International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218327

Cyber Crime Investigation and Preventing in Reference for Cloud Forensics : A Review

Kinjal Bhagariya, Dr. Ravi Sheth, Ms. Dharati Dholariya
School of Information Technology, Artificial Intelligence and Cyber Security Rashtriya Raksha University, Gandhinagar, Gujarat, India

Article Info
Volume 8, Issue 3
Page Number: 205-210

Publication Issue :
May-June-2021

Article History
Accepted : 20 May 2021
Published: 30 May 2021

ABSTRACT

We are aware that cloud computing evolves as a transformative and No Doubt helpful field for futures generations on account of its several economic benefits in each domain as well as commercial, public, governmental, organizational, etc. Cloud forensics one of the most important areas within the developing field is that the means that investigators conduct researches in the relevant ways in which a digital crime took place over the cloud. This area is known as cloud forensics. Cloud forensics is a relevant field that works on all of this problem. This paper gives an overall research perspective of cloud forensics including its logging measures that need forensics challenges and what is the help of the cybercrime investigation and preventing for cloud forensics and the currently available solutions.

Keywords : Crime, Cloud Forensics, Cloud Computing, Security, Digital Investigation, Crime Preventing

I. INTRODUCTION

National Institute of Standards and Technology has identified 65 cloud forensic challenges in its report published in 2014. Furthermore, the report has highlighted that conventional digital forensic tools and procedures can no more be used in investigating incidents occurring in the cloud. As a result of this, new process models that can guide procedures for conducting cloud forensic investigations are required.

A. Cloud computing:

Cloud computing has become a popular approach for data processing and storage. On this basis, cloud forensics is the intersection between cloud computing add network forensics. It mainly aims cloud base investigation and the prevention of cloud forensics. Cloud computing is a continuously growing and emerging technology. The hardware and software resources that provide diverse services over the network of the internet to deal with the user requirements are called “cloud”. Here resources seek advice from computing applications, software packages,virtual servers, and computing infrastructure. Cloud computing eliminates the costs and complexity of buying, configuring, and managing the hardware and software. The cloud framework mainly provides three categories of service Iaas (infrastructure as a service), Paas (Platform as a service), SaaS (Software as a service). The four well-known deployment

models used in cloud computing are public Cloud, private Cloud, Hybrid Cloud, and Community Cloud. Simply put, cloud computing is the delivery of computing services –including servers, storage, databases, networking, software, analytics, and intelligence-over the internet("the cloud ") to offer faster innovation, flexible resources, and economies of scale. You typically pay just for cloud services you use, helping tower your operating costs, run your infrastructure more efficiently scale as your business needs modification.

B. Cloud Forensics:

National Institute of Standards and Technology (NIST) [1] states "Cloud computing forensic science is that the application of scientific principles, technological practices and derived and tested methods to reconstruct and derived and tested methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of digital evidence". The most important of cloud forensics is describes by the author in 3 completely different aspects significantly technical, structure, and legal. The Technical aspects include the forensic tools, forensic mechanisms, and procedure for application of the forensics methodology in cloud computing which includes data acquisition method, evidence segregation, virtualization, and proactive measures. The author also identifies cloud forensics as an associate degree information base space between cloud computing and digital forensics.

C. Digital Forensics:

It is believed that digital forensics, as an associate freelance field, was developed once the late 90s when the number of computer crimes increased as a result of the Internet's surging popularity. Palmer was the first to define digital forensics. He said that digital forensics is the process of analyzing electronic information that is stored in multiple digital machines to work out and reconstruct the sequence of events that cause a selected incident.

The Many challenges known as the NIST working present into 9 categories [2]:

• Architecture :

Architecture challenges in cloud forensics include coping with variability in cloud architectures between providers; tenant data compartmentalization and isolation throughout resource provisioning; a proliferation of systems, locations, and endpoints that may store data; accurate and secure provenance for maintaining and preserving the chain of custody; infrastructure to support the seizure of cloud resources while not disrupting alternative tenants, etc.

• Data collection:

Is the acquisition stage, namely the stage of taking raw sources to be analyzed and extracted?

Examples, contents of memory, contents of hard disk, data traffic on the network, etc.

• Analysis

Analysis challenges in cloud forensics include correlation of forensic artifacts across and within cloud providers; reconstruction of events from virtual pictures or storage; metadata of integrity; The Analysis of the timeline using log data timeline analysis of log data including synchronization of timestamps; etc.

• Anti-forensics – hiding or obscuring data

Anti-forensics are a set of techniques used specifically to prevent or mislead forensic analysis. Challenges in cloud forensics include the use of obfuscation, malware, information activity hiding, or many other techniques to compromise the integrity of evidence; malware might Deterred virtual machine isolation methods etc.

• The trustworthiness of first responders to an incident:

Incident 1st responder challenges in cloud forensics embrace confidence, competence, and trustworthiness of the cloud providers to act as first-responders and perform data collection; difficulty in performing initial triage; processing a large volume of forensic artifacts collected; etc.

• Roles of data owners, managers, and users :

Management challenges in cloud forensics contain uniquely identifying the owner of the associate account; decoupling between cloud user credentials and physical users; easy obscurity and making fictitious identities online; determinative actual possession of data; authentication and access control; etc.

• Legal jurisdictions:

Legal challenges in cloud forensics contain identifying and addressing issues of jurisdictions for legal access data; lack of effective channels for international communication and cooperation during an investigation; data acquisition that relies on the cooperation of cloud providers, as well as their competence and trustworthiness; missing terms in contracts and service level agreements; issue subpoenas while no data of the physical location of data; seizure and confiscation of cloud resources may interrupt business continuity of other tenants;

• Technical standards and practices:

Standards challenges in cloud forensics include lack of even minimum/basic SOPs, practices, and tools; Lots of interoperability among cloud providers; lack of test and validation procedures; etc.

• Training:

Training challenges in cloud forensics include misuse of digital forensic training materials that do not apply to cloud forensics; lack of cloud forensic training and expertise for both investigators and instructors; limited knowledge by record-keeping personnel in cloud providers about evidence; etc.

Future work:

The rest of the challenges in cloud forensics are organized based on the forensic process in a cloud computing environment introduced in [3] and as follows; data collection, live forensics, evidence segregation, virtualized environments, and proactive measure. The challenge regarding the legal issue in digital evidence in a cloud environment was added and solve problem.

The Challenges implement to cloud computing and its implementation cyber forensic framework.

- I am using Tool testing Cloud flare.
- Cloud Flare using the cloud forensic service provider and its limitation check.

II. Literature Survey

Several valuable studies have attempted to investigate digital forensic and cloud forensics and these will be discussed below:

Kristyan, S. A et al. [4] (2020) Cloud computing technologies are one of the most developed knowledge fields today. However, the rapid growth of cloud computing has made cybercrime crime grow. This poses new challenges to investigating. This Model provides various data of the investigation process framework which is incredibly useful to research which the prevailing framework or methodology is effective in looking for manual proof that needs human involvement in each stage. In this process framework to main aim to reduce human interaction reduce at every stage.

Moussa, A et al [5] (2019) In the process of cloud forensic investigation, the roles and responsibilities of cloud consumers and cloud providers do not have clear delineation. Nevertheless, Consumers are responsible for collecting and analyzing data from their adopted cloud services for forensic purposes, thus, should have processes in place to identify, prioritize and collect data from cloud components

that they are responsible for. In the model, the authors have proposed steps that can minimize the large volume of data resulting from investigating cloud instances. In the live forensic procedure separation and correlation, processes are solutions to issues arising from the large volume of data in the cloud.

Sapna S. S [6] (2019) recently, organizations have made great efforts to migrate their infrastructure to the cloud environment. This makes the cloud a high-value target for malicious actors. Analyzing a compromised cloud instance requires the use of digital forensics that follows a scientific process to support or disprove the hypothesis. The purpose of the research is to look at the potential gaps in the current process and attempt to create a framework that standardizes digital forensics within cloud environments.

Zhang, Y et al. [7] (2017) with the rapid popularity of cloud computing, cloud forensics had become a research focus. However, compared with traditional digital investigation, cloud forensics faces more complex challenges. It is used for a chain of custody method. Traditional investigative approaches and digital forensics tools become less efficient, like the capability to provide required results on time and within resource constraints. One promising option for Cyber Crime Investigations is to use computational forensics based on advanced data analytics to prevent and combat cybercrime.

Hemdan, E. E. D. et al. [8] (2016) In recent times, cloud computing has become one of the essential computing paradigms. This can be thanks to the data security issues where cybercrimes are representing a real problem for them because of the huge damage that can cause. This process is facing complex challenges due to the dynamic nature of cloud computing. The Digital forensic is investigation process in the steps of the performing. This strategy is based on using enormous processing and storage cloud computing capabilities to handle and manage the digital evidence in a short time. This can be done by placing a forensic server on the cloud side.

Katilu, V. M et al. [9] (2015) Cloud computing has become a popular approach for data processing and storage. In this paper has reviewed current provenance collection approaches implemented in all three layers of the cloud architecture; the disadvantages of each approach have been highlighted. The minimum needs necessary for effective source assortment for cloud forensics and challenges of provenance collection have been presented and mentioned.

Research paper	**Featured Work**	**Classified Used**	**Limitation**	**Advantages**
Design Framework Forensics Readiness as a Service for Automatic Processing 2020.	Develop a forensics readiness platform on the cloud based on the cloud forensics readiness as a service model.	Maximize the use of digital evidence so that readiness can be achieved.	Is the implementation of the framework cloud computing device is very difficult?	It can make maximum use of evidence so that it can speed up investigations without disrupting business processes.
A Consumer-Oriented Cloud Forensic Process Model – 2019	Live forensic in cloud forensics. As a result, none of these models can fully cover	Live forensics investigator Methodologies That suits IaaS cloud	In the live forensic procedure separation and correlation, processes are	In the live forensic procedure as solutions to issues arising from

	the requirements identified.	forensics.	solutions to issues arising from the large volume of data in the cloud.	the large volume of data in the cloud.
FoRCE (Forensic Recovery of Cloud Evidence): A Digital Cloud Forensics Framework - 2019	1.Instantaneous memory and data acquisition utilizing Security Orchestration, Automation and Response (SOAR) 2.Adaptability to new cloud technologies	A qualitative method is used to get a more in-depth understanding.	The design of the framework depends on the capacity and specifications of the cloud service provider.	The framework focused on the isolation, collection, and preservation of the cloud instance so it can be used as evidence for analysis.
A Blockchain-based Process Provenance for Cloud Forensics - 2017	We will try to remove central nodes such as CA and PA. Through designing consultation mechanisms, complete the CA and PA	Anti-tampering and privacy preservation. Blockchain technology	With the existence of central management nodes (CA and PA), the system is too dependent on the honest performance of central nodes.	That no sensitive information leaks during the blockchain-based process provenance operation.
	functions depend on all nodes in the system.			
A Cloud Forensic Strategy for Investigation of Cyber Crime – 2016	In future work, we will all the strategies provide in cloud forensics.	This strategy can be as guided by the digital investigators and practitioners to follow it in performing the cybercrimes investigation.	All these challenges make the investigation process in the cloud environment, not an easy process	1..Reduce evidence acquisition time. 2.Decrease time to access protected documents
Challenges of Data Provenance for Cloud Forensic Investigations- 2015	Improving data provenance for cloud forensics.	Helping to identify properties necessary for cloud provenance. Various provenance collection solutions have been proposed based on different layers.	The method is implemented but this is high tolerance and scalability demand.	It is used Three-layer architecture. And using seize method .it is a very slow investigation process.

III.CONCLUSION

Cloud consumers and cloud providers need to work compelled to create an environment that will support the investigations to an extreme level when criminal incidents occur. There are many techniques to solve the challenges which are proposed by some researchers. This paper primarily concentrates on however these challenges in cloud forensics will be round-faced. How to solve the cases and to overcome the challenges and follow steps to induce the shreds of evidence during investigations are mentioned. There are still unsolved challenges and problems on which the researchers are working. Here many challenges and their solutions can be viewed and analyzed.

IV. REFERENCES

[1]. Moussa, A. N., Ithnin, N., Almolhis, N., & Zainal, A. (2019, August). A Consumer-Oriented Cloud Forensic Process Model. In 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC) (pp. 219-224). IEEE.

[2]. NIST Cloud Computing forensics Science working Group Information Technology Laboratory

[3]. Chen, G., Wu, D., Chen, G., Qin, P., Zhang, L., & Liu, Q. (2019, December). Research on Digital Forensics Framework for Malicious Behavior in Cloud. In 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (Vol. 1, pp. 1375-1379). IEEE.

[4]. J. Stachowski, Implementing Digital Forensic Readiness: From Reactive to Proactive Process. 2016.

[5]. Sampana, S. S. (2019, January). FoRCE (Forensic Recovery of Cloud Evidence): A Digital Cloud Forensics Framework. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 212-212). IEEE.

[6]. Zhang, Y., Wu, S., Jin, B., & Du, J. (2017, December). A blockchain-based process provenance for cloud forensics. In 2017 3rd IEEE International Conference on Computer and Communications (ICCC) (pp. 2470-2473). IEEE.

[7]. NISTIR D. 8006 (2014) NIST Cloud Computing Forensic Science Challenges accessed at http://csrc. nist.gov/publications/drafts/nistir8006/draft_nistir_8006. pdf Gary Palmer (2001), "A Road Map for Digital Forensic Research"[R]. Technical Report DTR-T001-01, DFRWS, Report From the.

[8]. Katilu, V. M., Franqueira, V. N., & Angelopoulou, O. (2015, August). Challenges of data provenance for cloud forensic investigations. In 2015 10th International Conference on Availability, Reliability, and Security (pp. 312-317). IEEE.

[9]. R. K. L. Ko, P. Jagadpramana, and B. S. Lee, "Flogger: A Filecentric Logger for Monitoring File Access and Transfers within Cloud Computing Environments," in In Proceedings of the 10th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE Press, 2011, pp. 765–771.

Cite this article as :

Kinjal Bhagariya, Dr. Ravi Sheth, Ms. Dharati Dholariya, "Cyber Crime Investigation and Preventing in Reference for Cloud Forensics : A Review ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 205-210, May-June 2021. Available at

doi : https://doi.org/10.32628/IJSRSET218327

Journal URL : https://ijsrset.com/IJSRSET218327