International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 1 ǁ 2022 ǁ PP. 34-36

Digital Forensic Investigation in Cloud Technology Phases

Saleh Ousman
Salehousmane9611@gmail.com,
Ajeenkya DYPATILUniversity

Abstract
Cloud Computing is becoming one of the most promising and emerging technology in the decade it offers various functionality to its user, mostly helping to access the resource quickly from cloud service provider, cloud forensic is part of cloud computing, this review paper presents various challenges in every step of cloud and digital forensic such collecting snapshots as evidence in cloud.
Keywords: *Cloud Computing, Cloud Forensics, Digital Forensics, Digital Evidences, Snapshots*

Date of Submission: 27-12-2021 Date of acceptance: 07-01-2022

I. Introduction

Cloud forensic is known as Digital forensic is part of computer forensic, it's mainly the identification, collection Analysis and presentation of digital forensic in cloud is called cloud forensic. In all new technology the security part is the most important aspect, digital forensic and cloud forensics are more useful in today'sworld.

In this paper we will be basically discussing the challenges and steps of digital forensics in cloud technology.

In the first section we will identify the useand working of digital forensic in cloud technology at the last we will have a global solution.

II. Digital Forensic challengesand steps

This step represents the challenges in every phase of cloud forensics.
2.1- identification
2.2- challenges
2.3- evidence collection
2.4 -examination and analyses 2.5- Presentation

2.1- Identification

Identification is simply a first step in investigation process to determine of a malicious activity that just occurs or happened.
Identification in cloud technology investigating attribute to identify by use of following

- Carry audit of a computer system
- Detection of any of anomalies detected by intrusion defense system
- feedback and complaint made

2.2- Challenges

Having access to logs is not easy tasks, that make identification very difficult, the easiness of accessing this log depend also from model of cloud used, in SaaS, Pass here is much difficult because of limitedaccess.
By nature, cloud is volatile, means data is set toerase automatically once the system is shutdown, Ram could have or contains evidences such names, id,passwords.
Lack of customer's awareness could be also the main issue investigator are facing it.

2.3- Evidence Collection

Evidence collection is the most important part, in digital forensic is to collect the evidence done by identification, it has to be preserved, preserving the data or information is to maintain the integrity, original data this cannot be duplicated or changed till full investigation is over.
As stated, earlier investigation in cloud is more complex than the traditional one.
This type of evidence collection leads us to take some Major point.

- Cloud instance isolation (Evidence isolation)

- Digital provenance (historicrecord)
- Documentation

2.4 - Examination andAnalyses

Once the data is identified, it goes under various examination technique
through several software available for facility of investigation or analyses on data.
Many tools are available can help recover data deleted, or modified.
ThisAnalysisissimilartocloudforensic examination
This step faces many challenges

- Lack of software or toolavailable
- Facility of sharingevidence
- Difficult to re conduct crimescenes

2.5- Presentation

The last phases is the presentation here in this phase the information is gathered with evidenceand proof, it is needed to be submitted in the court to prove crime, The information is summarized

III. General Solution

Here we brought a solution how to access the evidences in logs, according to Zafarullah he is a cloud researcher propose a system call log management system by using Eucalyptus is a Linux based open-source cloud tool. This tool provides such time, attacker's Ip address, type of browser used, http request.
In Examination and analysis, we faced lack of cloud forensic tools: recently black hat developed an open-source tool named OWADE (offline, windows, Analysis and data extractor).
This software allow investigation the website viewed by cloud user and also extractinformationstored in cloud; this version works only on windowsXp.
Without forgetting I would like to list FORST is cloud Management it acquires evidence from API logs, FORST is the first forensic tool built.
crime-scene reconstruction is a method built by investigators that allow to replay the event of attack it goes back at the state before attack before attack occur by using snapshots. In such scenario in depend on the cloud technology in some it is permissible.

IV. Conclusion and Futurework

Various challenges of cloud computing environment consist a break the process of digital forensics. There is no standard framework for digital forensics in cloud computing. To have a standard framework, there is a need to gather challenges and possible solutions. This reviewpaper presents various challenges in every step of cloud forensics with probable solutions that can mitigate those challenges. According to Zargari cloud is next field where security battle will perform, we have seen in decade the emerging of Cloud this will take us to Zargari theory.

References

[1]. Zargari S, Benford D. Cloud forensics: concepts, issues, and challenges. 2012 Third International Conference on Emerging Intelligent Data and Web Technologies; 2012. IEEE. pp. 236–43.
[2]. Word Press Used as Cloud Cover in New APT Attacks. Available from http://www.darkreading.com/attacks- breaches/dropbox-wordpress-used-as- cloud-cover-in-new-apt-attacks/d/d-id/1 140098. Accessed on 2015 Nov25.
[3]. Dzombeta S, Stantchev V, Colomo- palacios R, Brandis K, HaufeK. Governance of Cloud Computing Services for the Life Sciences. IEEE Computer Society.2014.
[4]. Alqahtany S, Clarke N, FurnellS. Christoph Reich2A forensic 10acquisition and analysis system for IaaS.
[5]. Almulla S, Iraqi Y, Jones A. A state-of- the-art review of cloud. 2014 ADFSL. 2014; 9:7–28.
[6]. Taylor M, Haggerty J, Gresty D, Lamb D. Forensic investigation of cloud computing systems. NetwSecur. 2011; 4–10.
[7]. Dykstra J, Sherman AT. Acquiring forensic evidence from infrastructure-as-a- service cloud computing: exploring and evaluating tools, trust, and techniques. Digit Investigate. 2012; 9:S90–8.
[8]. Reilly D, Wren C, Berry T. Cloud computing?: pros and cons for computer forensic investigations. Int. J. Multimed. Image Process. 2011;1:26–34.

[9]. Damshenas M, DehghantanhaA, Mahmoud R, Shamsuddin S. Forensics investigation challenges in cloud computing environments. cyber security. 2012 International Conference on Cyber Warfare and Digital Forensic (CyberSec); 2012; Kuala Lumpur. pp. 190–4.
[10]. ZawoadS,HasanR.DigitalForensicsin the Cloud. 2013.Symposium on Applied Computing—SAC '11; 2011. pp. 178.
[11]. Yan C. Cybercrime forensic system in cloud computing. Proceedings of 2011 International Conference on Image Analysis and Signl Processing, IASP 2011. pp.612–3.
[12]. Zawoad S, Hasan R. Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. 2013. pp.1–15.
[13]. Zaferullah Z, Anwar F, Anwar Z. Digital forensics for eucalyptus. 2011 Frontiers of Information Technology; 2011; Islamabad. pp.110–6.
[14]. Wolski R. Available from https://www.usenix.org/ conference/lisa09/eucalyptusopen-source- infrastructure-cloud-computing. 16/01/2016.
[15]. Marty R. Cloud application logging for forensics. Proceedings of the 2011ACM
[16]. Birk D, Wegener C. Technical issues of forensic investigations in cloudcomputing environments. 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering; 2011; Okland. pp. 1–10.
[17]. Kirubakaramoorthi R, Arivazhagan D, Helen D. Survey on Encryption Techniques used to Secure Cloud Storage System. Indian Journal of Science and Technology. 2015; 8(36):1–7.
[18]. Delport W, Olivier MS, Kohn M. Isolating a cloud instance for adigital forensic. ISSA. 2011.
[19]. Senthil KP, Kamal ARNB. Optimal Integrity Policy for Encrypted Data in Secure Storage using Cloud Computing. Indian Journal of Science and Technology. 2016;9(8):1–10