Chapter 15
Cloud Computing Forensics

Mario A. Garcia
Texas A&M University – Corpus Christi, USA

ABSTRACT

As computer technology evolved over the last 30 years, so did the opportunity to use computers to break the law. Out of necessity, digital forensics was birthed. Computer forensics is the practice of extracting information from the digital media in order to prosecute the individuals that carried out the crime. Forensic challenges presented by cloud computing are vast and complex. If a company becomes the target of a digital criminal investigation and they are using cloud computing, some unique challenges are faced by a digital forensics examiner. The data in the cloud only represents a "snapshot" of when it was sent to the cloud. Establishing a chain of custody for the data would become difficult or impossible if its integrity and authenticity cannot be fully determined. There are also potential forensic issues when the customer or user exits a cloud application. Items subject to forensic analysis, such as registry entries, temporary files, and other artifacts are lost, making malicious activity difficult to prove. The challenges of applying forensics to a cloud environment are tied to cloud security. This chapter discusses securing a cloud environment and how that would help with the forensic analysis.

INTRODUCTION

In today's fast paced global economy people are busier now than ever before. The financial strain has forced people to do more with less. Every day people are watching more and more companies close their doors. One of the ways corporations have been able to keep their heads above water is by reverting back to an old technology made new again in Cloud computing. The concept behind Cloud computing is the ability to store ones data on a server in the datacenter "The Cloud" and retrieve it via users digital devices (PC, laptops, tablets, and smart phone). Cloud computing demand for mobile technology has increased dramatically as more and more people have begun to move away from traditional desktops to using mobile devices and cloud services. Recent advances in computer communications technology and particularly Cloud computing is driving some of these changes.

A 2010 report by Gartner Consulting shows that cloud revenue will increase from 58.6 billion in 2009 to almost 150 billion in 2014 (Knipp, 2009). Cloud computing is a transformative technology that provides; on demand service, ubiquitous network access, location independent resource

pooling, rapid elasticity, and pay per usage. "As the cloud continues to grow new developments in cloud computing will continue to have a significant and far reaching impact now and in the future of IT systems, networks, and applications" (Berry, 2011).

CLOUD COMPUTING

Cloud computing is the digital version of Rent-A-Center. It has burst out on the scene with many executives and cloud providers touting its ability to be flexible, on demand and responsive to changes in the operating landscape for nearly any organization. However, there are still some myths as what is exactly involved with Clouding computing. Cloud computing is defined by the National Institute of Standards and Technology as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Barnes, 2010). Some of the key elements of Cloud computing includes:

- The infrastructure is owned and maintained by a third party called the Cloud Service Provider.
- Access to the cloud is provided via a subscription basis using a demand elastic pricing model in which the customer pays more if he uses more resources on the cloud. This is a major reason why many small and medium sized businesses use the cloud service because they pay for what they use.
- The services of cloud computing are delivered via the web making them platform and location agnostic. In other words, the end user needs to maintain their internet connection and all the other required services can be acquired through the internet.

Service Types

On Demand Self Service

Having on demand services requires less human interaction as well as network storage from a service provider. The key feature of this service is the ability for the cloud customer to acquire and release service capacity without human intervention from the service provider. This process enables the cloud customer to manage their computing needs for processing as well as storage on demand.

Broad Network Access

This allows data to be accessed via thin or thick client platforms and cloud based software application services. In most cases the cloud customer needs only a thin client, which they have. Because of this the benefits of cloud service is within reach of a very large segment of the business community globally.

Resource Pooling

The third party provider essentially serves multiple organizations by using pooled resources depending on the organization's need. Traditionally the server utilization rates have been rather low, around 10% of the server capacity in most cases. The cloud service provider is able to use virtualization technique and make their server capacity usable by multiple customers. In this aspect the cloud service has significantly increased the server utilization rate at the cloud service provider level.

Rapid Elasticity

Depending on an organization's needs, the capabilities can be scaled up or down to meet the organization's needs. For example, a business in US focused on tax preparation has a higher demand on their services for the period January through

7 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/cloud-computing-forensics/119860

Related Content

IoT-Fog-Blockchain Framework: Opportunities and Challenges
Tanweer Alam (2020). *International Journal of Fog Computing (pp. 1-20).*
www.irma-international.org/article/iot-fog-blockchain-framework/266473

Fog Computing to Serve the Internet of Things Applications: A Patient Monitoring System
Amjad Hudaiband Layla Albdour (2019). *International Journal of Fog Computing (pp. 44-56).*
www.irma-international.org/article/fog-computing-to-serve-the-internet-of-things-applications/228129

Multi-Layer Token Based Authentication Through Honey Password in Fog Computing
Praveen Kumar Rayani, Bharath Bhushanand Vaishali Ravindra Thakare (2018). *International Journal of Fog Computing (pp. 50-62).*
www.irma-international.org/article/multi-layer-token-based-authentication-through-honey-password-in-fog-computing/198412

Automate Model Transformation From CIM to PIM up to PSM in Model-Driven Architecture
Yassine Rhazali, Asma El Hachimi, Idriss Chana, Mohammed Lahmerand Abdallah Rhattoy (2020). *Modern Principles, Practices, and Algorithms for Cloud Security (pp. 262-283).*
www.irma-international.org/chapter/automate-model-transformation-from-cim-to-pim-up-to-psm-in-model-driven-architecture/238912

Domain-Based Dynamic Ranking
Sutirtha Kumar Guha, Anirban Kunduand Rana Dattagupta (2015). *Advanced Research on Cloud Computing Design and Applications (pp. 262-279).*
www.irma-international.org/chapter/domain-based-dynamic-ranking/138509