ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Analysis of Various Digital Forensic Techniques for Cloud Computing

Deoyani Shirkhedkar [1] and Sulabha Patil[2]
Dept. of Comp. Science and Engg.
T.G.P.C.E.T, Nagpur , M.S. India.

Abstract— Cloud computing is at its infancy stage and its security is still an open research issue. Malicious users take advantage of the current lack of advanced security mechanisms in the cloud. Cloud computing paradigm enables users to access computing resources without necessarily owning physical infrastructures. It is therefore easy for an attacker who intends to perform malicious activities in the cloud to create a remotely hosted desktop, perform their activities and then destroy the desktop later. With the remotely hosted desktop destroyed, there is very little evidence left that can be collected by forensic experts using traditional static digital forensic methods. The objective of this paper is to review the work of researchers in the area of digital forensic challenges in cloud environment.

Keywords: Cloud Computing, digital forensic, Hosted desktop

I. INTRODUCTION

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] The concept of virtualisation in computing involves operating systems running on another operating system as if they were running on their own hardware [11]. Virtualization provided grounds for the birth of cloud computing [10]. Such developments in computing paradigms present more opportunities for cyber crimes.

In Section II, a brief background on digital forensics ,cloud computing and cloud forensics is presented. In Section III, a brief overview of the work done by various researchers in the area of digital forensics in cloud environment is presented .Section IV discusses the digital forensic challenges presented by the cloud paradigm Section V concludes the paper .

II. BACKGROUND

This section, presents background concepts on cloud computing , digital forensics and cloud forensics.

A cloud has several uses, offering a variety of services and can be deployed in more than one way. The Open Cloud Manifesto Consortium [2009] consortium defines the key aspects as: The ability to scale and provision computing power dynamically in a cost efficient way and the ability of the consumer (end user, organization, or IT staff) to make the most of that power without having to manage the underlying complexity of the technology" Services in a cloud are grouped into three layers, i.e. cloud application, cloud platform and cloud infrastructure [10].

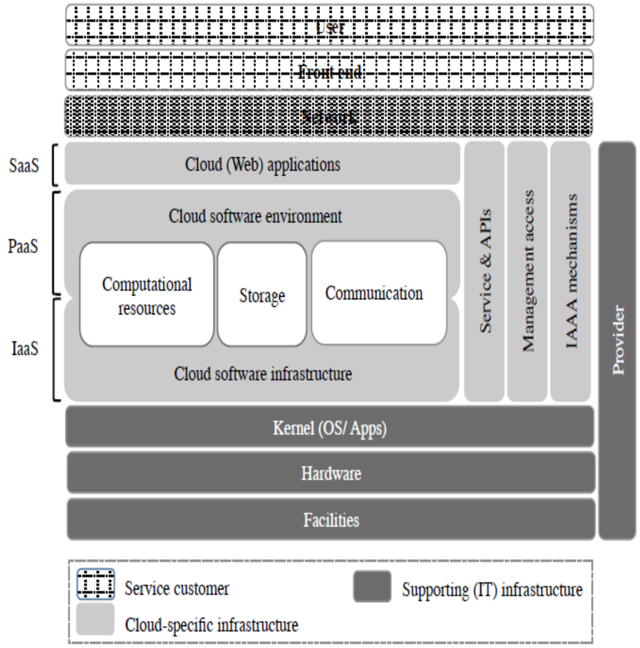

Figure 1 Three service models of cloud computing [5]

These layers in a cloud are offered as services, where we have software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS). One of the services offered in the cloud are Hosted Desktops . A Hosted Desktop is a virtual machine hosted in the cloud. In a hosted desktop, applications and data are hosted on a remote data centre and not in a local user machine as in traditional computers. Hosted desktop owners access their applications and data though ordinary desktops or thin clients. Such a hosted desktop can be used to commit cyber crime in the cloud in the same way as a criminal can use a physical desktop. The authors define cloud crime as "any crime that involves cloud computing where the cloud can be the object, subject or tool of crimes." It is when such crimes are committed in the cloud that the services of a forensic expert will be required.

A. Digital Forensics:

Digital forensics is a branch of forensic science concerned with the use of digital information (produced, stored and transmitted by computers) as source of evidence in investigations and legal proceedings. Digital Forensic Research Workshop has defined digital forensics as “The use of scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."[4]

A digital forensic process can be broken into four distinct phases:

a. Collection of artifacts (both digital evidence and supporting material) that are considered of potential value are collected
b. Preservation of original artifacts in a way that is reliable, complete, accurate, and verifiable
c. Filtering analysis of artifacts for the removal or inclusion of items that are considered of value
d. Presentation phase in which evidence is presented to support investigation.

Traditionally, two categories of digital forensics existed i.e., static digital and live forensics, Static forensics involves analysis of static data such as hard drives obtained using traditional formalized acquisition procedures. Live forensics involves the analysis of the system memory and any other relevant data while the system being analysed is running.[11]

B. 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. OVERVIEW

Dominik Birk and Christoph Wegener[1] describe the importance of research on digital provenance. Digital provenance, meaning meta-data that describes the ancestry or history of a digital object, is a crucial feature for forensic investigations .No research has been published on how cloud computing environments affect digital artifacts, and on acquisition logistics and legal issues related to cloud computing environments which has a huge impact on investigation processes in cloud computing environments the method of Virtual Introspection (VI) for live forensics of virtual instances could be helpful . VI is the process by which the state of a virtual machine is observed from either the hypervisor or from some virtual machines other than the one being examined. However, the fact that the hypervisor has full access to the resources of all VMs represents a significant risk to customers’ data. The issue whether VMs can ever be managed by a hypervisor, while simultaneously being protected from a compromised hypervisor remains an open research problem.

Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen[2] proposed a scheme of bilinear pairing. Cloud computing should also provide provenance to record ownership and process history of data objects in cloud in order for wide acceptance to the public The concept of provenance has been extensively studied for a long time, and widely used in the archival theory to denote the documented history of some data objects . Given its provenance, a data object can report who created and who modified its contents we propose a secure provenance scheme based on the bilinear pairing technique to provide trusted evidences for data forensics in cloud computing. Due to its comprehensive security features, the proposed *SP* scheme provides trusted evidences for data forensics in cloud computing and thus pushes the cloud computing for wide acceptance to the public.. George Grispos,William Bradley Glisson and Tim Storer[3]

This paper has argued that conventional methods and guidelines suggested for conducting digital forensics could well be insufficient in a cloud environment. If current forecasts are correct more businesses and organizations will be moving their data to cloud environments. Together with a continued growth in cyber{crime, this transition could mean there will soon be a demand to conduct forensics investigations in such environments. Such investigations would currently be hampered due to the lack of guidance concerning methods and software tools to retrieve evidence in a forensically sound manner. There is also the need for legal issues regarding clouds including data retention and privacy laws to be re-examined, following the widespread adoption of cloud technologies. Finally there is also the need for the digital forensics community to begin establishing standard empirical mechanisms to evaluate frameworks, procedures and software tools for use in a cloud environment.

Concepts of digital forensics[4] This chapter presented a review of digital forensic concepts. It identified the stages of digital investigative process and described the major types of digital forensic techniques used for examination and analysis of digital evidence.

This chapter presented a review of digital forensic concepts. It identified the stages of digital investigative process and described the major types of digital forensic techniques used for examination and analysis of digital evidence. As a final point, note that the need for effective and efficient digital forensic analysis has been a major driving force in the development of digital forensics. Manual browsing was initially the only way to do digital forensics. It was later augmented with various search utilities and, more recently, with tools such as mactimes and lazarus that support more in-depth analysis of digital evidence.

Shams Zawood and Ragib Hasan[5] systematically examine the cloud forensics problem and explore the challenges and issues in cloud forensics. They discuss existing research projects and finally ,highlight the open problems and future directions in cloud forensics research area. With the increasing use of cloud computing, there is an increasing emphasis on providing trustworthy cloud forensics schemes. Researchers have explored the challenges and proposed some solutions to mitigate the challenges. In this article, authors have summarized the existing challenges and solutions of cloud forensics.

Simson L. Garfinkel[6] This paper argues that we have been in a “Golden Age of Digital Forensics,” and that the Golden Age is quickly coming to an end. Increasingly organizations encounter data that cannot be analyzed with today’s tools because of format incompatibilities, encryption, or simply a lack of training. Even data that can be analyzed can wait weeks or months before review because of data management issues. Without a clear research agenda aimed at dramatically improving the efficiency of both our tools and our very research process, our hard-won capabilities will be degraded and eventually lost in the coming years. This paper proposes a plan for achieving that dramatic improvement in research and operational efficiency through the adoption of systematic approaches for representing forensic data and performing forensic computation.

Keyun Ruan, Joe Carthy, Tahar Kechadi and Mark Crosbie[7] stated challenges to cloud forensics

A. *Forensic Data Collection:*

The challenges are to recover the deleted data, identify the ownership of the deleted data, and use the deleted data for event reconstruction in the cloud.

B. *Virtualized Environments:*

Cloud computing provides data and computational redundancy by replicating and distributing resources. Most CSPs implement redundancy using virtualization.

C. *External Dependency Chains:*

CSPs and most cloud applications often have dependencies on other CSPs a cloud forensic investigation thus requires investigations of each individual link in the dependency chain. Correlation of the activities across CSPs is a major challenge .

D. *Live Forensics:*

Deleted data is an important source of evidence in traditional digital forensics. In the cloud, the customer who created a data volume often maintains the right to alter and delete the data Josiah Dykstra and Alan T. Sherman[8] stated that Forensic acquisition is a renewed challenge, one unsuited for today's tools, which will possibly be addressed by a combination of technological and legal approaches. We have begun to evaluate the ability of popular forensic tools to obtain evidence from a cloud environment. Cooperation with providers will empower consumers to understand their risks and give them leverage to prosecute crimes. The preservation and availability of forensically-relevant metadata remains an open problem.

Chu-Hsing Lin1, Chen-Yu Lee2 and Tang-Wei Wu[9]1 propose a new digital forensics structure for RSA signature in cloud computing. This cloud structure can archive privacy, save computing power on mobile devices token by forensics officers. By RSA signature protocol, the verifier can verify the evidences in the court. Moreover, this protocol could be applied to many areas, such as digital forensics, online voting, or E-commercial, etc

Keyun Ruan, Ibrahim Baggili (PhD),Prof Joe Carthy, Prof Tahar Kechadi[10] present the current results and analysis of the survey “Cloud forensics and critical criteria for cloud forensic capability” carried out towards digital forensic experts and practitioners. This survey was created in order to gain a better understanding on some of the key questions of the new field cloud forensics before further research and development information from log files in locations which were determined to have been accessed by the suspect.

IV. DIGITAL FORENSIC CHALLENGES

Following are the challenges posed by various researchers in the above mentioned papers under study:-

a. Digital provenance that describes the ancestry or history of a digital object is a crucial feature for forensic investigation
b. 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
c. Management issues which could arise during a cloud forensics investigation.
d. A second area of research in cloud forensics management is to handle and store such a large data set.
e. Secure provenance is of paramount importance to the flourish of cloud computing, yet it is still challenging today.
f. Physical inaccessibility of digital evidence makes the evidence collection procedure harder in cloud forensics.
g. 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
h. 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
i. The preservation and availability of forensically-relevant metadata remains an open problem

j. Procedure and a set of toolkits to retrieve forensic data involving confidential data under jurisdiction(s) and agreement(s) under which services are operating

V. CONCLUSION

This paper gives the overview of challenges posed by digital forensics in cloud environment. This paper also argues that there is a need of research in cloud forensics It also highlight some areas of digital forensic research in cloud as follows:-

a. Log data and other forensic information should be preserved
b. Need of VMI(virtual machine introspection)
c. Develop alternative frameworks and guidelines as well as tools to combat cyber-crime in the cloud.
d. Tools and procedures are yet to be developed for investigations in virtualized environment, especially on Hypervisor level.
e. Analyzing logs from different processes plays a vital role in digital forensic investigation ,gathering this crucial information in cloud environment is not as simple as it is in privately owned computer.
f. Forensic analysts need a tool for parsing, searching and extracting information from virtual machine snapshots, including suspended memory state.
g. Introduce data provenance in order to track the history and access of cloud objects.

VI. 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