International Journal of Engineering Research and Technology. ISSN 0974-3154 Volume 10, Number 1 (2017)

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
Email:surajsum21@gmail.com

Ms.Amrita A. Manjrekar
Computer science and technology department
Department of technology
Kolhapur, India
Email:aam_tech@unishivaji.ac.in

Abstract
Cloud computing in recent times used as a technology to allow users to right to use infrastructure, storage, software and deployment environment based on a pay and use model. Traditional digital forensics cannot handle the dynamic and multi-tenant nature of the cloud environment as it has to address reality of technical, legal, and organizational challenges typical to the cloud systems. This work focuses the challenges of digital forensics in the cloud. In recent times the cloud environment is misused by many clients for storing and distributing illegal information. 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, HyperShot Model

Introduction
Cloud computing has recent trends to allow users to access infrastructure, storage space, and software and deployment environment based on a pay and use model. Digital forensics in remote, ubiquitous provider controlled cloud computing systems is difficult when compared to traditional digital forensics. Criminal use of cloud computing is an impending possibility as cloud becomes omnipresent. Likewise, the need for digital forensic analysis of cloud computing environment and applications has become customary. Traditional digital forensic consist of following stages- **Identification** (Identifies the source of evidence), **Collection** (Capture evidence and related data), **Examination/Analysis** (Examine and Analyze forensic data), **Reporting and Presentation** (Presentation of collected evidence to court of law).
Cloud environment cloud data is deferent than regular digital environment and digital data; hence for cloud forensics must have different approach than regular forensics. In cloud forensics technical,ligal and organizational dimention are considerd while investigating any case the dynamic nature of cloud creates multiple challenges to digital invenstigation in cloud environment.

A Virtual Machine (VM) snapshot captures the state of a VM at a picky point in time. The genrated snapshot includes the configuration, disk data, and the current state. The purpose is to allow the user to relapse to the snapshot in the event something happens to the VM to reason it not to work properly. This principle is alike to a restore point in the windows OS. While using a snapshot, the configuration setting reverted include, but are inadequate to previous IP address, DNS names, universal unique identifier (UUID) and guest OS patch versions. Snapshot data files are stored as files and are regularly located in the same folder as the virtual machine by default. However, if the VM was imported with snapshots, they are stored in their own folder, and if the virtual machine has no snapshots, the virtual machine snapshot setting allows the snapshots to be stored in a precise folder for integrity Management. The functions associated with snapshots are as follows [21];

- CreateSnapshot creates a new snapshot and updates the present snapshot.
- RemoveSnapshot removes a snapshot and any allied storage.
- RemoveAllSnapshots eliminate all snapshots.
- RevertToSnapshot “rollbacks” a virtual machine.

This concept is important for two reasons.

- First, snapshots just like restore points can contain vital information that may not show in the current state of the machine.
- Second, since each snapshot generates a new child disk from the last child disk and the relationship may change, there could be multiple branches in the snapshot chain; Reconstructing events may require locating all snapshots, not just the most obvious ones[21].
- Cloud computing has recently emerged as a technology to allow users to access infrastructure, storage, software and deployment environment based on a pay-for-what-they-use model. Traditional digital forensics cannot handle the dynamic and multi-tenant nature of the cloud environment as it has to address

various technical, legal, and organizational challenges typical to the cloud systems. The dynamic nature of cloud computing allows abundant opportunities to enable digital investigations in the cloud environment [6] Addresses the challenges of digital forensics in the cloud environment and existing solutions to ease some of the challenges. Here introducing an efficient approach to forensic investigation in cloud using Virtual Machine (VM) snapshots

- Evidence Protection: Once the volatile data has been acquired, the hypervisor stores them on the disk. After being allocated, the evidence files will be protected by the Filesafe module from being accessed by malware or the compromised OS. Besides that, users can also set control policies for other sensitive files manually in the hypervisor, which will also be protected by the Filesafe module. The reliability is improved in three ways: reducing Trusted Computing Base (TCB) size by leveraging a lightweight architecture, collecting evidence directly from the hardware, and protecting the evidence and other sensitive files with Filesafe module [1].
- Addresses security policies for trusted virtual domain management such as secure addition and deletion of a virtual machine and the revocation of privileges associated with a virtual machine in a domain. They also discussed forensic analysis of attacks and fine granular detection of malicious entities and mechanisms for restoration of services. The proposed architecture provides mechanisms for enhancing the assurance of communications between the virtual machines in different domains [2].

Related Work

Zhengwei Qi, Chengcheng Xiang, Ruhui Ma, Jian Li, Haibing Guan and David S. L. Wei [1] et al discussed ForenVisor: A Tool for Acquiring and Preserving Reliable Data in Cloud Live Forensics. In this paper they proposed a special purpose hypervisor, called ForenVisor, which is dedicated to reliable live forensics. The reliability is improved in three ways: reducing Trusted Computing Base (TCB) size by leveraging a lightweight architecture, collecting evidence directly from the hardware, and protecting the evidence and other sensitive files with Filesafe module. They implemented a proof-of-concept prototype on the Windows platform, which can acquire the process data, raw memory, and I/O data, such as keystrokes and network traffic. They evaluate ForenVisor in terms of code size, functionality, and performance. This article highlighted the hardware-assisted virtualization technique and eliminates unused device drivers to reduce the TCB size, thereby decreasing the vulnerability of hypervisor.

Vijay Varadharajan and Udaya Tupakula [2] et al discussed Securing Services in Networked Cloud Infrastructures. In this paper, they proposed techniques and architecture for securing services that are hosted in a multi-tenant networked cloud infrastructure. This architecture is based on trusted virtual domains and takes into account both security policies of the tenant domains as well as specific security policies of the virtual machines in the tenant domains. they describes techniques for detecting a range of attacks such as attacks between the virtual machines within a trusted virtual domain, attacks between the virtual machines in different domains, malicious insider attacks and attacks against specific services such as DNS, database and web servers within a domain. They address security policies for trusted virtual domain management such as secure addition and deletion of a virtual machine and the revocation of privileges associated with a virtual machine in a domain. They also discussed forensic analysis of attacks and fine granular detection of malicious entities and mechanisms for restoration of services. The proposed architecture provides mechanisms for enhancing the assurance of communications between the virtual machines in different domains.

Saad Alqahtany, Nathan Clarke, Steven Furnell, Christoph Reich [3] et al discussed cloud forensics challenges, solutions and open problems. In this article they discussed cloud forensics issues according stages mentioned follows- Identification stage, Data collection and preservation stage, Analysis & Examination stage, Presentation stage.CSP dependency is major challenge and trust issue. This article also discusses current available solutions and open problem.

Emi Morioka, Mehrdad S. Sharbaf [4] et al present detail to investigate the forensic issues in cloud computing and provide possible solutions over that also guidelines, including existing case studies. The basics of traditional digital forensics and cloud computing are also discussed in this paper. Author work on live forensics concerns the value of the data that may be lost by powering down a system and collects it while the system is still running. The work considered using hypervisor, the prime target for attacks and there is an alarming lack of policies, procedures and techniques for forensic investigation of hypervisors.

Deevi Radha Rani, G. Geethakumari [5] et al proposed "An Efficient Approach to Forensic Investigation in Cloud using VM Snapshots" in that addresses the challenges of digital forensics in the cloud environment and existing solutions to ease some of the challenges. 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.

D. T. Meyer, G. Aggarwal, B. Cully, G. Lefebvre, M. J. Feeley, N. C. Hutchinson, and A. Warfield [8] et al Proposed Parallax: Virtual Disks for Virtual Machines as An alternative solution makes the snapshot generation an asynchronous process, with the hypervisor initiating the COW protection at a random point in time. HyperShot only records a VMs' memory and registers; it does not yet snapshot disk contents. We plan to extend it with an existing virtual disk snapshot solution, such as Parallax [14] or the disk snapshotter available with Hyper-V.

Diane Barrett, Gregory kipper Tecnical Editor Samuel Liles [9] et al , Focus on Virtualization and forensic a digital forensic investigators guide to virtual environments. Forensic analysis involves analyzing two main components of the system, first is memory and second hard drive. Analysis can be performed on the hard drive, finding individual files that

have been detected and recovering technique with the introduction of virtualization.

"A Novel Approach for Monitoring SQL Anti-Forensic Attacks Using Pattern Matching for Digital Forensic Investigation" [22] discusses about Anti-Forensic attacks in traditional way. The method need to be modified as per cloud infrastructure. The said system focuses on monitoring the Anti-Forensic attacks in the process of Digital Forensic Investigation

Proposed System

The proposed system will be hypervisor based system. This will be capture VM snapshot whose integrity cannot be compromised. Suitable hash technique will be used to preserve integrity of stored VM snapshot. This approach will be executed for multiple VM's.

A typical virtualization infrastructure includes a hypervisor, multiple guest VMs, and a privileged management VM, such as the root VM. The current virtualization architecture use Hyper-shot mechanism. This mechanism considers attacks that compromise the integrity of the snapshot either by tampering with the snapshot file's contents or with the snapshot service. By refer to all entities that could responsible to this attack from the root VM—whether it is a malware instance running in the root VM or a malicious administrator—collectively as a malicious root VM.

The system consisting of following modules:

Module 1: Identifying malicious activity:

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.

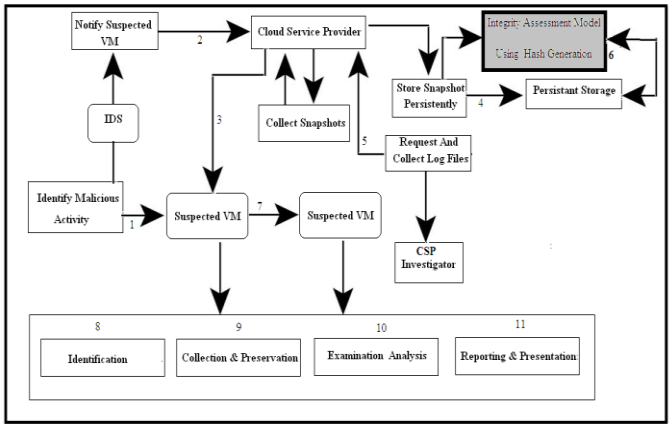

Figure 1: Proposed system architecture for digital forensics using VM snapshots as digital evidence with integrity assessment

Module 2: Integrity Assessment model

In this model integrity of the snapshot or evidence are obtained by trust based auditing for integrity checking scheme after collecting the desired large amount of data with the help of CSPs. The integrity must be preserved through this entire process. Also model having capability to captures and avoid VM snapshots whose integrity cannot be compromised by a rogue privileged VM or its administrators.

Integrity Assessment model using Hash Generation

To protect the integrity of the snapshot file from a malicious root VM, HyperShot creates message digests or hashes of the target VM's memory pages before the snapshot content is sent to the root VM. These hashes are stored inside the hypervisor, and thus are not accessible to the root VM.

Hyper Shot Model

The integrity module is mainly based on HyperShot model which comprises the following phases.

1) **Identification:**

In This step malicious activities are identified and reported, which arises when any individual or CSP authority places complaints against undesirable issues. This phase used to check two types of identification, i.e. Incident Identification and Evidence Identification.

2) **Collection & Preservation:**

Investigation related data collected by the physical acquisition. Availability of the resources, data preservation is done after the collection of data by Copy-on-Write Protection mechanism expressed in step 6.

3) **Examination:**

The main aim 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.

4) **Analysis:**

All the relevant data are analyzed using suitable and legally justified techniques (forensic tools) 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 analyzed report to the court.

5) **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.

6) **Copy-on-Write Protection**

Enhanced Copy-on-Write Protection HyperShot used to create trusted and consistent snapshots of VMs executing in a virtualization based cloud environment. Enable consistency is to pause the target VM during the entire snapshot process. To achieving consistency and security, HyperShot use an enhanced copy-on-write (COW) mechanism [2].

To set up the enhanced COW on a guest VM at the beginning of a snapshot,

1. The hypervisor will pause the guest VM and marks its memory pages read-only by iterating across its address space.
2. To protect the guest VM's state from untrusted modifications by the root VM during the snapshot, HyperShot also write-protects the corresponding memory pages mapped in the root VM's page tables.

3. For snapshots of the root VM, the COW setup is performed only on the root VM's address space because guest VMs cannot access the root VM's memory pages

Implementation

Ubuntu eucalyptus cloud (version 11.4, 4GB Ram) is created on ubuntu platform. In this two VM's are created with the help of windows VMWare. One VM is of WINDOWS XP-operating system, with 2GB ram and 30GB memory space; another is of Ubuntu with 2GB ram and 30GB memory space.

	XenServer 5.5	VMware vSphere 4.0
VM snapshots	**Free**	**Yes: Standard Edition and higher**
Real-time performance monitoring	**Free**	**Yes: Standard Edition and higher**
Live motion	**Free**	**Yes: Advanced Edition and higher**
VM backup enablement	**Free**	**Yes: Advanced Edition and higher**
VM load balancing	**Yes, Enterprise Edition**	**Yes: Enterprise Edition and higher**
VM high availability	**Yes, Enterprise Edition**	**Yes: Standard Edition and higher**

Table1: Comparison by tools used to setup cloud environment.

VM's are controlled from VMware workstations (Ubuntu front & Ubuntuback).Two VM are connected using putty tool. One VM is used for managing snapshots while another is used for analysis purpose.

VM snapshots are generated on regular time interval depending on running applications. These snapshots are saved at specific location and further given to analysis module.

Conclusion

This paper exhibits a basic Framework to the Digital Forensic Investigation using hypershot technique with integrity assessment module. In this system virtualization infrastructure includes a privileged management VM as a root VM. Integrity of the snapshot is protected from a malicious root VM using hash technique. This paper proposes a way to construct snapshot for public clouds built with the Eucalyptus cloud operating system. Current image-creation methods for Eucalyptus environments are bulky and time-consuming. Using this approach digital forensics investigation will become more reliable and accurate.

References

[1] 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

[2] V. Varadharajan; U. Tupakula, "Securing Services in Networked Cloud Infrastructures, " in IEEE Transactions on Cloud Computing ,vol.PP, no.99 ,pp.1-1 .doi: 10.1109/TCC.2016.2570752

[3] S. Zawoad and R. Hasan, "Trustworthy Digital Forensics in the Cloud," in *Computer*, vol. 49, no. 3, pp. 78-81,Mar.2016.doi: 10.1109/MC.2016.89

[4] S. Alqahtany, N. Clarke, S. Furnell and C. Reich, "Cloud Forensics: A Review of Challenges, Solutions and Open Problems, " *2015 International Conference on Cloud Computing (ICCC)*, Riyadh, 2015,pp.1-9.doi: 10.1109/ CLOUDCOMP. 2015.7 149635

[5] E. Morioka and M. S. Sharbaf, "Digital forensics research on cloud computing: An investigation of cloud forensics solutions," *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, Waltham,MA,2016,pp.1-6.doi: 10.1109/ THS.2016. 75 68909

[6] D. R. Rani and G. Geethakumari, "An efficient approach to forensic investigation in cloud using VM snapshots," *2015 International Conference on Pervasive Computing (ICPC)*, Pune, 2015, pp. 1-5. doi: 10.1109/PERVASIVE.2015.7087206

[7] M. Irfan, H. Abbas and W. Iqbal, "Feasibility analysis for incorporating/deploying SIEM for forensics evidence collection in cloud environment, " *2015 IEEE/ACIS 14th International Conference on Computer and Information Science (ICIS)*, Las Vegas, NV, 2015, pp. 15-21. doi: 10.1109/ICIS.2015.7166563

[8] G. Sibiya, H. S. Venter and T. Fogwill, "Digital forensics in the Cloud: The state of the art, " *2015 IST-AfricaConference*,Lilongwe,2015,pp.1-9.doi: 10.1109/ISTAFRICA.2015.7190540

[9] Abhinav Srivastava1, Himanshu Raj, Jonathon Giffin, Paul England "Trusted VM Snapshots in Untrusted Cloud Infrastructures." 15th International Symposium, RAID 2012, Amsterdam, the Netherlands, September 12-14, 2012, pp 1-21, doi: 10.1007/978-3-642-33338-5_1.

[10] Suchana Datta, Koushik Majumder and Debashis De. "Review on Cloud Forensics: An Open Discussion on Challenges and Capabilities." International Journal of Computer Applications 145(1):1-8, July 2016, Volume 145 - Number 1,doi: 10.5120/ijca2016910521

[11]]M. Carbone, W. Cui, L. Lu, W. Lee, M. Peinado, and X. Jiang. "Mapping Kernel Objects to Enable Systematic Integrity Checking." In ACM CCS, Chicago, IL, Nov. 2009. Pages 555-565,doi: 10.1145/1653662.1653729.

[12] A. M. Azab, P. Ning, Z.Wang, X. Jiang, X. Zhang, and N. C. Skalsky. "Hypersentry: Enabling stealthy in-context measurement of hypervisor integrity." In ACM CCS, Chicago, Oct. 2010. Pages 38-49.doi: 10.1145/1866307.1866313

[13] D. T. Meyer, G. Aggarwal, B. Cully, G. Lefebvre, M. J. Feeley, N. C. Hutchinson, and Warfield. "Parallax: Virtual Disks for Virtual Machines." In Proc. of ACM Eurosys, Scotland, Mar. 2008. Pages 41-54 ,doi: 10.1145/1357010.1352598

[14] T. Garfinkel and M. Rosenblum, "A Virtual Machine Introspection-Based Architecture for Intrusion

Detection," *Proc. Network and Distributed Systems Security Symp.*, The Internet Society, 2003, pp. 191-206.

[15] B. Hay and K. Nance, "Forensics examination of volatile system data using virtual introspection," ACM SIGOPS Operating Systems Review, vol. 42,no.3,pp.74–82,2008.doi: 10.1145/1368506 .1368517

[16] Dener Didone and Ruy J. G. B. de Queiroz, "Forensic as a Service – FaaS," The Sixth International Conference On Forensic Computer Science, Volume 2, Issue 9, pp 202-210. September 2014

[17] Waldo Delport, and Martin S. Olivier, "Cloud Separation: Stuck Inside the Cloud." Springer Berlin Heidelberg, 2012. pp 36-49.doi:10.1007/978-3-642-32287-7_4.

[18] Hay, Brian, and Kara Nance. "Forensics examination of volatile system data using virtual introspection." ACM SIGOPS Operating Systems Review 42, no. 3 (2008): pp 74-82.doi: 10.1145/1368506.1368517.

[19] Modi, Chirag, Dhiren Patel, BhaveshBorisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan. "A survey of intrusion detection techniques in cloud." Journal of Network and Computer Applications 36, no. 1 (2013):pp 42-57.

[20] N. Marangos, P. Rizomiliotis and L. Mitrou, "Digital forensics in the Cloud Computing Era, "*2012 IEEEGlobecomWorkshops*,Anaheim,CA,2012,pp.775-780.doi: 10.1109/GLOCOMW.2012.6477673

[21] Diane Barrett, Gregory kipper Technical Editor Samuel Liles "Virtualization and forensic a digital forensic investigators guide to virtual environments" Syngress 6 Aug 2010.

[22] Patil, Vaibhav T.and Manjrekar, Amrita A., "A Novel Approach for Monitoring SQL Anti-Forensic Attacks Using Pattern Matching for Digital Forensic Investigation", Security in Computing and Communications: International Symposium, SSCC 2013, Mysore, India, August 22-24, 2013. Proceedings, 2013, Springer Berlin Heidelberg, Berlin, Heidelberg, 162--167, 978-3-642-40576-1,