Abstract

In the present days, cloud forensic techniques cannot be accomplished by way of computer and network forensic techniques in conventional IT systems because of intricate complications such as crime scene reconstruction, isolating cloud instance, data provenance, evidence segregation, and dynamic nature of cloud computing. But they can be performed in a way that is reliable with the law by developing and presenting new suitable digital forensic procedures, approaches and techniques to assist digital investigators for investigation of cloud-based crimes in legal and efficient fashion. The digital investigators have to recognize the existing techniques and procedures which are inadequate in the cloud environment where forensic acquisition and analysis process will be inversely achieved.

Applying digital forensic techniques in cloud computing environment are facing complex challenges and obstacles which need to be resolved to perform a convenient cloud forensics. Thus, this thesis concerns with developing proficient digital forensic techniques for investigation of cybercrimes in the cloud computing environment in forensically sound and timely manner. The aim of this research is to study and resolve the following issues:

- Explore and identify challenges and opportunities for performing digital forensics investigation in the cloud computing environment. A literature review is done to understand and explore the cloud forensic challenges and opportunities.

- Secure cloud storage with understanding and identifying data remnants that are available after accessing, using and conducting Box cloud storage as a case study and provide a method to perform the forensic investigation of this cloud storage service in forensically sound manner. To do this, a cloud forensic approach is proposed for securing cloud storage and assisting digital investigators in performing digital forensics for Box cloud storage service as a case study.

- Perform forensic analysis of large volume of log data to reconstruct a timeline of cybercrime events in the cloud environment. Log data are considered one of significant evidence that aid to reconstruct what has happened during a certain period which means that can help to redraw cybercrime events. Due to the increase of the volume of log data that was generated from cloud services and infrastructures, it becomes a big challenge to handle and process these data using traditional tools and methods. A forensic approach is proposed using Apache Hadoop and Apache Spark to analyze the large size of log data and extract knowledge from them which can
assist digital investigators during investigating cloud-based crimes that occurred through a particular time and also to speed up the investigation of the cloud crime.

- **Specify a method to follow in the investigation of cybercrimes in private cloud environments.** A digital forensic approach for investigation of cybercrimes in a private cloud environment is proposed. The proposed approach can help digital investigators and practitioners in acquisition and collection of digital evidence from the private cloud infrastructures especially virtual machine which is considered the core element of virtualized cloud systems. Also, introduce a forensic methodology for investigating and analyzing virtual machine and its snapshots for helping in the reconstruction of criminal activities which can be done using a virtual machine.

- **Forensic investigation of VMware clustered ESXi hypervisors.** To solve this problem, a forensic acquisition application called Hypervisor Forensic Acquisition Application (HFAA) is proposed for helping in digital evidence acquisition process from clustered VMware ESXi servers. This application can provide an initial step and guide to digital investigators and researchers to develop new applications and tools for real-time forensic acquisition and analysis of virtualized environments like cloud computing. With some additional development and evaluation through adding new features to the proposed application, this can become a good tool for using in cloud forensic community.

- **Provide cloud services with ensuring that Cloud Service Providers (CSPs) support the digital investigation process (i.e. building cloud architecture support digital forensics).** In order to handle this problem, the design and implementation of a new Cloud Forensics Investigation Model (CFIM) are introduced to investigate cybercrimes in the cloud computing environment. The proposed system is a smart system that is able to take a snapshot of the state of running virtual machine in virtual datacenter and send to Trusted Center Server (TCS) which monitors the status of the VMs as well as store their snapshots to send them for Forensic Server (FS) for performing the forensics process. The proposed model supports a concept of Forensics as a Service (FaaS) that provide various benefits of conducting digital forensics through using Forensic Server on the cloud side.

- **Design and build a cloud forensic laboratory to investigate cybercrimes as well as provide a learning environment for law enforcement officers, researchers, and students.** A Cloud Forensic Laboratory (CFL) is suggested to face the sophisticated yet advanced level of cybercrimes taking place currently in classical IT and cloud systems. The proposed system can
benefit from enormous storage and processing capabilities which are provided by cloud computing to perform acquisition, extracting, analysis, examination and reporting for a large size of digital evidence for both of crimes in IT systems and cloud systems. The proposed system can help the digital investigators and practitioners to perform the digital investigation process.

The proposed work in this thesis would support an investigator and Cloud Service Provider (CSP) to understand how to accomplish digital forensic investigation in cloud computing environment. The digital forensic procedures that are recommended in this research can use for analysis of the cloud-based crimes against to cloud data. The proposed procedures would help the digital investigator in reducing the whole processing time of cloud-based crimes under forensic investigation. This research can be a way forward to fight cybercrimes in cloud computing environment as well as the proposed cloud forensic model presented in this work can be considered as a reference cloud forensic model.

In conclusion, this thesis delivers cloud forensic challenges and opportunities as well as provides a number of proposed solutions for recent critical forensic issues related to the investigation of cloud-based crimes in forensically sound and timely fashion.

**Keywords:** Cloud Computing, Digital Forensics, Cloud Forensics, Cybercrimes, Cloud Storage, Big Log Data Analysis, Apache Hadoop, Apache Spark, Virtualization, VMware, Hypervisors, and Forensics Laboratory.