International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST2182118

Analysis of Cloud Forensics : Review and Impact on Digital Forensics Aspects

Mamta Khanchandani[1], **Dr. Nirali Dave**[2]
[1]Assistant Professor, C. B. Patel Computer College, V.N.S.G.U., Surat, Gujarat, India
[2]Associate Professor, BMCCA (BMU), Surat, Gujarat, India

Article Info
Volume 8, Issue 2
Page Number : 639-646

Publication Issue
March-April-2021

Article History
Accepted : 25 April 2021
Published : 30 April 2021

ABSTRACT

Digital forensics is the science of finding evidence to digital crimes and attacks. Cloud Forensics is a part of Digital Forensics that watches over the crime that has taken place over the cloud and carries out an investigation on it. Cloud computing is an evolutionary technology based on a huge network, which spreads globally. Hence, Cloud Forensics is a part of Network Forensics, which in turn is a part of Digital Forensics. Cloud organizations along with the providers of cloud service and customers that uses cloud service, are still awaiting the establishment of an explicit forensic revolution. Without the much-needed forensic capability, they will not be able to safeguard the robustness of their system and suitability of their services that assist criminal and cybercrime investigations. In this paper, we review the forensic process, challenges in cloud forensics, and its impact on digital forensics.

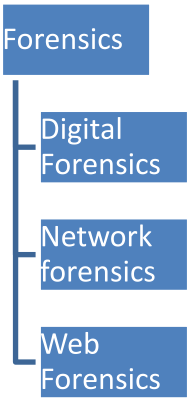
Keywords : Cyber Crime, Digital Forensic, Network Forensic, Cloud Forensics.

I. INTRODUCTION

In today's world, the Internet and other developments in the digital world have become broadly fragmented regarding how it is used. Browsing the web for information, watching videos and listening to music or using tools like e-mail, instant messaging or social platforms like Twitter or Facebook are nowadays some of the core uses of people across the globe[1]. The "dark side" of the Internet is apparent in everyday news. Spam, underground marketplaces, identity theft, password breaches, phishing and many other attack vectors as well as exploitation techniques are active trends in web-based interaction. Users give more and more of their private data to companies that use them to generate revenue, although many of these companies struggle to adequately protect their users' data. There are trust and confidentiality issues because of malicious methods and tools used to extract private information. Under such circumstances, digital forensics is used by entities like law enforcement, investigators and system administrators that help in restructuring the order of events and identifying traces of evidence left behind. Digital forensics as defined is the application of science to the law, in particular, **"the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data."** Digital forensics has received significant attention in recent years because of the vast increase in digital crimes. The increased cyber-attacks in today's technology-driven society have also increased the need for digital evidence in courts. Crime offenders should be held liable on a priority basis. The process used to solicit this digital evidence to be represented in courts is digital forensics. This process help courts, law enforcement agencies and investigators to obtain valuable evidence that can withstand the rigors of a courtroom. The current approach of obtaining evidences has two major shortcomings: a) the suspect's device, which is seized, has to be made available to the investigators and b) the traditional methods of data storage, information sharing and communication have been extended by the latest emerging online services. Law enforcement agencies can ask service operators to release certain information, but they are usually not obliged to request answers from other countries. As such, Digital forensics is a new field still developing in its infancy stage[2].

TYPES OF FOREnSICS

The forensic process is a process that is initiated after the crime occurs. It includes a series of investigation methods [12], procedures and techniques related to various crimes and the acquisition of evidence. Let us dive into the classification of forensics:



Types of Forensics (Figure 1) 1

Dig

Standards and Technology (NIST) standards, it is the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. "Digital Forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data." NIST 2011 – The NIST Definition of Cloud Computing [3].

Types of Digital Forensics

1) Static forensics: It is a traditional and most widely used approach to digital forensics[4]. It has defined procedures and the evidence collected has legal validity. Here, forensically-approved copies of the storage media are made. Various media analysis tools are further used to locate files and search their content for evidence. File creation and modification times can be established. Deleted files, browsing history, e-mail and other installed programs can be recovered. Here, forensic evidence is obtained by using different external devices like USBs, external hard drives, etc. or CD, DVDs and then the evidentiary data collected is brought into the forensic laboratory for investigators to perform various operations/steps forensically. But the biggest limitation is that it does not provide an entire picture of events.

2) Live Forensics:It is that approach to digital forensics which examines and analyse a case related to a live scenario. In live digital forensics, information is collected, examined, analysed and reports are generated. The tools used for live forensics can provide very clear pictures of knowledge such as memory dumps, various running processes, and open network connections. Thus, live forensics keeps the consistency and integrity of forensic data intact. It maintains the originality of evidentiary data without any tampering or losses. The problem with live

forensics is, by its temporal nature, it will not be able to reproduce the same results if required [5].

3) Network forensics: It is that approach to digital forensics related to monitoring, capturing, storing and analysis of LAN or WAN to extract crucial information and legal evidence to present in the court, identify the source of intrusion and security attacks. It fetches information on which network ports are used to access the information.

4) Web forensics: It is that approach to digital forensics [6] related to monitoring, capturing, storing and analysis of LAN or WAN to extract crucial information and legal evidence to present in the court, identify the source of intrusion and security attacks. It fetches information on which network ports are used to access the information.

5) Cloud forensics: Cloud Forensics is a part of Digital Forensics that watches over the crime that has taken place over the cloud and carries out an investigation on it. It gathers and preserves evidence in a way that can be presented in a court of law. Since the evidence is located in different geographical areas, it is harder to identify the data in cloud infrastructure. System log, user authentication log, database log, application log are few instances of evidence sources.

6) Mobile forensics: This branch deals with the recovery of electronic evidence from mobile phones, smartphones, SIM cards, call logs, SMS/MMS, Audios and Videos, GPS devices, tablets and game consoles. Nowadays, mobile phones are the most common source of digital evidence found at crime scenes. The information retrieved from mobile phones helps in the forensic investigation mainly to establish a connection between crime and criminal.

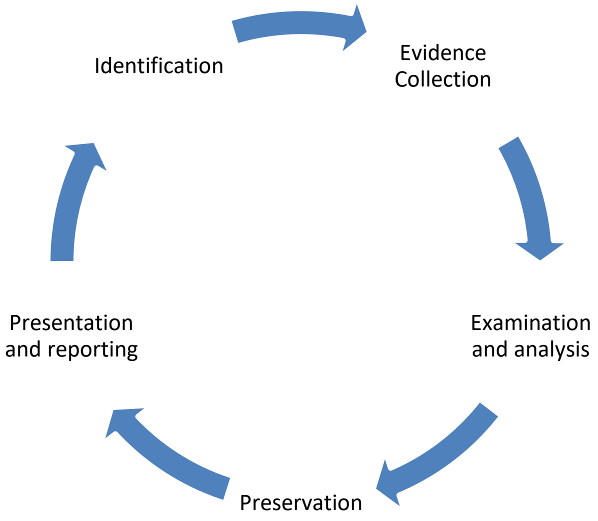
Cloud forensics

In recent years, Cloud Computing has received major importance [7] . It has been introduced to provide optimum help to forensic experts as it offers massive pool resources, cost-effective solutions, dynamicity and wide access for storage. Hybrid, private, and public models of cloud computing exists, in addition to multiple services, such as security as service, database as service, integration as service, and software as service. Cloud forensics is also helpful to optimize the general usage of IT infrastructures [8]. Most companies and organizations transfer their products and services across the cloud every day due to multiple benefits, including high scalability, reduced cost of IT infrastructure, business continuity, and access to automatic updates. As a result, cloud computing has been accepted with open hands in both public and private companies [9]. However, the number of crimes has substantially increased across the globe. According to NIST [10], **“Cloud forensics is the application of digital forensics in cloud computing as a subset of network forensics to gather and preserve evidence in a way that is suitable for presentation in a court of law.”** They have servers across the globe to host customer data. When a cybercrime occurs, legal jurisdiction and the laws governing the region throw unique challenges [11]. A court order issued in a jurisdiction where a data centre is residing likely will not apply to the jurisdiction for a different host in another country. In modern CSP environments, the customer can choose the region in which the data will reside, and this should be chosen carefully. The main concern for an investigator is to ensure the originality and integrity of digital evidence so it can be presented in a court of law. In some cases, CSPs will deliberately not disclose the details of the logs from customers. In other cases, CSPs have protocols where they cannot provide services to collect logs. The security team has no control as to whom the CSP will choose to collect digital evidence. If they are not trained according to a forensic standard, the chain of custody may not be eligible for admission in a court of law. Cloud computing is a well-defined technology based on a huge network, which spreads globally[14]. Hence, Cloud Forensics is a segment of Network Forensics, which in turn is a part of Digital Forensics [15]. Cloud organizations along with the providers of cloud service and customers that uses cloud service, are still awaiting the establishment of an explicit forensic revolution. Without the much-needed forensic capability, they will not be able to safeguard the robustness of their system and suitability of their services that assist criminal and cybercrime investigations. Cloud computing is the future. Cloud computing has become a new battlefield for cyber-crime where every day new challenges emerge to safeguard the cyber-attacks [13].

Cloud Forensics is considered a cross-discipline between Cloud Computing and Digital Forensics [16]. It is necessary to understand that it is a multi-dimensional issue. There are three main dimensions involved in Cloud Forensics: Technical, Organizational and Legal. The technical dimension presents various methods, procedures and tools, which are used to carry out the digital forensics process in cloud environments. The organizational dimension states that Cloud Computing consists of two entities: CSPs and cloud customers. There is a possibility that CSPs may outsource their services to other CSPs. The legal dimension stresses on multi-jurisdiction and multi-tenancy challenges. Existing regulations have to be followed for forensics activities to not breach any confidentiality measures. Cloud Computing is a new dimension in computing that is just as amusing to some as it is exciting to so many.

Cloud forensic process flow

The cloud forensic process flow is shown in Figure 1, which is described as follows:



Cloud Forensic Process(Figure-2)

Identification: The investigator identifies potential criminal activities if they have taken place or not. The crimes may include complaints filed by individuals, audit trails, suspicious events detected by IDS, etc.

Evidence collection: The investigator collects shreds of evidence from cloud service models like SaaS, IaaS and Paas without jeopardising its integrity as per the forensic standards [17]. The SaaS service model examines the data of each user through log files such as access log, application log, error log, data volumes, transaction log, etc. The IaaS service model examines the data such as system-level logs, raw machine files, backups, storage logs, etc. The PaaS service model examines the data of application-specific logs through API, malware software warnings, operating system exceptions, etc. All the collected evidence has to be preserved safely without it being tampered with for further investigation that can be done through a legal order to the cloud service providers. It is possible that data preservation will require large volumes of storage. The investigator addresses data preservation and privacy rules on the stored evidence [18].

Examination and analysis: the analyst examines the evidence information collected in the previous step by some forensic tools. The criminal data is merged, correlated and assimilated to produce a reasonable conclusion. The analyst analyses the data from the physical as well as logical files wherever they reside. There might be a need to share the testimony with the Law enforcement agencies or the victim organisation or an individual.

Preservation: All the collected evidence has to be preserved safely without it being tampered with for further investigation. All the log files need to be preserved since the information is located in different geographical areas.

Presentation and reporting: Finally, the investigator prepares a formal organised report about the findings of the case to be presented in the court of law.

II. LITERATURE REVIEW

Ruan et al. revealed, **"A procedure and a set of toolkits to proactively collect forensic-relevant data in the cloud are important".** It clearly shows that cloud forensic is advantageous to cloud environments in terms of an enhanced security level. An additional organizational dimension was discussed by Ruan et al. (2011) has discussed the possibility of integrating digital forensics in an organization to respond to cloud-based incidents [17].

Marco et al., Pangalos and Katos, Alenezi, et al., agree that **"cloud forensics help organisations improve their security strategies, be prepared for any attack, and reduce the number of security incidents".**

Moussa et al. proposed a study that states, **"IaaS consumers can utilize the framework to establish how they should gather the necessary digital evidence without having to rely on cloud providers".** However, the study is to be verified.

Ab Rahman et al. proposed a forensic-by-design framework for cyber-physical cloud systems (CPCSs). It demonstrated **"the design of a CPCS is based on the goal of simplifying and increasing the efficiency of forensic investigations."** The forensic-by-design framework is supposed to assist in digital investigations[19].

Dykstra et al. stressed on the importance of trust in cloud services so that a judge in the court of law can decide the trustworthiness of the evidentiary data.

Trenwith and Venter presented a noteworthy approach that helps reach digital forensic readiness in a cloud environment. This model proposed that a central logging facility that speeds up data gathering should be used.

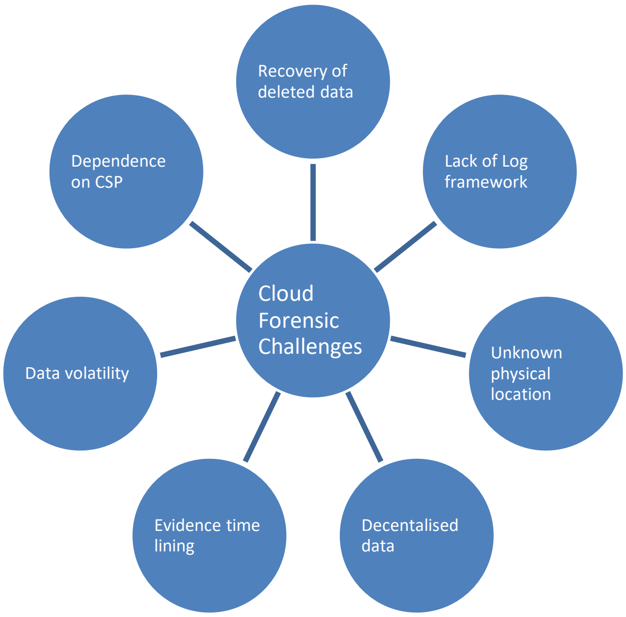
Ezz El-Din Hemdan and D. H. Manjaiah proposed a Digital Forensic accession for probe of Cybercrimes in a Private Cloud Environment. They came up with an experimental environment to introduce the forensic process in the private cloud. The most essential steps in the cloud forensic process are Data acquisition and collection from the Virtual machines [20]. They popularized live forensics and a dead forensics approach to investigate virtual machines in the private cloud environment.

M. Edington Alex, R. Kishore et.al. Highlighted some challenges faced by an investigator. In most of the research work, investigators need to rely on CSP so CSP can modify data and this can affects the complete investigation process. After securing permission from the international telecommunication union (ITU), they proposed a solution called forensic monitoring plane (FMP) implemented outside of the cloud premises to mitigate the dependency on CSP.

III. ISSUES AND CHALLENGES IN CLOUD FORENSICS

- Physical inaccessibility: Different jurisdiction distribution is an issue because data resides in different geographical locations.
- Lack of international collaboration in cross-nation data exchange.
- Lack of law advisory and regulations.

- Decreased accessibility and control over forensic data at all levels. System administrators require relevant logs to troubleshoot the system and fix up the errors. Investigators need relevant logs for their concerned investigation.
- There is a chance that the evidence might be deleted in Cloud Forensics. It becomes a challenge to recover the deleted data and reconstruct it for evidence usage.
- Lack of forensic expertise.
- Each cloud server contains files from many users. It becomes hard to separate an individual user's data from the others.
- Dependence on CSP: Investigators depend on CSP to acquire logs. There is no evidence other than CSPs that links a given information file to a particular suspect.
- CSPs are into an agreement with other CSPs to use their services; this leads to loss of integrity and confidentiality of data in some cases.
- Integrity of the collected evidence has to be maintained to present it in an admissible manner in the court of law.
- Strong encryption methods are required to store evidence safely [21]



Challenges in cloud Forensic (figure 3)

IV. RESEARCH AND OBJECTIVES

New problems are arising every day in the area of digital forensics. Many researchers have proposed various new solutions to test the attacks in real-time situations to deal with the issues and challenges of cloud forensics. CSPs have not yet accepted those proposed solutions. Hence it becomes necessary to propose immediate research in the area of digital forensics. Investigators solely depend on CSP to collect evidence in the form of hard disk, log files, etc. because of inaccessibility. Cloud computing services enable few vendors like Amazon and Google to provide on-demand services to the users by renting out physical machines or by allocating software services. These issues concern both the public and private sectors. This paper aims to provide a better awareness of several areas of cloud forensics like analysis of cloud service usage, the effectiveness of acquisition methods, understanding of commercial cloud environments and investigation of cloud forensic management under the large umbrella of digital forensics. The research gaps and challenges are identified and explained.

V. CONCLUSION

Cloud forensics is becoming the need based on the alarming rise in cyber-attacks hence leading to growing concerns of security. Security is the most significant factor in computing. In cloud forensics, services are provided by virtual machines by some live forensics and dead forensics. Security mechanism is needed as cloud logs are spread across different virtual machines that the customer is not aware of. Cybercriminals exploit these sources to exhaust all the cloud resources. This paper presents forensic processes, techniques of evidence collection, various issues and challenges in cloud forensics during an investigation. The field of cloud forensics will continue to evolve as technology changes in the ever-changing areas of digital and multimedia sciences.

VI. REFERENCES

[1]. NIST Cloud Computing Forensic Science Working Group. Nist cloud computing forensic science challenges. No. NIST Internal or Interagency Report (NISTIR) 8006 (Draft). National Institute of Standards and Technology, 2014.

[2]. Al Sadi, Ghania. "Cloud computing architecture and forensic investigation challenges." International Journal of Computer Applications 124.7 (2015).

[3]. Zawoad, Shams, and Ragib Hasan. Digital forensics in the cloud. ALABAMA UNIV IN BIRMINGHAM, 2013..

[4]. Geetha, Vaithianathan. "About cloud forensics: Challenges and solutions." The International Journal of Distributed and Cloud Computing 3 (2015).

[5]. Neware, Rahul, and Amreen Khan. "Cloud Computing Digital Forensic challenges." 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2018.

[6]. Ahmed, Irfan, and Vassil Roussev. "Analysis of Cloud Digital Evidence." Security, Privacy, and Digital Forensics in the Cloud (2019): 301.

[7]. Muhammad Ubaid Ullah, Raja, et al. "The challenges of cloud computing in forensic science." International Journal of Computer Trends and Technology (IJCTT) 67.7 (2019): 40-48.

[8]. Haimbala, Joolokeni. Avoiding dark cloud: Secure storage and trusted computing. Diss. Ph. D. Thesis, University of Westminster, 2016, 73p, 2016.

[9]. Arafat, Md Yasir, Bipasha Mondal, and Sreeti Rani. "Technical challenges of cloud forensics and suggested solutions." Int. J. Sci. Eng. Res. 8.8 (2017): 1142-1149.

[10]. Sharevski, Filipo. "Digital forensic investigation in cloud computing environment: impact on privacy." 2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE). IEEE, 2013.

[11]. Ruan, Keyun, et al. "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results." Digital Investigation 10.1 (2013): 34-43.

[12]. O’shaughnessy, Stephen, and Anthony Keane. "Impact of cloud computing on digital forensic investigations." Ifip international conference on digital forensics. Springer, Berlin, Heidelberg, 2013.

[13]. Ruan, Keyun, et al. "Cloud forensics." IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg, 2011.

[14]. Miranda Lopez, Erik, Seo Yeon Moon, and Jong Hyuk Park. "Scenario-based digital forensics challenges in cloud computing." Symmetry 8.10 (2016): 107.

[15]. Kulkarni, G., et al. "Mobile cloud computing: security threats." International Conference on Electronics and Communication Systems. 2014.

[16]. Wu, Xu. "Context-aware cloud service selection model for mobile cloud computing environments." Wireless Communications and Mobile Computing 2018 (2018).

[17]. Wang, Ping, et al. "Clustering-Based Emotion Recognition Micro-Service Cloud Framework for Mobile Computing." IEEE Access 8 (2020): 49695-49704.

[18]. Djemame, Karim, et al. "Paas-iaas inter-layer adaptation in an energy-aware cloud environment." IEEE Transactions on Sustainable Computing 2.2 (2017): 127-139.

[19]. Li, Yibin, et al. "Intelligent cryptography approach for secure distributed big data storage in cloud computing." Information Sciences 387 (2017): 103-115.

[20]. Li, Yibin, et al. "Intelligent cryptography approach for secure distributed big data storage

in cloud computing." Information Sciences 387 (2017): 103-115.

[21]. Agarkhed, Jayashree, and R. Ashalatha. "An efficient auditing scheme for data storage security in cloud." 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE, 2017.

Cite this article as :

Mamta Khanchandani, Dr. Nirali Dave, "Analysis of Cloud Forensics : Review and Impact on Digital Forensics Aspects", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 2, pp. 639-646, March-April 2021. Available at doi : https://doi.org/10.32628/IJSRST2182118
Journal URL : https://ijsrst.com/IJSRST2182118