International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 312-314, October-2023
https://doi.org/10.47001/IRJIET/2023.710041

Challenges of Digital Forensic in Cloud Computing

[1]Prof. Sunita K. Totade, [2]Tushar R. Salphale, [3]Shweta V. Tungar, [4]Prashik V. Waghmare, [5]Mohit D. Joshi

[1]Assistant Professor, Department of MCA, Vidya Bharati Mahavidyalaya, Amravati, India
[2,3,4,5]Student, Department of MCA, Vidya Bharati Mahavidyalaya, Amravati, India

***Abstract* - Cloud services are becoming the most promising technology of recent days. It provides scalable, flexible services to many users at the same time and it helps to quickly access resources from the cloud service provider. Digital forensics is part of the computer forensic science. Various cloud issues block the cloud forensics process, so there is no standard framework for cloud forensics can be drawn. This article summarizes the challenges, various challenges are also discussed in this article at each stage of cloud forensics in cloud computing.**

Keywords: Cloud Computing System, Cloud Forensics, Digital Forensics Process.

1. Introduction

Cloud technology enables convenient use when needed use of computing resources with minimal management work and communication with the service provider. Virtualization and the nature of multithreading the cloud offers better utilization of resources and exists basic cloud computing functions, but they do the main problems of the cloud. But with any new technology, security comes into play about whether the technology in question has good protection and privacy The implementation of this technique is very simple, but some techniques such as cloud computing, digital forensics and the cloud forensics is more useful in today's world, but less so it takes a lot of time to implement the security of these technologies. Digital forensics is a part of computer forensics. The identification, collection, analysis and presentation digital evidence called digital forensics. In this paper we discuss the challenges of each stage for digital forensics in a cloud computing environment.

2. Challenges of Cloud Forensics

This section presents the challenges in every phase of cloud forensics.

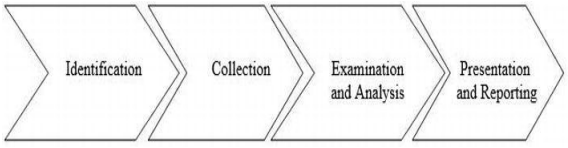

Figure 1: Cloud forensic process flow

1) Identification

The identification phase mainly defines the goal and the research process. Crime detection is an initial step in the digital research process model. Detecting malicious activity is easy the recognition phase. The most important thing here is how we say it is it a crime traditionally in digital forensics investigators detect crime in the following ways:

- If someone has made a complaint.
- Due to anomalies detected by the intrusion detection system.
- During the computer system audit.

Challenges:

i) Using evidence in logs:

Decentralized nature the cloud makes it difficult to identify the data. Availability of log files depends on maintenance cloud model. In SaaS, there is more to identify PaaS difficult due to limited access, detection is better in IaaS but not full access.

ii) Persistent data:

Cloud is essentially volatile, volatile data means that when the device is turned off, all data will be lost deleted in the same way in the cloud when the VM is completely powered off data is lost if it is not saved somewhere. RAM may contain valuable evidence such as username, passwords and encryption keys. Because RAM capacity increases and RAM memory increases use of data encryption.

iii) Lack of cloud management:

This is a subscription network connection to a common set of resources and resources are virtual in nature, namely physical no cloud ever knows the location of the resource user.

iv) Lack of customer awareness:

Everything is down in the cloud there is little control over the CSP and cloud user interaction with CSP is sometimes absent. CSP lack of transparency and little international regulation leads to the loss of important terms in relation to forensic investigations at the service level agreement (SLA). This problem affects all three service models.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 10, pp 312-314, October-2023

https://doi.org/10.47001/IRJIET/2023.710041

2) Collection and preservation of evidence

Evidence gathering collects evidence of what has been identified sources of evidence. The evidence collected must be maintained Data Retention is the maintenance of data integrity raw data should not be changed until the study is completed. In the traditional system, the research process starts by grabbing and taking the system hard drive a bit clever copy to keep the same integrity system but, in the cloud, it is practically impossible because evidence is intrinsically intact and changeable.

Challenges:

i) Data Integrity:

Researchers must maintain integrity of evidence maintains integrity raw data is very difficult for a cloud researcher. Data integrity is a complex part of the entire cloud process forensic data, as there is no need to change the original data the evidence is presented to the law.

ii) Cloud Situation isolation:

When a criminal incident occurs in the cloud, in the cloud case, and in collected evidence the cloud instance must be isolated for digital research. Isolation prevents possible corruption and contamination of collected evidence. Isolated cloud the example helps maintain the integrity of the evidence collected from the cloud case.

iii) Digital provenance:

This is an important feature of forensic science digital history descriptive studies object A secure origin system was proposed which performs reliable evidence of digital forensics in a cloud environment. This formula proves this cloud the evidence is admissible in court.

iv) Chain of Custody:

In the traditional research process scientists must create and preserve supply chain. The chain of descent is documentation from the testimonies collected, as who collects evidence, when and how evidence is preserved and by whom. Researcher required maintaining a proper chain of custody beforehand it documents.

3) Examination and Analysis

Once in a digital imaging process (DIP) model. Information is collected and stored using various research techniques and there are several software tools to help researchers FTK (Forensic Toolkit). All these tools are available to filter and search for pattern matching content or files or file types. Using these tools, one deleted or modified data can be restored. During the analysis stage, the evidence must be evaluated. The evidence obtained in the analysis phase is confirmed compare with alternative evidence confirm that evidence has not been changed. Research and the analysis phase of cloud expertise is similar digital forensics phase of investigation and analysis.

Challenges:

i) Lack of cloud forensics tools:

Cloud Forensics is cloud driven, Currently, there are mostly no cloud forensics tools cloud researchers use digital forensics and the web forensic tools in one cloud, but they are not adequate cloud expertise differs from digital and online in criminology never study these tools in the cloud is not enough. Many cloud researchers beginning to explore cloud-based forensics technology and some tools are already in place use, but we need better tools.

ii) Correlation of evidence from multiple sources:

In the cloud one resource is shared between cloud users. Evidence also comes from several sources that bring various problems to researchers.

Presentation:

The gathered evidence in the digital investigation process is needed to be submitted in the court of law to prove the crime. At the end of investigation, the investigator needs to present a report and it must be useful for cross- examination. The result report should be used by an organization to improve their security policy and must be documented for future investigation.

3. Research Methodology

Cloud Forensics is the process of analysing and gathering evidence from cloud-based systems and infrastructure for a legal investigation or security breach. As the use of cloud technology increases, so does the need for cloud-based forensic tools and techniques.

It is a complex and challenging field due to the dynamic and distributed nature of cloud computing. By developing new techniques, researchers can help investigators collect and analyse evidence from cloud environments more effectively.

It is important to note that cloud forensics investigation process can vary depending on the specific investigation.

ISSN (online): 2581-3048
Volume 7, Issue 10, pp 312-314, October-2023
https://doi.org/10.47001/IRJIET/2023.710041

4. Conclusion

In this paper, we discussed the technical challenges of implementation digital forensics in the cloud environment and presented requirements for forensic data from the cloud. There are many things that can be done to improve cloud computing for digital forensics. The collection is reliable proving the cloud is difficult because we have very little control clouds compared to traditional computer systems. This paper presents different challenges of digital forensic in cloud computing with the help of cloud forensic process flow. With each phase it describes the challenges in cloud. Digital forensic refers to investigations that are focused on challenges that occur primarily involving in cloud.

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] K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," in proceedings of the 7th IFIP International Conference on Digital Forensics, 2011.
[3] https://www.researchgate.net/publication/351049927_Recent_Challenges_in_Digital_Forensics
[4] https://www.intechopen.com/chapters/64377
[5] https://www.mailxaminer.com/blog/current-challenges-in-digital-forensics-investigations/

Citation of this Article:

Prof. Sunita K. Totade, Tushar R. Salphale, Shweta V. Tungar, Prashik V. Waghmare, Mohit D. Joshi, "Challenges of Digital Forensic in Cloud Computing" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 10, pp 312-314, October 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.710041

****

