCLUSION

The current research literature does not provide an easily-actionable model for security-driven monitor deployment within the cloud. We therefore present an actor-centric, asset-based model for monitor deployment that addresses this gap. We define a set of three actors that are concerned about the security of their cloud assets, identify the set of assets in cloud systems, and associate assets with the actors who control them. We then identify the threats to the assets as seen by each actor, and provide a methodology for deploying monitors based on the threat model we present.

The intent of our ongoing research is to develop a monitor deployment model that practitioners can apply to satisfy their security goals. In this paper, we present the foundations of our work. However, much can be done to build on our model. We are currently investigating and formalizing metrics for monitor deployment and attempting to classify monitor data to formalize the concept of monitor data stream utility.

## ACKNOWLEDGMENT

This material is based in part on research sponsored by the Air Force Research Laboratory and the Air Force Office of Scientific Research, under agreement FA8750-11-2-0084.

## REFERENCES

[1] Intel IT Center, "Peer Research: What's Holding Back the Cloud?" p. 31, 2012. [Online]. Available: www.intel.com/content/dam/www/public/us/en/documents/reports/whats-holding-back-the-cloud-peer-research-report2.pdf

[2] U. Thakore, G. A. Weaver, and W. H. Sanders, "An actor-centric, asset-based monitor deployment model for cloud computing," Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Tech. Rep., 2013, to appear.

[3] G. Aceto, A. Botta, W. De Donato, and A. Pescapè, "Cloud monitoring: A survey." *Computer Networks*, vol. 57, no. 9, pp. 2093–2115, 2013.

[4] N. of Standards and Technology, "Important actors for public clouds," 2010. [Online]. Available: http://www.nist.gov/itl/cloud/actors.cfm

[5] J. Spring, "Monitoring cloud computing by layer, part 1," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 66–68, 2011.