Cloud Computing Forensic Science

Sumanth V.

Assistant Professor,
Department of CSE,
R. R. Institute of Technology,
Bengaluru, Karnataka, India

Hemalatha R.

UG Student,
R. R. Institute of Technology,
Visvesvaraya Technological University,
Bangalore, India

ABSTRACT

This section discusses the characteristics of cloud computing forensic science, elaborates on why cloud computing challenges traditional digital forensics methods, and describes what constitutes a challenge for cloud forensics. Many experts consider forensic science to be the application of a broad spectrum of sciences and technologies to the investigation and establishment of facts of interest in relation to criminal law, civil law, or regulatory issues. The rapid advance of cloud services requires the development of better forensic tools to keep pace. However, the resulting techniques may also be used for purposes other than legal and regulatory issues to reconstruct an event that has occurred. Cloud computing forensic science is the application of scientific principles, technological practices, and derived and proven methods to reconstruct past cloud computing events through the identification, acquisition, preservation, examination, interpretation, and reporting of potential digital evidence.

Keywords: cloud computing, forensic.

INTRODUCTION:

Cloud computing has revolutionized the methods by which digital data is stored, processed, and transmitted. One of the most daunting new challenges is how to perform digital forensics in varioustypes of cloud computing environments. The challenges associated with conducting forensics in different cloud deployment models, which may cross geographic or legal boundaries, have becomean issue.

NIST carries out many research activities related to forensic science. The goals of these activitiesare to improve the accuracy, reliability, and scientific validity of forensic science methods and practices through advances in its measurements and standards infrastructure. As part of these activities, the NIST Cloud Computing Forensic Science Working Group (NCC FSWG) is identifying emerging standards and technologies that would help solve challenges, that is, the mostpressing problems fundamental to carrying out forensics in a cloud computing environment to lawfully obtain (e.g., via warrant or subpoena) all relevant artifacts, as well as to provide capabilities for security incident response and internal enterprise operations.

RELATED WORK:

To better understand the correlation between the cloud forensic science challenges and their cloud-based root cause, the NCC FSWG analyzed each challenge's relationship to the cloud functional capabilities (cloud processes or solutions) identified in the Cloud Security Alliance's(CSA's) Enterprise Architecture (EA) [9]and leveraged by the NIST Cloud Security ReferenceArchitecture (CSRA) [10].

The CSA's EA, reproduced in Annex C, Fig. 1, covers the following domains:

a. Business Operations and Support (BOSS) – has capabilities associated with cloud ITservices to support an organization's business needs.
b. Information Technology Operation & Support (ITOS) – has capabilities associatedwithmanaging the cloud IT services of an organization.
c. Security and Risk Management (S & RM) – has capabilities associated with safeguarding cloud IT assets and detecting, assessing, and monitoring cloud ITrisks.

The CSA's EA also identifies the corresponding data grouping into the following service layers:

a. Presentation Services – has capabilities associated with the end user interacting with acloud IT solution.
b. Application Services – has capabilities associated with the development and use ofcloud applications provided by an organization.
c. Information Services – has capabilities associated with storage and the use of cloudinformation and data.
d. Infrastructure Services – has capabilities associated with core functions that support thecloud IT infrastructure, such as facilities, hardware, networks, and virtual environments.

METHODOLOGY:

- **On-demand self-service:** A Consumer can automatically and unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each cloud service Provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g.,mobile phones, tablets, laptops, and workstations).
- **Resource pooling:** The Provider's computing resources are pooled to serve multiple Consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the Consumer generally has no control over or knowledge of the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to rapidly scale outward and inward commensurate with demand. To the Consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service(e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the Provider andConsumer of the utilized service.

EXPERIMENTAL RESULTS:

During preliminary analysis, some common topics were identified in these challenges, each of which overlaps several of the categories enumerated in the mind map. These topics appear to be orthogonal to those categories and are included here to provide additional insight into thechallenges.

Time: Time is frequently a critical issue as it relates to time synchronization and the possibledisappearance of evidence that is not quickly found, as Zimmerman and Glavach [13] point out. Once the information source is identified, do all involved entities have the time synchronized using a consistent time source such as Network Time Protocol (NTP)? If a forensic expert has a difficult time convincing your legal counsel that the time stamps from client-side log files match time stamps on provider-side log files, the forensics will be difficultto defend. In addition to using NTP to ensure that all server time is synced, the issue of time zones used in timestamps must be addressed in cloud forensics. Not all systems use Coordinated Universal Time (UTC) timestamps; when recorded in local time, the time zone offset must be collected from the server. Additionally, if evidence is not found quickly enough,it may be overwritten or lost in some other manner. Some example challenges in Annex A related to time include FC-05 (Timestamp synchronization), FC-14 (Real-time investigation intelligence processes not possible), FC-30 (Data available for a limited time), and FC-53 (International cloud services).

Location: Locating digital media can be a time-consuming process in cloud environment cases. Both backup and redundant storage are important, and an understanding of the topologywill aid in identifying physical locations of media storage. Locating the evidence can be a bighurdle. As pointed out by Zimmerman and Glavach [13], before network or computer forensicscan begin, the network or computer must be 'found.' There may only be traces of a virtual machine (VM) because the VM may reside on dispersed, internationally-located physical drives. When forensic data is collected on a physical resource, the justification for collecting that data on that particular resource must be shown by showing the validity of the logical to physical mapping. This is critical since all components

– computing, network and storage arevirtualized in the cloud. Some example challenges in Annex A related to location include FC-17 (Multiple venues and geo-locations), FC-25 (Decreased access and data control), FC-27 (Locating evidence), FC-37 (Additional evidence collection), FC-48 (Physical data location), and FC-60 (Decoupling user credentials & physical location).

CONCLUSION:

This document highlights many of the forensic challenges in the cloud computing environment fordigital forensic examiners, cloud Providers, law enforcement, and others. The information in thisdocument was developed as a result of examining recent research papers and involved the international community. It provides a definition of cloud computing forensics to scope this area and describes the relationship of each challenge to the five essential characteristics of cloud computing. The document also discusses how the challenges correlate to cloud technology by considering their relationship to the Cloud Security Alliance's Enterprise Architecture. The categories of challenges include architecture, data collection, analysis, anti-forensics, incident firstresponders, role management, legal issues, standards, and training. Finally, the results of overcoming each challenge are provided.

REFERENCES:

Buchanan W, Graves J, Bose N, Macfarlane R, Davison B, Ludwiniak R, (2011). Performance and student perception evaluation of cloud-based virtualized security and digital forensics labs. In HEA ICS Conference.

Cloud Security Alliance, Trusted Cloud Initiative, Enterprise Reference Architecture, https://downloads.cloudsecurityalliance.org/initiatives/tci/TCI_Reference_Architecture_v2.0.pdf

Executive Office of the President (2012). Principles for Federal Engagement in Standards Activities to Address National Priorities, January 17, 2012 https://www.whitehouse.gov/sites/whitehouse.gov/ files/omb/memoranda/2012/m-12- 08_1.pdf

Hogan M, Liu F, Sokol A, Tong J (2011). NIST Cloud Computing Standards Roadmap. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication(SP) 500-291. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909024

Liu F, Tong J, Mao J, Bohn RB, Messina JV, Badger ML, Leaf DM (2011) NIST Cloud Computing Reference Architecture (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 500-292. https://doi.org/10.6028/NIST.SP.500-292

Martini B, Choo KR, (2014) Remote Programmatic vCloud Forensics: A Six-Step Collection Process and a Proof of Concept. Proceedings of the 13th IEEE InternationalConference on Trust, Security and Privacy in Computing and Communications (TrustCom), 24–26 September 2014.

Mell P, Grance T (2011) The NIST Definition of Cloud Computing. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800- 145. https://doi.org/10.6028/NIST.SP.800-145

Ruan K, Carthy J, Kechadi T, Crosbie M (2011) Cloud Forensics. 7th IFIP Advances in Digital Forensics VII, G. Peterson and S. Shenoi (eds), vol. 361, pp. 35-46.

Zatyko K (2007) Commentary: Defining Digital Forensics. Forensic Magazine,January 2, 2007.
