Multimedia Tools and Applications (2021) 80:14255–14282
https://doi.org/10.1007/s11042-020-10358-x

An efficient digital forensic model for cybercrimes investigation in cloud computing

Ezz El-Din Hemdan[1] · D.H Manjaiah[2]

Received: 10 July 2020 / Revised: 28 September 2020 / Accepted: 22 December 2020 /
Published online: 22 January 2021

Abstract
In recent times, cloud computing adopted numerous organizations and enterprises for offering services with securely certifying that cloud providers against illegitimate activities. However, cost-effective forensics design and implementation for support the cloud-based cybercrimes investigation. To build cloud architecture support forensics is a significant and complex issue such as voluminous intricate legal, organizational, and technical defies due to the virtualization, distributing, and dynamic nature of cloud systems. Therefore, this paper presents an efficient Cloud Forensics Investigation Model (CFIM) to investigate cloud crimes in a forensically sound and timely fashion. Besides, the proposed system supports the concept of Forensic as a Service (FaaS) that provide innumerable benefits of conducting digital forensics through using Forensic Server on the cloud side. The investigational results proved that the proposed system can assist the digital investigators in their mission of investigation of cybercrimes in the cloud in a proficient manner.

Keywords Cloud computing · Cybercrimes · Digital forensics · Cloud forensics · And VM snapshot

1 Introduction

In recent years, Cloud computing has become one of the supreme prevalent computing exemplars which adopted by numerous companies and organizations because it delivers

✉ Ezz El-Din Hemdan
ezzvip@yahoo.com

D.H Manjaiah
manju@mangaloreuniversity.ac.in

[1] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

[2] Department of Computer Science, Mangalore University, Mangalore, India

various services that have a lot of welfares, for instance, optimize the general usage of IT infrastructures, a high degree of scalability, and availability of massive computing and storage resources. Cloud computing poses an inimitable mixture of characteristics involving on-demand self-service, measured service, rapid elasticity, and broad network access. With the advent of cloud computing proficiency that depends on a theory of distributing and dynamic nature of data centers around the world to provide these services with a method of cost-per-use plus the colossal amount of resources with cheap cloud computing services such as data storage. This makes the cloud systems subject to severe types of attacks by hackers and criminals, who may be able to hack and use these resources for illegal purposes, and also potentially can utilize the cloud to host or store evidence of their criminal data like terrorism-related materials. In addition to this, cloud services can also be used as a launching platform for new advanced types of attacks. Therefore, the security of cloud infrastructure represents a vigorous role for a guarantee to provide security services for customers especially from ticklish community sectors including healthcare and finance that tardily accept the migration of their work to the cloud.

Performing the cloud forensics process poses voluminous intricate jurisdictional, organizational, and technical challenges identification and seizure digital evidence from cloud systems by law enforcement and national security agencies, due to the virtualization, distributing, and dynamic nature of cloud systems. These challenges and issues such as crime scene reconstruction, isolating cloud instance, data provenance, and evidence segregation, can obstruct digital forensic investigators, law enforcement, and national security agencies and possibly prevent from acquiring and analyzing digital evidence in a forensically and timely fashion manner. Also, this digital evidence may be spread across several data centers in diverse countries over the world, so that to collect, identify, and preserve data, there may legal and jurisdictional issues which needed to complete the forensics process to reconstruct crime events. This lead researchers and scientists to think for a solution that needs to be resolved to perform convenient cloud forensics,

Currently, some researchers focused on study data security in the cloud, and while the other is interested in digital forensics explored and identified challenges and problems related to perform the digital investigation process in cloud environments as well as discuss incident response strategies. A little number of them start to propose new tools, procedures, and models to accomplish cybercrime investigation in the cloud. Plus, little work explains real case studies to illustrate the composite challenges related to cloud forensics in real cases.

Little work was done to design and implement new models and systems to support cloud infrastructure investigation through giving the cloud system developer and architect, ideas of these new models to consider them in the future during building novel security and forensics support cloud infrastructure. This step can guarantee to public sectors who pose critical and sensitive data to migrate to the cloud. Thus, this paper introduces the design and implementation of the Cloud Forensics Investigation Model (CFIM) to cloud-based cybercrimes investigation.

The proposed system is a smart system that able to take a snapshot sporadically for each Virtual Machine (VM) status which runs in the cloud and sends it to a Trusted Center Server (TCS) for storing VM snapshots. The VM snapshot is can be used by Cloud Investigators to extract evidence ‘data to reconstruct the cloud-based crime scenario. Likewise, the snapshot is significant because it is tricky with restarting the VM is that during the resume procedure, numerous files stored on the hard disk are altered, which may abolish evidence and thus the whole forensics process. The extra

drawback of resuming the suspended VM is that there is a loss of information stored in the memory as the state of the VM changes. This information could be vital to the investigation being carried out. The TCS server also is responsible for monitoring and recording the status of the VMs. One of the important issues related to the proposed model. The use of this model should be mentioned as one of the terms in the Service Level Agreement (SLA) between Cloud User (CU) and Cloud Service Provider (CSP) to guarantee the success of the investigation process in the cloud through using this system integrated with cloud infrastructure in the future. The proposed system also introduced a real example of Forensics as a Service (FaaS) by including the FS in the CSP side for performing the digital investigation process through using the enormous capabilities of the cloud computing resources such as processing, computing, and storage. The contribution of this work is concise as follows:

- Exploring challenges, and opportunities of cloud forensics.
- Provide an efficient cloud forensic system that able to take a snapshot sporadically for the state of each VM which runs in the cloud and sends it to TCS that works as a storage for VM snapshots.
- The proposed approach can be a solution to address the challenges faced while conducting a forensic investigation in the Cloud area.
- Offer Forensics as a Service within the proposed model through placing the forensic server in cloud infrastructure for performing cybercrimes investigation procedure through utilizing high abilities of cloud resources.

The rest of the paper is prepared as follows: Section 2 provides a brief knowledge about cloud forensics while related work is presented in section 3. Section 4 presents the proposed Cloud Forensics Investigation Model (CFIM) while the experimental results and analysis of the proposed model are presented in section 5. Finally, the conclusion and future work of this innovative research is offered in section 6.

2 Investigation of cloud-based cybercrimes

The dynamic nature of cloud computing makes the forensic investigation process more problematic work of a Cloud Investigator (CI) to investigate cloud-based crimes, extract digital evidence and reconstruct a cybercrime event, then send a final report to a court of law as admissible evidence about the committed crime that occurred in the cloud environment. The digital forensics investigation process in the cloud environment is called 'Cloud Forensics'. The term cloud forensics that describes the digital forensic investigation of cybercrimes in the cloud computing environment was first introduced by Ruan et al. [19] to recognize the rapidly emerging need for digital investigation in the cloud computing environment. Ruan's working definition of cloud forensics is: '*the application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach (e.g., remote, virtual, network, live, large-scale, thin-client, thick-client) towards the generation of digital evidence. Organizationally it involves interactions among cloud actors (i.e., cloud provider, cloud consumer, cloud broker, cloud carrier, cloud auditor) to facilitate both internal and external investigations. Legally, it often implies multi-jurisdictional and multi-tenant situations*' [20].

In 2014, NIST defined cloud forensics as "*the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of digital evidence*" [15]. Today, cloud forensics is challenging at best but can be performed in a manner consistent with federal law using the tools and techniques which we will develop them. Many complex challenges 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.

In the cloud environment, the digital forensics analysis strategies would have to vary for each model (i.e. services and deployment model). For example, the control over processes or network monitoring of the users is limited in SaaS and PaaS while in IaaS, the cloud user will have more control over computing resources [17]. The traditional digital forensics for computer systems will vary from the cloud models in a cloud environment. The collection process in the SaaS and IaaS models will not be the same, while in the SaaS model, the CSP will have control over application data, while in IaaS, and 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 the public deployment model [17]. Cloud forensics pose numerous challenges that may face digital investigators for performing the investigation process in the cloud as follows:

- *Vigorous Service Level Agreement (SLA):* Service Level Agreement (SLA) represents a contract between Cloud user and Cloud Service Provider (CSP). The SLA can illustrate the responsibility of CSPs at the time of any malicious incident. Discussing the importance and giving emphasis vigorous or robust SLA between the user and CSP. The robust SLA should explain and state how the CSP deal with the cybercrimes. A Trusted Third Party (TTP) can contribute to solving this problem by ensuring the quality of SLA and overcome the challenges of cross-border legislation.
- *Physical Access to Evidence:* Physical access to digital evidence, not an easy task due to the dynamic nature of the cloud. The impossibility of specifying the storage location where investigators do not even recognize where the data is located as it is distributed among numerous data centers. This represents a challenge for digital investigators.
- *Large Bandwidth:* The size of digital evidence in the cloud is increasing rapidly due to the huge amount of generating data so that the size of a virtual machine instance increasing depending on user usage. In the cloud forensics, the investigators have to download the VM instance to perform the forensic investigation process, but this will require large bandwidth issue for downloading the instance and perform the investigation process in a timely fashion manner. This introduces a challenging in the cloud forensics process
- *Multi-tenancy:* In the cloud, many users used virtual machines hosted on the CSP side. These VMs shared the same physical hardware resources so that data between multiple users may be on the same server. The data collection and acquisition is a challenge because it must take into consideration the privacy of other users on the same server during performing the investigation process.
- *Volatile Information:* Volatile information plays a vital role in the investigation process. The volatile information loss as soon as the power of the system. This information contains information such as process id, network log, and kernel objects. Attackers can delete this information by deleting them or shut down the running VM to prevent any traces after him/her.

In the other hand, as the digital forensics in the cloud pose complex challenges, there are several opportunities to apply the digital forensics in cloud computing environments as follows [19]:

- *Cost-effective:* implement the forensic service in a cloud computing environment called Forensic as a Service (FaaS) allows utilizing the huge capacities of cloud computing without transfer the digital evidence from the cloud to the other side to perform the investigation process which needs high bandwidth.
- *Data abundance:* replication of data in a cloud environment introduces the essential opportunity for cloud forensic for recovering the lost and deleted data from the cloud to prove the crime.
- *Scalability and flexibility:* cloud forensic services can utilize the facilities of scalability and flexibility resource use, for example, providing unlimited storage, compute and network resources pay-per-use
- *Policies and standards:* develop new standards and policies for cloud forensic science due to the rapid change of the technology of cloud computing and cybercrimes against it.
- *Forensics as a Service (FaaS):* Cloud computing introduces one powerful option for digital investigators called Forensic as a Service. 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. There are many benefits of conducting forensics in a cloud environment are as follows [2]:
- ***Reduce evidence acquisition time*:** if a server in the cloud is compromised, it can be cloned and made immediately available to a cloud forensics server.
- ***Reduce service downtime*:** due to the hardware abstraction in the cloud, specialized hardware will not have to be obtained to continue the acquisition of the evidence in some situations.
- ***Reduce evidence transfer time*:** the clouds distributed file system allows for making fast bit-for-bit copies.
- ***Reduce forensic image verification time*:** some cloud environments use a cryptographic checksum or hash that can drastically reduce the time required to hash files offline
- ***Decrease time to access protected documents:*** the pooling of CPU power available in the cloud can make decryption much faster.

3 Related work

Cloud Forensics has become one of the significant research areas in the cloud security domain. Performing the cloud forensics process poses sundry multifarious challenges due to the cloud dynamic nature. Several researchers identified and explored various complex challenges facing digital investigators when performing cloud forensics and some of the proposed solutions for palliating these problems but still there are technical problems require to be inspected. Dykstra et al. [5], described a system called FROST for the OpenStack cloud platform. The FROST can help and assist the digital investigators and examiners to collect and acquire a virtual machine image by providing the integrity of this image with cryptographic checksums. This tool offers trustworthy forensic acquisition of API logs, virtual disks, and guest firewall logs. Not like classical acquisition tools. DeeviRadha and G. Geethakumari [18] proposed an

efficient digital forensic investigation approach in a cloud environment based on a Virtual Machine (VM) snapshots.

Dykstra et al. Zafarullah et al. [29] performed an experiment using Eucalyptus to monitor its behavior, besides, logging external and internal communication and interactions between components of the Eucalyptus. Type of attack called Distributed Denial of Services (DDoS) launched to simulate an attacking scenario then they performed the logging process. They were able to trace the DDoS attack. In [4], they recommended a cloud management plane for using in the Infrastructure as a Service (IaaS) model where Cloud Service Providers (CSPs) can play an important role in data collection by providing a web-based management console.

Zawoad, Shams, Ragib Hasan, and Anthony Skjellum [22], introduced the Open Cloud Forensics (OCF) model which considered the new role of the Cloud Services Provider (CSP) to support reliable and effective digital forensics in the cloud. Simou, Stavros, et al. [30] proposed a meta-model for assisting the process of cloud forensics and moved current research one step further by identifying the major concepts, actors, and their relationships that participating in a cloud forensics process through the introduction of the new meta-model.

Povar, Digambar, and G. Geethakumari [17] emphasized the methods of finding and analyzing digital evidence in a cloud computing environment concerning the cloud user as well as the provider. They proposed and introduced a heuristic model for performing digital forensics in the cloud environment. Their proposed model emphasized the requirements of changes needed in data collection, preservation, and analysis of the digital investigation process. Dykstra et al. [3] introduced a hypothetical case study of child pornography to explain and illustrate the difficulty in the process of collection and acquisition of digital evidence. To prove the existence of contraband data about this case, digital investigators need to make copying or imaging process that bit-by-bit duplication of data. In the cloud environment, this process can do like confiscating the cloud server where many users store their data in the same storage of the cloud.

In [24], Delport et al. studied how the instance isolation to mitigate the multi-tenancy problem. This isolation is necessary to help the investigators to secure and protect digital evidence from the violation. Hirwani, Manish, et al. [10], created a Forensics Snapshot Analysis tool that requires that the two snapshots are of the same VM and the snapshots are converted to dd/raw format. The tool can then analyze the changes that have been made to the recent snapshot by comparing these two snapshots of the same virtual machine. This tool analyses the changes made to a recent snapshot of a virtual machine by comparing it to an earlier snapshot. Saad Alqahtany et al. [1], proposed an independent model to omit the involvement of CSP. They presented an agent-based method that is held in each virtual machine and sending the requisite information to a central Cloud Forensic Acquisition and Analysis System (Cloud FAAs) in infrastructure as a service model. Machine learning and data analysis [13, 14, 25–28] can be used in the cybersecurity domain for providing intelligent threat models in the cloud security domain. In [9] proposed a cloud forensic model that was the basic idea for implementing the proposed model in this research. In [6], they proposed a forensic approach Based on Metadata and Hash Values in the Cloud for Digital Objects. In [7], they explored the issues for cybercrimes investigation in the cloud environment. Likewise, in [8], they used log data for performing log data forensics mitigates the investigation process by identifying the malicious behavior and reveal the hidden malicious activities. This process may help in reconstructing the cybercrime events.

The existing literature has a dominant contribution in providing basic knowledge, new insight, vision, and ideas on how to study cloud forensic and design some works but still their

little mechanisms that are implemented and have proof of concept for real cloud environments. Thus, this paper designed and implemented a cloud forensics model as proof of concept for integrating the forensics process within cloud infrastructures to perform a forensic investigation effectively. Such kind of models could aid the user or cloud service providers to identify the problem and take automatic corrective action by applying the forensic investigation process with saving time and cost.

4 Proposed cloud forensics investigation model

Cloud Forensics pose numerous intricate challenges for performing the investigation process due to the dynamic nature of cloud computing to investigate cloud-based crimes and reconstruct a crime event, then send a final report to a court of law as admissible evidence about the committed crime. In this part, we will introduce the proposed model which works to take snapshots of running virtual machines periodically through using Trusted Center Server (TCS) within a cloud architecture. This model can help to track malicious users in the cloud environment in addition to, determine weaknesses of the running virtual machines for future use and finally provide support and help in the digital investigation process in the cloud. The basic idea is based on taking snapshots of a Virtual Machine (VM) whose activities can be identified through monitoring and record them, then the Cloud Service Provider (CSP) can provide log files and related files about the suspected VM to digital investigators and examiners to obtain digital evidence about an incident that occurred in the CSP's side. Then, performing the identification of the suspected VM, followed by moving or isolating to other locations to preserve confidentiality, privacy, and integrity of the remaining VMs which are running on the same cloud server. This step will protect digital evidence from tampering or modification to be accepted in the court of law. Properly collecting the evidence can help the digital investigator to find malicious users in the cloud.

4.1 Cloud forensics process

Here, the cloud forensics process includes the following stages as identification, collection, preservation, analysis, and finally presentation or documentation. During the presentation process, there is feedback to verify the digital evidence to ensure the integrity of it. Figure 1 shows the proposed cloud forensics process flow.

The verification of integrity can provide a feedback process as shown in Fig. 1 due to the nature of volatile data in a cloud computing environment. This to protect and ensure the integrity of the digital evidence from manipulation and tampering. The verification process can be done by the court of law on the evidence introduced by the digital investigators.

Fig. 1 Flow of cloud forensics process

4.2 Malicious scenario

In the cloud computing environment, users can use cloud infrastructures for launching severe attacks. For example, the user can use his/her virtual machine to make illegal activities, besides, storing his/her illegal materials. This section introduces a malicious scenario to simulate what may occur on the cloud side. The malicious scenario can happen in the cloud-like: **"**John is cloud user who conducted Cloud Service Provider (CSP) of Amazon to create an account to register and use Infrastructure as Service (IaaS) for creating a Virtual Machine (VM). Another user called Alex rented VM for launching attacks and storing illegal materials such as photos and videos. Alex launched an attack against the VM of John to steal his data and also control it to use in launching a Denial of Service (DoS) attack in the cloud environment. Then, John requested a digital investigator to investigate and find the WHO attacked his VM. The investigator started to conduct the Amazon CSP to provide and help to collect any digital evidence related to the incident of John's VM.**"**

In the above malicious scenario, several issues will meet the digital investigator during the investigation process. There are two scenarios in front the investigators may occur as follows:

a. Alex can manage and handle to collude with the Cloud Service Provider (CSP) after the incident. The log files can be modified and manipulated by the CSP so that no way to verify the correctness of the logs. This context, lead to Alex will remain undetected.
b. Even if the CSP was honest, Alex could finish and terminate the use of his VM. This lead no traces will be available to the investigators which makes it challenging in the cloud investigation process.

At the finale of the investigation process, if the investigator does not realize the truth, in this circumstance, the cloud user, John will be responsible for the committed case on the cloud. To identify who made the malicious attack, there is a necessity to present innovative methods, techniques, or models to help the digital investigators and examiners in their mission of cybercrime investigation successfully in the cloud environment.

4.3 Cloud forensics investigation model components and roles

This section provides a diagram for illustrating and explaining the investigation process in the cloud environment. The cloud forensics investigation model consists of five main elements which they play basic roles in this process. These elements are User (s), CSP(s), Attacker (s), Investigator(s), and the court of law as shown in Fig. 2. Figure 2 shows the relations between the basic elements as well as the roles of them during the digital investigation process as follows:

1. **User(s):** Request a Cloud Services Provider (CSP) to create a Virtual Machine (VM) with specific descriptions.
2. **CSP(s):** Response to the user and create the VM then a direct connection between the user and the required VM will establish.
3. **Attacker(s):** Perform and launch severe malicious attacks.
4. **Investigator(s):** Remotely control in connection with the cloud side to collect and acquire digital evidence to make the investigation process and prepare a final report about crimes in the cloud environment.

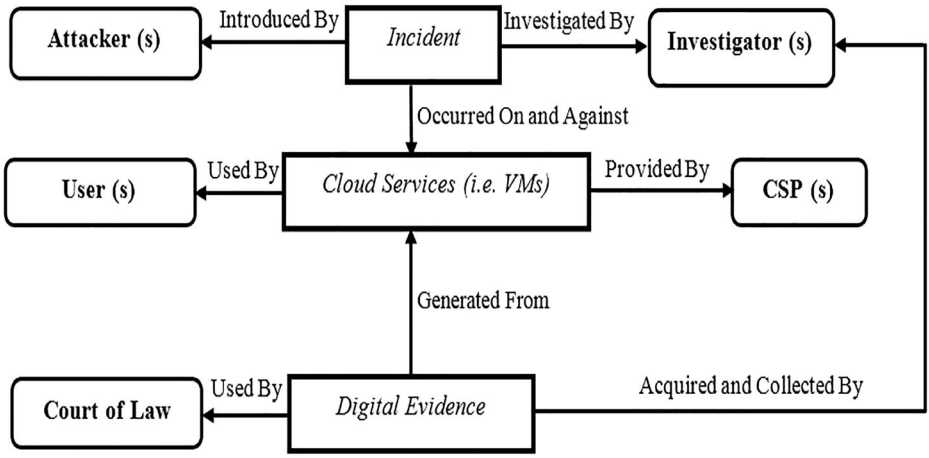


Fig. 2 Digital investigation process in cloud

5. **Court of law:** Responsible for adjudicate legal disputes among parties and accomplish the administration of justice in civil criminal, and administrative matters following the rule of law.

There are another three elements such as Incident, Cloud Services, and Digital Evidence that have an important role in a cloud environment and performing the investigation process as follows:

1. **Incident:** In the cloud, it is an occurrence or event that causes or perform illegal activities like attacks against cloud users or infrastructure.
2. **Cloud Services:** This means the services provided by the CSP such as renting virtual machines and cloud storage.
3. **Digital Evidence:** It is the evidential data extracted and collected from the cloud infrastructures such as log files to help the investigators for performing the investigation process. The digital evidence is considered as proof about an incident that has occurred.

4.4 Forensic investigation model supported cloud infrastructure

In the previous section, the investigation process in a cloud environment is introduced by defining the elements and roles of each element to understand this process and then propose new methods, techniques, and models. Based on the investigation model in Figs. 2, 3, we design a cloud computing system, which is shown in Fig. 4. This system works as an investigation model for supporting the cloud infrastructure in a forensically sound and timely fashion manner. The proposed system is called Cloud Forensic Investigation Model (CFIM).

We add to the previous model which is illustrated in Fig. 3 new elements such as a Trusted Center Server (TCS) and Forensic Server (FS). The TCS is an intelligent system that able to take a snapshot periodically for the state of each Virtual Machine (VM) which runs on the cloud servers and store them in related storage for supporting and providing the digital

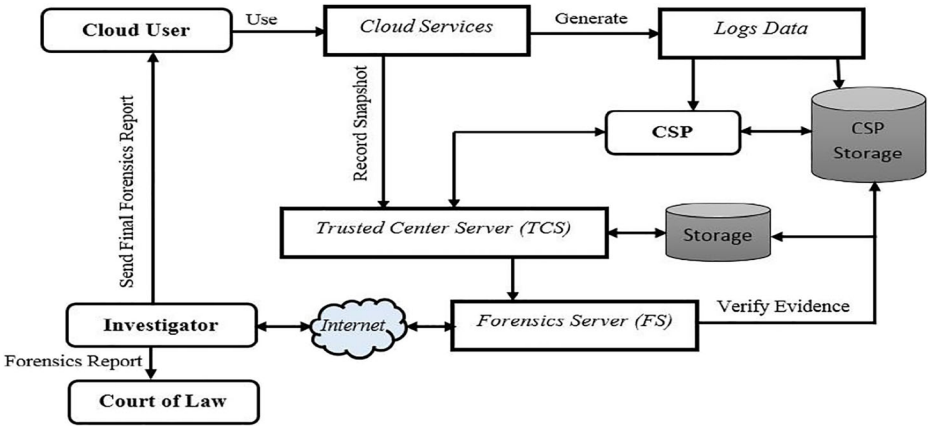


Fig. 3 CIFM supported cloud infrastructure

investigators with evidential data, besides, to using for backup and recovery purposes. The VM Snapshot allows automating the capture of plentiful pieces of information that are vital and critical during incident response and digital forensics. This information, including running processes, users on a system, network logs, open files and applications, Transmission control protocol (TCP), and User Datagram Protocol (UDP) port information. The other new component is the FS used to manage, handle, and process the extracted and collected digital evidence, this can be done remotely by the digital investigator.

The use of FS supports the concept of Forensics as a Service (FaaS) that provide several advantages and benefits of conducting forensics process in the cloud environment side rather than downloading the digital evidence in the investigator side which taking more time on delay in the investigation process. This delay in the time can delay the overall of the digital forensics process so that using the FS will help to benefit from the enormous capabilities of the cloud computing in performing the investigation process in a timely fashion way. To guarantee the

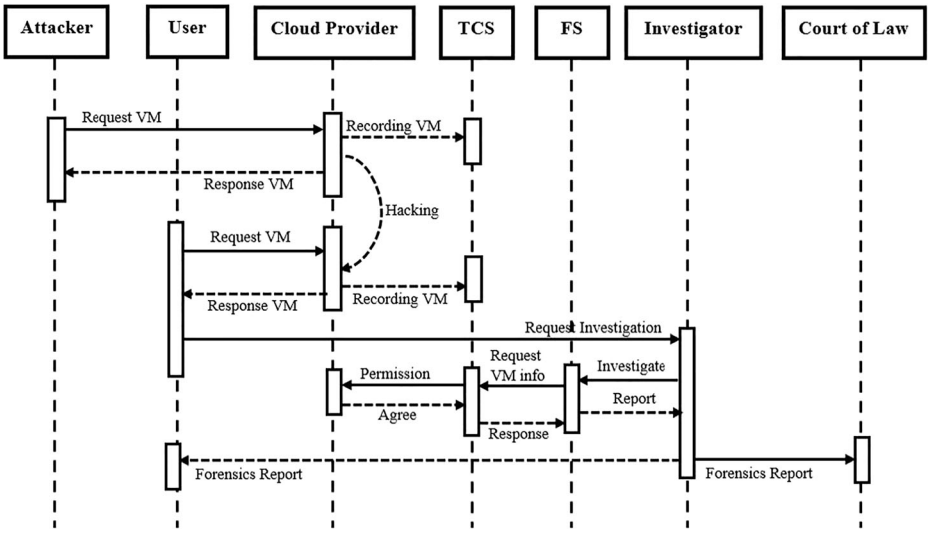


Fig. 4 Cloud forensics process flow based on CIFM model

success of the investigation process in the cloud by using this model, it should integrate the proposed model within the cloud infrastructure. Also, it is essential to mention this model in the Service Level Agreement (SLA) between Cloud User (CU) and Cloud Service Provider (CSP). The proposed model provides the following features to support cloud forensics:

- Prevent the loss of volatile data through recording snapshots of running VMs in persistent storage.
- Help to issue a search warrant in respect of the cloud environment through determining the location of TCS servers.
- No need to resume a suspend VM before the acquisition, which may potentially change the evidence through the use of VM snapshots.
- No need for large bandwidth to download an image of VM instance because the proposed model used the FS on the cloud side.
- Provide a proactive strategy by preserving regular snapshots of VMs that can significantly help incident response and handling.
- Provide the Forensic as a Service (FaaS) concept through the utilization of huge and massive computing and storage resources of cloud computing for performing the investigation process in a timely fashion manner.

4.5 Cloud forensics process based on proposed model

After defining the elements and their roles in the proposed model supported cloud infrastructures as shown in Fig. 3. This model can help in performing the investigation process in a forensically sound and timely fashion manner. The complete investigation process based on the proposed model flow illustrated in Fig. 4 as follows:

- The user requests a Virtual Machine (VM) with specific descriptions from CSP.
- The CSP responds with the required VM and then the user uses it.
- Another user (Attacker) requests a VM from the CSP.
- The CSP response to the user request and the VM created.
- In the background, Trusted Center Server (TCS) start to take periodically snapshot for running VMs.
- Hacking scenario occurred from the attacker to the user.
- After the hacking activity is done, the user starts to conduct a digital investigator to investigate this incident.
- The user sends a request to the digital investigator to investigate the committed incident against his/her VM.
- The digital investigator connects remotely to Forensic Server (FS) in the CSP side to request about the user VM.
- The FS request the TCS to send information about the attacked VM, then the TCS take permission from the CSP to provide the FS with the required VM.
- The TCS sends the required VM's snapshots and Base Files to the FS for the investigation purpose.
- The investigator remotely will perform the investigation process phases which are identification, preservation, analysis, and presentation to reconstruct the committed crime event.
- A final report was then generated about the committed crime.

- Finally, the investigator sends the report to the user or the court of law as admissible proof about the incident.

5 Implementation of proposed model

This section presents the experimental environment setup and implementation steps for the proposed model along with results analysis and discussion.

5.1 Experimental environment

The experimental environment is set up using VMware products is prepared on laptop Lenovo G5080 Core i5 with 12GB RAM and Hard Disk 500GB, where VMware Workstation 11 installed on the host machine, then five virtual machines are created as the follows: ESXi-5 Server1, Domain controller, vCenter/ Trusted Center Server (TCS), Forensic Server (FS) and the investigator machine. Figure 5 shows the implementation of the proposed model. For the experimental purpose, in the ESXi-5 Server1, two virtual machines are installed. The first VM (VM1) assigned to the cloud user and the second one (VM2) assigned to the malicious user (attacker), and a hacking scenario is launched from VM2 against VM1 to simulate a malicious activity in the cloud environment.

5.2 Practical scenario

In the cloud, various services can be provided by the cloud services provider to customers based on cost-per-use or some with the trial time that enables malicious criminals to perform malicious activities such as steal sensitive data of the customers in the cloud. Consequently, the cloud providers have to use protection and monitoring systems like Intrusion Detection/

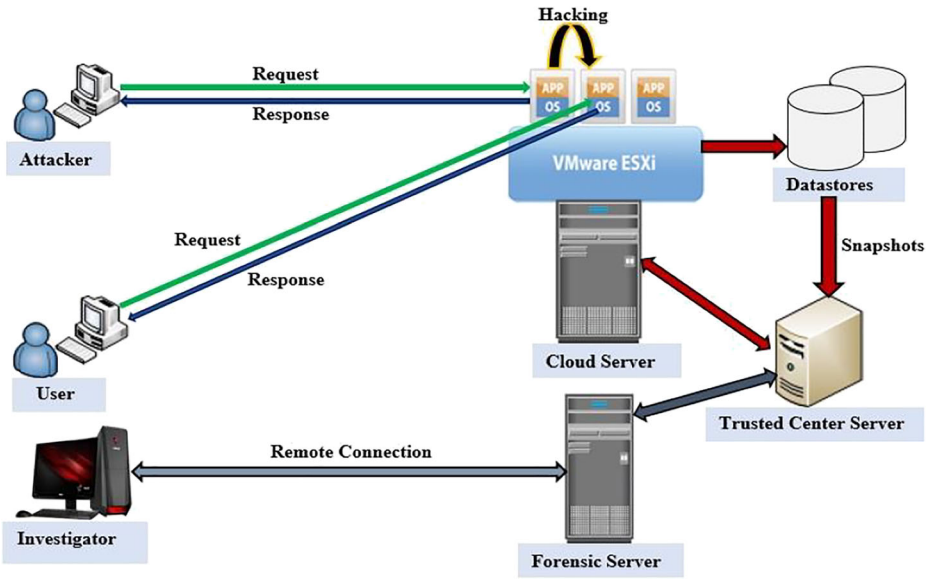


Fig. 5 Implementation of proposed model

Prevention System (IDS/IPS) and VM introspection to prevent these evil activities. Monitoring the behavior of VMs can be achieved by recording its snapshots. Snapshots are considered as a rich source of evidence for assisting the investigation to reconstruct and generate events [18]. The process of recording a VM snapshot is done through connecting to the ESXi server then store it with the VM files in the Datastore. The forensic server then requests the VM files included snapshot files to start the forensic investigation process. Finally, a forensic report is generated by the digital investigator. The general procedure to do this process is shown in Fig. 6 as follows:

1. Start record snapshots of specific VM.
2. The recorded snapshot will store in datastore with other VM files hosted on the ESXi server.
3. The forensic server requires the specific VM files to start the forensic investigation process.
4. Using transfer strategies like vMotion of VM to transfer VM files from datastore to the forensic server.
5. The investigator starts remotely performing a forensic investigation process.
6. The final forensic report will be generated after finishing the forensic investigation process.

For the research purpose in this paper, the practical procedure performed as follows:

1. Start recording and take snapshots for VM1 and VM2.
2. The recorded snapshot will store in the datastore of the ESXi server.
3. Launch the hacking scenario from VM2 “Attacker” with IP Address: 10.10.2.101 to VM1 “Victim” with IP Address: 10.10.2.100.
4. Start recording and take snapshots for VM1 and VM2.
5. The recorded snapshot will store in a data store of the ESXi server.
6. The forensic server requires the VM1 and VM2 files for the forensic investigation purpose.
7. Using transfer strategies to transfer VM from datastore to the forensic server. (i.e. Download VM files)

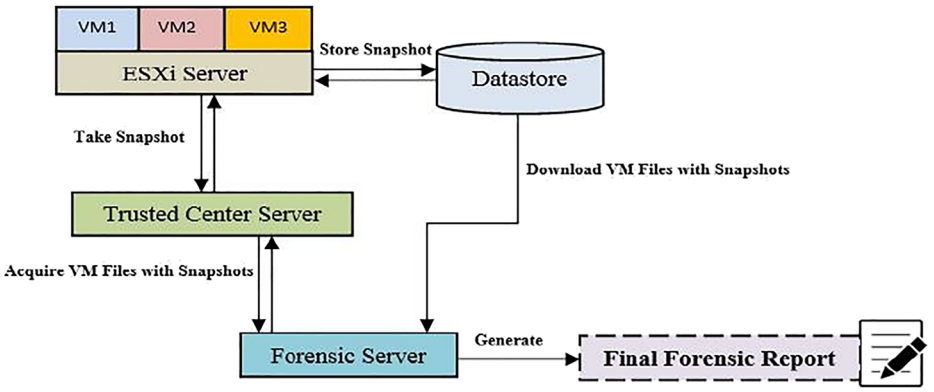


Fig. 6 Taking snapshot and forensic analysis of specific VM

8. The digital investigator starts remotely performing a forensic investigation process.
9. The final forensic report will be generated after finishing the forensic investigation process.

5.3 Results analysis and discussions

Before the implementation of the proposed model, we faced two problems. The first one, how the digital investigator will perform the investigation process using Forensic Server (FS) remotely and the second one is how the Trusted Center Server (TCS) record and take snapshots of running Virtual Machines (VMs) on VMware ESXi server. For the first problem, the digital Investigator can use the Remote Desktop Program (RDP) like on Windows operating system to remotely connect to the forensic server and perform the investigation process where digital forensics tools are installed. The Remote Desktop Connection Program for Windows is shown in Fig. 7. In the computer part, the investigators write the IP address or domain name of the forensic server then will request a password for authentication purposes to prevent unauthorized users from accessing it.

The second problem which represents the basic idea is taking a snapshot of running VMs. Most virtualization products like VMware's ESXi providing snapshot capability of running virtual machines. A VMware snapshot is a point-in-time image of a VM, including volatile data from Random Access Memory (RAM) and the virtual machine disk file. The resulting file can provide digital investigators with an encapsulated copy of the machine at the time when the breach or malicious activity occurs. Likewise, the snapshot of VM enabled the investigators to capture the entire state of the virtual machine at the time it is snapshotted. It is useful to revert repeatedly to the same state without having to create new virtual machines. The snapshot contains several vital information such as settings of the virtual machine, the state of all the virtual machine's virtual disks, and memory contents of the virtual machine that represent volatile data. VM Snapshots allow the preservation of evidence. Seizing the related files and taking them to a secure forensics location is easily accomplished. For implementing the proposed model, there are several solutions to take snapshots of VM such as follows:

Fig. 7 Remote desktop connection program

1. To use vmrun command-line utility included with the VIX API libraries. Vmrun utility enables administrators to control the running virtual machines in VMware product platforms, including Workstation Player, VMware Fusion, VMware sphere, and VMware servers. This utility uses to perform various tasks on virtual machines such as Snapshot captures and record virtual machines events as follows [21]:

- *Snapshots Capture:* Capture the state of a virtual machine at the time of the snapshot, including all data on virtual disks. You can take a snapshot of a virtual machine in any power state and revert to the snapshot at any time. Snapshot commands can list existing snapshots of a virtual machine, create a new snapshot, delete a snapshot, and revert a virtual machine to its state as of a specific snapshot. VMware Server limits you to one snapshot. For example, the following command shows take a snapshot of the virtual machine with VMware Workstation on a Linux host: *"vmrun -T ws snapshot /path/to/vm/Ubuntu/Ubuntu.vmx mySnapshot"*
- *Record and Reply:* Record and replay virtual machine events for later replay. The recording is called a snapshot object but is more like a movie. At this time, only VMware Workstation supports record and replay. These commands begin or end the recording of events, and begin or end the replay of a recording. For example, the following command shows start recording user events on a Windows guest, starting with a snapshot of virtual machine state: *"vmrun -T ws -gu <user> -gp <pass> beginRecording WinXP\WinXP.vmx session1"*

2. To use the command line on the ESXi host to take a snapshot of virtual machines. The following command explains how to take a snapshot of a virtual machine that runs on ESXi host: "*vim-cmd vmsvc/snapshot.create [VmId] [snapshotName] [description] [includeMemory] [quiesced]" where* the [**includeMemory**] and [**quiesced**] variables are boolean values. Set the value to 1 to enable or 0 to disable the snapshot option. For example, create a virtual machine with name '**my_snapshot**', the description is '**snapshot_test**' and the value of '**includeMemory**' and '**quiesced**' is 0 as follows: "*vim-cmd vmsvc/snapshot.create 10 my_snapshot snapshot_test 0 0"*
3. To write a PowerShell script to take periodically snapshot of the running virtual machines on the ESXi server. In the Windows, PowerShell script will write a description of the virtual machine and path to Datastores where it's stored, and finally the path to the destination where the virtual machine files will store. PowerShell script can use to take snapshot from one or multiple virtual machines as follows:

- *Create Snapshot for one Virtual Machine:* The following command illustrates calling the snapshot name "**Snapshot_1**". Replace "**VMname"** with the name of your VM and "**Snapshot_1**" with the name you would like to call the snapshot. After the command completes, a snapshot of the virtual machine with the specified name will be created. Note that the time required for completing taking a snapshot of the virtual machine will vary depending on the size of it. The command of creating a snapshot for one virtual machine is: *"Get-VM VMname | New-Snapshot -Memory -Quiesce -Name Snapshot_1"*
- *Create Snapshot for Multiple Virtual Machines:* For creating a snapshot of multiple Virtual Machines (VMs) with each Snapshot will be named "**Snapshot_2**". In the case of using vCenter for easy management of the ESXi severe where the VMs organized by folder in the vCenter.it has easily taken a snapshot of all VMs in the folder by specifying

the location. The following command taking snapshots of all virtual machines located under the "Folder1" folder: "*get-vm -location "Folder1" | New-Snapshot -Memory -Quiesce -Name Snapshot_2"*

4. Another solution, we proposed an application that can help the digital investigators to take snapshots of the virtual machine and extract useful information like several files created within the virtual machine and information about the storage system of the ESXi host. Figure 8 shows the functions that the proposed application can provide on VMware ESXi hosts. This application is a simple step to developing new forensics tools that can work with VMware products like ESXi for the investigation purpose.

Virtual machine acquisition The acquisition process of the virtual machine is a significant step in performing the forensic investigation process due to all the next stages will depend on it. In a virtualized environment, data for a virtual machine are stored in the storage area on a server and not on the local system like in Personal Computer (PC) and mobile phones. This led the digital investigators to investigate the storage area which includes multiple independent storage devices so that it will be difficult for them to collect and acquire data from these storage

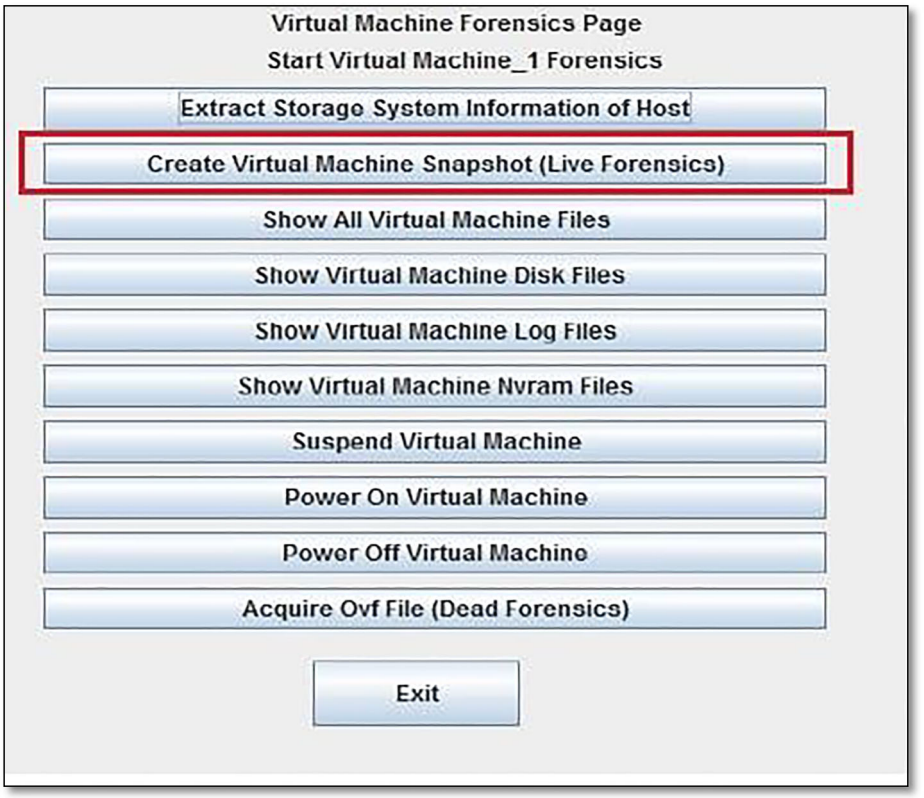


Fig. 8 Take snapshot of virtual machine using forensic application

devices. The solution to this problem is to acquire a virtual hard disk of the virtual machine. However, it is problematic to acquire data for a virtual machine since the virtual hard disk can be allocated in various ways as single or multiple files and via static or dynamic allocation. The data could be stored on one physical disk or distributed across multiple disks. Therefore, we use the hypervisor management system and shell connection program to acquire a virtual hard disk of the suspect user. Doowon Jeong et al. [11] proposed a digital investigation approach for Virtual Desktop Infrastructure (VDI) solutions. They focused on virtual desktop infrastructure and introduced various desktop virtualization solutions that are widely used like VMware, Citrix, and Microsoft. They illustrated and introduced methods for data acquisition of virtual machines through two ways which are, hypervisor management system and shell connection program as follows:

- *Hypervisor Management System:* Here, we focus on VMware hypervisor management system which is called vCenter for acquiring virtual machine through exporting or duplicating in addition to downloading VM files. Table 1 shows data acquisition and collection methods for virtual machine data using the hypervisor management system from VMware (i.e. vCenter).
- *Shell Connection Program:* VMware provides a command-line interface (CLI) with various administrative and management-oriented utilities. One such utility allows the acquisition of a copy of the state of the virtual machine. VMware can collect the raw data duplicated from the original virtual disk. VMware provides a method for collecting virtual machine data using the shell connection program as follows: Connect to the shell using vSphere PowerCLI Virtual disk collection command: copy-datastoreitem [datastore drive]:\[Source Path] [Destination Path].

Any virtual machine has several states such as running, suspended, or in a power-off state. Before data acquisition, the digital investigator should check the state of the virtual machine due to the acquisition method that is applicable varies, depending on its state, so that the digital investigators should understand which methods are suitable to facilitate the forensics process and save time. Table 2 shows the applicable acquisition methods with the state of the virtual machine.

Forensic analysis of virtual machines and their snapshots In a forensic analysis of virtualized environments, when the investigators working with suspended virtual machine images, they have two selections for acquiring the virtual hard disks-either resuming the suspended machine, then use bit-by-bit copy or to directly work with the virtual machine files. The problem with resuming the VM is that during the resume process, numerous files

Table 1 Data collection and acquisition uses VMware vCenter [11]

VM Export	VM duplication	VM configuration file download
Select VM-Menu-File-Export-OVF Template Export ⇒.ovf file Export	Select VM-duplication	Select Hypervisor or VM-Summary-Resource-Storage-select Datastore-Browse Datastore-select folder or file-download

Table 2 Data acquisition methods with virtual machine state [11]

Acquisition method	State of virtual machine		
	Running	Suspended	Turn off
VM export	No	No	Yes
VM duplication	Yes	Yes	Yes
VM configuration file download	No	Yes	Yes
CLI program	No	Yes	Yes

stored on the hard disk are altered, which may abolish evidence and thus the whole forensics process. The extra weakness of resuming the suspended VM is that there is a loss of information stored in the memory as the state of the VM changes. This information could be vital to the investigation being carried out. So, in this paper, authors focus on using snapshots of the running virtual machines in the virtualized environments such as cloud computing that can overcome the drawback that pointed out above. In this research, after taking and recording snapshots of the user and suspect virtual machine, the TCS sends it and related files to the FS to start the investigation process remotely by the digital investigators. In the FS, several important forensics tools are installed for effectively performing the investigation process. These tools such as AccessData FTK Toolkit, Encase, and Autopsy. Finally, a forensic report will generate to document the incident events in the cloud environment and send it to the cloud user or court of law as admissible proof about committed crime.

For the research purpose, the authors used the center as Trusted Center Server (TCS) to perform the function for both at the same time so it can benefit from the vCenter capabilities of taking periodically monitoring of the virtual machines in the one or multiple ESXi servers and the normal role for management of ESXi servers. In the experimental environment, after recording a snapshot of VM1 and VM2. The investigator started downloads the files of them to perform the forensic analysis process in the FS remotely. For each virtual machine, two snapshots are generated first one before hacking and the second after. At the beginning of the forensic analysis, forensic raw images from the virtual machine hard disk and their snapshots are created using the FTK imager tool with calculating the hash values for them without relying on write blockers. This methodology of creating hash values to ensure the integrity of digital evidence as well as guarantee the process is forensically sound. Using memory forensics analysis tools as Volatility Framework - Volatile memory extraction utility framework [23], which use to the extraction of digital artifacts from volatile memory (RAM) samples or memory dump for a VMWare Virtual Machine '.VMSN' file. For the victim or user machine, the two snapshots files are analyzed using the aforementioned tool using the following commands to extract image information, process list, and network connections as follows respectively:

1. C:\Python27\volatility-master>python vol.py **imageinfo** -f *Path of VMSnshotFileName.vmsn*
2. C:\Python27\volatility-master>python vol.py **pslist** -f *Path of VMSnshotFileName.vmsn*
3. C:\Python27\volatility-master>python vol.py **connscan** –f *Path of VMSnshotFileName.vmsn*

The output of memory analysis proof that there is a connection between the attacker machine and victim machine through the port 4444 that commonly used as the default listener port [16] for the Metasploit framework as shown in Fig. 9. This means that the

Offset(P)	Local Address	Remote Address	Pid
0x01706628	10.10.2.100:1037	10.10.2.101:4444	1092
0x01af4e70	10.10.2.100:1035	10.10.2.101:4444	1092

Fig. 9 Output of memory analysis for network connections

attacker may use the Metasploit framework for launching attacks against the user inside the ESXi server. Figure 10 shows the output of memory analysis for the process list, it noticed that the use of a cmd.exe process was used by an attacker to control the victim system. The next step is to the analysis of the hard disk of both machines of the victim and the attacker with IP Address '10.10.2.101' to extract and confirm the criminal activities of the attacker against the user with IP Address '10.10.2.100'. From Fig. 9, observed that there is a connection established between the victim and attacker as proof to help the investigators to identify which machine launched the hacking.

Before the hacking scenario is done, the user did some activities such as the snapshot created, create file1.txt, file2.txt, and file3.txt, then delete file3.txt and finally create a bitmap image called image1.bmp. After that the hacking scenario did as follows:

- Run the Metasploit framework to start the hacking process.
- Create a screenshot of the victim machine.
- Control the shell of the victim machine and do some activities such as create text1.txt,text2.txt, then delete text2.txt
- Perform key logging while the victim writing on a notepad in desktop and record and save it as dump1.txt.
- Upload to "C:\" in the victim machine, which a screenshot picture for the victim machine taken by the attacker. This image name is "PJEMVKZY.jpeg"
- Used the TightVNC program to monitor the screen of the victim machine.
- Denial-of-service Attack -DOS using hping3 10.10.2.100 –flood.

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x819cc9c8	System	4	0	52	245	------	0		
0x81877020	smss.exe	556	4	3	21	------	0	2016-11-17 05:18:02 UTC+0000	
0x8169f128	csrss.exe	620	556	10	299	0	0	2016-11-17 05:18:05 UTC+0000	
0x81895020	winlogon.exe	644	556	18	499	0	0	2016-11-17 05:18:05 UTC+0000	
0x81618628	services.exe	688	644	15	251	0	0	2016-11-17 05:18:06 UTC+0000	
0x8183fa08	lsass.exe	700	644	17	317	0	0	2016-11-17 05:18:06 UTC+0000	
0x818d5cf8	svchost.exe	872	688	15	188	0	0	2016-11-17 05:18:08 UTC+0000	
0x817b9aa0	svchost.exe	956	688	9	237	0	0	2016-11-17 05:18:09 UTC+0000	
0x8154eda0	svchost.exe	1092	688	53	1160	0	0	2016-11-17 05:18:11 UTC+0000	
0x81783560	svchost.exe	1292	688	4	55	0	0	2016-11-17 05:18:36 UTC+0000	
0x817875f0	svchost.exe	1428	688	13	204	0	0	2016-11-17 05:18:39 UTC+0000	
0x815ca7f0	explorer.exe	1460	1412	8	304	0	0	2016-11-17 05:18:40 UTC+0000	
0x815ee2c0	spoolsv.exe	1608	688	10	120	0	0	2016-11-17 05:18:42 UTC+0000	
0x8157b308	wscntfy.exe	608	1092	1	27	0	0	2016-11-17 05:18:58 UTC+0000	
0x814dc980	alg.exe	1020	688	6	103	0	0	2016-11-17 05:18:59 UTC+0000	
0x814b7d50	wuauclt.exe	888	1092	3	132	0	0	2016-11-17 05:19:57 UTC+0000	
0x81908da0	svchost.exe	1652	688	5	123	0	0	2016-11-17 05:52:00 UTC+0000	
0x81635020	cmd.exe	484	1092	1	42	0	0	2016-11-17 06:20:18 UTC+0000	
0x819022c8	cmd.exe	1964	1092	1	45	0	0	2016-11-17 06:21:09 UTC+0000	
0x816a4c10	logon.scr	428	644	1	15	0	0	2016-11-17 06:45:06 UTC+0000	

Fig. 10 Output of memory analysis for process list

User/victim machine analysis The first step in the forensic analysis of any system creates an image of it. Using the FTK imager tool, an image created for the victim machine included snapshots. As known in the digital forensics field, it must check the integrity of the digital evidence (image) using cryptographic hash algorithms such as MD5 and SHA1. Hash values for the images created and matched. AccessData FTK Imager v3.4.2.6 and Guidance Software EnCase v6.18 software are used to analyze the user machine to extract any proof related to the aforementioned criminal scenario. It was observed that three files and one image in the user machine which are created by the user in the Desktop as shown in Fig. 11. Also found links files for them when analysis using Encase as shown in Fig. 12. Figure 13 shows file3.txt in Recycler which is deleted by the user. One criminal activity done by the attacker was to capture a screenshot of the victim system by using the console to control his system, then uploaded it to the victim machine. The screenshot name is "PJEMVKZY.jpeg" as shown in Fig. 14. Another activity done by the attacker is created text1.txt file during using the console which found as shown in Fig 15.

To measure the performance of the user machine during the DOS attack, screenshots were captured to CPU and NETWORK performance before and during the attack as shown in Figs. 16, 17, 18 and 19. The change in the CPU and Network performances refers to illegal or criminal activity was occurring. This can help in the future with help of Intrusion detection systems to develop methods and procedures to perform forensics automatic according to changes in the system performances, which can reduce the time and cost of the digital forensic process.

Criminal/attacker machine analysis Here, after creating an image for the attacker machine using FTK Imager and hash values matched, the analysis process is done using an autopsy forensics tool. From the analysis was observed the screenshot in the attacker machine as shown in Fig. 20. Also observed there a screenshot image of the attacker system during using the TightVNC program to control the victim machine as shown in Fig. 21.

From the analysis of digital evidence related to the criminal/hacking scenario that aforesaid for the research purpose between both victim and attacker machines, found that there is an

Fig. 11 Files created by the user in machine desktop

Fig. 12 Links to the files created by the user

Fig. 13 Deleted file by the user

admissible proof that a machine with IP Address'10.10.2.101′ is responsible for the crime in the cloud that occurred against the user machine with IP Address '10.10.2.100′, thus conclude that the proposed model can assist and help digital investigators and examiners to reconstruct crime events in cloud computing environments in an efficient, forensically sound and timely effective manner.

Experimental results present an analysis of the proposed system for supporting an investigation of the cybercrimes in the cloud. The results reveal that the proposed system can assist the investigators in acquiring forensics data from a virtualized environment in a forensically sound and timely fashion. Likewise, From Table 3, the importance of the proposed system is quite evident. The proposed system is introduced to develop a forensic acquisition methodology from cloud infrastructure and forensically analysis it for supporting in the investigation of cybercrimes in an effective manner.

In summary, the advantages and limitations of the proposed system can be as follows:

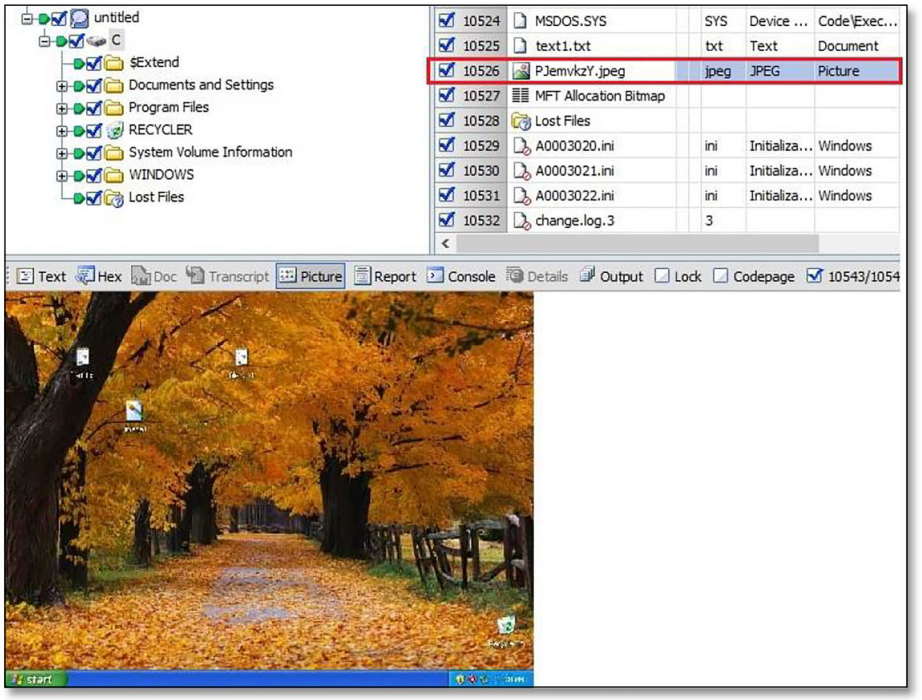


Fig. 14 Screenshot of victim system taken by the attacker

Fig. 15 Text1.txt file that created by attacker remotely in user machine

- **Advantage and benefits:** The proposed system provided several benefits to support cloud forensics such as:
  - Prevent the loss of volatile data through recording snapshots of running VMs in persistent storage.
  - Help to issue a search warrant in respect of the cloud environment through determining the location of TCS servers.
  - No need to resume a suspend VM before the acquisition, which may potentially change the evidence through the use of VM snapshots.
  - No need for large bandwidth to download an image of a virtual machine instance, because the proposed model used the FS on the cloud side.
  - Provide a proactive strategy by preserving regular snapshots of VMs that can pointedly support incident response and handlers when the incident occurs.
  - Provide the Forensic as a Service (FaaS) concept through the utilization of enormous computing and storage resources of cloud computing for performing the investigation process.
  - Ability to identify the criminals and attackers inside the cloud environment.

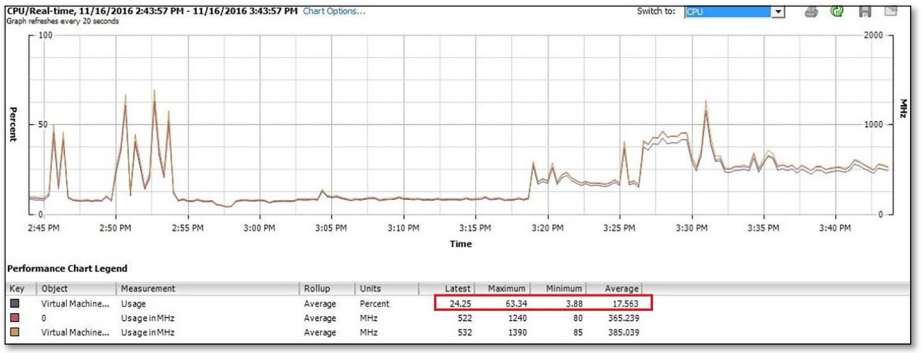


Fig. 16 CPU performance before DOS attack

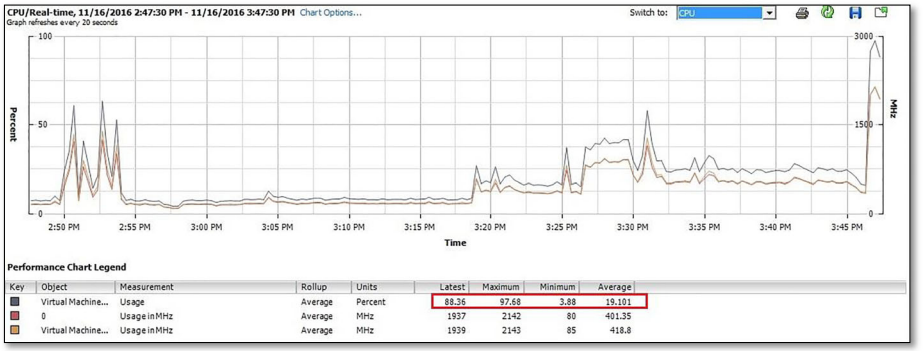


Fig. 17 CPU performance during DOS attack

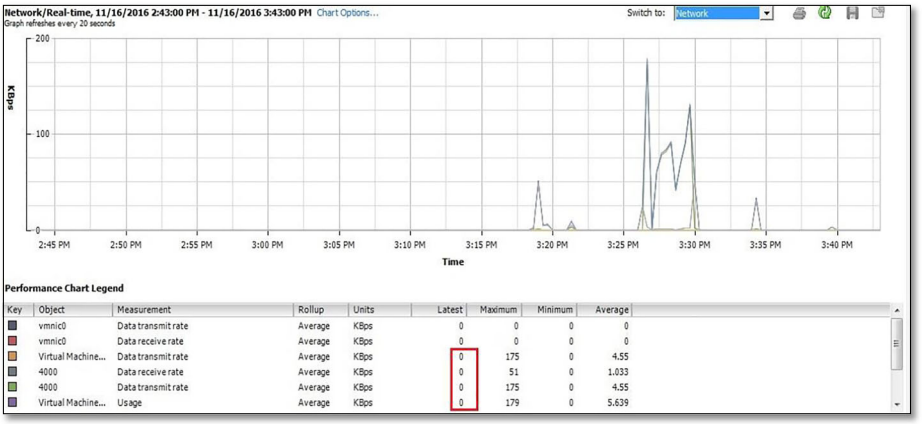


Fig. 18 Network performance before DOS attack

- **Limitations:** The proposed system has some limitations as:
  - It not taking on account the number of servers to deploy while implementing the proposed system, furthermore, it still doesn't address with efficiency the challenge of trust during taking the snapshots of the VMs, this will impact the evidence integrity in a cyber-crime.
  - It is difficult if not impossible to maintain a chain of custody relating to the exchange of the evidence among different forensics entities so may need to use in future Blockchain technology to guarantee the security and trust exchange of cloud-based digital evidence these entities.
  - The proposed system needs to apply with OpenStack, which supports different types of hypervisors such as Microsoft Hyper-V, Citrix XenServer, and Oracle VM.
  - Didn't taking in consideration of reducing forensic image verification time during the investigation process via VM snapshots

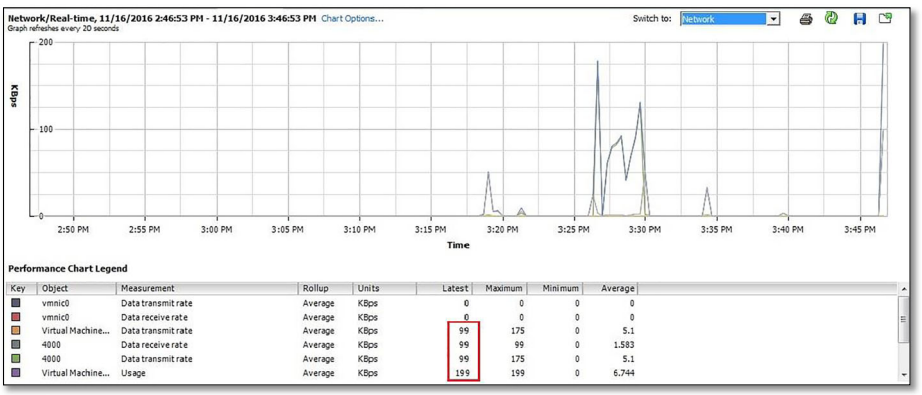


Fig. 19 Network performance during DOS attack

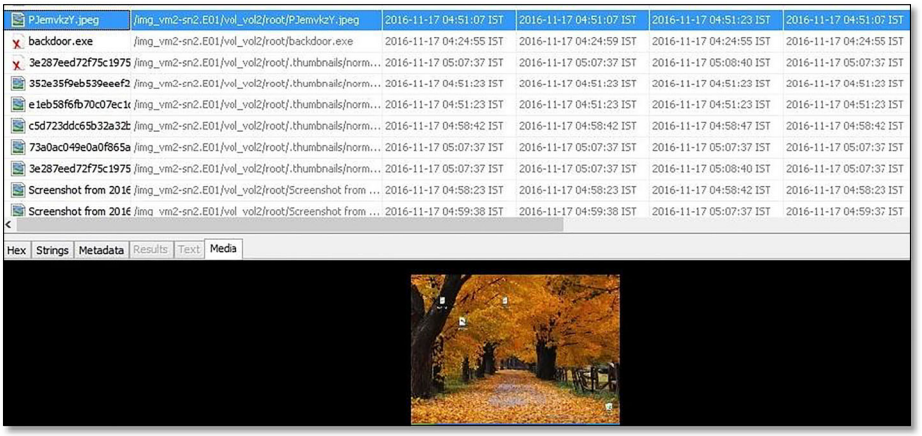


Fig. 20 Screenshot of victim system found in the attacker machine

6 Conclusion and future scope

Recently, several researchers recognized and explored numerous complex challenges facing digital investigators when performing cloud forensics and few of them projected solutions for palliating these problems but still many technical problems require being inspected. Therefore, this paper introduced the design and implementation of a cloud forensics model which is called 'Cloud Forensic Investigation Model (CFIM)'. The implementation of the proposed model within cloud architecture can increase the probability of tracking malicious users in the cloud environment, determine weaknesses in cloud services such as virtual machines for future use as well as support cloud forensics investigations in a forensically sound and timely fashion. In future work, we plan to integrate the proposed system with intrusion detection and prevention systems to reduce digital forensics process cost and time. Besides, utilizing the Blockchain technology in the cloud forensics realm in trust management of cloud-based digital evidence.

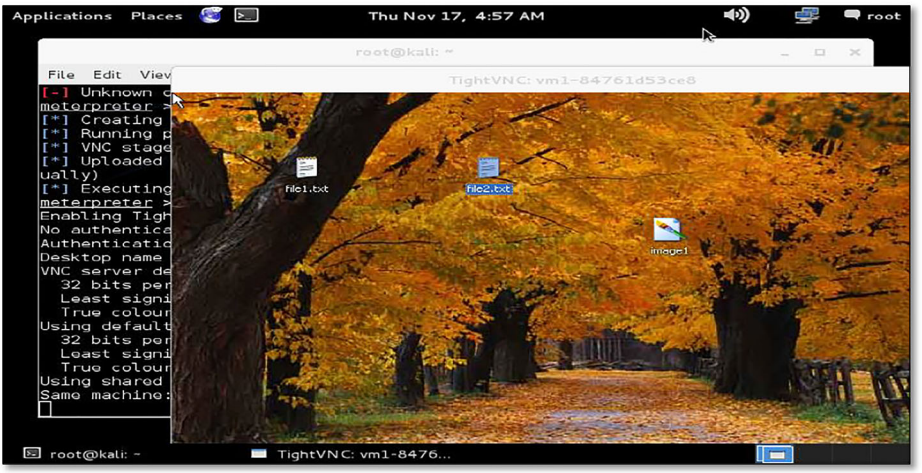


Fig. 21 Screenshot of attacker machine while using TightVNC program against victim machine

Table 3 Analysis study with the previously proposed systems

Work	Description	VM Snapshot	FaaS	Cloud forensics
[17]	A heuristic model for performing digital forensics in the cloud environment	No	No	Yes
[22]	identifying the major concepts, actors, and their relationships that participating in a cloud forensics process through the introduction of a new meta-model	No	No	Yes
[12]	A model that allows digital forensic readiness to be achieved by implementing a Botnet as a service (BaaS) in a cloud environment.	No	No	Yes
Proposed System	A smart system that able to take a snapshot sporadically for each Virtual Machine (VM) status which runs in the cloud and sends it to a Trusted Center Server (TCS) for storing VM snapshots	Yes	Yes	Yes

Appendix

'Forensic Report' Example

Final Forensic Report for Investigation attack in Virtualized Environment

1. **Case Number:** 20161210–001-CloudCrime.
2. **Examiner:** EZZ.
3. **Status:** Finished and completed.
4. **Crime Scene:** Cloud Computing Environment.
5. **The conclusion of Findings:**

- Screenshot image related to the victim machine.
- Network connection established using port 4444 between Victim Machine and attacker.
- Text1.txt file creates by attacker founded in the victim machine.
- Screenshot image of the attacker system during using the TightVNC program to control the victim machine.
- Noticed changes in CPU and Network performance during the DOS attack.

2. **Items analyzed**

- Two virtual machines, "Windows XP and Kali Linux" with their snapshots, which acquired from ESXi Server.

3. **Details of Findings:**

The findings related to virtual machines hosted by the ESXi server are:

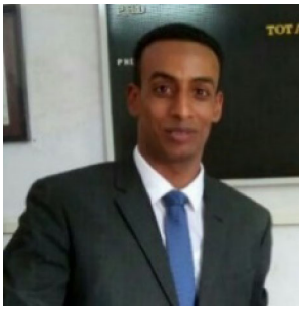
- The analyzed virtual machines were found to contain Windows XP and Kali Linux operation systems.
- Screenshots for the victim machine and 4 for the attacker machine.

Written By Examiner: EZZ.

References

1. Alqahtany S, Clarke N, Furnell S, Reich C (2016) A forensic acquisition and analysis system for IaaS. Clust Comput 19(1):439–453
2. Barrett D, Kipper G (2010) Virtualization and forensics: a digital forensic Investigator's guide to virtual environments. Syngress
3. Dykstra J, Sherman A (2011) Understanding issues in cloud forensics: Two hypothetical case studies. Journal of Network Forensics b(3):19–31
4. Dykstra J, Sherman A (2012) Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. DoD Cyber Crime Conference, January
5. Dykstra J, Sherman AT (2013) Design and implementation of frost: digital forensic tools for the OpenStack cloud computing platform. Digit Investig 10:S87–S95
6. Hemdan EE-D, Manjaiah DH (2015) Forensic analysis approach based on metadata and hash values for digital objects in the cloud. International Journal of Innovative Research in Computer and Communication Engineering 3(7):1–6
7. Hemdan EE-D, Manjaiah DH (2015) Exploring digital forensic investigation issues for cyber crimes in cloud computing environment. Proceeding of 1st International Conference on Computer Communication and Networks (i3CN)
8. Hemdan EE-D, Manjaiah DH (2017) Spark-based log data analysis for reconstruction of cybercrime events in cloud environment. 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT). IEEE
9. Hemdan EE-D, Manjaiah DH (2018) CFIM: toward building new cloud forensics investigation model. Innovations in Electronics and Communication Engineering. Springer, Singapore, pp 545–554
10. Hirwani, Manish, et al. (2012) Forensic acquisition and analysis of VMware virtual hard disks." Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)
11. Jeong D, et al. (2015) Investigation methodology of a virtual desktop infrastructure for IoT. Journal of Applied Mathematics
12. Kebande VR, Venter HS (2014) A cloud forensic readiness model using a Botnet as a service. The international conference on digital security and forensics (DigitalSec2014). Ostrava: The Society of Digital Information and Wireless Communication
13. Liu, Shouqiang, et al. "Research of animals image semantic segmentation based on deep learning." Concurrency and Computation: Practice and Experience 32.1 (2020): e4892.
14. Liu S, Yu M, Li M, Xu Q (2019) The research of virtual face based on deep convolutional generative adversarial networks using TensorFlow. Physica A: Statistical Mechanics and its Applications 521:667–680
15. Mell P, Grance T (2014) Nist cloud computing forensic science challenges. Draft NISTIR 8006
16. Port 4444 Details, http://www.speedguide.net/port.php?port=4444/ [last accessed 23-6-2020].
17. Povar D, Geethakumari G (2014) A heuristic model for performing digital forensics in cloud computing environment. Security in Computing and Communications. Springer, Berlin Heidelberg, pp 341–352
18. Rani D, Geethakumari G (2015) An efficient approach to forensic investigation in cloud using VM snapshots. IEEE International Conference on Pervasive Computing (ICPC)
19. Ruan K et al (2011) Cloud forensics. Advances in digital forensics VII. Springer, Berlin Heidelberg, pp 35–46
20. Ruan K, Carthy J, Kechadi T, Baggili I (2013) Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit Investig 10(1):34–43
21. Server, VMware (2008) Using vmrun to control virtual machines
22. Simou S, et al. (2015) A meta-model for assisting a cloud forensics process. Risks and Security of Internet and Systems. Springer International Publishing, 177–187.
23. Volatility Foundation, http://www.volatilityfoundation.org / [last accessed 23-6-2020].
24. Waldo Delport MK, Olivier MS (2011) Isolating a cloud instance for a digital forensic investigation. in Information and Computer Security Architecture (ICSA)
25. Xu Q (2013) A novel machine learning strategy based on two-dimensional numerical models in financial engineering. Math Probl Eng 2013:1–6
26. Xu Q (2019) Et al. "multi-feature fusion CNNs for Drosophila embryo of interest detection.". Physica A: Statistical Mechanics and its Applications 531:121808

27. Xu Q, Li M (2019) A new cluster computing technique for social media data analysis. Clust Comput 22(2): 2731–2738
28. Xu Q, Wu J, Chen Q (2014) A novel mobile personalized recommended method based on money flow model for stock exchange. Math Probl Eng 2014:1–9
29. Zafarullah Z, Anwar F, Anwar Z (2011) Digital forensics for eucalyptus. in Proceedings of Frontiers of Information Technology (FIT). IEEE:110–116
30. Zawoad, Shams, Ragib Hasan, and Anthony Skjellum (2015) OCF: an open cloud forensics model for reliable digital forensics." Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on. IEEE



Ezz El-Din Hemdan has received his B.Sc from the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2009. He received his M.Sc. From the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt, in 2013. He received his Ph.D. degree in the Department of Computer Science, Mangalore University, India in 2018. He has several publications in national/international conferences and journals. His research area of interest includes; Canacelable Biometric, Blockchain, Digital Twins, Image Processing, Virtualization, Cloud Computing, Internet of Things/Nano-Things, Cryptography, Data Hiding, Digital Forensics, Cloud Forensics, Big Data Forensics, Data Science and Big Data Analytics.

Manjaiah D.H is a Professor & Chairman in the Department of Computer Science, Presently the Chairman of the Board of Studies in Computer Science, Faculty Science and Technology at Mangalore University. He has done his Ph.D. in the area of Advanced Network Computing Paradigm and completed his M.Tech, from the National Institute of Technology Karnataka, Surathkal. Being involved in teaching and research for more than 25 - years. He has produced very valuable 15 - Ph.D. Scholars, who are all currently working in reputed organization and Educational Institutions in India and Overseas. Presently 08 plus 02 (overseas) scholars are undertaking research under his supervision He has technologically progressive the Novel awareness of Routing Algorithms for Mobile Ad - Hoc networks, Vertical Handoff Mechanisms for 4G - Networks and Enhancement of Digital Forensic Laboratory in INDIA. He also has immense knowledge of handling large scale research projects sponsored by various funding agencies like UGC, DST - SERB, and DST - VGST. He has delivered around 195 invited & Keynote talks in several international conferences, symposiums, workshops, and training sessions in INDIA and Abroad. He has authored and published around 136 in reputed International / National Journals and conferences on various topics in Mobile AD - HOC Networks, IPv4 and IPv6 mobility, Machine Learning and Deep Learning, Virtualization using Cloud Computing / Cybersecurity, and Digital forensics