A Survey on Deploying Forensic Process as a service in Cloud Computing

[1]Dhara Prajapati, [2]Gayatre S. Pandi

[1]M.E.Student, Dept. of Computer Engineering,
L.J. Institute, Gujarat , India.
[2] *Professor, Computer Engineering, L.J. Institute, Gujarat, India*

ABSTRACT

As new technologies develop criminals find ways to apply these technologies to commit crimes. With the explosion of web technologies almost all major businesses in the world have web presence thus exposing their data to legitimate and illegitimate users. Computers have become intrinsic part of our lives. Businesses have streamlined their operation saving millions of dollars because of the web technologies and services. Computer evidences admitted in courts could be any file or fragment recovered from the storage devices such as email, browsing history, graphics, photographs, or application documents. Evidence may be recovered from any storage medium installed in digital equipment such as computers, cameras, PDAs, or cell phones. All forensic work should be done with care including documenting clear chain of custody in order for the evidence to be admissive in a court of law.

Keyword : - *Cloud Computing, Fraud Detection, Digital Forensic*

1. INTRODUCTION

Investigation that takes place after an incident has happened. Cloud computing is a new computing model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). This cloud model is composed of five essential characteristics, three service models, and four deployment models. One of the most important time frames in Computer forensics is the initial response to a computer related crime and how to identify important evidence necessary to make a legal case against perpetrator. Investigation that takes place after an incident has happened.Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime**.** This Survey paper summarizes the role of Digital Forensic easy to find fraud trace and find a perpetrator.

Computer forensics process (identification, collection, examination, analysis and reporting)

2. METHODS USED

CLOUD FORENSIC PROCESS: **Identification** *:* Identification is reporting misuse of cloud or malicious activity such as deleting files, illegal use of storing files and so on. **Collection/Acquisition and Preservation:** Preservation is the protection the protection of the integrity of the evidence throughout the investigation Process.

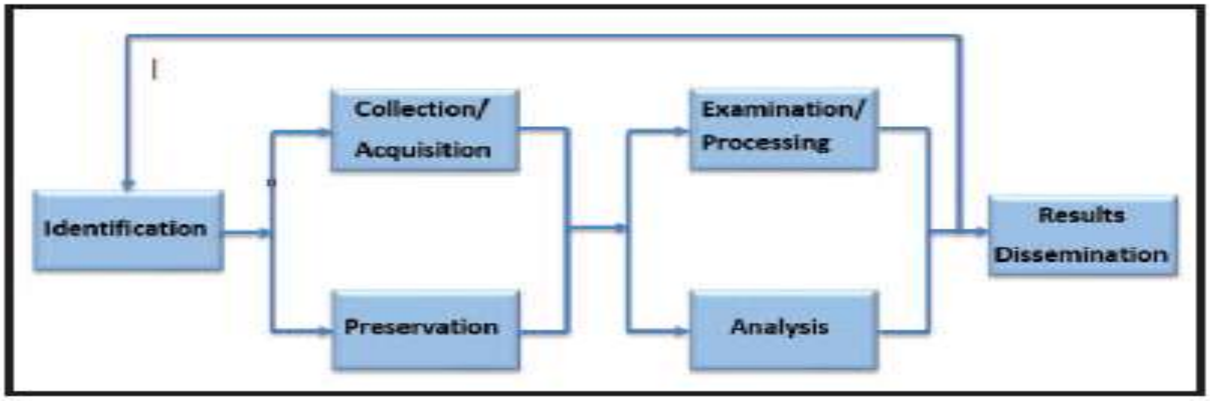

Fig-1: Forensic Process

Examination/Processing and Analysis Examination is defined as "Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity.

FORENSIC INVESTIGATION USING VM SNAPSHOTS AS EVIDENCE

Users can create VM of their choice from the available physical machines. In spite of users request, any cloud software like eucalyptus, Open Stack generates snapshots of a running VM continuously and stores it till the VM terminates. Maximum number of snapshots can be saved for a specific VM allotted. If maximum is reached older once are deleted.

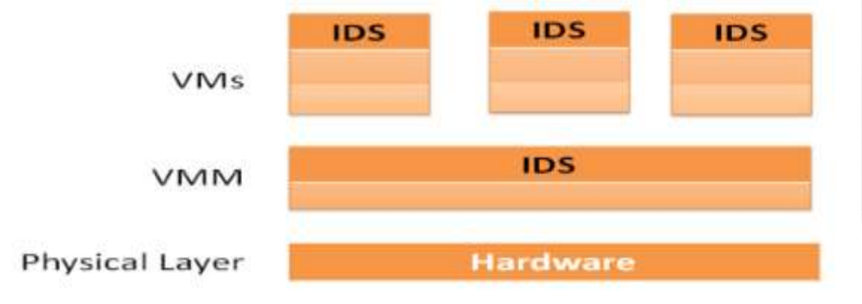

Fig -2: **Incorporating IDS at VMs and VMM**

Intrusion Detection Systems (IDS) are incorporated in all the VMs and VMM for monitoring malicious activities. Deploying, managing and monitoring the Intrusion Detection System is done by cloud service provider. The idea of I model is that the CSP stores. Snap shots of a VM whose activities are identified as malicious by an intrusion detection system. Simultaneously the CSP should be requested for log files of the suspected VM and the investigator collects and processes the log files to obtain the evidence

3. RELATED WORK

In [1] author has proposed Examining local machine and web browser database for the trace of client-cloud interaction can be easily revoked by deleting navigation data after browsing. Anyone with little knowledge in browser history and its database can erase all the trace of their interaction with cloud The collection from the management plane method is a very attractive option since it is user driven, but it requires trust in the management plane. Forensic support as a service is a natural choice and there is already a provider who offers this service.

In [2] author has proposed Cloud computing as a technology has immense potential and offers plenty of benefits for the HPC users. Users on the other hand still do not trust cloud for running their confidential applications.

Lack of transparency and security mechanisms are the major concerns. Cloud Service Providers need to enhance trust on their services. One of the ways to achieve this is to perform digital forensics in cloud. In this paper, we propose a digital forensic based model for VM introspection in cloud. We devised a framework that contains three components.

In [3] author has proposed The virtual nature of cloud computing is pushing digital forensics into a new horizon. Many challenges are existing in the cloud including jurisdictional and technical issues. This paper proposes forensic process that consists of four phases: Identification, Collection and acquisition, Examination and analysis and result dissemination.

In [4] author discussed the value of facilitating post incident cloud forensic investigations of service oriented architectures. The challenges are technical, organizational, legal and social – all of which hold back the integration of cloud data collection mechanisms to facilitate such investigations. Based on a preliminary analysis of the cloud reference architecture, the considerations presented are important for better integration of the missing considerations of forensic capabilities within a cloud forensic service oriented audit framework standardization process.

In [5] author has proposed a novel approach to enable digital forensics in the cloud environment with respect to performance by taking VM snapshot as evidence. The approach incorporates intrusion detection system in VM and VMM to identify the malicious VM and improves the cloud performance in terms of size and time by storing snapshots of malicious VM.

4. CONCLUSIONS

Computer forensics is a vital part of the computer security process. As more knowledge is obtained about how crimes are committed with the use of computers, more forensic tools can be fine tuned to gather evidence more efficiently and combat the crime wave on technology. Our future work is to implement the proposed approach with multiple VMs. Also, we plan to explore the implications of acquisition of evidence from cloud VMs and develop framework for digital forensics in cloud IaaS. In forensic investigation Information are Not completely secure and Difficult to find crime in the system Lack of transparency and security, accuracy low and Malicious activity and attacks on cloud difficult to prevent and investigate. Major issue in digital forensic is tracing a Fraud. so, in our Work we purpose Digital Forensic as a software as a services in Cloud Computing enviournment to detect fraud trace in ordered to avoid such fraudulent attacks in various place in cloud computing. Like bank/credit card transaction.

6. REFERENCES

[1] Emi Morioka and Mehrdad S. Sharbaf "Cloud Computing: Digital Forensic Solutions" IEEE, 2015, pp.589 - 594, DOI: 10.1109/ITNG.2015.99.

[2] Meera G, Geethakumari G"A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing. "2015 IEEE, 2015 Pages: 1 - 5, DOI: 10.1109/SPICES.2015.7091553

[3] Amna Eleyan, Derar Eleyan"Forensic Process as a Service (FPaaS) for Cloud Computing" IEEE ,2015, pp.157 - 160, DOI: 10.1109/EISIC.2015.14

[4] Sean Thorpe , Tyrone Grandison , Indrajit Ray "Towards a Forensic- based Service Oriented Architecture Framework for Auditing of Cloud Logs " IEEE 2013 Pages: 75 - 83, DOI: 10.1109/SERVICES.2013.76

[5] Deevi Radha Rani, G. Geetha kumari " An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots" IEEE 2015 pp. 1 - 5, DOI: 10.1109/PERVASIVE.2015.7087206

[6] Nasir Raza "Challenges to Network Forensics in Cloud Computing" IEEE 2015 pp 22 - 29, DOI: 10.1109/CIACS.2015.7395562

[7] https://en.wikipedia.org/wiki/Digital_forensics

[8] http://cloudtimes.org/2012/11/05/the-basics-of-cloud- forensics/