Forensic Acquisition Methods for Cloud Computing Environments

Diane Barrett
Bloomsburg University of Pennsylvania, USA

INTRODUCTION

Cloud computing environments add an inherent layer of complication to a digital forensic investigation. The content of this article explores current forensic acquisition processes, how current processes need to be modified for cloud investigations, and what new acquisition methods can help when it is necessary to garner evidence from a cloud computing based environment. The article is based on an expert panel Delphi study. The purpose of the qualitative Delphi study was to develop a robust contingency framework for deciding when to use traditional forensic investigative practices, when to use modified processes, and when it is necessary to develop new forensic investigative processes more appropriate to the cloud computing environment.

The lack of previous research on how current methods of forensic acquisition processes apply to cloud computing environments has created a gap that may hinder the continued growth of the digital forensics field. In order to garner a true picture of the application of forensic acquisition processes in cloud computing environments, querying a panel of subject matter experts (SMEs) provided the best possible information.

A section will be included that provides a recommendation on how to acquire evidence from cloud based environments while maintaining chain of custody. A final section will include recommendations for additional areas of research in the area of investigating cloud computing environments and acquiring cloud computing based evidence.

BACKGROUND

Cloud Computing Environments

Cloud computing is encompassed in the capabilities of almost all existing technologies. The cloud market is growing at a rate of 20 percent to 25 percent a year, and reached a size of $127 billion dollars in 2018. Approximately 30 percent of worldwide enterprise applications are offered via the cloud (Kathuria, Mann, Khuntia, Saldanha, & Kauffman, 2018). The concept behind cloud computing is a production environment in which resources and software services do not function locally. Instead, the Internet or the internal network of an organization seamlessly connects numerous host machines running on a virtualized platform (Skemp, 2019).

Joe-Wong and Sen (2018) provide a general layered architecture of cloud infrastructures as a basic model by classifying the architecture into three abstract layers using two models: deployment and service, along with a set of characteristics. The layers from the bottom up are infrastructure, platform, and application. The infrastructure layer provides fundamental computing resources such as processing, storage,

DOI: 10.4018/978-1-7998-3479-3.ch033

and networks. The platform layer delivers higher-level services and abstractions for integration of the ability to perform application functions in the environment. The application layer allows the capability for applications as a service (AaaS).

These three layers are further broken down into service models, deployment models, and attributes. The three well-recognized cloud service models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The four cloud deployment models are community, hybrid, public, and private. The attributes consist of measured and on-demand self-service, resource pooling, rapid elasticity, and broad network access. This is the exact layered architecture outlined by National Institute of Standards and Technology (NIST) in the final issuance of the cloud computing definition dated September 2011.

Environmental Variables

By 2015, as more and more businesses began to sign on as users, Amazon, Microsoft and International Business Machines Corporation (IBM) had all created cloud computing services. Since then, the popularity of cloud computing has increased because organizations are attracted by the affordability, accessibility, and flexibility of the services (Skemp, 2019). The ability to produce dynamic business environments by using cloud computing environments allow organizations of all sizes to respond rapidly to market changes and pursue creative resource saving solutions. Cloud computing environments offer unrestricted scalability and lower data-center setup costs by using multitenancy.

The multitenancy and virtualization characteristics of a cloud computing environment present difficult implementation demands in the areas of security and access control (Fatima, & Ahmad, 2019). The unique security and access control challenges presented by the use of multitenancy and virtualization in cloud computing environments exist because many individual environments share the same set of hardware. The sharing of storage blocks can result in the accidental and unauthorized flow of information (Fatima, & Ahmad, 2019). The diversity of services offered in cloud computing environments requires variable levels of granularity when implementing access control mechanisms. The risk of resource exploitation by unauthorized users is significantly increased when there are insufficient or untrustworthy authorization mechanisms implemented in a cloud computing environment (Chaudhary & Siddique, 2017).

Cloud computing environments offer many organizational benefits by providing scalability and elasticity but come with complex computing infrastructures. Every cloud deployment and service model instance is different. For example, one SaaS implementation can be completely different from the next. There are many challenges associated with the use of cloud computing environments and existing issues are only beginning to be addressed. As more and more businesses move to a cloud computing environment, automated service provisioning, virtual machine migration, server consolidation, and security are topics that have garnered the attention of the research community.

Digital Evidence Seizure

Digital forensics focuses on the retrieval and analysis of data found on digital devices relative to some type of unauthorized or criminal activity. Traditional digital forensics processes consist of crime scene evidence collection, evidence preservation, evidence analysis, and presentation of the analysis results (Mansour, 2016).

Current traditional digital acquisition processes include maintaining chain of custody control of forensic evidence data. This chain of custody control occurs in the evidence collection phase through the imaging of a system (Shah, Saleem, & Zulqarnain, 2017).