ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

Need of Digital Forensics in Cloud Computing Enviornment

Shraddha Suratkar [1]

Assistant Professor, Department of Computer Engineering, VJTI College, Mumbai, Maharashtra, India[1]

ABSTRACT: Cloud computing is one of the rapidly growing technologies in the field of Information Technology which is getting more and more attention from the information and communication technologies to industries recently. All the leading organizations show their interest in the services provided by cloud. But the increasing use of cloud services is attracting many internet users resulting in criminal activities. Thus, more efforts should be made in forensics analysis of cloud storage services. The cloud data should be prevented from getting compromised. A forensic tool should be developed which will analyse the metadata generated from cloud database to trace the criminal activities. Also, in case of deleted data, some provisions should be made to reconstruct the deleted data. This survey paper reviews the need of digital forensics in cloud computing. A brief literature on some challenges in implementing the phases of digital forensics in cloud computing is also mentioned along with comparative study of few tools available for digital forensics.

KEYWORDS*:* Cloud computing, MDD5, SHA, digital forensics, Forensic Investigation, Evidence, IaaS, PaaS, Dbaas.

I. INTRODUCTION

Digital forensics is a branch of science which pertains for acquiring, examining, analyzing, and possibly documenting and presenting the said artifacts and the reconstructed sequence of events as evidence in front of judiciary [1][3].Until recently, traditional digital investigations often excluded databases even though evidence can usually be found in them[2]. Although the field is still in its early years, it is quickly becoming an important part of many investigations due to the increased volume of information that may be helpful in solving different crimes and the large number of risks associated with the information stored on many databases. Of major importance in database forensics which is one of the branches of digital forensics has the ability to retrace the operations performed on a database and reconstruct deleted or compromised information on the database. This requirement affects how data is collected and analyzed during the forensics analysis of a database. Although new advance forensics tools like Idea, Arbutus etc. are coming into existence but the hackers are also becoming equally equipped with anti-forensics tools to erase those digital evidences or to produce delay in the digital evidence generation process. As a result the culprit is not getting punishment within the defined interval of time. Hence there is an imperative need of an open source database forensics tool which will forensically analyze the database said artifacts generating evidence preventing major database attacks as well as detecting anti-forensics attacks.

There is a big demand from forensic investigator to develop a forensic tool for cloud computing environment. Thus, the process of digital forensic is explained in section III of paper. Comparative study of forensics tools is included in section IV. The need of digital forensics in cloud computing is included in section V. Section VI explains why clouds are not forensics friendly. Requirements for forensics enabled cloud are explained in section VII of paper and Section VIII of Paper includes materials and methods used followed by conclusion in Section IX.

II. RELATED WORK

Following subsection feature published work describing the origin and evolution of Digital Forensics in Cloud Computing.

Recently, cloud computing has become very popular among businesses and individuals. This is because cloud model of computing promises increased flexibility, great reliability, massive scalability, and decreased costs. According to NIST [5], cloud computing is a model for always on, convenient, on demand network access to a shared pool of configurable resources (e.g. networks, servers, storage, applications and services) that can be rapidly

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

provisioned and released with minimal management effort or service provider interaction. Cloud computing provides computing services and storage by using virtualization which makes the cloud resources invisible to the user. A common application of cloud computing service is cloud storage services. Cloud storage services such as Dropbox provide storage to the individuals and businesses. Cloud storage services are used by people for backup purposes and for sharing documents, pictures, videos, and multimedia files with others. The advent of cloud storage services has raised concerns about the degree of security of could environment [15]. The advent of cloud storage services has raised concerns about the degree of security of could environment [16]. This is because current cloud offers proprietary solutions for dealing with security issues. Another concern is that computer forensics investigation in the cloud computing environment is more complicated. Challenges to cloud forensics have been categorized into technical, legal and organizational [10].It is suggested that more research and development of methodologies and tools on evidence gathering from the cloud environment are needed [14].

III. PROCESS OF DIGITAL FORENSICS

Digital forensics is the process of obtaining, preserving, analyzing, documenting digital evidence from digital devices, such as PCs, server, PDA, digital camera, fax Machine, iPod, smart phone, and various memory storage devices and presenting the evidence against criminal in court of law. Thus, computer forensics are divided into six phases as illustrated in Figure. l. The following is a brief description of the six phases [1].

- Evidence identification: This phase identifies various sources of digital evidences from various digital devices..
- Evidence collection: This phase gathers physical items those contain potential digital evidences.
- Evidence acquisition: This phase creates multiple copies of the information according to the defined sets for analysis.
- For example, we usually use the computer forensics tool to create a disk image.
- Evidence preservation: This phase is focused on using the methods that are reliable and verifiable.
- Evidence analysis: This phase extracts digital information that is significant to criminal investigation.
- Evidence presentation: The final phase documents the analyzing results. And it could present the digital evidence against criminal.

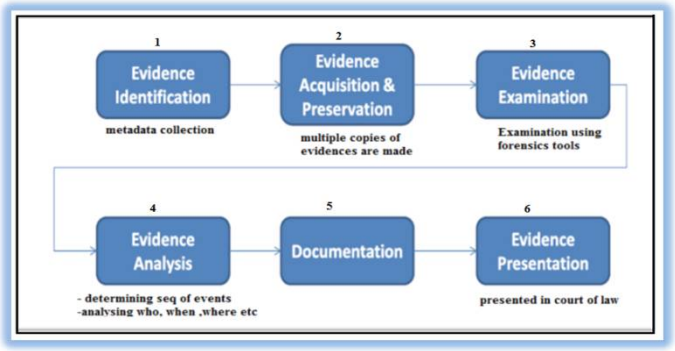

Fig. 1 A multi-staged digital forensics process

IV. COMPARATIVE STUDY OF FORENSICS TOOLS

The research work in the field of digital forensics pertains that most of the areas of this field are still in dark ages. The unavailability of fully developed tools for digital forensics is a reflection of the little amount of research that has been done in the field. These tools should allow information from different sources on a database to be gathered and assist in investigating and recovering of information regardless of the complexity of data or dimensions involved in the investigation. They should also be able to determine when and what data has been compromised or damaged .Quite a number of researches are also on-going on the development of new tools. Although many of the tools being used for digital forensics have been helpful for collecting data and identifying transactions that indicate fraudulent activities,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

most of these tools are not accurate or precise enough to be used as a forensics tool. Table below (Table 1) shows the comparative study of different forensic tools.

Name	Platform	License	Description	Drawbacks
EnCase	Windows	proprietary	Forensic tool to Perform only text indexing and searching.	No log analysis or network analysis possible.
FTK	Windows	proprietary	Multi-purpose tool commonly used to index acquired media.	No log analysis or network analysis possible.
PyFlag	Windows	Open source	Can examine forensics images, memory dumps, logs and network captures	Manual analysis of reports of multiple digital evidences sources is to be done.
OCFA	Windows	Open source	Perform only text indexing and searching	No log analysis or network analysis possible
Wireshark	Windows	proprietary	Examine only network Captures.	No log analysis or text index searching is possible.
The Sleuth Kit	Unix like/Windows	proprietary	A library of tools for both Unix and Windows. Perform only text indexing and searching.	No log analysis or network analysis possible.
Oracle Log Miner	Independent of platform	Utility Provided to Oracle purchasers only.	A utility that can be used to analyze only the redo and undo log files that are created by an Oracle database	It did not support retrieval of data from columns with Large Object (LOB) data types.
SQL Trace	Independent of platform	Interface provided with SQL Server	Interface made available through extended stored procedures to identify poorly running SQL statements, and to debug other performance problems.	It does not audit or monitor systems on continuous basis. It is inadequate in tracing what, when, or who is being audited.

Table 1: Study of different digital forensic tools

V. NEED OF DIGITAL FORENSICS IN CLOUD COMPUTING

A. Classification of Cloud Computing Services

Cloud computing has been classified based on the types of services it provides [4]. These classifications are briefly summarized here.

1) Infrastructure as a Service: IaaS (Fig. 2) refers to on-demand provisioning of infrastructural resources, usually in terms of VMs. The cloud owner who offers IaaS is called an IaaS provider. This is also called Utility Computing.

2) Platform as a Service: PaaS (Fig. 2) refers to providing platform layer resources, including operating system support and software development frameworks.

3) Software as a Service: SaaS (Fig. 2) refers to providing on demand applications over the Internet.

4) Database as a Service: Dbaas (Fig. 3) is a cloud-based approach to the storage and management of structured data. DBaaS delivers database functionality similar to what is found in relational database management systems (RDBMSes) such as SQL Server, MySQL and Oracle.

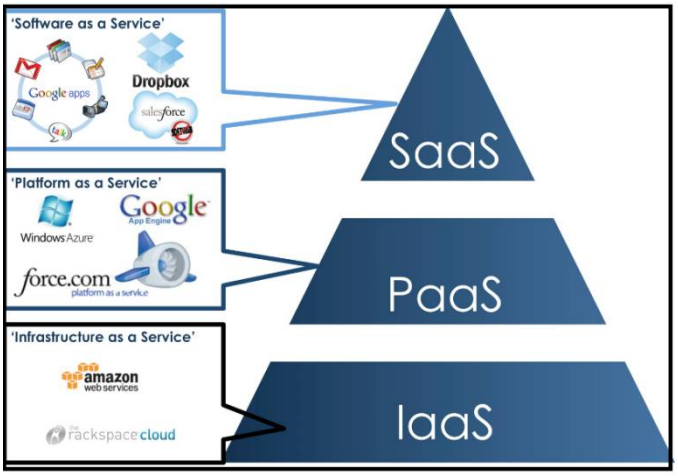

Fig. 2 Cloud computing Services

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

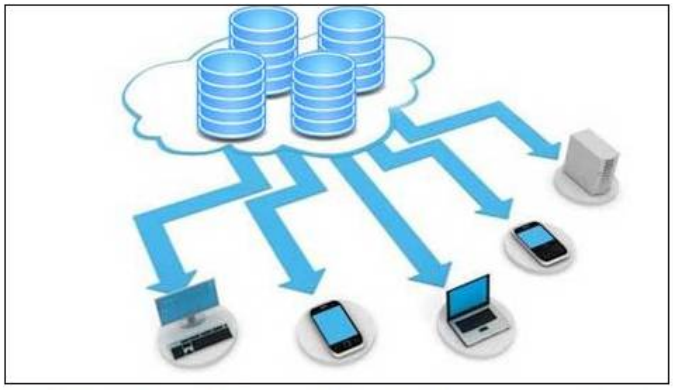

Fig. 3 Database as a Service by Cloud

Cloud Computing could be in the form of public, private, hybrid, or virtual private [5]. The services are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion. These services could be in the form of general enterprise application development infrastructure, server or storage services. Cloud storage services are becoming more popular among business and individual users in recent years. Various computer users are taking advantage of opportunities to automate backups, make files available offline or from any computer, share files and photos, and so on for free. In addition, uses of smart phone apps allow an even greater level of access to people who want to be able to access their files from anywhere. While Cloud storage services are quite useful, there are some concerns about the security of data being on the cloud even if they are in password-protected accounts. Another concern about cloud storage providers comes from computer forensics investigators. With the data being stored on the cloud servers with unknown locations, it would be very difficult for computer forensics investigators to acquire and examine possible misuse of resources by criminals.

B. Need of Digital Forensics in Cloud computing

Cloud computing technologies have significant potential to revolutionize the way organizations provision their information technology (IT) infrastructure. Migration to cloud computing involves replacing much of the traditional IT hardware found in an organization's data centre (including servers, racks, network switches and air conditioning units) with virtualized, remote, on-demand software services, configured for the particular needs of the organization. These services can be hosted and managed by the user organization (on a reduced hardware base), or by a third-party provider. Consequently, the software and data comprising the organization's application may be physically stored across many different locations, potentially with a wide geographic distribution. However, the use of cloud computing presents significant challenges to the users of clouds (both individuals and organizations), as well as regulatory and law enforcement authorities. When security breaches, attacks or policy violations occur, it may be necessary to conduct a digital forensic investigation [6].

VI. WHY CLOUDS ARE NOT FORENSICS FRIENDLY

Following are the characteristics of cloud computing which obscure the process of cloud forensics [7].

i) Massive storage system: As the storage system is no longer local, law enforcement agents cannot confiscate the suspect's computer and get access to the digital evidence even with a subpoena. Live Forensics analysis is not possible in cloud. In a cloud, each server contains files from many users. Hence, it is not feasible to seize servers from a data center without violating the privacy of many other benign users. Moreover, even if the data belonging to a particular suspect is identified, separating it from other users' data is difficult. The fidelity of the evidence is also questionable, because other than the cloud provider's word, there is no usual way to link a given evidence to a particular suspect.

ii)Inaccessibility of Evidence: In traditional computer forensics, investigators have full control over the evidence (e.g., hard disks , router logs, process logs). Unfortunately, in a cloud, the control over data varies in different service models. Cloud users have highest control in IaaS, least control in SaaS and no control in DbaaS. This physical

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

inaccessibility of the evidence and lack of control over the system make evidence acquisition a challenging task in the cloud. For example, in SaaS, it is not possible for customers to get a log of their system, unless the CSP provides the logs. In PaaS, it is only possible to get the application log from the customers. To get the network log, database log, or operating system log we need to depend on the CSP. In IaaS, customers can only get the operating system logs, they do not have access to network or process logs.. For example, Amazon does not provide load balancer logs to the customers, and it is not possible to get MySql log data from Amazon's Relational Database Service. In Dbaas, customers do not get any of the audit log files from database

iii) Cloud computing is a multi-tenant system: Traditional computing is a single owner system while cloud is a multi tenant system. To give an analogy, the cloud can be compared to a motel, while the other can be compared to a personal house. In a cloud, multiple Virtual Machines (VM) can share the same physical infrastructure, i.e., data for multiple customers can be co-located. An alleged suspect may claim that the evidence contains information of other users, not her. In this case, the investigator needs to prove to the court that the provided evidence actually belongs to the suspect. Conversely, in traditional computing systems, a suspect is solely responsible for all the digital evidence located in her computing system. Moreover, in the cloud, we need to preserve the privacy of other tenants. The multi-tenancy characteristic also brings novel side-channel attacks that are difficult to investigate.

iv) Cloud has volatile data: Volatile data cannot sustain without power. Data residing in a VM are volatile, as after terminating a VM, all the data will be lost. In order to provide the on demand computational and storage service, CSPs do not provide persistent storage to VM instances. There is, though, a way to preserve VM data by storing an image of the VM instance. An attacker can exploit this vulnerability in the following way: after doing some malicious activity (e.g., launch DoS attack, send spam mail), an adversary can terminate her VM that will lead to a complete loss of the evidence and make the forensic investigation almost impossible. A malicious user can also fraudulently claim that her instance was compromised by someone else who had launched a malicious activity. In the absence of any evidence, it will be difficult to prove her claim as false via a forensic investigation.

v) Chain of custody: It is one of the most vital issues in traditional digital forensic investigation. Chain of custody should clearly depict how the evidence was collected, analyzed, and preserved in order to be presented as admissible evidence in court . In traditional forensic procedure, it is trivial to maintain W's of corruption event of a suspect. On the other hand, in a cloud, we do not even know where a VM is physically located. Also, investigators can acquire a VM image from any workstation connected with the internet. The Investigator's location and a VM's physical location can be in different time zones. Hence, maintaining a proper chain of custody is challenging in clouds.

vi) Integrity of an Evidence: Currently, investigators are completely dependent on CSPs for acquiring cloud evidence. However, the employee of a cloud provider, who collects data on behalf of investigators, is most likely not a licensed forensics investigator and it is not possible to guarantee his integrity in a court of law. A dishonest employee of a CSP can collude with a malicious user to hide important evidence or to inject invalid evidence to prove the malicious user is innocent. On the other hand, a dishonest investigator can also collude with an attacker. Even if CSPs provide valid evidence to investigators, a dishonest investigator can remove some crucial evidence before presenting it to the court or can provide some fake evidence to the court to frame an honest cloud user. In traditional storage systems, only the suspect and the investigator can collude. The three-way collusion in the cloud certainly increases the attack surface and makes cloud forensics more challenging.

VII. REQUIREMENTS OF CLOUD COMPUTING FOR DIGITAL FORENSICS

For forensics enabled cloud, following points should be implemented:

i) Storage of volatile data from cloud in Persistent databases: As CSPs do not provide constant storage to VMs, turning off or rebooting a VM will eventually lose all the data residing in that VM. Volatile data must be stored in persistent databases so that even if a malicious user terminates her virtual machine, we can still gather the evidence.

ii) Maintaining the integrity of Generated Evidence: After preserving all the evidence, CSPs need to ensure the integrity of the evidence in order to prevent it from several anti-forensics attacks carried out to tamper the generated evidence. Without integrity preservation, the trustworthiness of generated evidence will be questionable. It may happen that the forensic investigator himself is a fraud and tampering the cloud database. Hence some hashing method like MD5 or SHA can be applied on the generated evidence which later can be validated in order to check the integrity of generated evidence. Trusted Platform Module (TPM) can also protect the integrity of cloud evidence. By using a TPM, we can get machine authentication, hardware encryption, signing, secure key storage, and attestation. It can provide the integrity of the running virtual instance, trusted logs, and trusted deletion of data to customers.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

iii) Providing proper chain of custody information: Besides preserving the integrity of evidence, CSPs also need to provide proper chain of custody information. As provenance provides the history of an object, by implementing cloud provenance, CSPs can provide the chronological access history of evidence, how it was analyzed, and preserved, which can ensure the chain of custody for cloud forensics. However, as all the evidence and the access histories are under the control of CSPs, they can always tamper with the provenance record. Moreover, from the provenance data in the cloud, an attacker can learn confidential information about the data stored in the cloud. To protect provenance information from these types of attack, we need a secure provenance scheme[7].

iv)Accessibility of Evidence: Unlike traditional computer forensics, a forensic investigator should have full control over the data in all types of services provided by cloud environment.

VIII. ALGORITHM OF PROPOSED SYSTEM

A)Identify the types of cloud services (PaaS, IaaS, SaaS, Dbaas).

B)Determine the type of forensics investigation (live/dead).

C) Collect all local copies of evidence files from the suspected machines.

D) Create multiple copies of collected evidence for analysis and maintaining their integrity with signature algorithms.

E) Analysis of Evidence files for traces of any malicious activity.

F) Documenting the evidence against criminal.

IX. CONCLUSION & FUTURE SCOPE

Cloud computing technology is the biggest evolution in the world of Information technology. But along with its increasing use, it is also falling prey to many criminal activities. Due to newly appearing threats and challenges, the current forensics tools are not adequate to carry out digital forensics investigation of the cloud services. Large amount of data can be collected as evidence but it is very difficult to integrate the data on a single platform. Thus, growing challenges require new solutions in the forensics field. To date the research work focuses only on the growing challenges but work on new technologies is still in dark ages.

Forensic investigator needs some open source tools to handle the number of growing cyber crimes. There are many tools are available but there is need develop an open source forensic tools for cloud as investigator can access the tool anywhere and can store data on the cloud. The basic study of the requirement for developing the computer forensic tool in a cloud computing environment have been mentioned in this paper along with the need to focus on forensics enabled cloud environment.

REFERENCES

[1] Slim Rekhis and Noureddine Boudriga, “A SYSTEM FOR FORMAL DIGITAL FORENSIC INVESTIGATION AWARE OF ANTI-FORENSIC ATTACKS” IEEE transactions on Information Forensics and Security, vol. 7, no. 2 April 2012.
[2] O.M. Fasan and M.S. Olivier, “ON DIMENSIONS OF RECONSTRUCTION IN DATABASE FORENSICS” Seventh International workshop on Digital Forensics & Incident Analysis (WDFIA)2012.
[3] Sriram Raghavan, “DIGITAL FORENSIC RESEARCH: CURRENT STATE OF THE ART” Springer CSIT (March 2013) 1(1):91–114 DOI 10.1007/s40012-012-0008-7.
[4] OneDrive Tutoruial: http://windows.microsoft.com/en-us/windows-8/getting-started-onedrive-tutorial
[5] Ahmad Ghafarian, "FORENSICS ANALYSIS OF CLOUD COMPUTING SERVICES", Science and Information Conference 2015 July 28-30, 2015 | London, UK
[6] Stavros Simou, "CLOUD FORENSICS SOLUTIONS: A REVIEW", Springer International Publishing Switzerland 2014.
[7] Shams Zawoad, "DIGITAL FORENSICS IN CLOUD" Crosstalk September/October 2013.
[8] Monali P. Mohite, " OVERCAST: DEVELOPING DIGITAL FORENSIC TOOL IN CLOUD COMPUTING ENVIRONMENT", IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15
[9] F. Daryabar, A. Dehghantanha, N.I. Udzir, N. F. Mohsani, S.B. Shamsuddin and F. NoRouzizadeh, “A SURVEY ABOUT IMPACT OF COMPUTING, ON DIGITAL FORENSICS,” International Journal of Cyb er- Security and Digital Forensicxs, 2013, vol. 2(2), pp. 77-94.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 9, September 2016

[10] Q. Zhang, L. Checg, R. Boutaba, "CLOUD COMPUTING: STATE-OF-THE-ART AND RESEARCH CHALLENGES," Journal of Internet Service Application, 2010, Vol. 1, pp. 7-18.
[11] OneDrive Tutoruial: http://windows.microsoft.com/en-us/windows- 8/getting-started-onedrive-tutorial
[12] P. Mell, T Grance, NIST Special publicatrion 800-145, Definition of Cloud.
[13] A. Saxena, G. Shrivastava, and K. Sharma, "FORENSICS INVESTIGATION IN CLOUD COMPUTING ENVIRONMENT," International journal of Forensics Computer Science," 2012, vol. 2, pp. 64-74.
[14] U. Thakore, "SURVEY OF SECURITY ISSUES IN CLOUD COMPUTING," College of Engineering, University of Florida.