Chapter 1
Forensic Investigations in Cloud Computing

Diane Barrett
Bloomsburg University of Pennsylvania, USA

ABSTRACT

Cloud computing environments add an inherent layer of complication to a digital forensic investigation. The content of this chapter explores current forensic acquisition processes, why current processes need to be modified for cloud investigations, and how new methods can help in an investigation. A section will be included that provides recommendations for more accurate evidence acquisition in investigations. 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.

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, why current processes need to be modified for cloud investigations, and how new methods can help in an investigation. A section will be included that provides recommendations for more accurate evidence acquisition in investigations. 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 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 (Budriene & Zalieckaite, 2012).

DOI: 10.4018/978-1-5225-7492-7.ch001

Pallis (2010) provides 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, 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

Complex and dynamic business environments such as cloud computing environments drive organizations of all sizes to respond rapidly to market changes and pursue creative resource saving solutions. In addition to being a technology solution, cloud computing is a new business model. 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 (Almutairi, Sarfraz, Basalamah, Aref, & Ghafoor, 2012). 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 (Werner, 2011). 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 (Werner, 2011).

Cloud computing environments offer many organizational benefits by providing scalable but 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 newly emerging challenges associated with the use of cloud computing environments and existing issues are not yet addressed. Automated service provisioning, virtual machine migration, server consolidation, and the management of power and security are just beginning to garner research community attention.

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 (Garfinkel, 2010). Traditional digital forensics processes consist of crime scene evidence collection, evidence preservation, evidence analysis, and presentation of the analysis results (Greengard, 2012). Current traditional digital acquisition processes include maintaining