Design and Implementation of a Cloud Based Computer Forensic Tool

Monali P. Mohite
Department of Computer Technology
Y.C.C.E
Nagpur, India
mohitemonali5@gmail.com

S. B. Ardhapurkar
Department of Computer Technology
Y.C.C.E.
Nagpur, India
shrikant.999@gmail.com

Abstract— **Nowadays, Cloud computing is receiving more and more attention from the information and communication technology industry recently. Thus, From the demand of cloud users digital forensics in cloud computing are a raw expanse of study linked to the increasing use of information processing governance, internet and digital computer storage devices in numerous criminal actions in both traditional and Hi-Tech. The digital forensics, including handle, conduct of, study, and document digital evidence in a court of law. Digital Forensic tool in a cloud computing environment is a big demand from forensic investigator. Thus, in the process of digital forensics, it is needed to create an image of the original digital data without damage and to show that the computer evidence existed at the specific time. The evidences are then analyzed by the forensic investigator. After the proof is examined, it is obliged to make a report to embrace it as legitimately successful confirmation in the law court. To give an advanced crime scene investigation benefit on cloud environment, a cloud based computer forensic tool is proposed in this paper.To probe the evidence multiple features are provided in this tool like data recovery, sorting, indexing, hex viewer, data bookmarking.**

Keywords- ***Computer Forensic, Cloud Computing, Digital Evidence, Forensic Investigation***

I. INTRODUCTION

Referable to the speedy growth of information technology, information community has become an important application on the net. And information technology brings peoples' convenience in their everyday lives and workplace. On the other hand, the cyberspace also becomes a hotbed for the increase of crime while cyber crimes are made quickly in cyberspace. As a result, cyber crimes, investigate not only get very complex, but likewise really hard. Digital forensics, including hold, keep up, study, and record advanced confirmation in a court of jurisprudence. Investigating officers ought to be held or confined digital equipment at the crime scene when a cybercrime occurred, then they gathered digital evidences and investigate them. Digital evidence stored on digital devices play an important function in a wide scope of cyber crimes however, digital data is fragile because it can be easily changed, copied, stored or destroyed [1]. Forensic investigation needs to provide full descriptions of the digital crime scene so the primary goals of digital forensic analysis are fivefold: i) to recognize the occasions, ii) to determine their impact, iii) to secure the fundamental confirmation, iv) to avert future incidents and v) to recognize the incitement reasons and Intendance of the attacker for future predictions [2]. Forensic Investigator uses a special tool for the above purpose. Most popular forensic tools, such as FTK and EnCase, are all commercial software. In that respect are several forensic tools are available, but they are for desktop application and are very costly. The investigator needs to convey the laptop and introduced tool with them on the crime sites. Today with the help of cloud technology we can access any information related to anyone from anywhere at any time, but this arises a new threat to private and confidential information [9]. And in that case the cloud based computer forensic tool will run better in this situation where examiners can access tool form cloud portal and perform investigations. The various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. CLOUD COMPUTING

Cloud Computing is an emerging model that separates applications and info resources from the infrastructure, and the mechanisms used to demonstrate them. The National Institute of Standards and Technology (NIST) provides the definition of Cloud Computing as [3] [4]: "Cloud computing is a theoretical account for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g.., Network servers, storage application and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is not a new technology, but it is a new method of providing computing resources and applications on demand. This style consists of five basic characteristics, three service models, and four deployment models. Table 1 shows a NIST cloud structure.

978-1-4799-1797-6/15 $31.00 © 2015 IEEE
DOI 10.1109/CSNT.2015.180

IEEE computer society

Essential Characteristics	On-demand self-service A broad network access Resource pooling Rapid elasticity Measured service
Service models	Software as a Service Platform as a Service Infrastructure as a Service
Deployment Models	Private cloud Community cloud Public cloud and Hybrid cloud

Table 1. NIST cloud

III. Digital forensic

Digital forensics is a branch of forensic science encompasses the process of organizing, acquisition, keeping up, examining and analyzing and also reporting of digital data [5]. The basic purpose of this digital forensics is to improve and to acquire legal evidence found in digital media [6]. After the evidence analyzed, it is asked to get the documentation in order to embrace it as legally effective evidence in the courtroom of jurisprudence. Buchanan et al. Proposed a cloud-based Digital Forensics Evaluation Test (D-FET) platform to measure the carrying into action of the digital forensics tools [6]. From the definitions, we can say that digital forensics is comprised of six primary stages shown in Fig 1:

1. Identification: Identification process involves two main steps: identification of an incident and the identification of the possible evidence to study the incident.
2. Collection: In the assembling process, an investigator extracts the digital evidence from different types of bulk storage media, e.g., Hard disk, pen drive, storage card etc. While extracting the evidence investigator needs to maintain the whole of the evidence to show that the extracted copy of data is same as the original one.
3. Acquisition: In the acquisition phase, copy of the original information is constructed. A disk image of the data available on physical media is created using computer forensics tool.
4. Preservation: It is a require to preserve, imaged or duplicated data or information to protect the collection in case of any legal injury and also for further analysis or reference. When saving the image of this collected data, forensics investigator needs to assure that there is no change of data duplicated. So, for this purpose write block and hashing is normally required (MD5 or SHA1).
5. Organization/Examination and Analysis: There are two main steps in organization process: examination and analysis of the digital evidence. In the test phase, an investigator extracts and inspects the data and in the analysis phase, he interprets and correlates the available data to come to a result, which can prove or disprove civil, administrative, or criminal allegations.
6. Presentation: In presentation process, an investigator arrives at an organized report to state his findings about the campaign. This report should be appropriate enough to confront in the court of jurisprudence.

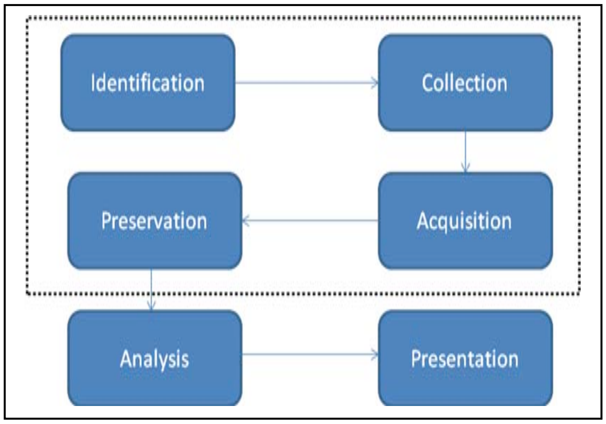

Figure 1. Digital Forensic Phases [1]

IV. Existing system

In that respect are several digital forensic tools existing which are functional both as free open source tools as well as commercial solutions. Here some selected samples both from commercial as well as free open source forensic tools [7] including Encase, Recover My Files, Recuva, Blade and FTK. A brief description of each plan is presented beneath:

Encase: Forensic is the worldwide standard in digital investigation technology for forensic practitioners who ask to conduct efficient, forensically-sound data collection and investigations using a repeatable and defensible process.
Recover: My Files are data recovery software (commercial software), which recover deleted files emptied from the Windows Recycle Bin, or became a red ink due to the format or corruption of a hard drive, virus or Trojan infection, unexpected system shutdown or software failure.
Recuva: is a free tool, which recovers deleted file from your Windows computer, Recycle Bin, digital camera card, or MP3 player.
Blade: is a commercial tool that designed for advanced professional forensic data recovery solution by a group called Digital Detective Group. It supports all of the major forensic image formats and it is more than just data recovery tool.
FTK: is a commercial tool and a court-accepted digital investigations platform built for speed, stability and comfort of usage. It provides comprehensive processing functions such as: dtSearch/Entropy, Data and Meta Carving, and Known File Filter.

Some forensic tools are available as open source for cloud forensic [1]:

1. AIR (Automated Image Restore): This tool supports for Linux operating system, it uses the command “DD” and “dcfdd” to develop graphical user interface function to provide facility for forensic staff create an image of the information.
2. TSK (The Sleuth Kit): This tool supports for Unix or Microsoft operating system files and partitions. It provides facility for forensic staff to restore files, produce image files and rootkit hidden files.
3. AFB (Autopsy Forensic Browser): This tool supports for the Unix operating system. It provides facility for forensic staff to investigate the file system and volumes of a computer.

V. Proposed System

In the existing system, the investigator needs to carry laptop with the installed toolkit for the complete forensic investigation steps. The proposed CBCFT (Cloud Based Computer Forensic Tool) allows an investigator or forensic examiner to access the tool from the cloud portal on his machine or on any machine available on the site and it’s a very cheap and low maintenance tool to investigate the case.

A. *Workflow of Cloud Based Computer Forensic Tool*

In our research, the victim machine is divided into two categories. One category is that the victim machine is still working while some other class is the victim machine already shut down. This CBCFT works as shown in Fig 2. When a victim machine is off. As per the Computer forensic procedure to investigate any case, remove the mass storage media from a machine. Access the CBCFT from cloud portal, connect the media to the investigator laptop or to the available local machine. Then an investigator creates a bit of the bit image of a storage medium. After making an image forensic investigatory upload it on the cloud or save on local machine for quick processing. Then the created forensic image is opened in CBCFT for performing analysis. Multiple features are offered to perform analysis like Viewing Index and Search Results, Multiple Sorting Fields, Data bookmarking, Hex Viewer, data carving.

Viewing and indexing provide facility such as the ability to look across multiple types of data and await at the effects on a single screen, the powerful index search capability, and searching data based on user-customized tags. Examiners can sort files according to different surveys, including all four time stamps (File Created, Last Accessed, Last Written and Entry Modified), file names, file signatures and extensions, hash value, full path, permissions. In bookmarking files, lots of files, and other objects that are of interest as potential evidence are found. These particulars can be checked off and saved for inclusion in the test report. These marked sections are denoted to as “bookmarks,”. Hex

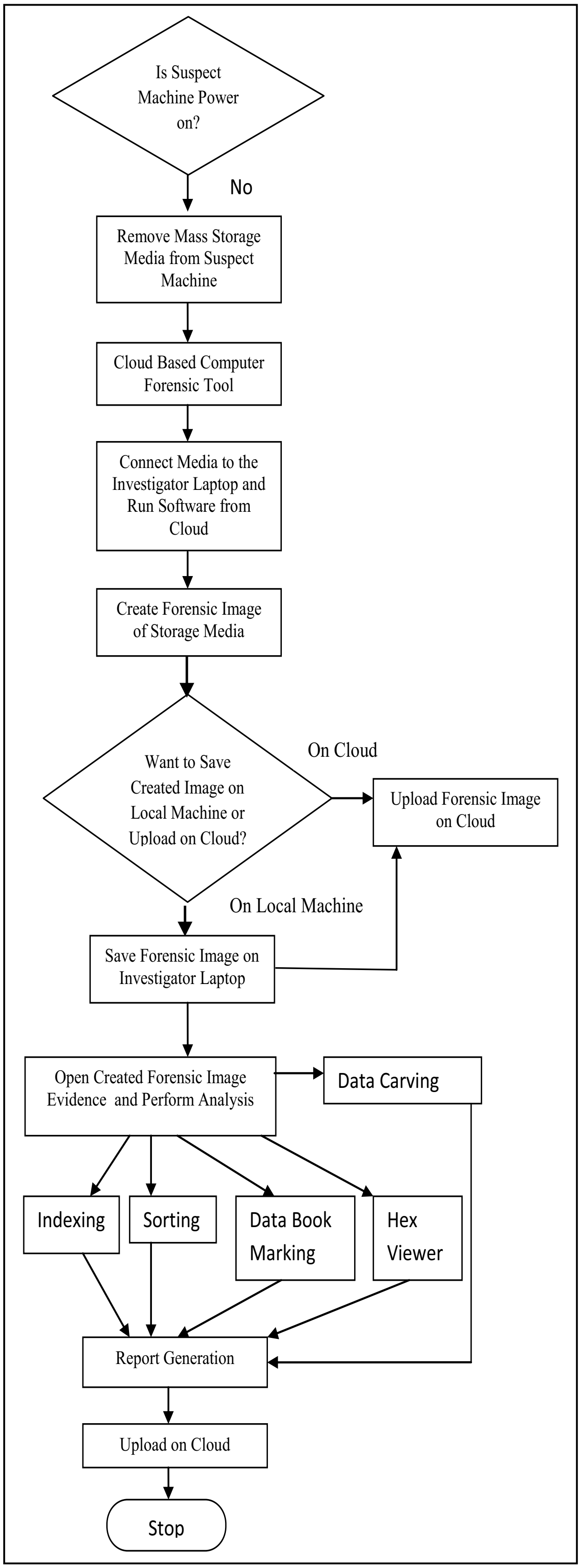
Is Suspect Machine Power on?
No
Remove Mass Storage Media from Suspect Machine
Cloud Based Computer Forensic Tool
Connect Media to the Investigator Laptop and Run Software from Cloud
Create Forensic Image of Storage Media
Want to Save Created Image on Local Machine or Upload on Cloud?
On Cloud
Upload Forensic Image on Cloud
On Local Machine
Save Forensic Image on Investigator Laptop
Open Created Forensic Image Evidence and Perform Analysis
Data Carving
Indexing
Sorting
Data Book Marking
Hex Viewer
Report Generation
Upload on Cloud
Stop

Figure 2. Workflow of Cloud Based Computer Forensic Tool

viewer displays the binary value in hex format. Data recovery used to retrieve the erased information. After completion of analysis phase the final form of a forensic examination is reporting the findings, which must be well-organized and delivered in a format that the target audience will see. This report is presented in courtroom of law and it uploads on a cloud.

B. Cloud Based Computer Forensic Tool Architecture

In a Cloud Based Computer forensic Tool, the digital forensic investigation team can use a any on-site available personal computer, or laptop to access the tool. In this cloud model, the users do not need to purchase hardware, software licenses or implementation services. Unlike the embodiment of Fig 3. Shows the architecture of CBCFT. The Forensic investigator access CBCFT from cloud. Then he looks for digital evidence like mass storage media. Once the detective finds the evidence he created a bit to bit image of a storage medium using CBCFT and investigator can upload the image on cloud or he can store it on the local machine. Once the image is created, it is then examined by the forensic examiner using the several functions provided in CBCFT like indexing, sorting, hex viewer, bookmarking, data recovery. And final phase is to create a documentation of examining case to show the report in court of jurisprudence.

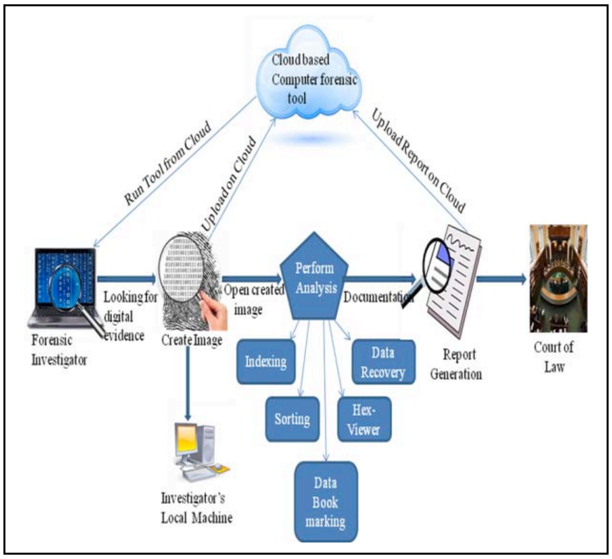

Figure 3. Cloud Based Computer Forensic Tool Architecture

C. Implementation of Cloud Based Computer Forensic Tool

The CBCFT is mainly split into eight function modules to address the eight digital forensic phases are as follows as given in Fig 4. : Cloud Interface module, Create Image module, index and view search module, sorting module, data bookmarking module, hex viewer module, data recovery module, report generation module. This tool uses Windows Server 2012 as the "Cloud OS", the updated Windows Server is designed for data center scale and the ability to work in concert with Windows Azure to enable support for sophisticated cloud architectures and support for multiple devices. [8]. The updated Windows Server is designed for data center scale and the ability to work in concert with Windows Azure to enable support for sophisticated cloud architectures and support for multiple devices.

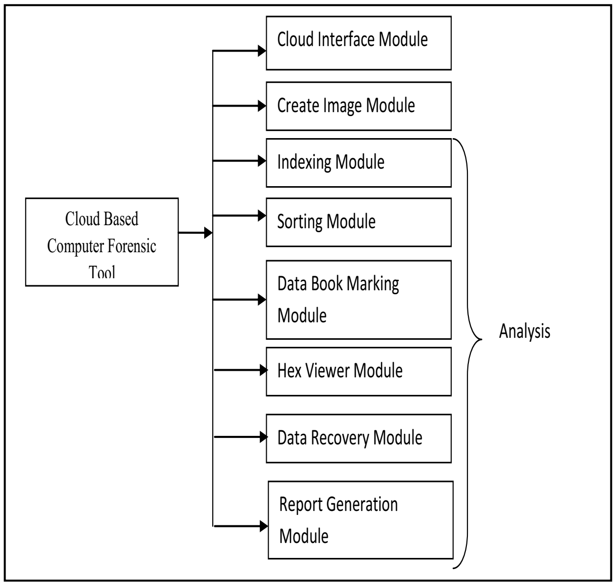

Figure 4. Implementation of CBCFT

D. Advantages of Cloud Based Computer Forensic Tool

1. Power to research and analyze a great deal of information rapidly and efficiently.
2. Data stored in cloud so it can be easily accessible when required, then no data loss.
3. Highly elastic because resources are easily released or occupied on the basis of demand.
4. Optimized usage of storage media.
5. As data is stored on cloud there is unlimited storage.
6. An application that is quite storage, extensive are easier to use in the cloud environment compared to the same when used by the governing body with its own.
7. The upkeep of infrastructure is simplified thus, less headaches for the IT team.
8. Lower outage is provided by cloud computing services, thus providing uninterrupted services to the user.
9. Keeping crucial data backed up using cloud storage services is the need of the hour for most of the organizations.

VI. Conclusion and Future work

Even though cloud computing is immature; the standards of security and service are still evolving. The estimate of cloud computing will provide a viable way for the design of Cloud Based Computer Forensic Tool in the hereafter. Cloud computing would help a digital forensic examiner team achieve efficient use of investigation tools. The aim of implementing cloud computing systems in digital forensics is to serve digital forensic investigation. It helps free them from hard work and makes opportunities to utilize the services of computer forensic experts who may be in remote fields. A cloud based computer forensic tool is really important in digital forensic investigation work. But there are many aspects need improvement. We shall extend our work to explore how making cloud computing serve digital forensic investigation better.

References

[1] Yi-Hsiung Ting, Chung-Huang Yang, "Design and Implementation of a Cloud Digital Forensic Laboratory, Symposium on Cryptography and Information Security 2013.

[2] Mamoun Alazab, Sitalakshmi Venkatraman, Paul Watters," Effective Digital Forensic Analysis Of The NTFS Disk Image", Special Issue on Applied Computing ICIT Conference – 2009

[3] D. Reilly, C Wren, T. Berry "Cloud Computing: Forensic Challenges for Law Enforcement" in International Conference for Internet Technology and Secured Transactions (ICITST), 2010 .

[4] Shams Zawoad, Ragib Hasan," Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems"

[5] Farid Daryabar, Ali Dehghantanha, Nur Izura Udzir, Nor Fazlida binti Mohd Sani, Solahuddin bin Shamsuddin, Farhood Norouzizadeh," A Survey About Impacts of Cloud Computing on Digital Forensics", International Journal of Cyber-Security and Digital Forensics (IJCSDF) The Society of Digital Information and Wireless Communications, 2013.

[6] Anand Kumar Mishra, Priya Matta, Emmanuel S. Pilli and R. C. Joshi "Cloud Forensics: State-of-the-Art and Reasearch Challenges" in International Symposium on Cloud and Services Computing 2012.

[7] Sultan Al Sharif, Mohamed Majed Al Ali, Naser Salem, Farkhund Iqbal, May El Barachi, and Omar Alfandi "An Approach for the Validation of File Recovery Functions in Digital Forensics' Software Tools" in International Conference on New Technologies, Mobility and Security (NTMS), 2014.

[8] AMD + Windows Server® 2012 White Paper. http://sites.amd.c om/us/Documents/AMD-WindowsServer_White_Paper.pdf.

[9] Shrikant Ardhapurkar, Tanu Srivastava1,Swati Sharma1,Mr Vijay Chaurasiya ,Mr. Abhishek Vaish "Privacy and Data Protection in Cyberspace in Indian Environment" in International Journal of Engineering Science and Technology 2010.