Chapter 8: Design of Cloud Forensic Laboratory for Investigation of Cybercrimes

The number of cybercrimes is increased in the last decades against classical IT and cloud infrastructure so that there is a need to design and implement a cloud forensic laboratory to investigate and reconstruct crime events that occurred against them as well as introduce a digital evidence to a court of law as admissible proof about the committed crime. Currently, we are living in the era of big data where the volume of data is increasing in an incredible way so that amount and volume of data that have to be processed in digital forensics analysis continue to rise and increase in an incredible way. Thus, this chapter proposed a Cloud Forensic Laboratory (CFL) to face the sophisticated yet advanced level of cybercrimes taking place currently comprises of various layers requiring levels of analysis consequently in classical IT and cloud systems. The proposed system will benefit from enormous storage and processing capabilities which providing by cloud computing to perform acquisition, extracting, analysis, examination and reporting for large size of digital evidence for both of crimes in IT systems and cloud. The proposed system will help the digital investigators and practitioners to perform the digital investigation process in forensically sound and timely fashion manner.

The rest of this chapter is organized as follows: Section 8.1 provides a brief introduction while related work discussed in section 8.2. Section 8.3 introduces the proposed Cloud Forensic Laboratory (CFL) while the preliminary architecture with analysis is provided in section 8.4. Finally, the chapter conclusion is presented in section 8.5.

8.1 Introduction

In recent times, the number of crimes is increasing incredible way around the world as well as the volume of data is increasing in an incredible way so that amount and volume of data that have to be processed in digital forensics analysis continue to rise and increase in an incredible way. Crimes can be subject to classical IT systems and new technologies as cloud computing. Cloud computing become one of the utmost popular and essential computing paradigms. Cloud computing is an emerging revolutionary technology that has started
changing the way where people live and work. A research done by Market Research Media states that the global cloud computing market is expected to grow at a 30% Compound Annual Growth Rate (CAGR) reaching $270 billion in 2020 [3]. With the growth of cloud and related services, security and privacy in the cloud have become very critical issues in cybersecurity field where hackers can use cloud infrastructure with exceptional bandwidth, storage, and computing power to launch their illegal activities and attacks. According to a recent survey done by IDC, 74% of IT executives and CIOs mentioned that the security is the main reason to prevent their migration to use the cloud computing services [4].

Digital Forensics is the science of extracting, analyzing and examining digital evidence which is extracted from any digital device like mobile phones, network devices, and other devices that generate digital data. Recently, the cyberspace becomes a hotbed for the growth of crime and traditional view to cybercrimes is changed because the appearance of cloud computing that depends in a theory of distributed systems which are distributing around the world to provide services for the organizations and individuals with a method of on-demand manner or cost-per-use. Thus traditional cybercrime techniques will change to adapt to a dynamic nature of the cloud computing environment. As a result, investigation of cybercrimes not only become more complex but also more difficult and digital investigators and examiners have to change and expand their methods, strategies, and procedures to investigate cybercrimes in the cloud environment so that there is a need for designing and implementing a Cloud Forensic Laboratory (CFL) based on cloud computing platform that is required for investigation of cybercrimes which are cloud or classical IT based.

The proposed system generates a forensic report about the committed crime for presenting in a court of law as admissible proof about the committed crime. Nowadays, we are living in the era of big data where the volume of data is increasing in an incredible way so that the proposed system will use the huge capabilities of cloud computing for acquisition, extracting, and processing as well as analysis large volumes of digital evidence. With the CFL setup, precisely investigating an entire range of large size digital forensic cases is possible under one roof for all types of forensics ranging from computer forensics to cloud forensics passing by mobile forensics and network forensics. The proposed Cloud Forensic Laboratory can provide the following functions:
Performing digital investigation of cybercrimes that occurred in Classical IT Systems.

Performing digital investigation of cloud-based crimes.

Training students, researchers and law enforcement officers.

8.1.1 Motivation

The motivation for creating the proposed CFL can be as follows:

- Challenges which make cloud cannot be used to store data for many sectors such as business, healthcare, banks or national security agencies, which require an audit and regulatory compliance.

- Many public sector units like police, banks, and courts, use forensic services for many disputed cases. These sectors, many times should wait for forensic reports from central forensic Labs for long times. This lead to delay justice system.

- Limitation of forensic laboratory for the investigation of cybercrimes in classical IT systems, cloud computing, and new emerging technologies.

- New challenges in cyber forensics domain such as big data, cloud computing, cloud forensics, and Voice over IP (VoIP).

- Forensic investigation of cybercrimes takes a long time for getting final results about specific crime for presenting in a court of law.

- The high volume of digital evidence required huge capabilities for processing and analysis.

- New emergency technologies such as fog computing, Internet of Things (IoT) and Big Data that need huge capabilities for investigating crimes related to them.

- Cloud computing provides huge capabilities of storage, processing and computing resources that help to perform the investigation process in a timely fashion manner.

8.1.2 Contribution

In this chapter, we describe the design and implementation for Cloud Forensic Laboratory (CFL) to investigate crimes related to classical digital systems and new technologies as cloud
computing and Internet of Things and other new technologies depend on cloud computing. The proposed system utilizes massive distributed cloud computing processing and storage to handle and analyze digital evidence related to classical IT system as well as cloud infrastructures. The idea of a system can apply on a small level and big level. This means CFL can use for training purpose for law enforcement officers and students and researchers in universities. Also, can apply on the country level through state level or entire country level via collaboration between states. This can reduce costs and time because if inside each state share forensics resources and will be no delay for analysis cases to provide for a court of law.

8.2 Related Work

More and more criminals are exploiting the speed and anonymity that new technologies offer in order to commit a diverse range of criminal and illegal activities. As cybercriminals continue to develop and advance their techniques, they are also shifting their goals focusing more on business espionage and accessing government information. To fight fast-growing cybercrime, companies and governments must collaborate globally to develop an effective model that can control the threats in addition to create a dedicated centralized forensic laboratory for investigating crimes case to understand the weakness in the digital systems.

Many researchers worked in designing and implementing digital forensic laboratory for help digital investigators for investigating cybercrimes in forensically sound and timely manner. Cody Miller et al [89], developed an architecture for a cloud-based distributed processing platform called Forensicloud. This architecture is designed to reduce the time for processing the digital evidence by utilizing the power of a high-performance computing platform in addition to adapting current tools to operate in this environment. This architecture gives digital investigators the ability to use licensed and unlicensed tools that they may not have had access to before and permits some of these tools to be run on computing clusters.

Yi-Hsiung Ting et al [90], designed and implemented a Digital Forensic Laboratory (DFL) based on cloud computing platform. The proposed system can produce a forensic report automatically and it not only stores digital evidence in a central storage but also provide multiple forensic tools for analyzing the digital evidence. Curtis Jackson et al [91],
proposed a multi-phase scenario-based design concept within an open source virtualized environment to extract evidential data to validate the hypervisor’s ability to provide a portal for threats auditing and monitoring that is effective, undetectable, and non-interruptive. George Grispos et al [92], identified some issues associated with placing a digital forensics server in the cloud side for performing a digital forensic investigation and they are not used a cloud-based analysis platform to perform digital forensics. Vassil Roussev et al [93], discussed a MapReduce model that used many clusters that process data. They implemented Message Passing Interface (MPI) MapReduce which uses MPI and Phoenix to make the current implementation of MapReduce more efficient.

8.3 Proposed Cloud Forensic Laboratory

8.3.1 Preliminary Software Requirements

There are many requirements for building the proposed Cloud Forensic Laboratory such as follows:

- **Dedicated Hardware Cluster Servers and Storage systems:** These servers will be provided and storage by Cloud Providers in cloud side according to the Laboratory requirements.

- **Virtualized Environment Software:** There are many virtualization solutions were considered when designing and implementing the Cloud Forensic Laboratory (CFL) such as OpenStack [48], Citrix XenServer[94], Microsoft Hyper-V[95] and VMware ESXi[96]. The OpenStack and VMware ESXi will be best choices for the CFL because they have many features rather than the others.

- **Digital Forensics Tools:** There are various digital forensics tools that can help the digital investigators and examiners in performing the investigation process such as Encase, FTK Imager, Packet Capturing and Analysis Tool, Media Content Indexing Tool, Password Recovery and Data Decryption Tool, Disk Imaging Tool and many other forensics tools.

- **Tools for processing large size of digital evidence:** There are many tools for processing a large amount of data such as:
  - **Bulk Extractor** [97] is used to extract many types of digital evidence involving credit card numbers, IP addresses, or user-defined regular expressions. This tool
operates on disks images, files, and directories, and memory dumps and can support parallel execution to enhance and reduce processing time. It reads the input from start to end and passes the data to scanners that recognize the data. If the data was compressed, then it will decompress and sent back through the scanners. Bulk Extractor then creates report files that contain the locations of the identified files on the input.

- **Sleuth Kit Hadoop Framework** [39] is a project that incorporates The Sleuth Kit into a Hadoop cluster. Cloud computing allows for faster processing of data. The Sleuth Kit Hadoop is a framework that uses The Sleuth Kit (TSK) on top of Apache Hadoop. It consists of three phases that it uses to analyze data. These phases are ingested, analysis, and reporting. Ingest retrieves information about the file system and the files on the image. The analysis stage uses various modules of TSK to analyze the data. Finally, the reporting stage generates reports on the analysis. TSK Hadoop uses Apache Hadoop to distribute the process of analysis across several nodes. Hadoop has a distributed file system, a job scheduler, and a MapReduce programming model for parallel processing. Using Hadoop and TSK together will increase processing power and reduce processing time.

### 8.3.2 Rules for Implementation of CFL

There are many rules to implement official Lab that can be acceptable in a court of law as follows:

- **Rules for the CFL that must follow**
  1. Digital forensic tools are documented in enough details and suitably validated.
  2. The integrity, preservation, protection, and confidentiality of digital evidence must be considered.
  3. Assurance of hardware and software that are used during investigation process in the lab are working probably.
  4. A security system for preventing unauthorized persons to access the lab.
  5. Management system for managing everything inside the lab.
- **How will the CFL satisfy previous rules that must follow?**
  
The CFL can satisfy the previous rules through the following ways:
  
  1. Providing all documents about tools and their validations.
  2. Using hash values and encryption for the assurance of digital evidence.
  3. Check all hardware and software to ensure that they work perfectly.
  4. Use strong registration system to allow only authorized persons to access the lab.

### 8.3.3 Proposed Strategy for Investigation of Cybercrimes

#### 8.3.3.1 Proposed Strategy Flowchart

The flowchart of proposed strategy is shown in Figure 8.1

![Proposed Strategy Flowchart](image)

**Figure 8.1:** Proposed Strategy Flowchart.
8.3.3.2 Description of Proposed Strategy

The proposed strategy steps can be described as follows:

1. Start strategy
2. Crime has occurred.
3. If the crime was in the cloud then
4. Start cloud forensics
5. Determine types of service models
6. If the virtualized server is power on then
   7. Perform live forensics
   8. Acquire volatile data
   9. Power off the VM
   10. Acquire suspend VM
   11. Create disk image from VM
   12. Send the evidence to the forensic server for analysis purpose
13. Else
14. Perform Dead forensics
15. Acquire suspend VM
16. Create disk image from VM
17. Send the evidence to forensic server for analysis purpose
18. Start the analysis and examination process
19. Generate final report
20. Send the report to court of law
21. Else
22. Start digital forensics
23. If the system is power on then
   24. Perform live forensics
   25. Acquire volatile data
   26. Power off the system
   27. Create disk image from hard disk of the system
   28. Send the evidence to forensic server for analysis purpose
   29. Start the analysis and examination process
30. **Generate final report**
31. **Send the report to court of law**
32. **Else**
33. **Perform Dead forensics**
34. **Create disk image from hard disk of the system**
35. **Send the evidence to forensic server for analysis purpose**
36. **Start the analysis and examination process**
37. **Generate final report**
38. **Send the report to court of law**
39. **End of Strategy**

### Discussion related to Proposed Strategy

Building a cloud forensic strategy for performing the investigation of crimes in the cloud requiring understanding the type of evidence that will extract and collect from which side, Cloud Service Provider (CSP) side or Cloud User (CU) side, this can facilitate the cloud forensic process through save time and cost by following systematically process. Figure 8.2 shows the investigation of cloud computing system. In this Figure, the digital investigator can connect to the cloud user side and CSP side to investigate the crime where on the cloud side, digital evidence can be extracted from physical devices such as laptop, mobile phone and Personal Computer (PC) that are used to access the cloud services while in the CSP side, the investigators can extract the digital evidence from virtualized environment that includes hypervisors (i.e. virtual machine manager), virtual machines, cloud network devices and others connectivity devices that are used within the cloud infrastructure.

![Figure 8.2: Cloud Forensic Investigation.](image)

---

182
As shown in Figure 8.2, the digital investigators have to follow a systematically forensic process for handling and investigation of crimes in both of cloud user and CSP sides to reconstruct a complete timeline about an incident or crime that occurred against or using the cloud infrastructure.

In the cloud environment, the digital forensic analysis strategies would have to vary from each model (i.e services and deployment models). For example, the control over the process or network monitoring by the users is very limited in SaaS and PaaS while in IaaS, the cloud user will have more control over computing resources [73] as tabulated in Table 8.1. Table 8.1 shows how CSP can manage and control of cloud services. The traditional digital forensics for computer systems will vary for the cloud models in a cloud environment. Collection process in the SaaS and IaaS models will not be same where, in the SaaS model, the CSP will have control over application data, while in IaaS, the cloud user will have control over data generated by the virtual machine. On the other hand, in the private deployment model, investigators have physical access to the digital evidence data, but they merely can get physical access to the data in public deployment model [73].

Cloud computing can provide a powerful service for the digital forensic community known as Forensic as a Service (FaaS). The forensic investigator can deliver the FaaS by utilizing the huge capacities of cloud computing. This makes digital forensics as an “on-demand” service for allowing for as much storage and processor power as needed to conduct an investigation. A Forensic server will reside on the cloud side, offline, until the need arises for using it. Naturally, the cloud resources could be used for sorting, searching, and hashing the evidence data. There are many benefits of performing forensics in a cloud environment are as follows [5]:

- Decrease evidence acquisition time.
- Reduce time to access protected documents
- Reduce forensic image verification time.
- Virtually unlimited log storage.
- Reduce service downtime.
- Improve log indexing and searches.
- Reduce evidence transfer time.
Utilizing the FaaS, the digital investigators after extracting and collecting the digital evidence then send them to the forensic server that resides on the cloud side. This forensic server can utilize the enormous capabilities of cloud computing to handle and process the extracted evidence in timely fusion and forensically sound manner.

**Table 8.1:** Cloud Service Provider ‘S Control Over Services Models [73].

<table>
<thead>
<tr>
<th>Layer</th>
<th>Model</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>X</td>
<td>X</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td>X</td>
<td>X</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Runtime</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>X</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Vitalization</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Servers</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

**8.3.3.4 Security and Network Performance Issues**

**8.3.3.4.1 Authorization**

Authorization means only authorized digital investigators or person who have permission to access cloud forensic laboratory remotely through use classical access methods such as confirming users who will have unique login credentials. This can use to secure access to the CFL from secure places such as universities for training or law enforcement officers. The security of user machine is very significant to prevent unauthorized users to access digital evidence or cases in CFL. Figure 8.3 shows login check procedure to access virtual machine for performing forensic analysis.
8.3.3.4.2 Digital Evidence Security and Authentication

Security and confidentiality of the digital evidence during transmission to a forensic server in the cloud side is a very crucial issue to guarantee the integrity and verification of acquired and collected data from the crime scene to be accepted in the court of law as admissible proof about the incident and crime. In Figure 8.4, a protection procedure is proposed to protect the digital evidence during transmission to a forensic server on the cloud side. This procedure uses compression and encryption mechanisms. The compression is used to compress the digital evidence to reduce the size and reduce the time for transfer to the forensic server. The encryption is used to encrypt the digital evidence to protect it from attacks during transmission through the Internet. Also, authentication of digital evidence is an essential step during the forensic process to ensure the integrity of evidence. This can be done through using cryptographic hashing algorithms such as Message Digest (MD5) and security...
Hashing Algorithm (SHA1) which are common in the forensic community to ensure authentication data during processing and storage.

![Diagram of Digital Evidence Protection Scenario]

**Figure 8.4:** Digital Evidence Protection Scenario.

### 8.3.3.4.3 Network Performance and Latency

Unlike traditional digital forensics laboratories, the design of cloud forensic laboratory depends to upload digital evidence from local systems to remote forensic servers in the cloud. This means it important to use the high-speed Internet to upload data to cloud forensic server. This may be not available in all places but for example in the USA, there is Internet 2 with a high-speed connection. Thus, the speed of Internet can be one of the obstacles to use forensic servers to analysis and examine digital evidence related to crimes which are occurred in traditional IT systems but in crimes related to cloud systems, it will not be a significant problem because the transfer will be inside cloud systems. For example, theoretical time for data transfer is shown in Table 8.2.

<table>
<thead>
<tr>
<th>Size of Evidence</th>
<th>100 Mbit/s</th>
<th>10 Gbit/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 GB</td>
<td>02:57:29</td>
<td>00:01:44</td>
</tr>
<tr>
<td>500 GB</td>
<td>14:47:28</td>
<td>00:08:40</td>
</tr>
<tr>
<td>1 TB</td>
<td>30:17:31</td>
<td>00:17:44</td>
</tr>
<tr>
<td>5 TB</td>
<td>151:27:39</td>
<td>01:28:44</td>
</tr>
</tbody>
</table>

**Table 8.2:** Theoretical Time of Data [89].
8.3.3.5 Some Applications of Proposed CFL in Digital Forensic Community

The proposed CFL can be used in the Forensic Community as follows:

1. **Training students and law enforcement officers:** the CFL can be used for training about how to perform forensic investigation process as shown in Figure 8.5.

   ![Figure 8.5: Training Students and Law Enforcement Officers.](image)

2. **Investigation of cloud-based crimes:** the CFL can be used in the cloud to investigate the cloud-based crimes as shown in Figure 8.6.

   ![Figure 8.6: Investigation of Cloud-based Crimes.](image)

8.3.3.6 Case Study: India

In recent times, The Internet is being more used by its criminals to reach economics problems for numerous organizations around the world worldwide. Also, IT explosion has made children and women easy victims to the cybercrimes. The internet is very rapidly becoming a household commodity in many countries such as India. As more homes have access to the Internet, more children and women would be using the internet and more are the chances of falling victim for these cybercrimes.

India is a country in South Asia. It is the seventh-largest country by area, the second-most populous country, and the most populous democracy in the world. India is considered
as the second largest democracy of the world so the crimes in India taking place every day as compare to crime the legal and justice system is entirely unable to provide proper and speedy justice, large number of people facing unusual delays in justice delivering in Indian courts it means a common man is badly affected. India is facing a shortage of skilled cyber experts and cyber tools to tackle cyber cases rapidly, due to lack of unavailability and awareness of tools, methods and proper training and most of the time people not aware correct tools that need to be used. Thereby, there is a need to increase cyber forensic facility in all states of India to help in processing cybercrimes case in particular time.

New challenges in cyber forensic security such as Botnets, phishing, cloud computing, cloud forensics, Voice over IP (VoIP). Several public sector units such as Police Stations, Banks, Courts, Consumer Forums, and various organizations who have to depend upon to forensic services for several disputed cases, they have to wait for the forensic reports from central forensic laboratories for many months that lead to an unusual delay in the legal justice system. After having an acute shortage of forensic laboratories, there a serious demand in creating different laboratories around India to establish super-specialty forensic laboratories to ease down growing pending cases from forensic laboratories, which can lead to delay in Courts due to reports so, the presence of various digital forensic laboratories will bridge the huge gap with quality services without unwanted delay.

Create Cloud Forensics laboratory in India (i.e. as a case study) can be helpful to fight and reduce risks of cybercrimes. Utilizing the idea of the proposed model to establish in state level and therefore country level can be a good solution to face a shortage in qualified officers or experts and researchers in academia through building such type of laboratories for investigation of crimes as well as training and collaboration over country level through taking advantages of cloud computing resources. Also, this collaboration can be extended over international between countries. This section explains how to plan to build the proposed laboratory at the country level.

As shown in Figure 8.7, the proposed system can use to build inside a state of a country with accessing from different locations, for example, eight locations, in the country at any time from anywhere. Similar but for country level, Figure 8.8 shows a diagram for central cloud forensic laboratory between various states, for example, eight states, to collaborate in digital forensic cases to save time and costs.
8.4 Preliminary Architecture of Proposed System

Simply here the architecture components for the proposed laboratory will discuss. A simple environment is consisting of five machines, ESXi-5 Server, Windows Server 2012R as Domain Controller and Windows Server 2012 R as vCenter, Windows 7/ Windows Server
2012 R as Forensic Server and Finally Windows 7 as Digital/Cloud Investigator as shown in Figure 8.9. The preliminary CFL components are shown in Table 8.3 where ESXi Server, Domain Controller, and vCenter are representing the virtual datacentre in the cloud environment. The Forensic server represents the server for performing digital investigation process onto the digital evidence from the cloud side or from outside the cloud which will be uploaded by the digital/cloud investigators. The forensic server contains various forensics tools that can help the digital/cloud investigator for performing the investigation process in effective and efficient manner. The investigator can connect and communicate with the forensic server using remote connection program to manage and handle the digital evidence.

From the primary architecture of a proposed system which depends on using cloud computing capabilities so it will fulfill its essential characteristics as follows:

- Be accessible by trainers, researchers, and law enforcement officers and investigators to analyze evidence as desired.
- Be available to access from anywhere in the entire country or an entire state.
- Utilize huge virtualization processing and storage resources.
- Be able to expand or shrink based on the requests of the users (i.e. trainers, researchers, and law enforcement offices).
- Plan processing based on priority and consumption of the users (i.e. trainers, researchers, and law enforcement offices).

### Table 8.3: Preliminary Architecture Components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Program</th>
<th>Function/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>ESXi Server</td>
<td>Create and manages Virtual machines</td>
</tr>
<tr>
<td>Hypervisor Management System</td>
<td>vCenter</td>
<td>Manage the hypervisor</td>
</tr>
<tr>
<td>(HMS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Management System</td>
<td>Domain Controller</td>
<td>Create, delete and authenticate users</td>
</tr>
<tr>
<td>(AMS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital/Cloud Investigator</td>
<td>Windows/Linux Operating System</td>
<td>Connect to forensic server and perform investigation process</td>
</tr>
<tr>
<td>Forensic Server</td>
<td>Digital Forensics Tools</td>
<td>Manage and handle crime cases</td>
</tr>
<tr>
<td>Remote Connection Program</td>
<td>Remote Desktop Connection</td>
<td>Access to Forensic Server</td>
</tr>
</tbody>
</table>
8.4.1 Preliminary Analysis

Due to the huge cost of implementing real cloud system, a simple test experimental is setup as shown in Figure 8.10 to execute test procedure in Figure 8.11. The test environment is set up using Laptop Lenovo G5080 Core i5 12GB RAM with Hard Disk 500GB. VMware Workstation 11 installed on the host machine then creates two virtual machines, ESXi-5 which work as Virtualization (Hypervisor) Server, vCenter which work as Hypervisor Management System. Inside the ESXi, two virtual machines are installed as forensic machines to handle digital evidence remotely. The hypervisor and hypervisor management system are required to create and manage Virtual machines. A local storage device such as the hard disk of a hypervisor system can be used as a storage unit for the virtual machines. However, in the majority of cases, shared storage devices are used because organizations require many virtual machines to offer private cloud computing services to their members.
Various forensics tools can be installed in the virtual machines to support the digital/cloud investigator for performing the investigation process in effective and efficient manner. The investigator can connect and communicate with his/her machine using remote connection program to manage and handle the digital evidence. The access process for the virtual machine is shown Figure 8.10 as follows.

1. A login request is sent to the connection management system.
2. The connection management system sends the user login information to the authentication management system.
3. If user authentication succeeds, the connection management system asks the hypervisor to assign a virtual machine, which is stored in the shared storage.
4. The connection management system provides that virtual machine to the customer.
5. Then, the virtual machine can be used as a private desktop remotely.

For analysis the digital evidence inside the cloud, a virtualization cluster of virtual machines can use to handle and process data. Using virtualization cluster can bring both advantages and disadvantages [89].

1. **Advantages are:**
   - Virtual machines can run several operating systems required by the specific tool being used.
   - They have dedicated computing resources.
   - The specific tool should not have to be altered to run on them.
   - A virtualization cluster can also be as big or as small as it needs to be since nodes of the cluster can be added and removed with little difficulty.

2. **Disadvantages are:**
   - The need for a custom scheduler to schedule incoming jobs.
   - Virtualization overhead.
   - No default Message Passing Interface (MPI).
   - The necessity for a customs agent on each node to accept incoming jobs.
Figure 8.10: Access Forensic Server by Digital Investigators.

Figure 8.11 shows a preliminary Forensic Investigation procedure to handle digital evidence such as two different pieces of evidence as tabulated in Table 8.4. Simply for compression of the evidence (Evidence_1 and Evidence_2), A 7zip program with also encrypt them using AES-256 to secure evidence against unauthorized users. Hash values after image the digital evidence is generated using FTK image to ensure the integrity of data after uploading to the cloud.

Table 8.4: Digital Evidences for Test Purpose.

<table>
<thead>
<tr>
<th></th>
<th>Evidence_1</th>
<th>Evidence_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compressed</td>
<td>1.40 GB</td>
<td>936 MB</td>
</tr>
<tr>
<td>Decompressed</td>
<td>1.46 GB</td>
<td>990 MB</td>
</tr>
<tr>
<td>MD5 checksum</td>
<td>c436e65ce5ba3389636d4304b6f2ec</td>
<td>c9edcbe240c44864b19decdf8516c02ac</td>
</tr>
<tr>
<td>SHA1 checksum</td>
<td>5289ff61372d1f0132c554e26a5a074d10f6f22c</td>
<td>e335b9398ed35117296c1ae67e449881f1be30e8</td>
</tr>
</tbody>
</table>
Figure 8.11: Preliminary Forensic Investigation Procedure.

8.4.2 Web-based Management Cloud Forensic Laboratory

This work uses PHP as a development language. PHP’s main purpose is to deal with dynamic pages and developers can change the PHP code to control page rendering while digital investigators browse. Table 8.5 is the development tools and test environment. This work uses PHP as the developing language to implement the proposed Cloud Forensic Laboratory (CFL). First of all, digital investigators have to log in the laboratory which could recognize the user using the list of digital investigators in the databases. Figure 8.3 is the login checking
procedures which can assure the identity. Before logging into the laboratory, the system verifies logger’s username and password. Then, will start the session to identify digital investigators is the same person who has been defined. By checking username and password, the system can confirm the identity of them. If their identity is digital investigators, the system will automatically direct to the home page of Cloud Forensic Laboratory. Otherwise, it will show a login failed page.

**Table 8.5: Development Environment Tools in Forensic Server.**

<table>
<thead>
<tr>
<th>Component</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows</td>
</tr>
<tr>
<td>Web Server</td>
<td>Apache Wamp Server</td>
</tr>
<tr>
<td>Language</td>
<td>PHP and HTML</td>
</tr>
<tr>
<td>Database</td>
<td>MySQL</td>
</tr>
<tr>
<td>Forensic Tools</td>
<td>Encase, FTK Imager, Wireshark, HashCalc</td>
</tr>
</tbody>
</table>

Figure 8.12 is CFL login page. After logging into the proposed system, the web page will be redirected to the home page of the proposed system. In this work, we just provided some pages that may be helpful for the digital forensics to perform the investigation process. These pages such as Digital Evidence Upload, Select Forensic Image, Digital Evidence Analysis and Forensics Report as shown in Figure 8.13.

Digital investigators can select local digital evidence from a web page, and then they can upload them to the cloud forensic laboratory. Figure 8.14 is the local digital evidence uploading page.

After uploading the digital evidence, the investigators can continue to analyze the digital evidence using various types of forensics programs such as Encase, FTK Image, HashCalc, Wireshark, and Autopsy. Forensic analysis page is shown in Figure 8.15. Finally, the digital investigators will store some information about the forensic case in the database as a forensic report as shown in Figure 8.16.

The proposed CFL is a cloud-based forensic laboratory which can provide a fast response the cybercrime investigate. Forensic investigators could collect and store digital
evidence in the CFL. One of CFL’s advantages is having a friendly user interface for investigators.

![CFL Login Page](image)

**Figure 8.12:** CFL Login Page.

![CFL Main Page](image)

**Figure 8.13:** CFL Main Page.
Figure 8.14: Digital Evidence Upload Page.

Figure 8.15: Forensic Analysis Page.
8.5 Chapter Summary

In last decades, a number of cybercrime cases are growing in the cyberspace for performing illegal activities. To discover and trace who performed these cybercrimes, there is a need to a process to investigate the crime scene to extract digital evidence. The process of performing digital investigation to extract digital evidence from a crime scene is known as digital forensics.

There is a serious need to design and implement a laboratory to help law enforcement officers and digital investigators who are working in collecting and extracting digital evidence from suspicious digital systems after the crime occurred. This chapter introduced and presented the idea of designing and implementing of Cloud Forensic Laboratory (CFL) which is based on cloud computing platform for investigation of cybercrimes that are a cloud or classical IT based. The proposed CFL can decrease the time that required to investigate cybercrimes in the cloud through using enormous capabilities of cloud computing. Finally, a forensic report can be generated about the committed crime for presenting it in a court of law as admissible proof. The proposed system can improve the investigation process by providing an environment for the digital investigators and experts to access various forensic tools and test environments remotely.