ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots: An Overview

Rahila A. Sayeda, Prof. Shardha Khonde

P.G. Student, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, India

Professor, Department of Computer Engineering, Modern Education Society's College of Engineering, Pune, India

ABSTRACT: Digital Investigation on the cloud platform is a challenging task. Preservation of evidences is the ultimate goal behind performing cloud forensics. In the Virtual Scenario, Virtual Machines contain evidences. 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 is logged in VM, whereas activities of CSP (Cloud Service Provider) is 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.

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.

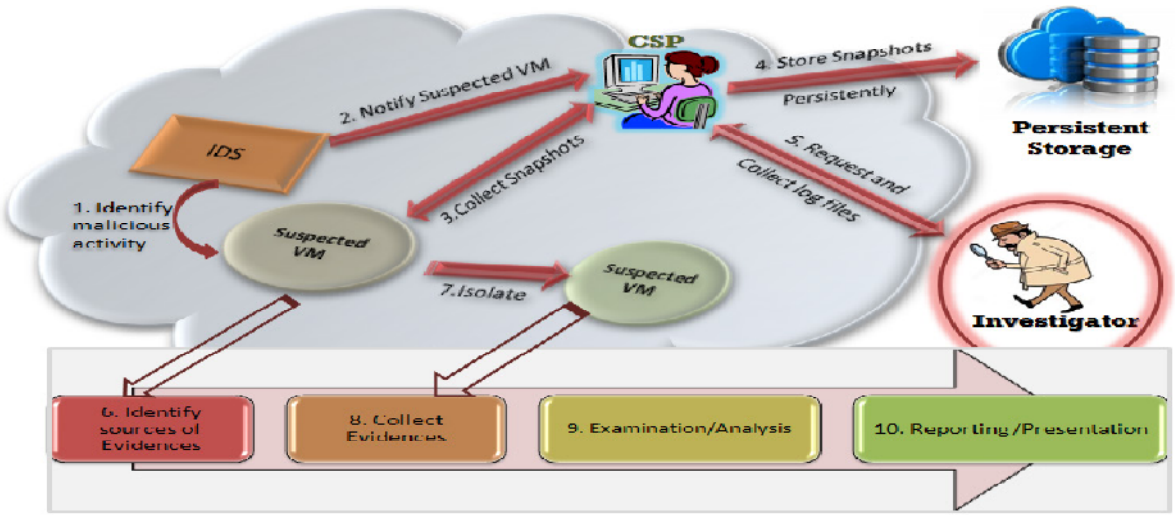

Figure 1: Current Cloud Scenario

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

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 Fig. 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.

II. LITERATURE REVIEW

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 has contributed 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.

Deevi Radha Rani and Geethakumari G proposed a An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots [1]. The technique of Forensic investigation of VM using snapshots as an 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 a 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.

Relevance to current Research
In this paper, 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 Raju Alluri and Geethakumari G **[2]** A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing in IEEE, 2015
Authors 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Relevance to current Research
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 Ritzdorf Nikolaos, Karapanos Srdjan Capkun proposed [3] Assisted deletion of Related Content in ACM, 2014 Hubert and Karapanos in their paper 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 affected 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 was 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.

Relevance to current Research
Deletion of content using assisted deletion of the content that are 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. Digambar Powar and Dr. G. Geethakumari [4] Digital Evidence Detection in Virtual Environment for Cloud Computing in ACM, 2012
Authors at Hyderabad a technique for Cloud Computing domain and that was named Digital Evidence Detection technique. Some conventional methods were discussed in their work which were used as a tool for performing forensic observations and those methods were useful to learn and examine the behavior 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.

Relevance to current Research
In the above mentioned research paper, author 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 proposed Providing Security and Integrity for Data Stored In Cloud Storage in ICICES, 2014. The author in their research work, 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, author 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 worked for minimizing the computational overhead. They performed encryption only for some bits out of the entire block of file. As a result, at the side of client the overhead was lowered and thus the scheme was more accepted by the users. [5].

Relevance to current Research
The work presented in this paper 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.

No.	Paper Title	Author Name	Key Points	Remark
1	An Efficient Approach to Forensic Investigation in Cloud using VM	Deevi Radha Rani, G. Geethakumari, 2015	Incorporates Intrusion Detection System on VMs which allows it to monitor itself and on VMM to detect malicious activity through snapshots between VMs [1]	Improves the performance of cloud and can be implemented for multiple VMs.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

	Snapshots			
2	A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing	BKSP Kumar Raju Alluri, Geethakumari G, 2015	1) A proper triggering condition will only make the investigator to get the needed data 2) During the collection of data the corresponding virtual machine (VM) has to be paused for a while, leading to performance degradation [2].	Address the issues concerned with evidence collection by using the techniques of virtual machine introspection.
3	Assisted deletion of Related Content	Hubert Ritzdorf Nikolaos Karapanos Srdjan Capkun, 2014	A system IRCUS assists the user in securely removing project-related content [3]	Used to protect data confidentiality by assisting deletion of related content, where the user is presented with files that should be securely deleted together.
4	Digital Evidence Detection in Virtual Environment for Cloud Computing	Mr. Digambar Powar and Dr. G. Geethakumari, 2012	Focus mainly on finding and analyzing digital evidence in virtualized environment for cloud computing using traditional digital forensic analysis techniques [4].	Virtual machines that are present on a physical system or running on a portable storage device can be detected or analyzed.
5	Providing Security and Integrity for Data Stored In Cloud Storage"	Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari, 2014	A method was proposed to save our data in the cloud storage secure and provide an integrity check to verify if integrity is preserved or not while we retrieve our data [5].	Use less computational power and processing time.

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.

III. METHODOLOGY OF PROPOSED SURVEY

Virtual Machine Introspection:

It is an Antimalware which analyses and Identifies the attack on VM. Virtual Machine Monitor (VMM) or a VM running under the VMM analyzes the attacked VM when attack is identified. This technique is called Virtual Machine introspection (VMI) and was first introduced by Garfinkel and Rosenblum. Malicious events can be identified by performing Virtual Machine Introspection which is the technique of examining a running VM from either another VM not under examination or from the hypervisor. Live Forensic analysis is also done on the target system using open-source VMI library and Xen Suite. Virtual Machine Introspection is suggested as the most practical approach to identify the malicious VM. If the intrusion detection system resides on the host, it may be susceptible to attack and if intrusion detection system resides in the network it is more resistant to attack. A virtual machine introspection based approach to intrusion detection is proposed where the Intrusion Detection System is outside the host for good attack resistance.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

Digital Provenance:
Digital Provenance is something which describes the History of the Digital Objects in Cloud for an Investigation which will be acceptable in the court of law. Digital provenance is an essential feature for forensic investigations which describes the history of a digital object. Muniswamy and group proposed the secure provenance scheme which performs digital forensics with trusted evidence in cloud environment. This scheme proves that cloud data evidence is acceptable in court of law. In researchers identified four properties that are crucial for provenance systems and introduced protocols to store data provenance using cloud services. Also provenance is accessible as a layer on top of cloud. Implementing secure provenance in cloud environment increased the importance of data on the cloud.

Isolating Cloud Instance:
The process of separating the cloud instance which is a part of crime incident in order to prevent it from corruption and contamination of data. When crime incident happen on cloud, cloud instance and evidence collected from cloud instance need to be isolated for digital investigation. Isolation prevents from possible corruption and contamination of collected evidence. Isolating cloud instance helps to preserves the integrity of the evidence collected from the cloud instance. Delport and group introduced new techniques to isolate instances on a cloud which are referred in our proposed approach.

Log Model:
Log Model is something which keeps track of all the activities performed in the Cloud which can again be used for Forensic purpose. Logging is a challenging issue in cloud computing systems and becoming prevalent in all service models. Ting presented that some kind of forensics can be made a little easier on cloud if logging ability is improved and proposed a log model that suits for SaaS and PaaS. In SaaS, a log can be used locally and synchronously to verify the actions on cloud providing SaaS without interacting with Cloud Service Provider. To use the proposed log model to PaaS cloud there is need to depend on Cloud service Provider to provide log module to the third party. The proposed model based on logging may ease the challenges of the forensics for nonrepudiation of behaviours in cloud.

Regeneration of events:
Regeneration of events is possible by taking the Snapshots of each and every particular event in Cloud. 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. Belorkar and group proposed a new method to regenerate crime events with continuous snapshots. Leading Cloud Service Providers like Eucalyptus, OpenStack 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.

Forensic Investigation using VM Snapshots as Evidence:
Cloud service providers provide various types of services to users, few users from specific organization frequently use the same kind of service based on pay-per-what-they-use and some providers provide free trial period with unlimited bandwidth and storage capacity which gives users an opportunity to perform malicious activities. Malicious users can steal the sensitive and confidential information from cloud users which in turn affect the trust of the CSP. Cloud necessitates protection from these malicious activities and CSP should have a provision to use either introspection or Intrusion Detection System to monitor customer VMs and detect malicious activity. Users can create VM of their choice from the available physical machines. Inspite of users request, any cloud software like eucalyptus, OpenStack 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. In a cloud environment snapshots are rich sources of evidence for digital investigation and can regenerate the events. Storing and managing huge store of VM snapshots is difficult. Snapshots can decrease the performance of a virtual machine based on how

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 1, January 2019

long the snapshot is stored and how much it changed from the time previous snapshot is taken. 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. Our proposed model incorporates Intrusion Detection System on VMs which allows it to monitor itself and on VMM to detect malicious activity between VMs Figure mentioned below 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.

IV. CONCLUSION AND FUTURE WORK

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] Deevi Radha Rani, G. Geethakumari "An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots" International Conference on Pervasive Computing (ICPC), 2015.
[2] BKSP Kumar Raju Alluri, Geethakumari G"A Digital Forensic Model for Introspection of Virtual Machines in Cloud Computing" IEEE, 2015.
[3] Hubert Ritzdorf, Nikolaos Karapanos, Srdjan Capkun "Assisted Deletion of Related Content"ACM, 2014.
[4] Mr. Digambar Powar, Dr. G. Geethakumari "Digital Evidence Detection in Virtual Environment for Cloud Computing" ACM, 2012.
[5] Saibharath S, Geethakumari G "Cloud Forensics: Evidence Collection and Preliminary Analysis" IEEE, 2015
[6] Mr. Chandrashekhar S. Pawar, Mr. Pankaj R. Patil, Mr. Sujitkumar V. Chaudhari "Providing Security and Integrity for Data Stored In Cloud Storage" ICICES, 2014.
[7] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky "Scenario-based Design for a Cloud Forensics Portal" IEEE, 2015.
[8] NIST, "NIST Cloud Computing Forensic Science Challenges", National Institute of Standards and Technology Interagency or Internal Report 8006, 2014.
[9] Jaonie M. Wexler, Apple bonjour just yet, http://www.webtorials.com/content/2012/04/dont-rush-to-bid-adieu-to-apple-bonjour-just-yet.html
[10] David Maxwell, Cloud Lounge,http://www.cloud-lounge.org/why-use-clouds.html
[11] Amit Kumawat, 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] Openstack, OpenStack command-line interface cheat sheet, http://docs.openstack.org/user-guide/cli_cheat_sheet.html
[14] 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