Chapter 5.11
A Survey of Cloud Computing Challenges from a Digital Forensics Perspective

Gregory H. Carlton
California State Polytechnic University, USA

Hill Zhou
California State Polytechnic University, USA

ABSTRACT

Computing and communication technologies have merged to produce an environment where many applications and their associated data reside in remote locations, often unknown to the users. The adoption of cloud computing promises many benefits to users and service providers, as it shifts users' concerns away from the physical location of system components and toward the accessibility of the system's services. While this adoption of cloud computing may be beneficial to users and service providers, it increases areas of concern for computer forensic examiners that need to obtain data from cloud computing environments for evidence in legal matters. The authors present an overview of cloud computing, discuss the challenges it raises from a digital forensics perspective, describe suitable tools for forensic analysis of cloud computing environments, and consider the future of cloud computing.

INTRODUCTION

As computing and communications technologies continue to expand rapidly, cloud computing is emerging as a method by which services are provided, often without the knowledge of the users. Contemporary computing environments typically consist of some type of workstation and network connection, and nontechnical computer users may give little consideration as to where applications or data reside. Often, user applications and data exist on remote computing and storage systems while users access their applications and data from

DOI: 10.4018/978-1-4666-0879-5.ch5.11

the mysterious "cloud" without understanding the physical locations of these devices.

It is not just the nontechnical computer users that are often unaware of the physical computing infrastructure. One of the appeals of cloud computing is the concept that users need not be concerned with the physical location of data, services, or devices in order to utilize these services. Many organizations realize numerous benefits from implementing systems based on cloud computing, as this approach often provides cost savings, increased flexibility, and perhaps higher reliability and lower maintenance.

The increase of cloud computing usage brings an increase in legal matters (i.e., civil lawsuits or criminal investigations) in which data from cloud computing environments are used as evidence. This directly results in an increase in the need to conduct computer forensics examinations from cloud computing environments. Computer forensics examiners must determine the authenticity of the data used as evidence; therefore, it is essential that computer forensics examiners have a thorough understanding of the infrastructure used in cloud computing.

This paper provides an orientation to cloud computing for forensics examiners. We first offer an overview of cloud computing, then a discussion on cloud computing from a forensics perspective, and then we describe forensic tools that are useful in examinations of cloud computing environments. Lastly, we present a view of the future of cloud computing. The following sections address each of these areas, and we are hopeful that this paper will provide useful information to forensic examiners and it will encourage researchers to expand upon the concepts presented.

OVERVIEW OF CLOUD COMPUTING

Most of today's computer users are impacted by cloud computing in some form, and it is becoming an increasingly attractive approach for organizations that seek to transition from in-house data centers to remote, third-party managed data centers (Brodkin, 2009). While the usage of cloud computing is increasing, the concept of cloud computing triggers different perceptions in different people, largely since the nature of cloud computing is not based on a single technology. Instead, it is a combination of many existing technologies, including thin clients, virtualization, online storage, and service oriented architecture (SOA) (Amrhein & Quint, 2009). Similar to the apologue described in John Godfrey Sax's poem, *The Blind Men and the Elephant*, (Saxe), people have different views on the composition and significance of cloud computing yet fail to capture the big picture. For many end-users and managers, the idea of cloud computing is nothing newer than exchanging information and documents through web-based, e-mail services, such as Hotmail or Gmail, and others recognize the concept as an extension of the timesharing model developed in the 1960s (Schneier, 2009). However, from IT professionals' perspectives, these elder computing models hardly resemble the contemporary cloud computing age, as new inventions of virtualization, online collaboration, connectivity, and processor power combine to create our current era of computation. Recognizing the array of technological components comprising cloud computing, the National Institute of Standards and Technology (NIST) offers the following definition: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction" (Mell & Grance, 2009).

Prominent enterprises that offer cloud computing services include Amazon, IBM, and Microsoft Corporation. An example is Amazon's Elastic Compute Cloud (EC2) web services, where individuals are provided with an image running a chosen operating system, and users are permitted