RESEARCH ARTICLE OPEN ACCESS

Cloud Forensics: Drawbacks in Current Methodologies and Proposed Solution

Devashree Shirude, Shivani Soman, Ved Paranjape, Geet Pradhan
(Department of Computer Science and Engineering, Maharashtra Institute of Technology, Pune-38)
(Department of Computer Science and Engineering, Maharashtra Institute of Technology, Pune-38)
(Department of Computer Science and Engineering, Maharashtra Institute of Technology, Pune-38)
(Department of Computer Science and Engineering, Maharashtra Institute of Technology, Pune-38)

ABSTRACT
Cloud Computing is a heavily evolving domain in technology. Many public and private entities are shifting their workstations on the cloud due to its robust, remote, virtual environment. Due to the enormity of this domain, it has become increasingly easier to carry out any sort of malicious attacks on such cloud platforms. There is a very low research done to develop the theory and practice of cloud forensics. One of the main challenges includes the inability to collect enough evidence from each and every subscriber of a Cloud Service Provider(CSP) and thus not being able to trace out the roots of the malicious activity committed. In this paper we compare past research done in this field and address the gaps and loopholes in the frameworks previously suggested. Overcoming these, our system/framework facilitates the collection, organization, and thereby the analysis of the evidence sought, hence preserving the essential integrity of the sensitive and volatile data.

Keywords: cloud computing, cloud forensics, digital forensics, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), virtual environment

I. INTRODUCTION

'Making life easy while on the go !' is the underlying objective of Cloud Computing. A “cloud” basically an Internet-based model which offers to provide numerous processing resources and data to computers and other computing devices on demand. Cloud functions by enabling ubiquitous, on-demand access to a variety of resources like networks, data, memory/storage, applications, games and more. These resources can be used and managed easily on the go with the users only being charged for their actual usage. Also, these resources derived from eclectic sources can be accessed from different corners of the world.

"All that glitters is not gold !" All of us are very much familiar with this saying regardless of the context of annotation.

In the context of the current buzzwords in technology: "Cloud Computing" and "Cloud Platforms", this saying holds a very significant stature. These current upcoming technologies successfully entice a large number of users in the public as well as private domains. These umpteen users tend to conveniently ignore the horde of issues related to security and data privacy initially, until they fall prey to them themselves. There was/is no such fool-proof system that can address such sensitive issues by providing a system that will allow the innocent end users to use the cloud platform in any form being absolutely carefree. In the subsequent paper, we aim to strike at the various shortcomings discovered in the varied research carried out in the field of Cloud Forensics entailed by the proposal of a new system architecture.

Initially, we will take a look at the benefits as well as the issues of cloud briefly.The common benefits associated with adopting cloud computing are:

- Reduced Investments and Proportional Costs
- Increased Scalability
- Increased Availability and Reliability

"Every coin has two sides" and so does these cloud platforms! Many of these severe issues encountered by the majority of both the public as well as private cloud consumers are listed below :

- Increased Security Vulnerabilities
- Reduced Operational Governance Control
- Limited Portability Between Cloud Providers
- Multi-regional Regulatory and Legal Issues

To address the issue of increasing vulnerability of the cloud platform at the user's end, forensics in the field of computer science is gaining popularity. The increase in issues like frauds on the cloud, DDOS attacks, depriving of services and other such malicious activities on the cloud, the field of Cloud Forensics has caught the attention of the cyber experts and forensic experts. Day by day as the cloud is gaining more and more popularity, it is becoming a matter of grave concern for the forensic experts as the number of attacks on innocent users followed by their depravity of rights and sensitive data are increasing at an alarming rate.

II. LITERATURE REVIEW

There are already several cases of attacks carried out on information stored in cloud systems. For example, in January 2010, Google announced that its Single Sign On software had been hacked [1]. In another incident [2] a hacker penetrated Twitter's financial documents and other business information stored in a Twitter employee's Google account. It is clear that security breaches of cloud service providers are increasingly common.

Computer forensics is the process of preserving, collecting, confirming, identifying, analysing, recording, and presenting crime scene information. Wolfe defines computer forensics as "a methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format" [3]. According to a definition from NIST [4], computer forensics is "an applied science to identify an incident, collection, examination, and analysis of evidence data". In computer forensics, maintaining the integrity of the information and strict chain of custody for the data is mandatory. Several other researchers define computer forensic as the procedure of examining computer system to determine potential legal evidence [5], [6].

[7] defines Cloud forensics as the application of computer forensic principles and procedures in a cloud computing environment.

The study carried out in [7] proposed the following flow for - Forensic Process Flow as shown in Fig 1 :

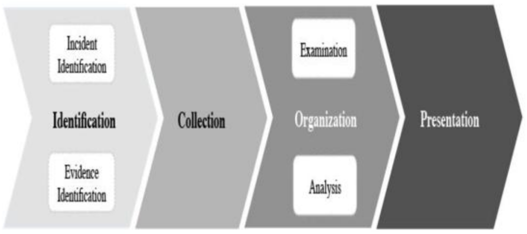

Fig. 1. Forensic Process Flow

Identification: Identification process is comprised of two main steps: identification of an incident and identification of the evidence which will be required to prove the previously identified incident.
Collection: In the collection process, an investigator extracts the digital evidence from different types of media e.g., hard disk, cell phone, e-mail, and many more. Additionally, he needs to preserve the integrity of the evidence.
Organisation: There are two main steps in organisation process: examination and analysis of the digital evidence. In the examination phase, an investigator extracts and inspects the data and their characteristics. In the analysis phase, he interprets and correlates the available data to come to a conclusion, which can prove or disprove civil, administrative, or criminal allegations.
Presentation: In this process, an investigator makes an organised report to state his findings about the case. This report should be appropriate enough to present to the jury.

The papers seen above have addressed only the theoretical aspects of cloud forensics. They have sidelined the practical implementation and thus, up to a certain extent, have failed to address the practical aspects of their statements.

III. CURRENT METHODOLOGIES

In [8], the authors have proposed the Open Cloud Forensics Model(OCF). Based on this model, they have proposed and a cloud computing architecture and validated the proposed model with a case study inspired from a lawsuit. In the following year [9], they implemented their proposed model on top of OpenStack.

On similar lines in [10], they have described the design, implementation, and evaluation of FROST—three new forensic tools for the OpenStack cloud platform. Operated through the management plane, FROST provides the first dedicated forensics capabilities for OpenStack, an open-source cloud platform for private and public clouds.

Their implementation supports an Infrastructure-as-a-Service (IaaS) cloud and provides trustworthy forensic acquisition of virtual disks, API logs, and guest firewall logs.

Their tools are user-driven, allowing customers, forensic examiners, and law enforcement to conduct investigations without necessitating interaction with the cloud provider.

In the above practical implementation solutions provided, the designs fail to address the supporting of an extensible set of forensic objectives, including the future addition of other data preservation, discovery, real-time monitoring, metrics, auditing, and acquisition capabilities.

One open problem of the above proposed solution is preservation of data in the cloud. Rapid elasticity is a feature of cloud computing, but it comes with the challenge of preserving data in an investigation until that data can be identified and retrieved. OpenStack needs the capability for manual or automatic data preservation to maintain the record of activity of a malicious cloud user.

Another open problem is the evolution and maturity of OpenStack. OpenStack has an active development community and regular software releases. Future modifications to OpenStack may affect FROST's functionality.

FROST implements only the acquisition phase of the forensic process, and does not address solutions for other phases of the process affected by cloud computing such as organisation, analysis and presentation.

IV. PROPOSED FRAMEWORK

Currently, as stated above, there exists no such cloud model which provides forensic friendly Platform as a Service (PaaS) environment. What we aim to propose through our model is a forensically sound cloud platform which provides easy access to volatile cloud specific data/evidence. Prior to developing such a model, we need to identify the stakeholders and define a scope for the project. The possible stakeholders could be Cloud Service Providers' administrators, forensic analysts/investigators and cloud customers.

The basic underscoring objective of our project is to offer a forensic friendly cloud framework. Hence we aim at bringing together all the required evidence in a particular format so as to aid the forensic analyst in order to eventually to carry out the required enquiries followed by the suitable prosecution in a licit fashion.

The avoidable side-effects of our project scope will be trying to minimise the inclusion of the non-essential logs in the eventual evidence-report, simultaneously maximising the reliability, relevance and authenticity of the evidences collected preserving the chain of custody at each stage.

V. CONCLUSION AND FUTURE WORK

There currently exists no such forensically secure cloud platform and there are certain loopholes in existing tools. For example, all the current systems and tools available for cloud forensics do not readily monitor real time systems which is a major shortcoming as both the crime scene details as well as the evidence collection and presentation becomes too cumbersome and difficult. Hence the underscoring objective of the project is to design such a system overcoming these fall-throughs.

We are trying to minimise the inclusion of the non-essential logs in the eventual evidence-report, simultaneously maximising the reliability and relevance as well as the authenticity of the evidences collected preserving the chain of custody at each stage.

Also understanding the social relevance of the project as to benefit the end-users as well as the forensic experts by trying to provide a "safe" cloud environment, we foresee a fully-functional forensic friendly cloud framework that benefit the interests of all the stakeholders involved eventually.

Eventually we will try and add a legal dimension to our project by which we can encompass multiple licit documents onto a single platform and hence make the system universal and generalised. A possible integration with pre existing CSP may also be considered in the future.

REFERENCES

Journal Papers:

[1]. J. Markoff, *(2010)*, "Cyberattack on Google Said to Hit Password System," *The New York Times*.[Online]. Available:*http://www.nytimes.com/2010/04/20/technology/20google.html?sudsredirect=true.*

[2]. J. D. Sutter, *(2009)*,"Twitter Hack Raises Questions About Cloud Computing," [Online]. Available: *http://edition.cnn.com/2009/TECH/07/16/twitter.hack/index.html*

[3]. J. Wiles, K. Cardwell, and A. Reyes, The best damn cybercrime and digital forensics book period. *Syngress Media Inc, 2007.*

[4]. K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Special Publication, pp. 800–86, 2006.*

[5]. D. Lunn, "Computer forensics–an overview," *SANS Institute, vol. 2002*, 2000.

[6]. J. Robbins, "An explanation of computer forensics," *National Forensics Center, vol. 774*, pp. 10–143, 2008.

[7]. Shams Zawoad and Ragib Hasan,Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems, *26th February-2013 (arXiv: 1302.6312v1).*

[8]. S. Zawoad, R. Hasan, and A. Skjellum, "OCF: An Open Cloud Forensics Model for Reliable Digital Forensics," *Proc. th IEEE Int'l Conf. Cloud Computing (CLOUD), 2015 , pp. 437-444.*

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

[10]. Josiah Dykstra,Alan T. Sherman,"Design and Implementation of FROST: Digital Forensic Tools for the OpenStack Cloud Computing Platform," *International Journal of Digital Forensics & Incident Response, vol. 10, pp. S87-S95,2013.*