Journal of Information Security and Applications 42 (2018) 18–28

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Towards a practical cloud forensics logging framework

Ameer Pichan*, Mihai Lazarescu, Sie Teng Soh

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

ARTICLE INFO

Article history:

Keywords:
Cloud computing
Cloud forensics
Digital forensics
Digital evidence
Logging
Cloud service provider
Cloud service user

ABSTRACT

This paper exposes and explore the practical issues with the usability of log artefacts for digital forensics in cloud computing. Logs, providing detailed events of actions on a time scale have been a prime forensic artefact. However collection of logs for analysis, from a cloud computing environment is complex and challenging task, primarily due to the volatility, multi-tenancy, authenticity and physical storage locations of logs, which often results in jurisdictional challenges too. Diverse nature of logs, such as network logs, system logs, database logs and application logs produces additional complexity in the collection and analysis for investigative purposes. In addition there is no commonality in log architecture between cloud service providers, nor the log information fully meets the specific needs of forensic practitioners. In this paper we present a practical log architecture framework, analyse it from the perspective and business needs of forensic practitioners. We prove the framework on an ownCloud - a widely used open source platform. The log architecture has been assessed by validating it against the Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence guidelines. Further validation has been done against the National Institute of Standards and Technology published report on Cloud Computing Forensic Challenges, i.e., NISTIR 8006. Our work helps the forensic examiners and law enforcement agencies in establishing confidence in log artefacts and easy interpretation of logs by presenting it in a user friendly way. Our work also helps the investigators to build a collective chain of evidence as well as the Cloud Service Providers to provision forensics enabled logging.

© 2018 Elsevier Ltd. All rights reserved.

1. Introduction

Cloud computing has revolutionized the computing industry in the recent years. Cloud computing offers unlimited computing power and storage on a pay per service model, which enables the business to shift the Information Technology (IT) service expenditures from Capital Expenditure (CapEx) to Operational Expenditure (OpEx), resulting in rapid uptake of cloud computing services. The Bessemer Venture Partner (BVP) Cloud index (which tracks the top public companies), reported that the cloud market will triple in next five years reaching US$500 billion of total market capitalization by 2020 [1]. The BVP State of the Cloud Industry 2018 report predicts strong growth in cloud computing uptake and the rise of innovative cloud services (e.g., Serverless Computing, Payment as a Service) [2]. Also the Right Scale 2017 State of the Cloud Report mentioned that the cloud adoptions continues to grow and companies started running majority of their business applications in cloud computing environment [3]. Despite the fact that the cloud computing is uniquely susceptible to the confusion and hype that surrounds it.

Though the cloud computing offers significant benefits, there has been growing concern about the security, privacy, legal, and jurisdictional aspects of cloud environment and the way the cloud computing stores and process customers data [4]. Further to that researchers have pointed out that the cloud infrastructure is not matured to support digital forensic needs as well, and identified issues and challenges associated with conducting forensics in the cloud [5–7]. Researchers also have noted that, till date, there is no vendor which facilitates the forensic investigation in the cloud [8]. National Institute of Standards and Technology (NIST) identified 65 cloud forensic challenges, in its report titled *NIST Cloud Computing Forensic Science Challenges* i.e., NISTIR 8006 report [9].

One of the challenges identified in the NISTIR 8006 report is the *Criminals access to low cost computing power* [9]. The availability of massive computing power at low cost is a motivational factor for malicious actors to use the cloud computing infrastructure to conduct cyber crime, or to store counter band materials [10]. It has been reported that Amazon cloud infrastructure has been used to store nasty SpyEye banking trojan and launch attack on financial institutions, affecting seriously the financial institutions in US, UK, Canada, Germany and Australia [11]. Criminals quickly disappear by

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

https://doi.org/10.1016/j.jisa.2018.07.008
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

terminating their account, but forensic examiners still should be able to trace the malicious act to the actors. The proposed model in this work helps to address the traceability of malicious activity, even after the actors have terminated their cloud services.

Many researchers have established cloud logging is an essential need for cloud forensics. Event logs, application logs, system logs, network logs are fundamental forensic log artefacts. By collating all the logs and putting them over a time scale helps to connect the chain of events. Therefore, many research work has been carried out in the related area; such as securing the logs, ensuring the integrity and trust worthiness of logs, secure transportation of log and enabling cloud to provide secure logging as a service [10,12–16]. However, none of the work looked from the angle of what forensic practitioners wants in the log. Therefore in this work, we examine the logging requirements for forensic needs which the law enforcement wants such that it can provide better value and practical benefit to the investigator. We propose a forensic enabled cloud forensic logging framework, and support it with experimental results. We then validate the framework using sample case studies and using Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence (hereafter referred as ACPO guidelines) and NISTIR 8006. We further elaborate the model's capabilities, helping to build a corroborated chain of evidence in support of cloud forensics.

The rest of the paper is organized as follows: Section 2 provides the basic concepts and definitions. Section 3 describes related work conducted in this field and the motivation to carry out this specific research. Section 4 explains the methodology, architecture and environment used to carry out the experiments and to conduct the proof of validation. We describe the results and analyse of the findings in Section 5. Finally we conclude this paper in Section 6 along with the possibility of future work and Section 7 (Appendix A) lists the detailed test results.

2. Basic concepts

Cloud Computing. Cloud computing realizes the computing resources and IT services as a utility. Cloud computing benefits the Cloud Service Users (CSUs) by providing uninterrupted services with reduced or no maintenance overhead. It is a new way of service delivery model for computing resources and enables universal access, any time from anywhere over the Internet [17]. Amazon Web Services (AWS), Microsoft Azure and Google's App Engine are examples of Cloud computing.

Digital Forensics. Digital Forensics is an investigative process to determine and relate the evidence to establish factual information for judicial review. NIST defined digital investigation as *"the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data"* [18].

Cloud Forensics. Cloud Forensics is the science and art of applying digital forensics in a cloud computing environment. NIST defines cloud forensics as *"the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence"* [9]. The nature of Cloud computing architecture poses numerous challenges to cloud forensics in comparison to traditional digital forensics in an in-house IT systems [4,5,19].

Logging for Forensics. In a digital world, logs provides a systematic representation of the state of an object and the actions that has been taken producing a change in status of the object, generating events. Systematic and secure logging of those events, storing and making it available to the investigators, are an important and fundamental part of the cloud forensics. Because of the black box nature of the cloud, co-mingling of data, volatility, data integrity, jurisdiction, privacy of co-tenants etc. causes big challenges in producing a reliable logs for forensic purposes. Investigators have to depend upon the Cloud Service Provider (CSP) for the logs. Unfortunately there is no established process to verify that the CSPs are providing correct logs to the investigators either [10]. Despite, the logs provide highly valuable information to the investigators.

3. Related work and motivation

3.1. Related work

Forensic identification and data collection is a post crime activity, whether it is traditional forensics or cyber crime. In a cloud computing scenario, the evidence identification and collections is even more challenging due to ephemeral nature of cloud computing environment and geographic distribution of the physical systems [5,19]. The importance of cloud computing applications to provide some form of audit trail, as a digitally admissible evidence is of critical importance for cloud forensics [6]. However, researchers mentioned that cloud forensics is still in its infancy, neither the cloud providers nor the forensic community have yet put forward how they will implement the cloud platform forensic ready [19]. Therefore several researchers have looked at the problem of capturing trustworthy logs from multiple dimensions. Marty [14] provided a guideline for cloud application logging. Sang [16] described a log based approach for cloud forensics primarily for Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS) models, but the approach heavily depends on the CSPs providing support. In an attempt to find a solution for forensic investigation Zafarullah et al. [20] proposed a method for identifying and extracting log entries relevant to forensics from Linux operating system and security logs. They conducted experiments in Eucalyptus cloud environment and could produce fingerprints to reconstruct an event. Dykstra et al. [21] evaluated popular forensic data acquisition tools and proved that they can successfully return volatile and non-volatile data from the cloud, and examined various levels of trust required in the cloud. Further to that they developed an open stack tool, namely Forensic Open Stack Tools (FROST) to collect logs from virtual disks, application logs and firewall logs which works at the cloud management plane requiring no trust of the guest machine [22]. Zawoad et al. [23] proposed a Secure-Logging-as-a-service which stores entire virtual machines' logs and provides access to forensic purpose securely. They further expanded their work in which they presented a scheme for tamper proof secure logging, and proved that the integrity of the log can be ensured, even if the cloud actors such as CSP, the CSU and the investigator collude. The scheme ensures that any violation of the integrity property, can be detected during the verification process [10]. A layered cloud logging architecture was presented in the work of Patrascu et al. [15], including the way of monitoring activities in a cloud infrastructure.

Even before the advent of cloud computing, many research work have been carried out on the topic of secure logging for forensic purpose [13,24]. The secure logging principles outlined in those papers are valid for cloud computing environment too, though conducting various digital forensic process, especially the evidence acquisition is a complex process in cloud computing environment. A generic scheme that allows keeping the audit logs on an untrusted machine was presented by Shneirer et al. [24]. They proved that even if an attacker takes control of the untrusted machine the scheme ensures that the attacker gains little or no information from the logs and limits the attacker's ability to corrupt the log files undetectably. These principles can be extended for cloud

Download English Version:

https://daneshyari.com/en/article/6884537

Download Persian Version:

https://daneshyari.com/article/6884537

Daneshyari.com