Memory Forensics in a Cloud Environment

[1]Prasad Purnaye, [2]Dr. Vrushali Kulkarni

[1]*Assitant Professor, SCET, MIT World Peace University, India*

[2]*Professor, SCET, MIT World Peace University, India*

***Abstract*— Cloud Computing is being adopted by industry on a large scale. With the thriving use of cloud technology people who are adopting cloud are very much concern about the security aspect of the cloud. Cloud Service Providers (CSPs) are doing their best to prevent any lawlessness incidence. But even hackers are adopting new techniques to barge into the highly secured cloud. Now when it comes to cloud forensics, traditional forensics tools cannot cope up with the system. We propose a Cloud Forensics Model which will maintain the necessary information about the tenants which can be used in the evidence collection phase of the forensic investigation.**

***Keywords*— cloud computing, forensics, memory forensics, volatile data.**

1. INTRODUCTION

Distributed computing is one of the advancements in the Information Technology (IT) industry, which gave birth to the Cloud. The Cloud became popular forthwith its inception. Increasing use of the cloud brought the majority of a transactions on to the cloud platform, which ultimately lured hackers and cybercriminals. The indifferent architecture of cloud which allows sharing of resources by creating a resource pool has given birth to its vulnerabilities. These vulnerabilities may lead to a data breach. Any of such threat when is exploited for cyber-crimes can contribute a cloud crime. Cloud forensics Investigation approach is different and a notch difficult than that of a traditional digital forensic investigation. Especially the collection phase of the entire forensic investigation process is difficult because of the physical unavailability of the resources. In this document, we briefly introduce a new approach to collect and categories evidence which might help the investigation process.

The remainder of this paper is sorted as: Section 2 elaborates digital forensics and problems associated with cloud forensics. In Section 3 we have discussed memory forensics in detail. This section also talks about the significance of the volatile data. We have proposed a Cloud Forensics model in Section 4. We have concluded the paper gist and specified future scope of the proposed model.

2. DIGITAL FORENSICS

Digital forensics as defined by NIST is an applied science for “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” [1]. Collecting evidence has major issues in the cloud environment because of the physical inaccessibility of the resources [1] [2] [3] [4] [5]. In view of these open challenges, log based solutions are mentioned by authors [1] [2] [4]. Disk images, packet capture files, files, file signature and extracted named entities are major artifacts in an investigation [7]. Some of the artifacts are volatile in nature. There are tools available to access and analyze these different artifacts [6]. Most of the tools are windows based and not designed for cloud environment. Cloud forensics framework like FROST [10] and proposed concept of OCF [11] surely have given direction towards working cloud forensics model. There are only two ways of collecting the evidence from cloud either by enabling APIs of VMM/hypervisor [10] or by adding data collecting modules in the cloud services [11].

3. MEMORY FORENSICS

3.1 SIGNIFICANCE OF MEMORY FORENSICS

Volatile data resides in the memory. If a user shuts down his or her virtual machine the data in the memory is gone. Information from the volatile memory can contribute to the reconstruction of a crime scene [3]. There is an abundance of information accessible in the memory. The Memory has all the data about running programs, open documents and library handle, system, passwords, and cryptographic keys. Unpredictable information in memory additionally contains decoded information, (which is encoded and thus) inaccessible for analysis. But the memory could be highly volatile in nature. The order of collecting data plays a crucial role while collecting evidence during an investigation. While gathering proof one ought to continue from the enduring data sources to the less unstable [5]. There are two different ways to get evidence from the memory: Hardware-based acquisition and Software-based acquisition [4]. In the hardware-based acquisition, the computer's processor is suspended, and a copy of the memory is acquired using direct memory access (DMA). The hardware-based acquisition is expensive because of the cost of the hardware involved. Software-based acquisition of volatile data can be executed using a trusted toolkit. One drawback of software-based memory acquisition is evidence crawler may change the memory conceivably overwriting the pertinent information. Data persistent in a volatile memory of a virtual machine is affected by a multitude of factors including the configuration of the virtual machine.

3.2 CHALLENGES IN COLLECTION

The elasticity of cloud computing allows it to scale-up and scale-down the resources including memory of the VM. With such a dynamic memory allocation, the memory evidence collection process becomes complex and dynamic in nature. Cloud incorporates virtualization. Virtualization is prime security concern in cloud computing [9]. Memory virtualization uses a two-stage mapping process which is maintained by the guest operating system and VMM. Hardware-based acquisition of the evidence from a cloud platform is not possible because of the virtualization of the memory. A software toolkit can be used at the hypervisor level or at the guest OS level to get hold of the memory. This software approach cannot acquire actual memory content because the software program which will collect the data will also use memory to run. Ultimately, we can get some useful data even if it is not original. The memory dump can then be stored on a separate server followed by the later analysis by different tools [6]. Birk and Wegener's solution of continuous synchronization of volatile data [1] will need extra resources for storing forensic evidence. It's not efficient to collect and store all the volatile memory data for evidence. Memory data along with other information related to a VM can yield good analysis.All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

4. PROPOSED MODEL

We propose an approach to identify possible evidence from the virtual memory and preserve it as evidence repository on the persistent data storage. The use of a triage model [2] specifies the artifact finding sequence on a data.

4.1 CLOUD MODEL SELECTION

Memory forensics requires control of the operating systems which the VMs are running. Variations in the service models affect the control which a CSP has over the resources as shown in table I. The memory forensics is difficult in IaaS model where the CSP cannot have control over the operating systems of the VMs.

Table 1: CSPs Control in Cloud Service Models

CSPs Level of Control	**Cloud model**		
	SaaS Model	PaaS Model	IaaS Model
Application	Yes	No	No
Operating System	Yes	Yes	No
Network	Yes	Yes	No
Hardware	Yes	Yes	Yes

4.2 DATA TO BE STORED AND MONITORED

Proposed system would be dumping RAM content of each VM at specified interval. The differential data update on the memory dump will save significant space and redundant. Along with the raw RAM contents, the system is also memory dumps Network information, network configuration, active users, open ports, running processes and timestamp of the system. The Volatile crawlers fetch the data and dump it on the cloud server where the server agent is managing all incoming data.

4.3 STOCHASTIC FORENSICS

Reconstruction of the crime scene has great importance in digital forensics, which is easier to implement if we have some artifacts. But in case of no artifacts, it becomes very difficult to even begin

Vol 11, Issue 7,July/2020

ISSN NO:0377-9254

with the forensics. Jonathan Grier has introduced stochastic forensics process [8] for such scenarios wherein the artifacts are not available, or the available data does not have any direct relation with the event that has happened. We are using access time logs of the virtual machines file system and applied stochastic forensics to visualize the pattern.

4.4 SYSTEM ARCHITECTURE

The system architecture for the proposed model is explained in this section. Figure 1 depicts the components for evidence collection from private cloud.

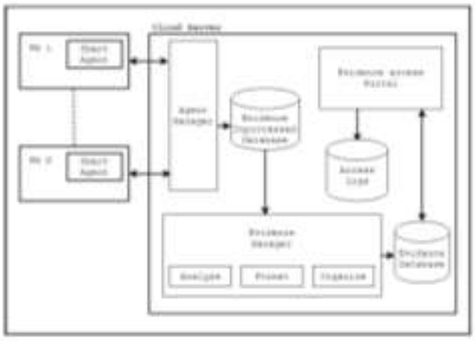

Figure 1 System Architecture

4.4.1 SMART AGENT

Smart agent collects the logs. It will monitor running processes and files updated by them. It will check recently updated files and send them to agent manager. Data will be encrypted before sending for security concerns. Encryption done by using SHA algorithm. Then encrypted data will be send to Agent Manager using SSH. Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. The best-known example application is for remote log into computer systems by users. SSH provides a secure channel over an unsecured network in a client server architecture, connecting an SSH client application with an SSH server.

4.4.2 AGENT MANAGER

Agent manager communicates with Smart Agent via SSH. It is responsible for decryption of data received from Smart Agent. It creates evidence unprocessed database and stores data received from Smart Agent. It will monitor All VM and keeps track of Smart Agent Availability.

4.4.3 EVIDENCE MANAGER

Evidence Manager is responsible for analysis of unprocessed evidences. Data will be formatted into relevant format and user wise organized. Finally, it will store potential evidences into evidence database.

4.4. EVIDENCE ACCESS PORTAL

Forensic experts will get access to potential evidences by using Evidence Access Portal. Experts authentication logs are maintained for chain-of-custody and data integrity

5. RESULTS AND DISCUSSIONS

Evidence gathered by the system can be classified into two categories. One of the categories is memory dumps which are generated at the agent manager level that can be used in reconstruction of the crime scene. Second evidence is in the form of logs which gives total files accessed on a specific month. The comparison here is based on a stochastic characteristic [8] of the data parsed by smart agent in the VMs. The graphs below vouch for the abnormal behavior on the file system and according to the theory published in [8] the analysis can be made whether the internal data files have been copied or not.

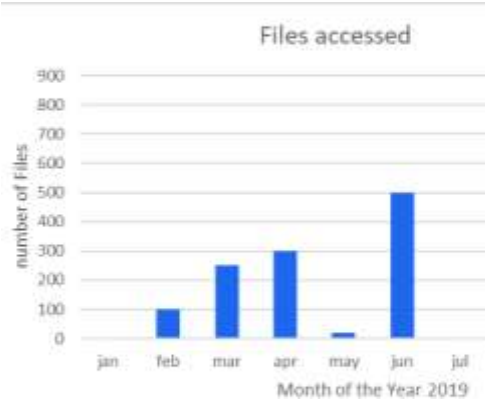

Figure 2: Graph before copying the files

Figure 2 shows the graph generated from the data collected by smart agent. The huge surge indicated in the graph data from Figure 3 confirms that the files are accessed in the month of June 2019.

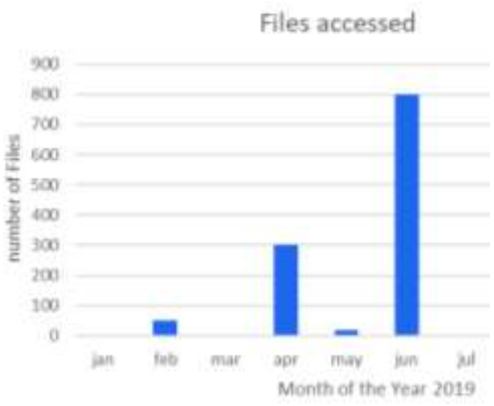

Figure 3 Graph after copying the files

5.1 FEATURES OF THE PROPOSED MODEL.

The cloud model reads and stores the information about open ports, file MAC timestamp, Network Logs, Memory dump and stores on a persistent storage server. The Cloud synchronizes volatile data from each VM simultaneously and stores it securely in the database. The system uses Xplico to analyze the protocols. Xplico reproduces the protocol's application information and it can perceive the protocols with a method named Port Independent Protocol Identification (PIPI).

6. FIRST-ORDER HEADINGS

The primary requirement of cloud forensics is to access the information. To do that, it is mandatory to know precisely where the information is found and effectively obtain it. Preserving volatile data of tenants can make forensic analysis much easier. Every data has a creditable influence in forensic investigation. Section 3.2 identified few hurdles in the process of cloud forensics; the proposed system addresses data collection issue from cloud platform. In future, we look forward to developing and integrate a cloud forensics tools which could be used effectively across all cloud platform, standardizing the cloud forensics investigation process.

REFERENCES

[1] T. Sang, “A Log Based Approach to Make Digital Forensics Easier on Cloud Computing,” in 2013 Third International Conference on Intelligent System Design and Engineering Applications, 2013, pp. 91–94.

[2] D. Birk and C. Wegener, “Technical Issues of Forensic Investigations in Cloud Computing Environments,” in 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2011, pp. 1–10.

[3] M. Damshenas, A. Dehghantanha, R. Mahmoud, and S. Shamsuddin, “Forensics Investigation Challenges in Cloud Computing Environments,” in Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, 2012, pp. 190–194.

[4] R. Marty, “Cloud application logging for forensics,” Proc. 2011 ACM Symp. Appl. Comput. - SAC ’11, p. 178, 2011.

[5] Z. Zaferullah, F. Anwar, and Z. Anwar, “Digital Forensics for Eucalyptus,” in 2011 Frontiers of Information Technology, 2011, pp. 110–116.

[6] Carvajal, Leonardo, Cihan Varol, and Lei Chen. "Tools for collecting volatile data: A survey study." 2013 The International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE). IEEE, 2013.

[7] Garfinkel, Simson L. "Digital forensics research: The next 10 years." digital investigation 7 (2010): S64-S73.

[8] Grier, Jonathan. "Detecting data theft using stochastic forensics." digital investigation 8 (2011): S71-S77.

[9] Hashizume, Keiko, et al. "An analysis of security issues for cloud computing." Journal of internet services and applications4.1 (2013): 5.

[10] Josiah Dykstra and Alan T Sherman. Design and implementation of frost: Digital forensic tools for the openstack cloud computing platform. Digital Investigation, 10:S87–S95, 2013.

[11] Zawoad, Shams, Ragib Hasan, and Anthony Skjellum. "OCF: an open cloud forensics model for reliable digital forensics." 2015 IEEE 8th International Conference on Cloud Computing. IEEE, 2015.

[12] Kim-Kwang Raymond Choo, Christian Esposito, Aniello Castiglione ”Evidence and Forensics in the Cloud: Challenges and Fu90 Cloud Forensic : Examination and Analysis Research Directions”, IEEE Cloud Computing, pp:14-19, Volume: 4 , Issue: 3 2017.