Digital Investigation 13 (2015) 38–57

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Cloud forensics: Technical challenges, solutions and comparative analysis

Ameer Pichan*, Mihai Lazarescu, Sie Teng Soh

Department of Computing, Curtin University, Kent Street, Bentley, Perth, WA 6102, Australia

ARTICLE INFO

Article history:
Received 17 October 2014
Received in revised form 17 March 2015
Accepted 23 March 2015
Available online 14 April 2015

Keywords:
Cloud computing
Cloud forensics
Cloud service provider
Cloud customer
Digital forensics
Digital evidence
Service level agreement
Amazon EC2

ABSTRACT

Cloud computing is arguably one of the most significant advances in information technology (IT) services today. Several cloud service providers (CSPs) have offered services that have produced various transformative changes in computing activities and presented numerous promising technological and economic opportunities. However, many cloud customers remain reluctant to move their IT needs to the cloud, mainly due to their concerns on cloud security and the threat of the unknown. The CSPs indirectly escalate their concerns by not letting customers see what is behind virtual wall of their clouds that, among others, hinders digital investigations. In addition, jurisdiction, data duplication and multi-tenancy in cloud platform add to the challenge of locating, identifying and separating the suspected or compromised targets for digital forensics. Unfortunately, the existing approaches to evidence collection and recovery in a non-cloud (traditional) system are not practical as they rely on unrestricted access to the relevant system and user data; something that is not available in the cloud due its decentralized data processing. In this paper we systematically survey the forensic challenges in cloud computing and analyze their most recent solutions and developments. In particular, unlike the existing surveys on the topic, we describe the issues in cloud computing using the phases of traditional digital forensics as the base. For each phase of the digital forensic process, we have included a list of challenges and analysis of their possible solutions. Our description helps identifying the differences between the problems and solutions for non-cloud and cloud digital forensics. Further, the presentation is expected to help the investigators better understand the problems in cloud environment. More importantly, the paper also includes most recent development in cloud forensics produced by researchers, National Institute of Standards and Technology and Amazon.

Introduction

The advent of cloud computing in recent years has produced major technological advancement in the way Information Technology (IT) services are provisioned and deployed. Cloud computing, which can be used by individuals as well as corporations, continues to grow at remarkable rate due to its many favorable features. Among others, adopting cloud computing users can alleviate big capital investments, replacing them with low cost and more flexible operational expenses, while taking advantage of its speed, agility, flexibility, infinite elasticity and more importantly mobility because services can be accessed anytime from anywhere. The offered features have fuelled a phenomenal growth in cloud services market. Independent studies conducted by organizations, such as the European Network and Information Security Agency (ENISA) and Gartner, predicted a sharp increase in the adoption of cloud

* Corresponding author.
E-mail address: ameer.pichan@postgrad.curtin.edu.au (A. Pichan).

http://dx.doi.org/10.1016/j.diin.2015.03.002
1742-2876/

computing services by corporate organizations, educational institutions and Government agencies (Gartner, 2014; IEEE, 2014). A study by Market Research Media found that the global cloud computing market is expected to grow at a compound annual growth rate of 30% reaching $270 billion by 2020 (Zawaod and Hasan, 2013). The growth is mainly fuelled by the cost savings and pay per use model offered by cloud computing. A similar case study conducted on cloud migration reported an average cost saving of 37% when organizations move their infrastructures to Amazon EC2 cloud, in addition to potentially eliminating 21% of the support calls, showing compelling reasons to adopt cloud computing (Khajeh-Hosseini et al., 2010). A recent study conducted by RightScale group on the adoption of cloud computing, concluded that cloud adoption reaches ubiquity with 87 percent of the surveyed organizations using public cloud. Amazon Web Services (AWS) leading the cloud adoption at 54 percent (RightScale, 2014).

On the other hand, Cloud Security Alliance (CSA) reported a corresponding growth in cloud vulnerability incidents. Specifically, CSA's report shows that cloud vulnerability incidents between 2009 and 2011 have more than doubled, with top three cloud service providers (CSPs), i.e., Amazon, Google and Microsoft, accounted for 56% of all non-transparent cloud vulnerability incidents. The report also cited that the number of vulnerability incidents over the past five years has risen considerably (CSA, 2013b). The increasing security incidents in the cloud are caused, among others, by easy user account registration provided by CSPs, unfettered accessibility, and virtually unlimited computing power. In essence, attackers can open bogus accounts to the cloud, use them to carry out their acts, terminate the accounts and disappear into ether once their malicious acts have been performed. Easy access and almost unlimited power of the cloud allow the attackers, using cloud as a platform, to perform their powerful attacks from anywhere in short periods.

While it is impossible to prevent all attacks totally, they should be traced back to the attackers. Digital forensics is commonly used to track and bring criminals into justice in a non-cloud (traditional) computing environment. However, traditional digital forensics cannot be directly used in cloud systems. In particular, distributed processing and multi-tenancy nature of cloud computing, as well as its highly virtualized and dynamic environment, make digital evidence identification, preservation and collection, needed for forensics, difficult. Note that cloud systems have been hardly designed with digital forensics and evidence integrity in mind, and thus forensics investigators face very challenging technical, legal and logistical issues. Professional organizations, such as CSA and National Institute of Standards and Technology (NIST), and researchers have published papers related to cloud computing in areas such as cloud governance, security and risk assessment (CSA, 2011; Iorga and Badger, 2012; Jansen and Grance, 2011). However, only very little work has been done to develop the theory and practice of cloud forensics (Casey, 2012; Zawaod and Hasan, 2013); some have argued that cloud forensics is still in its infancy (Zawaod and Hasan, 2013).

Recently, several researchers have addressed cloud forensic challenges and issues, and proposed solutions to address the challenges (Damshenas et al., 2012; Daryabar et al., 2013; Grispos et al., 2013; Reilly et al., 2011; Taylor et al., 2011; Zawaod and Hasan, 2013). Since then there has been many advancement in the cloud forensic area. In particular, NIST has formed cloud forensics working group and produced draft publications in July 2014 (NIST, 2014a), and CSPs have started delivering services which supports forensics, e.g., Amazon's security suite of products (AWS Security Centre, 2014) and CloudTrail used for logging in the AWS Cloud (AWS Security Centre, 2013a).

In this paper, we present a comprehensive analysis of cloud forensic challenges and recommended solutions, in the current context as we walk through the forensic phases commonly used in the non-cloud digital forensics. In detail, the contributions of this paper are as follow.

- It presents the forensic process systematically and lists the challenges per different phases of the process, primarily for Infrastructure-as-a-Service cloud model. Its systematic approach would enable forensic practioners and information security professionals to easily comprehend and understand the problem as they go thru the different phases of forensics process.
- It provides a comprehensive analysis of the solutions and evaluates the recommended solutions.
- It identifies the area where the solutions are still immature or not yet fully developed and identifies the opportunities for future work.

The rest of this paper is organized as follows. Section 2 provides the technical background, detailing an overview of cloud computing and its various service and deployment models. The section also presents an overview of digital forensics and cloud forensics and describes the forensic process. Section 3 presents the cloud forensics challenges and solutions and provides a critical analysis of suggested solutions encountered in different phases of the forensic process. Section 4 presents summary of the survey findings and future work. Finally, we conclude this paper in Section 5.

Technical background

Cloud computing: overview

The NIST defines cloud computing as "*a model for enabling ubiquitous, convenient, on demand* network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." (Jansen and Grance, 2011).

In simple terms the cloud computing is a service delivery model, in which IT services are offered as a service to consumers and billed as per usage. The services can be accessed, using a thin client such as web browser, via Internet at any time and from anywhere. The cloud