ISSN: 2321-7782 (Online)
Volume 2, Issue 6, June 2014
International Journal of Advance Research in
Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Design of digital forensic technique for cloud computing

Deoyani Shirkhedkar[1]
M.Tech. Student (Comp. Sci. and Engg.)
T.G.P.C.E.T,
Nagpur, M.S. – India

Sulabha Patil[2]
Assistant ProfessorM.Tech.(CSE)
T.G.P.C.E.T,
Nagpur, M.S. – India

Abstract: Cloud computing is facing many challenges as far as security is concerned. Digital provenance that describes the ancestry or history of a digital object is a crucial feature for forensic investigation A second area of research in cloud forensics management is to handle and store a large data set. Secure provenance is of paramount importance to the flourish of cloud computing, yet it is still challenging today. Physical inaccessibility of digital evidence makes the evidence collection procedure harder in cloud forensics. We are going to propose digital forensic technique for cloud environment which will detect two attacks DDos and unauthorized file sharing.

Keywords: cloud computing, digital forensic, hosted desktop.

I. INTRODUCTION

Cloud computing has the potential to become one of the most transformative computing technologies, following in the footsteps of mainframes, minicomputers, personal computers, the World Wide Web and smartphones [7] National Institute of Standards and technology (NIST) defined Cloud Computing as “a model for enabling convenient, on computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [12] Clouds use the multi-tenant usage model and virtualization to ensure better utilization of resources. However, these fundamental characteristics of cloud computing are actually a double-edged sword – the same properties also make cloud-based crimes and attacks on clouds and their users difficult to prevent and investigate. [5].

In Section II, a brief background on cloud forensics is presented. In Section III, a brief overview of digital forensic challenges presented by the cloud paradigm is discussed. In Section IV, a proposed technique that addresses the issues of digital forensics in a cloud environment is presented. Section V concludes the paper.

II. BACKGROUND

This section, presents background concepts on cloud forensics.

A. CLOUD FORENSICS

Cloud forensics is a cross discipline of cloud computing and digital forensics. Cloud computing is a shared collection of configurable networked resources (e.g., networks, servers, storage, applications and services) that can be reconfigured quickly with minimal effort [11]. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law [7].

Cloud forensics procedures will vary according to the service and deployment model of cloud computing. For SaaS and PaaS, we have very limited control over process or network monitoring. Whereas, we can gain more control in IaaS and can deploy some forensic friendly logging mechanism. The first three steps of computer forensics will vary for different services and deployment models. For example, the collection procedure of SaaS and IaaS will not be same. For SaaS, we solely depend on the CSP to get the application log, while in IaaS, we can acquire the Virtual machine instance from the customer and can enter into examination and analysis phase. On the other hand, in the private deployment model, we have physical access to the digital evidence, but we merely can get physical access to the public deployment model.[5]

III. Cloud Forensic Challenges

Digital forensic faces various challenges in the cloud computing environment. Digital provenance that describes the ancestry or history of a digital object is a crucial feature for forensic investigation. Iaas vm do not have any persistent storage. In most of the cases all volatile data is lost if vm is rebooted or powered down. Management issues which could arise during a cloud forensics investigation. A second area of research in cloud forensics management is to handle and store such a large data set. Secure provenance is of paramount importance to the flourish of cloud computing, yet it is still challenging today. Physical inaccessibility of digital evidence makes the evidence collection procedure harder in cloud forensics. Volatile data cannot sustain without power. When we turn off a Virtual Machine (VM), all the data will be lost if we do not have the image of the instance. Chain of custody is defined as a verifiable provenance or log of the location and possession history of evidence from the point of collection at the crime scene to the point of presentation in a court of law. It is one of the most vital issues in traditional digital forensic investigation. The preservation and availability of forensically-relevant metadata remains an open problem. Procedure and a set of toolkits to retrieve forensic data involving confidential data under jurisdiction(s) and agreement(s) under which services are operating.

IV. Proposed Techniques

In this section, we propose and present a technique for forensic investigation in cloud. The proposed technique addresses issues such as:

1. To detect following two network attacks.

   (a) Intrusion

   (b) DDos

2. To collect forensically sound evidence in a cloud environment

A. *DIGITAL FORENSIC SERVICE APPLICATION SCENARIO*

A virtual machine hosted in a cloud environment is used to commit crime as it used to be done with physical computers.. In this section, two scenarios of criminal activities carried out in the cloud are considered, i.e., DDoS attacks and unauthorized file sharing.

B. *ENVIRONMENTAL SET-UP*

The environment is set up using two Desktop PC's, each running Ubuntu 12.04. Here, open source cloud manager, OpenStack will be used. One of the hosts running OpenStack host virtual machines. Three virtual machines can be deployed in OpenStack where one virtual machine can be used to launch attacks and one of the Virtual machines can be used to monitor communications between the attacker and the victim virtual machine. The attacker uses the second physical host to access their virtual machine hosted in OpenStack. The monitoring virtual machine can use WireShark and nmap to monitor activities occurring in the victim machine.

In this proposed system we create three virtual machines as follows:-

1) VM1 - This is the attacker machine with IP address 10.0.1.21.Ubuntu desktop is installed on this machine for GUI.

2) VM2- This is the victim machine with IP address 10.0.1.16.Apache server is installed on this machine.

3) VM3- This is monitor which monitors the system. Monitoring tools wireshark and nmap are installed on this machine.

All virtual machines will be SSH unabled. NTP server is configured for this cloud. Each VM can be accessed by using three ways terminal, browser and GUI. The attacks will be performed by attacker machine on victims and monitor, will monitor them. The system state can be recorded before and after attack by system monitor. We can get Log information from WireShark.

V. Conclusion

This paper proposes a digital forensic technique for cloud environment. The propose system will address the issues in cloud forensics like live forensics. It also detect two attacks the DDos attack and unauthorized file sharing.

References

1. Dominik Birk , Christoph Wegener" Technical Issues of Forensic Investigations in Cloud Computing Environments"
2. Rongxing Lu,Xiaodong Lin,Xiaohui Liang and Xuemin(Sherman) Shen," Secure Provenance : The Essential of Bread and Butter of Data Forensics in Cloud Computing"
3. George Grispos Tim Storer William Bradley Glisson," Calm Befor the Storm:The Challenges of Cloud Computing in Digital Forensics"
4. Concepts of digital forensics
5. Shams Zawoad, Ragib Hasan," Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems",26 Feb 2013
6. Simson L. Garfinkel," Digital Forensics Research:The next 10 years",www.elsevier.com/locate/diin (2010)
7. Keyun Ruan,Prof.Joe Carthy,Prof. Tahar Kechadi,Mark Crosbie," Cloud Forensics:An Overview"
8. Josiah Dykstra , Alan T. Sherman,"Understanding Issues In Cloud Forensics:Two Hypothetical Case Studies"
9. Chu-Hsing Lin, Chen – Yu Lee and Tang- Wei Wu ," A Cloud – aided RSA Signature Scheme for Scaling and Storing the Digital Evidences in Computer Forensics" International journal of security and its Applications vol.6.No.2,April ,2012
10. Keyun Ruan,Prof.Joe Carthy,Prof.Tahar Kechadi,Ibrahim Baggili(PhD)," Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability:A Preliminary Analysis"Jounal of Network Forensics vol.3,Issue 2011
11. George Sibiya,Hein S. Venterand Thomas Fogwill,"Digital Forensic Framework for a cloud Environment",IST-Africa 2012 conference proceedings
12. Rainer Poisel, Erich Malzer, and Simon Tjoa," Evidence and Cloud Computing: The Virtual Machine Introspection Approach" Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 4, number: 1, pp. 135-152
13. Wireshark: The world's foremost network protocol analyser, [Online] Available at: http://www.wireshark.org/ [Accessed 30 November 2014].
14. http://nmap.org/, [Accessed 10 December 2014].
15. https://cloudsecurityalliance.org/, [Accessed 20 November 2014].
16. D. Birk, Technical challenges of forensic investigations in cloud computing environments.[Online]Available at: http://www.zurich.ibm.com/~cca/csc2011/submissions/ [Accessed 15 November 2014].
17. C. V. Blanco, The opennebula virtual infrastructure engine, [Online] Available at: http://www.xen.org/files/xensummit_germany09/OpenNebula.pdf[Accessed20November 2014].
18. R. Buyya, S. Pandey, and C. Vecchiola, Cloudbus toolkit for market-oriented cloud computing. 2009. CloudCom, Springer-Verlag Berlin Heidelberg, pp 24–44.
19. S. Castro, Virtual machine trojan: A new type of threat. [Online] Available at: http://www.infosegura.net/VMTthreat.html [Accessed 15 November 2014].
20. E. W. Hobson, Qinetiq white paper: Digital investigations in the cloud, QinetiQ Digital Investigations Service, Farnborough, UK, 2010.
21. Deoyani Shirkhedkar,Sulabha Patil, " Analysis Of Various Digital Forensic Techniques for Cloud Computing", International Journal of Advanced Research in Computer Science, ISSN No. 0976-5697, Volume 5, No. 4, April 2014.