A Survey on digital forensic investigation and its challenges in cloud using VM snapshots

M.Sirisha

Assistant professor , Computer science and engineering department, Mallareddy college of Engineering and technology,Telangana state,India

Abstract

Cloud computing is becoming most promising technology in recent days. It offers the scalable elastic services to many users at a time and it helps to access the resources quickly from cloud service provider. Digital forensics is part of computer forensics. Various challenges of cloud hinder the process of cloud forensics so that no standard framework for cloud forensics can be designed. This paper gathers the challenges and possible solutions. 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. 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.There is need of dedicated digital forensic framework for cloud environment. System proposes an efficient approach to forensic investigation in cloud using Virtual Machine (VM) snapshots.

Keywords *: cloud computing, virtual machine (VM) snapshots ,Digital forensics process, cloud forensics,Eucalyptus*

1. Introduction

Cloud is a developing innovation and cloud primarily based definitely potential is the currently received belief that encourages clients to switch records to the internet as well as allows second openness to available assets and impart data to everybody whenever of time. Be that as it can, Cloud is an innovation that makes a test for the person who is exploring and discovering the criminological confirmations which could help inside the clinical studies as information located away on cloud may be gotten to from anywhere and from any framework and nearly no degree of follows are abandoned.

The twenty first century is thought to be the duration of digital international. there was the appropriation of desktops because it have been. these days with out computer systems and net one cannot get by using as we are reliant on those machines for all our artwork. thinking about starting from domestic to training till saving cash or maybe company working the whole thing has now been mechanized to computer systems. pcs consist of all our vital information in the virtual configuration. The most pulverizing take a look at of cloud is to keep the unapproved erasure of the positioned away facts on cloud considering that you could still surely erase the stuff without a appropriate approval. The records cancellation is truly reliant on erasure of hubs that are indicating some information in digital machine. It gives on-line records storage, infrastructure and alertness.We want not to install a bit of software on our neighborhood pc and that is how the cloud computing overcomes platform dependency problems. for this reason, the Cloud Computing is making our commercial enterprise utility cell and collaborative.

2. Cloud Service Model

There are various courses in which a cloud administration can be utilized and used as well. In the cloud computing space, three diverse ways to deal with cloud-based administrations exists. They are[1][2]:

2.1 Infrastructure as a Service (IaaS)

In IaaS demonstrate, the components of foundation, for example, Virtualization, Storage, Networking, Load Balancers et cetera can be outsourced to a Cloud Provider like Microsoft. The Cloud supplier will charge a bill for you in view of computing force every hour and the measure of assets assigned to you and devoured according to chose in the administration level understanding (SLA) of the Cloud benefit.

2.2 Platform as a Service (PaaS)

By this arrangement display clients can get a fundamental working framework and square administrations that can help you to execute your own applications or any of the outsider applications. No should be worried about the lower level components which are one out of the recorded components, for example, Infrastructure, Network Topology, Security and Load Balancers, since every one of these components would be taken tend to you by the Cloud Service Provider. The Provider gives you a completely operational OS with real stage programming to work upon it.

2.3 Software as a Service (SaaS)

SaaS display, gives licenses to application to the Cloud clients as administration on request, membership, pay according to you request show, or at no cost charge when there is chance to produce benefit from sources other than the client.

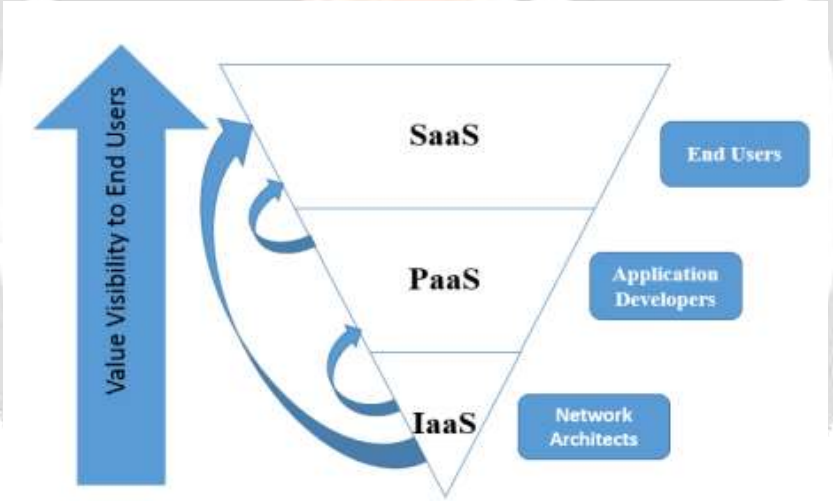

Figure : Cloud Service Model

3.Deployment Models of Cloud

Mainly there are four deployment models in Cloud, described as follows and represented in the following figure. Models have been standardized by an organization named National Institute of Standards and Technology (NIST).

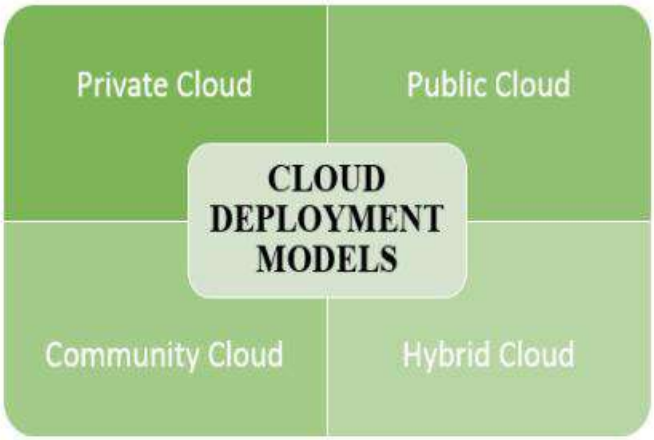

Fig: Deployment models of cloud

1. **Open Cloud:** Cloud that is receptive by the client and it is kept up by an outsider CSP. Here the CSP is accountable for the whole administration of administrations being given. On the off chance that cloud is to be sent for a general mass it is called open cloud.
2. **Private Cloud:** This is kept up by a solitary association. The cloud is conveyed for any organization or for organization's private use. Here CSP and client are inward as it were.
3. **Group Cloud:** Cloud conveyed for any group or for at least two organization having a similar vision and mission. This is like private however can be drawn closer by some particular group as it were.
4. **Half breed Cloud:** It can even be utilized by consolidating any of the three sorts of cloud. Utilizing this can enhance the use as it consolidates points of interest of both of which it has been joined. Thus, the cloud moves the workloads amongst open and private facilitating to keep any burden to the clients.

Virtualization

Virtualization is a stage that gives the financially savvy conveyance to clouds and server farms. It gives a choice to Virtual Machine Introspection (VMI) by means of hypervisor[10]. VMI is a situation to screen the movement of a Virtual Machine (VM). Virtualization innovation technique is utilized to effectively or inactively screen remotely and undetected frameworks.

4. Brief survey of digital forensics using VM

The system of Forensic examination of VM using previews as a confirmation that can be seemed as a proof earlier than courtroom. In that machine, programming put away and saved up depictions of going for walks VM chose by the client which went about as a decent affirmation. VM can be made with the aid of the purchaser in line with his choice from the physical machines that are accessible[3]. Any cloud programming like that of Eucalyptus instead of demand of a patron, takes the depictions of the machines stores until ended. The substantial stockpiling management of depictions of VM gets to be quite tough because it impacts the execution of the framework too.A version has been presented for the self-exam of VM. They split the whole Introspection into 3 sections as referred to under. a) reading virtual machines by using mulling over the switch space in which the nonstop watching of change area is finished. It offers the information approximately present day manner of the VM. b) A self-exam approach for VM cases. on this 3 models had been utilized, to acquire as lots specific information proof may be amassed and reduce the semantic hole. anyhow, later, out of those three strategies in-band approach become ended up being much less valuable for live medical as it changed the statistics on the season of accumulating stage. c) A Terminated technique based Introspection for virtual Machines in Cloud Computing. This stuck each manner that changed into ended and later changed into ad libbed to seize simply the approaches that were discovered some distance fetched. A framework which allows the patron to reduce the comparative and related files, substance of any venture. This

framework did no longer motivated the purchaser or frameworks segments in any feel as it become coordinated mounted with the arrangement of customer itself[5]. It starts working from purchaser area and jelly the facts alongside its metadata. when they done their work, understood that the following precision and the overhead become realistic. The consequences had been suitable to be applied with the cease purpose of sending. The intend to the framework become to help customers through displaying all of the associated facts of task to be reduced and it changed into fruitful in giving it[9].

4.1 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.

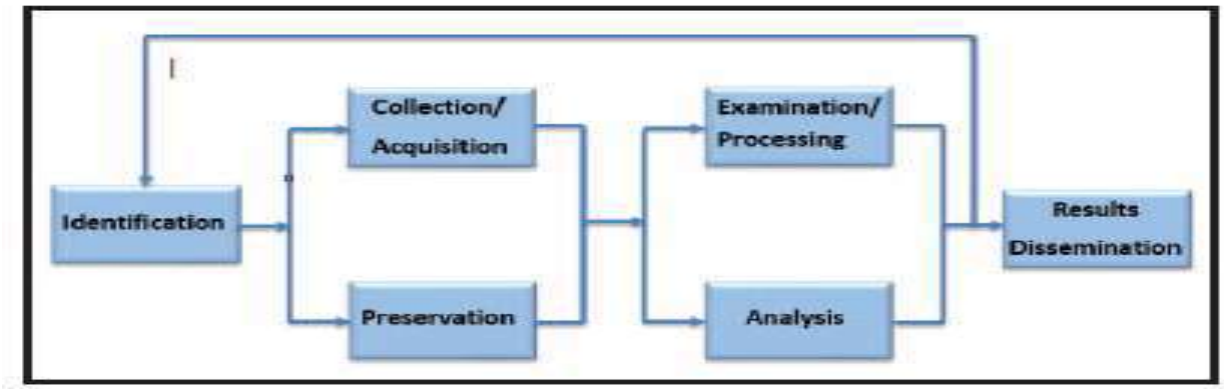

Fig: Forensic Workflow Process

4.2 Virtual Machine Introspection

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 [8]. 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 [1].
Poisel et al. [7] proposed hypervisor forensics and presents the possibility of acquiring evidence from hypervisors to perform digital forensics. 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 [8]. In [2] the authors proposed the use of Forensic Virtual Machines (FVM) to analyze memory space of other virtual machines. FVMs are small virtual machines whichcan monitor other VMs to find symptoms in real time via Virtual Machine Introspection.

4.3 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[3] 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 [4] 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 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 [1].

5. conclusion

on this paper, we have proposed a singular method to allow virtual forensics in the cloud environment with recognize to performance by using taking VM photo as proof. The technique incorporates intrusion detection machine in VM and VMM to discover the malicious VM and improves the cloud performance in phrases of length and time via storing snapshots of malicious VM. The proposed technique takes snapshots of suspected VMs and stored in continual garage, for this reason improves the overall performance of cloud. Our future paintings is to put into effect the proposed technique with a couple of VMs. additionally, we plan to discover the consequences of acquisition of evidence from cloud VMs and develop a framework for digital forensics in cloud IaaS.

6. References

[1] An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots
Deevi Radha Rani Computer Science and Engineering KL University, Andhra Pradesh, India ,
G. Geethakumari Computer Science and Information Systems BITS Pilani – Hyderabad Campus, Hyderabad, India

[2] Martini and K.K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital* Investigation, vol. 9, no. 2, pp. 71–80, November 2012.

[3] K.Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud Forensics," *Advances in Digital Forensics VII,* vol. 361, no. IFIP Advances in Information and Communication Technology pp. 35-46, 2011.

[4] J. Dykstra and A. Sherman, "Understanding issues in cloud forensics: Two hypothetical case studies," *Journal of Network Forensics*, vol. b, no. 3, pp. 19–31, 2011.

[5] Saibharath S, Geethakumari G "Cloud Forensics: Evidence Collection and Preliminary Analysis" IEEE, 2015

[6] Trusted VM snapshot in public cloud infrastructure for digital forensic investigation
Mr.Suraj U. Madhale *Computer science and technology department Department of technology Kolhapur, India* ,Ms.Amrita A. Manjrekar ,*Computer science and technology department Department of technology ,Kolhapur, India*

[7] Z. Qi; C. Xiang; R. Ma; J. Li; h. Guan; D. Wei, ―ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics,‖ in *IEEE Transactions on Cloud Computing* , vol.PP, no.99, pp.1-1 doi: 10.1109/TCC.2016.2535295

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

[9] Curtis Jackson, Rajeev Agrawal, Jessie Walker, William Grosky "Scenariobased Design for a Cloud Forensics Portal" IEEE, 2015.

[10] NIST, "NIST Cloud Computing Forensic Science Challenges", National Institute of Standards and Technology Interagency or Internal Report 8006, 2014.