INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY ISSN: 2456-6683 Volume - 5, Issue - 11, Nov - 2021
Monthly Peer-Reviewed, Refereed, Indexed Journal Scientific Journal Impact Factor: 5.743
Received on : 11/11/2021 Accepted on :25/11/2021 Publication Date: 30/11/2021

A Survey on Cloud Forensics Frameworks

[1]Sheena Mohammed, [2]Dr. R Sridevi, [3]Dr. K.S Sadasiva Rao
[1] Research Scholar, CSE Department, JNTUH, Hyderabad, India
[2] Professor, CSE Department, JNTUH, Hyderabad, India
[3] Professor, MCA Department, CBIT, Hyderabad, India
Email - sheenamd786@gmail.com, sridevi.rangu@jntuh.ac.in , sadasiva_mca@cbit.ac.in

Abstract: *Cloud computing is being adopted by practically all commercial enterprises in today's technological era because of its benefits. The flexible environment provides the way to easily perform even malicious activities on the cloud too, and also make the job of investigator very tough. Rendering to numerous readings and surveys, cloud-based data has become the major target for cyber-attacks. . This necessitates the use of forensics on the Cloud .The current cloud forensic investigations face the issues such as lack of standard framework, lack of specific forensic tools etc. There are number of traditional digital forensic tools and techniques are available which are even used in the cloud environment but these tools are discredited because of distributed nature of the cloud. In each level of the forensic investigation, the present frameworks and tools for cloud forensics face numerous problems. This article presents the challenges and comparative analysis on existing forensic frameworks on cloud environment.*

Key Words: *Cloud forensics, CSP, DoS, DDoS, TamForen, LSTM.*

1. INTRODUCTION:

Cloud computing is one of the hotfoot-creating fields in Information Technology. It's not an exaggeration that there is almost every business association has embraced cloud computing into their business applications. Cloud computing permits the people and the associations to send their product foundation on far-off, virtualized conditions which are called clouds. As a rule, the clouds are provided by the trusted parties known as Cloud Service Provider (CSP). The essential characteristics of cloud computing include (a) On-demand self-service (b) Broad network access(c) Resource-pooling (d) Rapid elasticity (e) Measured service [1]. There are three service models offered by cloud computing including [2] (i) Software as a Service (SaaS) (ii) Platform as a Service (PaaS) (iii) Infrastructure as a Service (IaaS). The clouds are categorized into a public, private, commodity, and hybrid cloud based on the ownership and managing capabilities [3].Without exaggeration, cloud computing has progressed to the point that it is difficult to find a company that does not use one of the three service models SaaS, PaaS, or IaaS to host its business applications [4].

2. CRIME AND CLOUD:

As technology advances and businesses become more reliant on IT systems, crime is on the rise, and the cloud is no exception. The versatile nature of the cloud also makes it very easy for criminals to carry out criminal operations. For example, criminals can utilize the cloud as a business platform in the same way that businesses use the cloud to host apps like run software fronts or backend applications, etc. Criminals can also use the cloud to launch DoS (Denial of Service) and DDoS (Distributed Denial of Service) cyber-attacks, which pool millions of susceptible, compromised machines into malware and use it to launch attacks. [5]. Another option is to use a cloud platform that allows you to fast and temporarily increase the victim's processing power and network bandwidth, allowing you to mount an attack to temporarily disable the victim's systems before resuming normal operations. Because cloud systems provide enterprises and criminals with flexibility, ease of use, global access, and low- cost IT resources, they can be used for employee misdeeds. As more businesses move to the cloud, commercial cloud platforms are becoming a primary target for cyber thieves; it has long been known that popular cloud platforms store increasing volumes of vulnerable data. As a result, an attacker's main concern is not locating a single target business, but rather locating a vulnerable cloud location. We can't say that cloud isn't more secure than a company's infrastructure; in fact, well-managed enterprise-class cloud platforms are more resilient, durable, and secure than poorly managed small business networks. However, because of the aggregation of data and common access mechanisms, the cloud will always be a target for criminals [5]. According to the Verizon Business 2020 Data Breach Investigations Report, 86 percent of all cyber- attacks were carried out for monetary gain, up from 71% in 2019, and cloud-based data has become a prime target [6].

3. CLOUD FORENSICS – LITERATURE SURVEY

Rieona Fernandes [7] discussed the cloud forensics challenges and process, which includes evidence identification and collection without breaking the law, preservation using crypto shedding to recover deleted data, examination using event correlation tools, and presentation in a court of law to prove the crime. Kim- Kwang Raymond Choo [8] focuses on cloud logging systems and pulls together ideas from several disciplines to meet the primary current difficulties associated with cloud forensics Malek Harbawi et al. [9] analyzed a variety of characteristics, features, and technology and concluded that there is still a significant gap between current digital forensics tools and the ideal digital forensics concept. According to Kara Nance et al. 10], it requires top-down study in digital forensics that considers subcategories of the problem such as Process Control Systems, Legal concerns, education, and research.

Back door, spoofing, Man in the Middle, replay, TCP Highjacking, Social Engineering, Dumpster Diving, Password Guessing, Trojan Horses, and malware are all feasible assaults in the cloud, according to Laura Savu [11] and shows the need for new technologies, research in the field of cloud computing. Emi Morioka [12] proposes cloud forensics solutions based on existing digital forensic tools such as FTK, Encase, Memoryze, AWS Export, and others, all of which have limitations and require further refining before being used on a cloud platform. In cloud computing, Abdulghani Ali Ahmed et al. [13] present a proactive methodology to improve the process of identifying and gathering cyber-crime evidence. The challenges, tools, and solutions of forensic investigative processes in a cloud computing context were discussed by Benjamin Yakson et al. [14]

The requirements that a cloud forensic process model should at least cover to be employed by cloud-consuming agencies were outlined by Ahmed Nour Moussa [15]. Shams Zawoad [16] proposes an Open Cloud Forensic Model for Reliable Digital Forensics which indeed needs the implementation of OCF supported, forensics-aware cloud infrastructure. Ahmed Alenezi [17] proposed a framework through which to identify the key technical, legal, and organizational factors that influence forensic readiness. Abha Belorkar et al. [18] suggested a method of regenerating events with continuous snapshots. The back-end calculations were proposed using the fuzzy clustering concept of distance. The resulting evidence is expected to be sequenced, integrated, and much stronger. Raffel Marty [19] has shown that log collection and logging guidelines are an essential building block of any forensic process and proposed a framework in this regard.

Shams Zawoad, et al. [20] introduced Secure Logging-as-a- Service, which stores virtual machines' logs and provides access to forensic investigators ensuring the confidentiality of the cloud users. Saibharath S et al. [21] proposed and implemented a data collection and rendering mechanism for the cloud through the Hadoop file system. Ben Martini [22] proposed an integrated conceptual digital forensic framework for cloud computing which is based on iterating the phases of the forensic investigation process. Fei Ye [23] proposed the tamper-proof mechanism, TamForen of cloud evidence, even though the security of the transmission channels from cloud nodes to the BFA and between nodes still affects the tamper-proof effect for evidence. Most of the researches focused on the cloud forensic investigation process as in Figure 1, and shown that there is a still need of developing efficient frameworks and tools that would be applicable for cloud forensics.

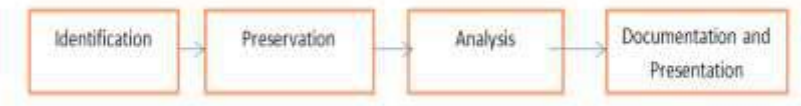

Fig. 1 Stages in digital forensics process

4. CLOUD FORENSICS FRAMEWORKS - COMPARATIVE ANALYSIS:

The challenges in stage of investigation process are briefed in the table 1. The comparative analysis of existing cloud forensic frameworks proposed by various researchers is shown in table 2. The parameters such as evidence extraction, preservation, security, classification, and prioritizing the evidence are taken to compare the frameworks which are shown in table 3.

TABLE 1: CLOUD FORENSICS -CHALLENGES

Phase	Identification	Preservation	Analysis	Presentation
Challenges	Log data retrieval	Evidence integrity	Lack of forensic tools	Testimony-complexity
	Hardware access	Privacy	Data volume	Documentation
	Volatility of data	Time-synchronization	Encryption	
	Distribution and	Manpower	Deleted data	

	Collaboration			
	Incomplete data	Chain of custody	Reconstruction	
	CSP dependency	Imaging	Log formats	
	SLA-not standardized	Multi-jurisdiction	Identity	
		Multi-Tenancy		

TABLE 2: CLOUD FORENSICS FRAMEWORKS –COMPARATIVE ANALYSIS (A)

Sl.No	Framework	Process model	Limitations
1	Forensics framework for cloud computing[24]	• client request to CSP • FMP monitoring tool forwards the request to the server and the response to the client, and it forensically images the request and saves it in the forensic server. • A forensic investigator for analyzes the evidence collected from the forensic server. • The activities performed on the forensic server are likewise forensically captured and preserved on the forensic server. • If the investigator suspects the CSP, he requests evidence sources from the CSP and compares them to each other, ensuring the integrity of the acquired data.	Model monitors the entire inbound and outbound connections, collects bit by bit stream, and stores outside the cloud environment which needs an additional server and also causes privacy issues.
2	Tam Foren [23]	•There are two core components: Bloom Filter Agent(BFA) and Evidence Credibility Verification (ECV) •BFA monitors the cloud nodes, obtains potential evidence, and generates provenance data. •ECA module verifies the evidence.	The security of transmission channel from cloud nodes to BFA and between nodes still affects the evidence.
3	An integrated conceptual cloud forensic framework [22]	• Evidence source identification and preservation. • Collection. • Examination and analysis • Iterate the above three phases • Reporting and presentation	Still need to develop a library of digital forensic methodologies
4	Forensic Based Cloud[25]	• Implement System as a service • The preservation stage is online • The logs are thrown on web server called evidence publisher	Integrity of logs is the main concern. Still it is linear to time.

TABLE 3: CLOUD FORENSICS FRAMEWORKS –COMPARATIVE ANALYSIS (B)

Sl.No	Framework	Investigation Process				
		Evidence extraction	Preservation	Security of evidence	Classification of evidence	Prioritization of evidence
1	Forensics framework for cloud computing[24]	√	√	×	×	×
2	TamForen[23]	√	√	√	×	×
3	An integrated conceptual cloud forensic framework [22]	√	√	√	×	×
4	Forensic Based Cloud[25]	√	√	×	×	×

These frameworks have their own limitations, where there is still need of development of efficient cloud forensic tool for extracting and analyzing the evidences in the cloud environment.

5. CONCLUSION:

This paper reviews the existing forensic frameworks in the cloud environment and shows the necessity of developing the specific forensic tools in cloud environment which intern help the investigator to focus on most relative evidences.

REFERENCES

1. NIST definition of cloud computing by National Institute of Standards and Technology, special publication 800-145. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
2. Mohammad UbaidullahBokhari, QahtanMakkiShallal, YahyaKordTamandani: Cloud computing service models: a comparative study, Article in IEEE Network • March 2016
3. Tinankoria Diaby, Babak Bashari Rad: Cloud Computing: A review of the Concepts and Deployment Models, I.J. Information Technology and Computer Science, 2017, 6, 50-58 Published Online June 2017 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijitcs.2017.06.07
4. G. Kiryakova, N. Angelova, L. Yordanova: Application of Cloud Computing Services in Business, Trakia Journal of Sciences, Vol. 13, Suppl. 1, pp 392-396, 2015 Copyright © 2015 Trakia University Available online at: http://www.uni-sz.bg ISSN 1313-7069 (print) doi:10.15547/tjs.2015.s.01.067 ISSN 1313-3551 (online).
5. https://www.huntsmansecurity.com/blog/cyber-crime-and-cloud-security/
6. https://www.telecomtv.com/content/security/remote-working-and-an-increase-in-cloud-based-data-is-spurring-cyber-attacks-38713/#:~:text=Unsurprisingly%20the%20vast%20majority%20of,has%20become%20a%20prime%20target
7. Rieona Fernandes, Rencita Maria Colaco, Sharadhi Shetty, Rama Moorthy H : A New era of Digital Forensics in the form of Cloud Forensics, Proceedings of the Second International Conference on Inventive Research in Computing Applications (ICIRCA-2020) IEEE Xplore Part Number: CFP20N67-ART; ISBN: 978-1-7281-5374-2.
8. Kim- Kwang Raymond Choo , Christian Esposito and Aniello Castiglione: Cloud computing for business, 978-1-4673-1740-5 /12/$31.00 ©2012 IEEE.
9. Malek Harbawi and Asaf Varol: The Role of Digital Forensics in Comdating Cybercrimes, ISBN:978-1-4673-9865-7/16/$31.00© 2016 IEEE
10. Kara Nance, Brian Hay , Matt Bishop: Digital Forensics: Defining a Research Agenda, 978-0-7695-3450-3/09 $25.00 © 2009 IEEE.
11. Laura Savu: Cloud Computing-Deployment models, delivery models, risks and challenges, 978-1-4244-9283-1/11/$26.00 ©2011 IEEE.
12. Emi Morioka, Mehrdad S. Sharbaf: Digital Forensics Reaseach on Cloud Computing: An investigation of Cloud Forensics, 978-1-5090-0770-7/16/$31.00 ©2016 IEEE.
13. Abdulghani Ali Ahmed, Chua Xue Li: Locating and Collecting Cybercrime Evidence on Cloud Storage: Review, 978-1-5090-5493-0/16/$31.00 ©2016 IEEE.
14. Benjamin Yakson, Adam Davis: Analysis of the Current State of Cloud Forensics- The Evolving Nature of Digital Forensics, 978-1-7281-5052-9/19/$31.00 ©2019 IEEE.
15. Ahmed Nour Moussa, Narafidah Ithnin , Nawaf Almolhis, Anazida Zainal: A Consumer-Oriented Cloud Forensic Process Model, 978-1-7281-0755-4/19/$31.00 ©2019 IEEE.
16. Shams Zawoad, Amit Kumar Dutta, Ragib Hasan: OCF: An Open Cloud Forensic Model for Reliable Digital Forensics, 2159-6190/15 $31.00 © 2015 IEEE, DOI 10.1109/CLOUD.2015.65.
17. Ahmed Alenezi, Raid Khalid Hussein, Rober J. Walters , Gary B. Wills: A Framework for Cloud Forensic Readiness in Organizations, 978-1-5090-6325-3/17 $31.00 © 2017 IEEE, DOI 10.1109/MobileCloud.2017.12.
18. Abha Belorkar, G. Geethakumari: Regeneration of events using system snapshots for cloud forensic analysis, 2016 (IEEE).
19. Raffel Marty: Cloud Application Logging for Forensics, 978-1-4503-0113-8/11/03..$10.00,ACM.
20. Shams Zawoad, Amit Kumar Dutta, Ragib Hasan: secLaaS: Secure Logging-as-a-Service for Cloud Forensics, 978978-1-4503-1767-2/13/05..$15.00, ACM.
21. Saibharath S, Geethakumari G: Cloud Forensics: Evidence Collection and Priliminary Analysis, 978-1-4799-8047-5/15/$31.009©2015 IEEE.
22. Ben Martini, Kim-Kwang Raymond Choo: An integrated conceptual digital forensic framework for cloud computing, 1742-2876/$ – see front matter ª 2012 Elsevier Ltd. All rights reserved. http://dx.doi.org/10.1016/j.diin.2012.07.001
23. Fei Ye1 Yunzhi Zheng1 Xiao Fu1 Bin Luo1 Xiaojiang Du2 Mohsen Guizani3: TamForen: A tamper-proof cloud forensic framework, Trans Emerging Tel Tech. 2020;e4178, © 2020 John Wiley & Sons, Ltd.
24. M. Edington Alex a , R. Kishore: Forensics framework for cloud computing, 0045-7906/©2017 Elsevier
25. Gayatri S. Pandi and K. H. Wandra: Secured Forensic Framework for Various Users in the Virtualized Environment of Cloud, © Springer 2020 https://doi.org/10.1007/978-981-13-7166-0_72