Network Attack Detection using Forensic Investigation in Cloud using VM Snapshots: An Overview

Mahesh Dhumal[1], Prof. Monika Rokade[2]

PG Student, Sharadchandra Pawar College of Engineering, Junnar, Pune, India[1]

Assistance Professor, Sharadchandra Pawar College of Engineering, Junnar, Pune, India[2]

ABSTRACT: Digital Investigation on the cloud platform is a challenging task. Preservation of evidences is the ultimate goal behind performing cloud forensics. Virtual Machines contain evidences in virtual scenario. If once VMDK (Virtual Machine Disk file) is destroyed, it is impossible to recover your VM. At present there does not exist a single mechanism that can recover a destroyed (deleted) VM again which is the flaw in VM itself. All the activities on the VM are logged in VM, whereas activities of CSP (Cloud Service Provider) are logged on the server. So even if someone deleted the VM, all the evidences will be lost. This creates a disaster for the user and acts as a barrier for a forensic investigator to dig out the private crucial data of user that was stored in the Virtual Machine sometime. We proposed with this research work, we explore the existing mechanisms and challenges in the current cloud scenario and propose an idea to prevent the unauthorized deletion of the Virtual Machines snapshots.

KEYWORDS: Cloud computing, Virtual Machine, Intrusion Detection, cloud security, Intrusion Detection System

I. Introduction

Cloud is an emerging technology and cloud based storage is the newly adopted idea that facilitates users not only to upload data to the web but also allows instant accessibility to available resources and share data with anyone at any point of time. But Cloud is a technology that creates a challenge for the person who is investigating and finding out the forensic evidences that may help in the forensic analysis as data stored on cloud can be accessed from anywhere and from any system and very little amount of traces are left behind.

The 21st century is known to be the age of digital world. There has been the adoption of computers to a great extent. Today without computers and Internet one cannot survive as we are dependent on these machines for almost all our work. Taking into consideration starting from home to education till banking and even corporate functioning everything has now been automated to computers. Computers contain all our important data in the digital format.

With this the need to store the digital data has increased and virtual environment has replaced the physical storage for storing all our credentials as shown in Figure 1. The most devastating challenge of cloud is to prevent the unauthorized deletion of the stored data on cloud because one can easily delete the stuff without any proper authorization. The data deletion is totally dependent on deletion of nodes that are pointing to some information in Virtual Machine.

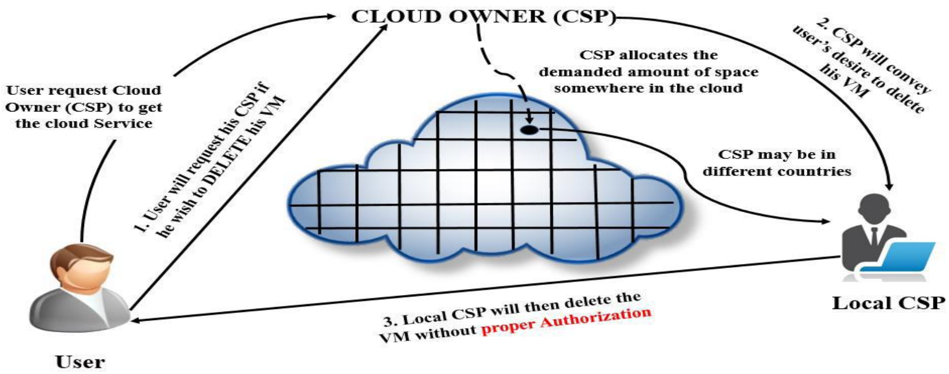
CLOUD OWNER (CSP)
User request Cloud Owner (CSP) to get the cloud Service
1. User will request his CSP if he wish to DELETE his VM
CSP allocates the demanded amount of space somewhere in the cloud
2. CSP will convey user's desire to delete his VM
CSP may be in different countries
Local CSP
3. Local CSP will then delete the VM without proper Authorization
User

Figure 1: Curent Cloud Scenario

II. LITERATURE SURVEY

A critical assessment of the work has been done so far on Cloud Forensics to show how the current study related to what has already been done. Numerous companies are now a days migrating to cloud due to greater economic issues. But for small and medium sized companies the security of information is the primary concern. For these companies the best alternative is to use managed service which is also known as outsourced service in which they are provided with the full package of service including antivirus software to security consulting and the alternative model that provides such outsourced security is known as Security as a service (SECaaS). Scientists and researchers together presented their latest ideas and findings on what the real world scenario is and what all efforts are made but it was found that despite of being so much research work in the field of cloud forensic there is only a fraction part of the total work that hascontributed for the wealth of the society. However cloud came into existence in the mid of 90's yet it is not taken up by everyone fully. There have been lots of works before in this field and variety of methods for the forensic analysis of cloud yet there is a huge room for improvement that needs to be carried forward into the research.

DeeviRadha Rani and Geethakumari G [1] proposed the technique of Forensic investigation of VM using snapshots as evidence that can be shown as a proof in front of court of law. In that mechanism, software stored and maintained snapshots of running VM selected by the user which acted as good evidence. VM can be created by the user as per his choice from the physical machines that are available. Any cloud software similar to that of Eucalyptus instead of request of a user, takes the snapshots of the machines stores till terminated. Snapshots can be stored only till it reaches the maximum but when once maximum is reached the snapshots which were taken long before gets deleted. So the huge storage management of snapshots of VM becomes difficult as it affects the performance of the system also, the author proposed a model in which VM was combined with an IDS. This helped to observe the destructive activities being performed between the VMs by thoroughly monitoring it. The basic idea behind this work was to store the log of destructive activities in the form of snapshots using the IDS placed in the system. Simultaneously, the CSP were asked for the logs of the doubtful VM and those logs were collected by the investigator. Investigator then works on those log files to obtain the evidences which can be helpful to investigator.

BKSP Kumar RajuAlluri and Geethakumari G [2]presented a Model for the self-analysis of VM. They split the entire Introspection into three parts as follows. a) Analysing virtual machines by taking into consideration the swap space where the continuous monitoring of swap space is done. It provides the information about current process of the VM. b) A self-analysis method for VM instances. In this three models were used, to collect as much accurate data evidence can be collected and reduce the semantic gap. But later, out of these three methods in-band method was proved to be less useful for live forensic as it modified the data at the time of collection phase. c) A Terminated Process based Introspection for Virtual Machines in Cloud Computing. This captured every process that was terminated and later was improvised to capture only the processes that were found doubtful. The proposed method for performing the digital forensic observation in Cloud on VM for introspection which addressed the issues related with the assembling of evidences. For resolving they made use of certain methods of introspection on VM. This work can be useful in current research if incorporated as a part of the investigation process.

Hubert RitzdorfNikolaos, KarapanosSrdjanCapkun proposed [3] Assisted deletion of related Content in ACM, 2014 Hubert and Karapanos has discussed a system which helps the user of that system to diminish the similar and associated files, contents of any project. This system did not affect the user or systems components in any sense as it was directed embedded with the system of user itself. It starts functioning from user space and preserves the files along with its metadata. When they executed their work, realized that the resulting accuracy and the overhead were feasible. The results were appropriate to be used for the purpose of deployment. The aim to the system was to aid users by displaying all the associated files of project to be diminished and it was successful in providing it. Deletion of content using assisted deletion of the content that is related was proposed here. User was presented with all the associated files to be diminished securely organized manner. This aided user by maintaining the confidentiality of their data. This can help in current research also as it any system is providing facility to delete files this can be integrated.

Mr.DigambarPowar and Dr. G. Geethakumari [4] proposed a technique for Cloud Computing domain and that was named Digital Evidence Detection technique. Some conventional methods has been discussed in their work which has been used as a tool for performing forensic observations and those methods were useful to learn and examine the behaviour of the digital evidences in a virtualized environment called Cloud. Also the feasible solutions are shown in which forensic practices can be performed in virtual environment. Also authors have introduced the feasible solution in which forensics can be practiced in virtual environment. This work is a crucial stage as it leads to appropriate data evidence collection and presentation that can be an aid to forensic investigator.

Mr.Chandrashekhar S. Pawar, Mr.Pankaj R. Patil, Mr.Sujitkumar V. Chaudhari[5] proposed mechanism for Providing Security and Integrity of Data Stored In Cloud Storage.The authors in their research work have tried to propose a solution to lessen the workload and simultaneously provide the integrity and security of the data which is kept on Cloud in a well-organized way. But as the data stored on cloud is not easily approachable by the users, it becomes difficult to ensure its integrity. So, authors have proposed a technique which once combined with SLA after agreement with CSP and user allows user can test the integrity of data. Also author have worked for minimizing the computational overhead. They have performed encryption only for some bits out of the entire block of file. As a result, at the side of client the overhead has lowered and thus the scheme has been more accepted by the users.

Saibharath S and Geethakumari G [6] have implemented a data collection and rendering mechanism for cloud through hadoop file system using struts 2.0 MVC framework integrated with hadoop and cloud, a web software tool has been successfully implemented to do cloud forensics. Pre-processing of the evidence files have performed through log and VM disk drives clustering. It helps in minimizing the time of forensic investigation. Using the correlation function between drives helps the investigators to perform cross drive analysis. As future work, a soft clustering model with definite search strategy can be designed.

Curtis Jackson1, Rajeev Agrawal2, Jessie Walker3, William Grosky4 [7] proposed virtual environment for testing utilizing Proxmox, an open source virtualization management tool, and KVM, a virtualized environment. Initially they have captured data from VM. In phase 2 investigation of the Virtual Machine Monitor has been done, which creates, observes and manages the virtual machine. In the last phase of this project, they have designed scenarios of cyber-attacks and data loss. These enacted scenarios are logged by the Virtual Machine Monitor. Comparing the datasets from the initial attack scenarios to the Virtual Machine Monitor’s data, they have identified and verified the activity in the Virtual Machine Monitor’s dataset. This data has been useful to enhance our understanding of VMI how it does and should interact with the hypervisor. Using this dataset from the first phase, they have been able to identify activities for threats and normal activities.

Ting Sang[8] stated a log-based model for cloud environment. The log based model can help to reduce the complexity of forensic for nonrepudiation of behaviours on cloud. However, it is totally no enough for the other kinds of digital forensics. What makes matters worse is that, till now, there are still no guidelines or standards for the cloud security. Most of times, we modified the guidelines of traditional digital forensics to suit for cloud computing environment independently.

FilipoSharevski [9] presented an initial effort to describe the potential privacy implication that might arise during the cloud forensic investigation. Additionally, he has approached every dimension of the cloud investigation process with a set of preliminary recommendations that can greatly contribute in the formal definition of privacy requirements in the extremely complex cloud environment. The work presented here is generic in nature and can be easily extended to cover privacy aspects in different cloud service or deployment models against various types of cybercrimes, cyber-attacks or incidents that may have potential impact on the cloud entities’ privacy, this work is an important step that not just contributes to the improvement of the cloud forensic process, but to the overall evolution of the digital forensic science.

Zhen Chen, Fuye Han, Junwei Cao, Xin Jiang, and ShuoChen[10] proposed cloud computing systems to explore the large volume of collected data from CNSMS to track the attacking events. An IaaS cloud platform has been constructed with Eucalyptus and existing cloud platforms such as Amazon EC2 and S3 were used for comparison purposes. Phishing attack forensic analysis as a practical case has presented and the required computing and storage resource has evaluated by using real trace data. The result shows that the proposed scheme is practical and can be generalized to forensic analysis of other network attacks in the future. This work has been supported by the National Key Basic Research and Development (973) Program of China. In summary, the work presented in this paper is built on previous research to explore how security of data stored on cloud relates to people’s trust. While earlier work focused on data storage impacts people, we focus on its impact on the world wide acceptance of cloud.

Based on this above research we are proposing a system to implement the proposed approach with multiple VMs. Also, we plan to explore the implications of acquisition of evidence from cloud VMs and develop a framework for digital forensics in cloud IaaS.In summary, the work presented in this paper have been built on previous research to explore how security of data stored on cloud relates to people’s trust. While earlier work focused on data storage impacts people, we focus on its impact on the world wide acceptance of cloud.

All the existing approach to cloud computing varies with different providers and different service models and deployment models. Thus digital forensics in cloud varies according to the service and deployment models. In Infrastructure as a Service (IaaS) model digital forensics is affable as compared with Software as a Service (SaaS) and Platform as a Service (PaaS) model. This is because of its limited control over infrastructure. The types of evidences collected for investigation vary with service models. In SaaS and PaaS, log information is collected as evidence and in IaaS, VM image is taken as evidence. We can get access to the physical devices in private deployment model but not in the public cloud. The work presented in this survey takes due care of the data which is kept on cloud as it not only provides the integrity check but also security for the data as well. This lets us to test the integrity at the moment of retrieving the stored data from Cloud.

III. METHODOLOGY OF PROPOSED SURVEY

There are too many systems which are used for attack detection and forensic IDS in cloud environment. The traditional digital forensic process undergoes the following steps which can be incorporated in cloud forensics considering its different service and deployment models.

Identification: Reporting against malicious activities is considered as identification which arises when any individual or CSP authority places complaints against undesirable issues. This phase comprises with two types of identification, i.e. Incident Identification and Evidence Identification.

Collection & Preservation: Due to the distributed architecture of cloud, the traditional digital forensics process faces lots of challenges. Since data collection is nothing but the physical acquisition of investigation related data, in most of the cases investigators are supposed to be dependent upon CSPs. This dependence never guarantees 100% availability of the resources, neither its preservation after the collection of data. The storage capacity of the collecting device is another important issue since no data is put in a single location in cloud architecture.

Examination: After collecting the desired large amount of data with the help of CSPs, these are to be processed through a combination of manual and automated processes too. The main motto of examining is to extract and assess data of the particular interest of the classified incident scene. The integrity must be preserved through this entire process.

Analysis: All the relevant data are analysed using suitable and legally justified techniques so that the proper suspected hosts or data can be identified through this investigation procedure. Investigators must be able to meet up with all queries those are raised during the presentation of the analysed report to the court.

Reporting & Presentation: These are the final stages of any investigation process. Report must be comprised with all the details of this investigation process (explanation against what, why and how). The detail report is to be presented to the jurisdiction section with authenticity and accuracy without tampering the evidences which is the most crucial part of the investigation. For acquiring digital evidence the most widely used mechanism is to take snapshots of the events occurred. Snapshots can be restored sequentially using their time of creation to regenerate the crime incident. The proposed a new method to regenerate crime events with continuous snapshots. Leading Cloud Service Providers like Eucalyptus are also giving a provision to take snapshots of the cloud events. In Eucalyptus the snapshots taken will be stored in the walrus component. It was noticed that the size of the snapshot will be the same as that of the original.

Even though snapshots can be stored to the secondary storage, maintaining huge store of snapshot for each VM event will be difficult, time consuming, expensive and would degrade the performance. Also the CSPs should have a mechanism to segregate and provide mappings as to which snapshot belongs to which VM. Through our approach we propose to address this issue.

In the propose a system which incorporates Intrusion Detection System on VMs which allows it to monitor itself and on VMM to detect malicious activity between VMs. The proposed system shows that 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.

Users can create VM of their choice from the available physical machines as shown in Figure 2. In spite of user's request, any cloud software like Amazon, EC2 generates snapshots of a running VM continuously and stores it till the VM terminates. Malicious activities are identified when users of that VM perform any activity like excessive access from location, upload malware to a number of systems in the cloud infrastructure, intense number of downloads and uploads in a short period of time, launch dynamic attack points, cracking passwords, decoding / building web tables or rainbow tables, corruption or deletion of sensitive data, malicious data hosing, altering data, executing botnet commands.

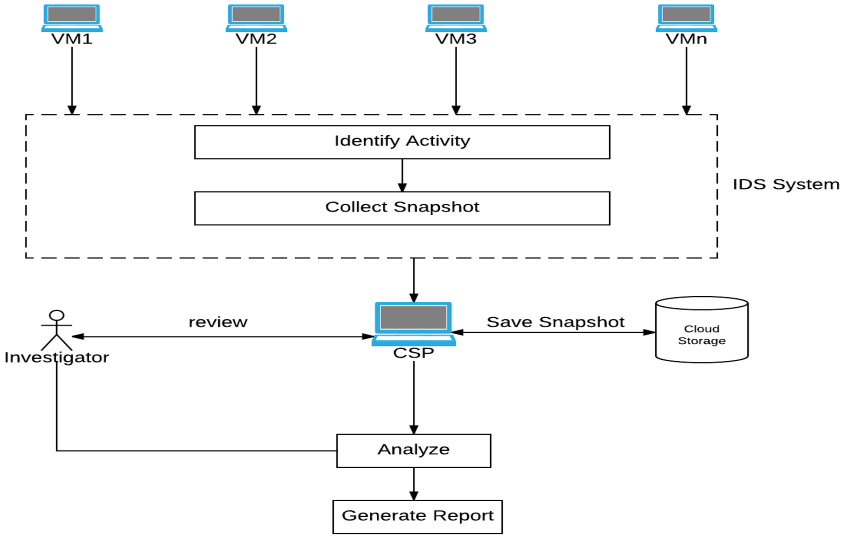

Figure 2: Proposed System

To collect proper and correct evidence, the suspected VM is monitored for some more time after it is identified to performing malicious activities. The more time the suspected VM is monitored the more it can be sure of the possibility of malicious behaviour.CSP stores snapshots of a VM whose activities are identified as malicious by an intrusion detection system. Simultaneously the CSP request for log files of the suspected VM and the investigator collects and processes the log files to obtain the evidence.

Once the investigator identifies the sources of evidence, the suspicious VM is moved to other nodes to preserve confidentiality, integrity and authenticity of other VMs. By moving or isolating, VM evidence can be protected from contamination and tampering.

IV. CONCLUSION

In this paper, we have 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. The proposed approach takes snapshots of suspected VMs and stored in persistent storage, hence improves the performance of cloud. 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 a framework for digital forensics in cloud IaaS.

REFERENCES

[1] DeeviRadha Rani, G. Geethakumari “An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots” International Conference on Pervasive Computing (ICPC), 2015.

[2] BKSP Kumar RajuAlluri, Geethakumari G“A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing” IEEE, 2015.

[3] Hubert Ritzdorf, NikolaosKarapanos, SrdjanCapkun “Assisted Deletion of Related Content”ACM, 2014.

[4] Mr. DigambarPowar, Dr. G. Geethakumari “Digital Evidence Detection in Virtual Environment for Cloud Computing” ACM, 2012.

[5] Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari “Providing Security and Integrity for Data Stored In Cloud Storage” ICICES, 2014.

[6] Saibharath S, Geethakumari G “Cloud Forensics: Evidence Collection and Preliminary Analysis” IEEE, 2015

[7] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky “Scenario-based Design for a Cloud Forensics Portal” IEEE, 2015.

[8] Ting Sang, “A Log-based Approach to Make Digital Forensics Easier on Cloud Computing”CPS,2013

[9] FilipoSharevski “Digital Forensic Investigation in Cloud Computing Environment: Impact on Privacy”

[10] Zhen Chen*, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen”CloudComputing-BasedForensicAnalysisforCollaborativeNetwork SecurityManagementSystem”

[11] AmitKumawat, Cloud Service Models,http://www.cmswire.com/cms/information-management/cloud- service-models - --iaas -saas-paas-how-microsoft-office-365-azure-fit-in-021672.php

[12] Cloud Tweaks, Cloud deployment Models,http://cloudtweaks.com/2012/07/4-primary-cloud-deployment-models/

[13] Amazon EC2 instances deletion in Cloud, https://aws.amazon.com/choosing-a-cloud-platform/?sc_channel=PS&sc_campaign=acquisition_IN&sc_publisher=google&sc_medium=cloud_computing_b&sc_content=sitelink&sc_detail=%2Bamazon%20%2Bclouds&sc_category=cloud_computing&sc_segment=choosing_a_cloud_platform&sc_matchtype=b&sc_country=IN&s_kwcid=AL!4422!3!92346737581!b!!g!!%2Bamazon%20%2Bclouds&ef_id=WKf9NAAAADDF7BAD:20170224152021:s

[14] Openstack, OpenStack command-line interface cheat sheet,http://docs.openstack.org/user-guide/cli_cheat_sheet.html