Received: 10 December 2020 | Revised: 27 December 2020 | Accepted: 4 January 2021 | Published on: 27 January 2021

DOI: 10.1002/spy2.149

RESEARCH ARTICLE

WILEY

Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring

Sheunesu Makura[1] | **H. S. Venter**[1] | **Victor R. Kebande**[2] | **Nickson M. Karie**[3] | **Richard A. Ikuesan**[4] | **Sadi Alawadi**[5]

[1]University of Pretoria, Pretoria, South Africa

[2]Lulea University of Technology, Luleå, Sweden

[3]Edith Cowan University, Joondalup, Australia

[4]Qatar Community College, Doha, Qatar

[5]Uppsala Universitet, Uppsala, Sweden

Correspondence
Victor R. Kebande, Lulea University of Technology, Luleå, Sweden.
Email: victor.kebande@ltu.se; vickkebande@gmail.com

Abstract

An increase in the use of cloud computing technologies by organizations has led to cybercriminals targeting cloud environments to orchestrate malicious attacks. Conversely, this has led to the need for proactive approaches through the use of digital forensic readiness (DFR). Existing studies have attempted to develop proactive prototypes using diverse agent-based solutions that are capable of extracting a forensically sound potential digital evidence. As a way to address this limitation and further evaluate the degree of PDE relevance in an operational platform, this study sought to develop a prototype in an operational cloud environment to achieve DFR in the cloud. The prototype is deployed and executed in cloud instances hosted on OpenStack: the operational cloud environment. The experiments performed in this study show that it is viable to attain DFR in an operational cloud platform. Further observations show that the prototype is capable of harvesting digital data from cloud instances and store the data in a forensic sound database. The prototype also prepares the operational cloud environment to be forensically ready for digital forensic investigations without alternating the functionality of the OpenStack cloud architecture by leveraging the ISO/IEC 27043 guidelines on security monitoring.

KEYWORDS

cloud, digital, forensic, ISO/IEC 27043, operational, readiness, security

1 | INTRODUCTION

Information Technology (IT) has recently transformed the way organizations operate by providing an effective means of executing their tasks. IT has enabled the automation of tasks across organizations and this has led to increased productivity. This use of IT across organizations has resulted in the following advantages: faster communication, remote access, and the storage of data in digital systems. Nevertheless, it is important to note that, nearly every organization in this modern era makes use of IT for its operations in various ways. Also, IT systems are assisting organizations in decision making, storage of organizational records, automating organizational processes, and increasing throughput.

Such advancements in IT have led to the development of cloud computing technologies. Various organizations have adopted the cloud paradigm as a model for running their business solutions. Organizations can obtain access to cloud

applications that enhance their business operations at minimal costs. The availability of cloud-based applications at the global level has led to the reduction of costs and easy access to the same applications regardless of the geographical location. This means that there is no need for the organization to avail the same cloud-based applications per each organizational site. The continued advancement of cloud computing technology over the years has allowed organizations to utilize cloud-based applications and services. Cloud-based infrastructure usage has indeed grown and in particular public cloud infrastructure expenses have had a yearly growth rate of 17.7% (more than 200 billion dollars) in the years 2010 to 2015.[1] Examples of public cloud services include Amazon's Elastic Compute Cloud (EC2), Google's AppEngine and Microsoft's Azure Services platform.[2]

The use of cloud computing services has unwrapped many opportunities for organizations, however, these opportunities also bring with them formidable security and privacy challenges. One of these challenges arises from large volumes of data (big data) that Cloud Service Providers (CSPs) store. As big data gets uploaded onto the cloud, questions arise with regards to the security and seclusion of the data. Further questions asked include who owns the data, who has access to the data, and whether or not the data is encrypted.[3]

Some organizations are wary of adopting cloud computing because they are afraid that the cloud infrastructures can be hacked, which might lead to organizational data loss, the disruption of IT systems, and a reduction in performance and availability.[4] Organizations are more concerned with keeping the data secure whether when it is in storage media or when it is in transit. As a result, it becomes necessary that the data stored in cloud infrastructures are protected at all times. The protection ensures the confidentiality, availability, and integrity of data. Besides, should there be a compromise then an investigation should follow to determine the causes of the incident[5,6] through digital forensics.

Digital forensics (DF) is defined as the process of using scientifically demonstrated techniques in the "collection, preservation, analysis and presentation of digital evidence" obtained from electronic devices to reconstruct events that appear to be criminal.[7] It makes use of scientifically proven methods in conducting any type of digital investigation.[8] DF can be used to answer a variety of questions about what would have caused the incident when it happened, and about how the incident unfolded. These questions usually arise after an incident has occurred. An incident in this context is a threat or violation of computer security policies.[9] Examples of incidents include organizational data loss or a malware intrusion. Finally, DF can provide means to prevent security problems within cloud infrastructures by identifying potential security threats and assist in the creation of solutions to security problems.

To protect data in the cloud, there is a need for proactive approaches. This approach entails consistently and continually monitoring the movement and storage of information within the cloud. This approach also prepares organizations to be forensically ready before potential security incidents happen. In the case where an incident has already happened, there arises the need to investigate and conduct an analysis of evidence to uncover what happened or the root cause of the problem. This fact-finding mission can be done through digital forensic readiness (DFR).

Tan[8] outlines digital forensic readiness (DFR) as the capability of a digital forensic investigation agency in boosting the usage of collected digital evidence whilst reducing the expense of a digital forensic investigation to responding to an incident. Digital forensic investigations can be a challenge for organizations due to the costs that may be involved in modifying a cloud infrastructure since reprogramming the cloud is costly and time-consuming.[10] Potential digital evidence (PDE) is defined as any collected digital data that might be relevant to a digital forensic investigation. In order to bring out the problem that is being addressed in this paper the authors give a description of the following case scenario, where more details become apparent in the later sections of this paper:

> This case scenario focuses on solving a case where an employee uses the credentials of the manager who has authorized access to retrieve confidential company information hosted on the company's FTP site. The company has rules and regulations, which forbids employees from accessing the FTP site. However, the company allows only managers to have access to the FTP site. The employees are also not allowed to access social media sites during working hours (8am to 4pm). A cloud instance was setup in OpenStack environment and a security monitoring application was deployed on the cloud instance to conduct monitoring given that the users/employees had good understanding of the Service Level Agreements (SLAs). One unsuspecting user managed to violate this code of conduct and while doing this, the user downloaded some softwares through a pop-up which installed a malware accidentally. The Keystrokes entered by the users accessing the FTP site that included the username and password and the social media site employed by the user to gain unauthorized entry into the site were captured by the by this security monitoring application.

Based on the mentioned scenario, it is imperative to note that, detecting the violation needs proper planning and preparation in order to detect potential security incidents. As a result of the above-mentioned scenario, the authors give the contribution of this paper as follows:

1. Demonstrate approaches for achieving digital forensic readiness in the operational cloud using Openstack
2. Align the digital forensic approaches based on the recommendations of ISO/IEC 27043 guidelines on security monitoring
3. Generate a contextual discussion based on the propositions and the scenario.

The remainder of the paper is organized as follows. In Section 2, a Background is given. This is followed by DFR approaches in the operational cloud in Section 3 and ISO/IEC 27043 guidelines and recommendations in Section 4. A discussion and evaluation of the propositions are given in Section 5. A conclusion and a mention of the future work of the study are given in Section 6.

2 | BACKGROUND

This section presents a background study on digital forensics process models, forensic readiness in the cloud, botnets, cloud computing, and ISO/IEC 27043 international standard process groups. Digital forensic process models are discussed to show the stages of digital investigations from a scientific view, while forensic readiness is discussed to show the proactive side of before incident detection as part of incidental preparedness. Consequently, botnets are discussed because they have been employed as software applications with the capability of extracting digital information. It is worth to note that the scope of this research is inclined in pre-incident preparation as highlighted in the ISO/IEC 27043: guidelines.

2.1 | Digital forensic process models

Any scientific method follows a predefined set of processes, with DF, as a science, following a scientific process. A DF process model is a scientific method that follows a predefined set of forensic processes. Various digital forensic process models have been proposed in literature; Reith et al[11] Carrier & Spafford[12]; Beebe & Clark,[13] Agarwal et al[14]; Ikuesan & Venter,[15] Valjarevic & Venter,[16] Kebande and Venter.[17] However, this research study only focuses on one of the process models, the Harmonized Digital Forensic Investigation Process Model (HDFIPM). Hence, a brief description is provided below to present an insight into some of the processes covered in the process model.

Researchers in[16] proposed a process model titled, the Harmonized Digital Forensic Investigation Process Model (HDFIPM) which has formalized processes also shown in Figure 3 from a high-level standpoint. The HDFIPM formalizes the processes that have to be followed in a standardized approach by setting guidelines for digital forensic investigations. An important aspect about the HDFIPM is that it also complies with the legal recommendations and requirements for a digital investigation hence increasing admissibility of potential evidence during litigation.[16] Furthermore, the HDFIPM model consists of the following phases (in chronological order): "incident detection, first response, planning, preparation, collection, transportation, storage, analysis, presentation, and conclusion." It also consists of concurrent processes, which happen throughout the phases, and these are: "obtaining authorization, documentation, information flow, preservation of chain of evidence, and interaction with physical investigation."[16] This process model constitutes part of the ISO/IEC 27043 standard which forms the basis of our study. The software prototype used in this research study also follows some of the phases in the HDFIPM process model, which are the collection (as mentioned in ISO/IE 27043), transportation, and storage phases. The next section describes how the digital forensic processes are implemented on the cloud.

2.2 | Forensic readiness in the cloud

The cloud computing entails the use of a virtual platform to host software services. This virtual platform can be used on several different workstations connected via a network. A virtual platform is one that can be provided by

a cloud operating system.[19] A typical digital forensic investigation (DFI), uses the traditional search and seizure method, in which the investigator seizes a particular electronic device such as a laptop and makes a bit by bit copy of the seized device.[20] This procedure is easy when one has access to the physical device, but in a cloud environment, this becomes a challenge because the data centers and cloud infrastructures may be sitting in different areas/jurisdictions.[21]

There exists no formal structure of conducting DFR in a cloud infrastructure.[17] Consequently, several international standards, such as the ISO/IEC 27043:2015, have been developed as an international standard seeking to provide a formal method for conducting DFR. ISO/IEC 27043 consists of readiness processes that seek to maximize the potential worthiness of computer evidence to lower the costs involved in a typical digital forensic investigation.

Kebande and Venter[14] argue that there lacks a structured approach for conducting DFR in the cloud without the need to adjust or change the existing cloud structure. This alteration of the existing cloud infrastructure is a huge challenge because of the costs incurred in performing DFR in the cloud.[14] ISO/IEC 27043 itself does not directly target the cloud environment but encompasses all DFR processes that can be conducted in any type of environment.

Nevertheless, Agarwal et al[14] argues that DFR can be implemented by using a systematic and proactive methodology in the collection and storage of digital evidence. De Marco[1] notes further that the DFR capability in the cloud can be attained through the employment of an information collecting system with capabilities to both collect sensitive data and warn the host system before an incident occurs. Researchers in[22] also proposed technical, legal and organizational factors influencing DFR for Infrastructure as a Service to cloud consumers. Their main focus though was in understanding and identifying factors that contribute to cloud forensics readiness and how these factors can help to achieve forensics readiness in the cloud.

In another research[23] elaborates on the requirements needed in order for the cloud to be forensically ready when a modified Non-Malicious Bot (NMB) is used. The focus of the research was simply to outline the requirements for achieving DFR in the cloud from a legal, technical and operational standpoint. Recent research by[5] has further explored the design and implementation of a feasible technique for performing DFR in any cloud environment. The research employed a modified NMB whose functionality were adjusted to perform forensic logging for DFR purposes. Their technique was meant to allow organizations perform DFR in the cloud without interfering with the operations and functionalities of the existing cloud architecture or infrastructure.

More research by[24,25] presented an architectural design of a Cloud Forensic Readiness as-a-Service (CFRaaS) that used an NMB solution as a forensic agent. The main focus was to bring out the requirements that are needed in order for the cloud to be forensically ready. To achieve this, the authors identified important dependencies and indicators that provided a synergistic relationship during the time of designing the CFRaaS. To further elaborate on the issues and challenges of Cloud Forensic Readiness[6] presented some of the challenges faced when an Agent-Based Solution (ABS) is used in the cloud to extract Potential Digital Evidence (PDE) for DFR purposes. The aim of the ABS was to modify the functionality of a malicious botnet to act as a distributed forensic agent to conduct DRF. Their focus however was mainly on technical and operational challenges that are encountered when trying to achieve DFR in the cloud environment.

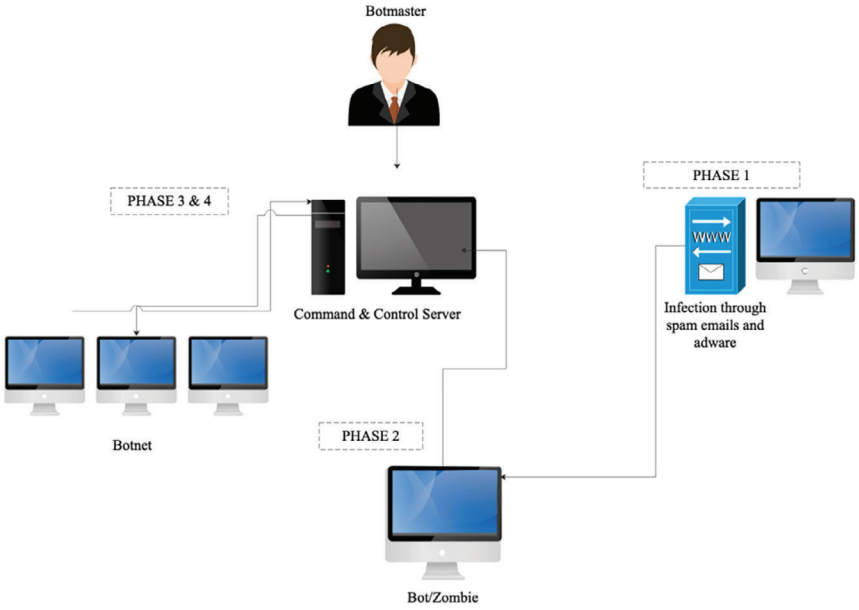
A study by Van Staden and Venter[14] focused on the usage of performance monitoring tools to attain DFR in the cloud. This study made use of a Learning Management System (LMS) as performance-monitoring tools in acquiring data from the LMS. Their results show that it is possible to acquire digital data while using the performance monitoring tool. Therefore, this data can be used by DFIs during forensic investigations.

Nonetheless, there is concern on the way digital forensic investigations are executed to combat threats and attacks in a cloud platform and one of these concerns include predominantly the absence of DFR.[8] To explore more on this, the reader is encouraged to read other research works by[10,17,26,27] as well the reference architecture for a cloud forensic readiness system by.[25]

2.3 | Botnets

The name botnet is derived from the term "bot" or simply "robot," which is a piece of software that can be used to infect a device and automate tasks over the Internet. A cluster of these bots forms what is known as a network of bots or botnets, which are a group of interconnected devices. However, botnets are usually controlled by an attacker remotely.[28] Furthermore, botnets are capable of sending a huge amount of spam mails in a limited space of time.[28] As a result, they have been used by cybercriminals to orchestrate criminal activities such as sending spam emails, performing distributed

FIGURE 1 Structure of a botnet



denial of service attacks (DDoS), providing an attacker with full access to an infected system and keystroke logging as is shown in Figure 1.

The process begins at phase 1 (see Figure 1), in which the botnets infect a machine connected to the Internet through methods including email or drive-by downloads. Once the botnet executes on the infected machine, it connects to the command and control server and thus constituting phase 2 of the process. Here, the cybercriminal or "Botmaster" gains control of the botnet remotely and can start passing instructions to the command and control server through this remote control. The botmaster can then use these botnets to perform a variety of malicious attacks such as infecting other computers thereby increasing the number of botnets (phases 3 & 4). The botmaster can also use the botnets to execute distributed denial of service (DDoS) attacks, distribute spam, or steal confidential data such as credit card details and passwords. The group of botnets or "zombies" all link back to a command and control server where they receive instructions from the attacker. Thus, the botnets' major function is to infect computers. It is worth noting that, the use of botnets in this work stems from the need to collect digital information from the different environment for purposes of forensic analysis. The authors, also note that there may exist some legal ramifications, however, more on this has been highlighted in the subsequent sections to follow.

2.4 | OpenStack architecture

OpenStack is an open source cloud operating system for creating and managing cloud infrastructures. It is managed by the OpenStack Foundation. It started in 2010 through a collaboration between NASA and Rackspace Hosting.[29] It provides a cloud computing environment where virtual servers and cloud resources are made available to the clients. OpenStack operates on both private and public clouds.

OpenStack's cloud computing resources (Figure 2) are deployed as Infrastructure as a Service (IaaS). OpenStack consists of three main components namely:

a **Nova**—This is also known as Openstack Compute infrastructure. It is responsible for the management of cloud instances within OpenStack. It has similarities to Amazon Elastic Compute Cloud (EC2) and Rackspace Cloud servers Nova is used in the management of networks of cloud instances within OpenStack. It provides an administrative interface for the management of cloud instances, networks as well as access control.[29-31]
b **Swift**—Also known OpenStack Object Storage Infrastructure. It provides virtual object containers with a huge amount of storage space essential to store and retrieve data to be used by cloud instances. Swift is designed for storage of large volumes of data for a prolonged time.[29-31]
c **Glance**—is also known as OpenStack Image Service Infrastructure. Glance is used for providing the compute image repository. All cloud instances are launched from glance images.[29-31]

FIGURE 2 OpenStack architecture

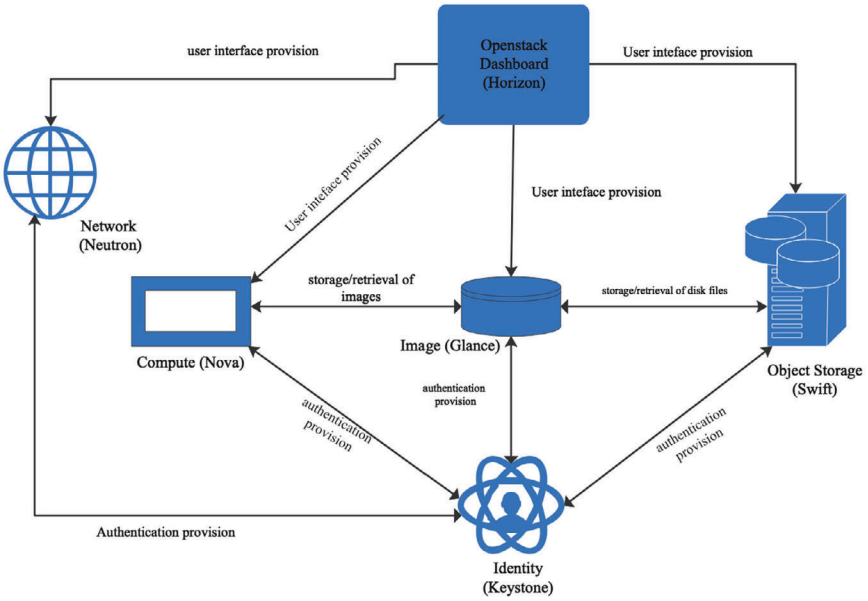


FIGURE 3 Digital investigation process classes[18]

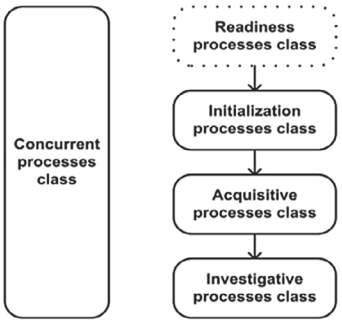


Figure 2 shows the OpenStack Architecture. The OpenStack Dashboard provides a user interface to control the OpenStack components namely Nova, Glance and Swift. The dashboard is explained in detail, in the following section. The three main components discussed above are shown as compute, image and object components. The other OpenStack component, named identity in Figure 5.1 is responsible for user authorization and authentication by OpenStack. It is also known as Keystone.

OpenStack is designed in a way to give cloud administrators a platform to deploy IaaS infrastructure and supply tools for creating and managing cloud instances on top of existing cloud infrastructure. This research study makes use of OpenStack cloud operating system to provide a cloud environment to test the proposed prototype to harvest digital information in OpenStack in order to attain DFR.

2.5 | ISO/IEC 27043:2015 process groups

ISO/IEC 27043, is an international standard that entails, "information technology, security techniques, and incident investigation principles and process."[18] Also, "ISO/IEC 27043:2015 provides guidelines based on idealized models for common incident investigation processes across various incident investigation scenarios involving digital evidence."[18] These set of guidelines provided by the ISO/IEC 27043 can then be used by DFIs to attain DFR in the cloud. The ISO/IEC27043 consists of digital investigation processes divided into five classes and these are namely the "Readiness Processes, Initialization Processes, Acquisitive Processes, Investigative Processes, and Concurrent Processes" Figure 3 diagrammatically describes the relationship between these processes.

Infer from Figure 3 that the digital investigation processes are multi-layered. They begin with the readiness process class and end with the investigative process class. The concurrent processes are unique in that they run throughout all the

four process classes. According to the ISO/IEC 27043 standard, the concurrent class consists of the following processes, "managing information flow, documentation, obtaining authorization, preserving the chain of custody, and preserving digital evidence." These processes are important for DFIs to perform at each of the processes to preserve digital evidence. The readiness process classes at a high level are examined further since this research only deals with DFR.

The readiness process class is a "class of processes dealing with setting up an organization in such a way that, in the case that a digital investigation is required, such organization possesses the ability to maximize its potential to use digital evidence whilst minimizing the time and costs of an investigation."[18] Thus, the goal of any DFR process is "to maximize the potential use of digital evidence whilst minimizing the time and costs of conducting a digital forensic investigation."[8]

3 | DFR TECHNIQUES IN OPERATIONAL CLOUD

This section introduces the technique that has been used to plan and prepare for incidents as part of forensic readiness as mentioned in ISO/IEC 27043. The authors utilize botnets, which is presented as a forensic agent making use of some of the "botnet" characteristics to harvest digital information in an operational cloud environment.

In a traditional forensic investigation, the forensic image is created before the digital forensic investigation takes place. This is possible since the DFI has access to the device that needs to be imaged. This becomes a challenge in the case of a cloud environment because the data centers and cloud infrastructures may be sitting in different areas.[21] Also, there are no clear guidelines for conducting DFR in the cloud.[32] Therefore, the lack of standardized guidelines for conducting DFR in the cloud necessitates the use of the prototype as a proof of concept on how a proactive DFR approach can be implemented in an operational cloud environment.

3.1 | High-level representation

This approach provides a technique of proactive gathering of digital evidence in an operational cloud environment as per the guidelines of ISO/IEC 27043. The chosen cloud environment is OpenStack, which is an open-source cloud operating system. The prototype proactively collects digital information on cloud instances hosted on the cloud and stores the collected digital information in a forensic sound database. The prototype creates a cryptographic hash of the collected information and, in that way, maintains the integrity of the collected data. It operates in a way similar to that of how a botnet operates; however, in this case, the use is not for malicious intents but with a positive connotation. Botnets were chosen in this research due to the attributes they possess and in particular their stealthiness, resilience, and capability of gathering data.[33] It is worth underscoring here that the prototype in question is represented as a botnet possessing characteristics that enable the collection of digital information in an operational cloud environment for DFR purposes. The following section provides an in-depth description of the prototype and the way it operates.

3.1.1 | Prototype flow processes

The prototype follows the following processes that are (labeled 1 to 5) shown in Figure 4. The processes are explained in detail in the following subsections.

- **Deployment (1)**

  OpenStack deploys the prototype to the cloud instances through file transfer protocol. The cloud instances are hosted in an operational cloud environment. Once the prototype has been deployed to the specific cloud instance, the command and control server can then be used to execute the prototype. Through this, the prototype is executed in an operational cloud instance, once the deployment process is complete,[26] term this the "infection" process to signify the stage that the agent-based solution (ABS) executes to collect digital information. The command and control server is responsible for executing the prototype.
- **Forensic evidence collection (2)**

  This is the process where the prototype starts to acquire digital data from the cloud instance. The digital data collected by the prototype includes CPU usage, RAM usage, and keystrokes on the keyboard.

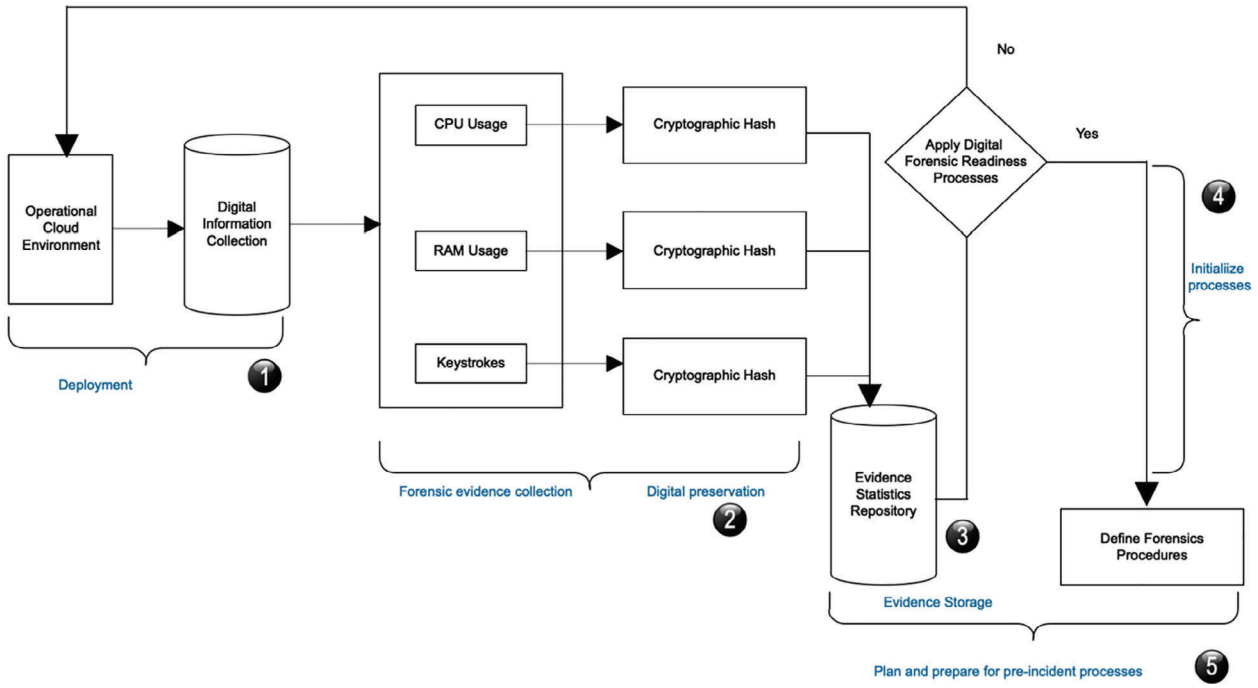


FIGURE 4 Prototype flow processes

- **Potential digital evidence preservation (2)**
  The prototype hashes the collected digital information in this process. Hashing is a preservation technique mention in the ISO/IEC27043 standard. Thus, the hashing here ensures the integrity of the collected information. Once integrity is maintained, the collected information can then be used in conducting digital forensic investigations.
- **Evidence statistics repository (3)**
  The collected evidence is stored in a forensic database in this process. A MySQL database is used as it can store digital data. A DFI can access what was stored on the database later and use the information to perform digital forensic investigations.
- **Process initialization (4)**
  At this stage forensic processes are initialized and according to ISO/IEC 27043, this process happens after incident identification
- **Plan and prepare for pre-incident processes (5)**
  This process addresses the need for digital forensic readiness after achieving digital forensic readiness. The process confirms to the guidelines of ISO/IEC 27043.

3.1.2 | Implementation in OpenStack

OpenStack is an open-source cloud operating system that creates and manages cloud infrastructures.[34] The system, which is managed by the OpenStack Foundation, started in 2010 through a collaboration between NASA and Rackspace. It provides a cloud computing environment where virtual servers and cloud resources are made available to the clients.

The cloud instances considered in this study are run on the OpenStack infrastructure where they firstly target the VM. The cloud instances can be launched from the available OpenStack images. This research study made use of the Windows Server 2012 image to spawn cloud instances within OpenStack. The prototype was deployed to these cloud instances to test it in a cloud environment, in this case, OpenStack. Figure 5 shows the three (3) cloud instances that we created to run in OpenStack.

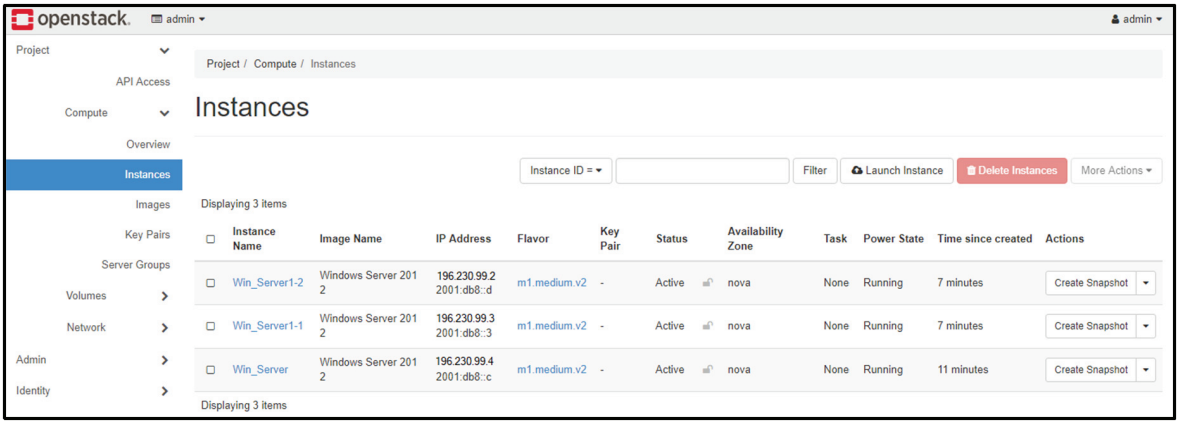


FIGURE 5 Cloud instances in OpenStack

These instances were spawned from the Windows Server 2012 cloud image. The instance name column provides the name for each instance (*Win_Server*, *Win_Server1-1*, and *Win_Server1-2*). Each cloud instance is given a specific IP address by the OpenStack Network management component called Neutron. The cloud instances shown in Figure 5.1 above have a "running" state, which means that they are operating without any problems.

Various activities can be performed on the cloud instance. For example, you can access the Internet, install applications, copy and move folders and files. The completion of the setting-up of the cloud instances enables the performing of operations such as the deployment and testing of applications on the cloud. The next section discusses how the prototype was deployed into the cloud instances and the various tests performed.

3.1.3 | Execution in cloud instance

The experimental set up to deploy the executable to cloud instances followed the setup presented by[26,27] in deploying the prototype to virtual machines in order to collect digital forensic information. Figure 5 shows the experimental set up used by both researchers. Making use of the set up mentioned in Figure 5 the prototype is executed through the command and control server (label 1). Label 2 depicts the transfer of data between the command and control server and the cloud instances. The prototype collects PDE and dispatches it to the command and control server where it is kept in a forensic database.

It is worth noting that the prototype does not modify the functions of the Openstack architecture described in the background section. The prototype is capable of connecting through the Openstack modules. The collected digital data passes through the OpenStack network management component, Neutron. Neutron provides the networking services for the cloud instances hosted on Openstack, this has been shown in Figure 6 and an explanation follows for the steps labeled 1 to 6.

- *Step 1*: The forensic tool collects digital information within the cloud instance on the Nova network. Each cloud instance has a virtual Network interface Card (NIC) which handles network packets. The collected digital information collected by DFECS gets sent through the NIC.
- *Step 2*: The collected digital data get sent to the virtual NIC of the compute host.
- *Step 3*: The collected digital data get transferred to the network bridge of the compute node. The bridge is used to apply the inbound/outbound firewall rules.
- *Step 4*: The collected digital data get sent to the main NIC of the compute node.
- *Step 5*: Once the collected digital data is on the main NIC, it gets transferred to the compute node's default gateway. But before reaching the gateway, the data passes through the step 2 switch. The layer 2 switch was configured to accept inbound/outbound network traffic.

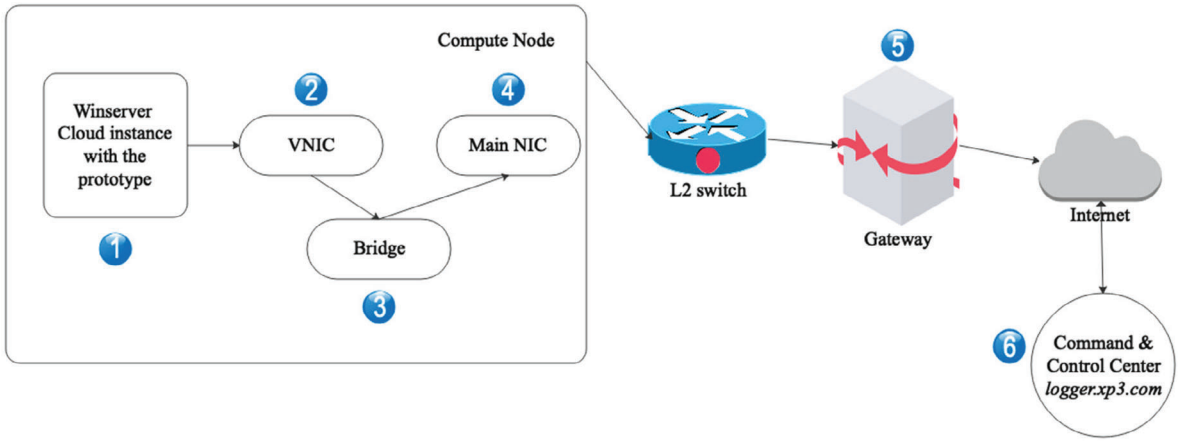


FIGURE 6 Steps of gathering digital information in the cloud instance

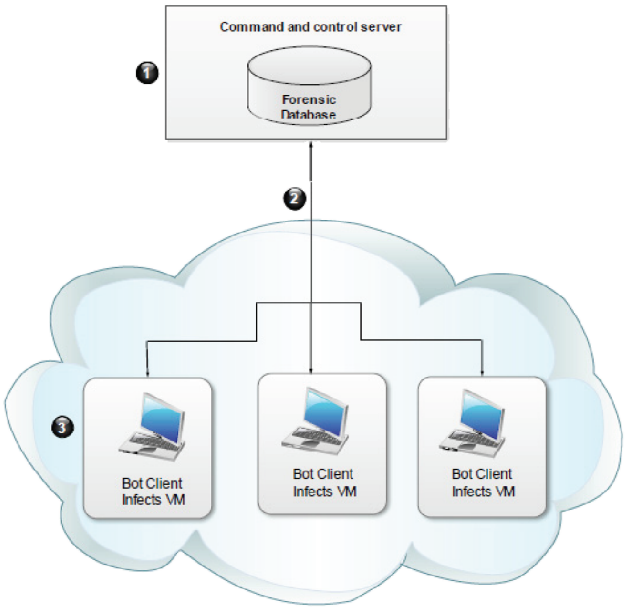


FIGURE 7 Experimental setup of the prototype[22]

- *Step 6*: The collected digital data is transferred to the external internet and arrives at the command and control center hosted at the logger.xp3.com site. A PHP function is responsible for translating the raw data into the captured digital information. This information is then stored in MySQL tables.

The C&C server shown in Figure 7 forms part of the prototype. The VMs (label 3) is the cloud instances setup in OpenStack. It is worth noting here that the use of OpenStack simulates an operational cloud environment to test the prototype.

It is important to note that because of the standardized requirements on readiness the agent is deployed in stealth mode-this is one of the requirements that it needs to achieve forensic objectives. This indicates that it operates behind the scenes such that even a cloud user making use of the cloud would not be disturbed. Figure 6 shows the execution process when the stealth mode is disabled to show how the prototype operates. Once the forensic agent executes, it starts collecting digital information namely CPU usage, RAM usage, and the keystrokes typed on the keyboard. These get captured at a 2-second interval which is the secondary injection after the initial infection by the botnet to the C&C server.

Once captured, the "chunk" of captured raw data is hashed and is sent to the command and control server through a POST method to HTTP host logger.xp3.com (see Figure 8) where the command and control server is hosted.

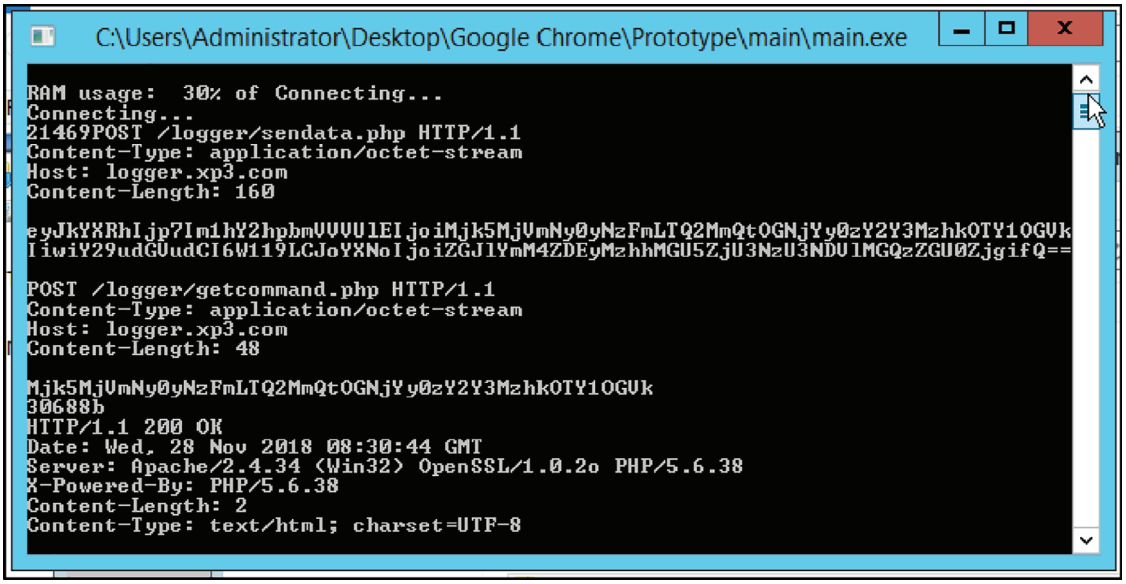


FIGURE 8 Execution in the cloud instance

3.2 | Digital evidence collection, preservation, and storage

The main aim of this prototype is basically to 'infect' the virtual instances in the could with a positive connotation in in what in the long run contributes to forensic preparedness. In essence, after deploying the forensic tool, the following are achieved: The tool monitors the CPU usage, RAM usage and then concurrently collects keystrokes in a forensic readiness approach. This is useful, owing to the fact that, a pre-analysis of the accumulated evidence is important during incident response procedure as is mentioned in ISO/IEC 27043. Figure 7 shows the collected digital information relayed from the command and control server.

The name column in Figure 9 describes the type of digital information collected by the prototype. These are namely CPU, RAM, and keystrokes. Once captured, the "chunk" of captured raw data is hashed and is sent to the command and control server through a PHP POST method to HTTP host logger.xp3.com (see Figure 8) where the command and control server is hosted. As part secure potential digital evidence acquisition strategies, the ISO/IEC suggests that it is important to hash the collected evidence for integrity purposes also as a sound process for handling digital evidence. This can only be achieved by way of making verifiable images and using hash functions. A PHP function is responsible for translating the raw data into the captured digital information. This information is stored in MySQL tables. The captured hashes can be viewed from the command and control server as shown in Figure 10. The "rawData" column shows the captured digital information, at a particular time interval. Each of the chunks of digital information captured gets hashed and the hash is recorded as shown in the hash column.

The MySQL database also records the username of the particular cloud user logged in at the time the information was captured. The "total" column shows the value captured. An evaluation of the compliance of the developed process in line with the ISO/IEC 27043:2015 standard is presented in the next section. This considers, particularly, the planning processes group of the readiness processes group of the standardization.

3.3 | Revisiting the case scenario

We revisit the scenario (from Section 1) by exploring the impact when the security goals are compromised, however, it should be noted that the scenario's aim is more focused on achieving DFR based on ISO/IEC guidelines. Based on the scenario highlighted in Section 1, the observation we made after a user was able to access the FTP site and the prohibited social media is as follows:

The user accessed the ftp site: ftp://ftp.mycompany.com, entered the username: ***peter*** and password: ***P@ssworD***, which are the managers' credentials, and pressed enter to gain access to the site. After a few minutes, the user also accessed

	id	name	username	value	total	description	date	logEntryId
Edit Copy Delete	1811	Keyboard	Cloud User1	o	0	Keystroke	1543397424504	16
Edit Copy Delete	1044	Keyboard	Cloud User1	m	0	Keystroke	1543396567017	10
Edit Copy Delete	1300	CPU	Cloud User1	50	100	CPU Load	1543396590365	12
Edit Copy Delete	1812	Keyboard	Cloud User1	g	0	Keystroke	1543397424516	16
Edit Copy Delete	1045	Keyboard	Cloud User1	a	0	Keystroke	1543396567256	10
Edit Copy Delete	1301	RAM	Cloud User1	41	2146930688	Ram usage	1543396590558	12
Edit Copy Delete	1813	Keyboard	Cloud User1	l	0	Keystroke	1543397424709	16
Edit Copy Delete	1046	CPU	Cloud User1	50	100	CPU Load	1543396567279	10
Edit Copy Delete	1302	CPU	Cloud User1	52	100	CPU Load	1543396591371	12
Edit Copy Delete	1814	Keyboard	Cloud User1	e	0	Keystroke	1543397424806	16
Edit Copy Delete	1047	Keyboard	Cloud User1	i	0	Keystroke	1543396567401	10
Edit Copy Delete	1303	RAM	Cloud User1	41	2146930688	Ram usage	1543396591561	12
Edit Copy Delete	1815	CPU	Cloud User1	50	100	CPU Load	1543397425222	16
Edit Copy Delete	1048	RAM	Cloud User1	41	2146930688	Ram usage	1543396567477	10
Edit Copy Delete	1304	CPU	Cloud User1	50	100	CPU Load	1543396592374	12
Edit Copy Delete	1816	RAM	Cloud User1	41	2146930688	Ram usage	1543397425415	16
Edit Copy Delete	1049	Keyboard	Cloud User1	l	0	Keystroke	1543396567648	10
Edit Copy Delete	1305	RAM	Cloud User1	41	2146930688	Ram usage	1543396592564	12
Edit Copy Delete	1817	CPU	Cloud User1	50	100	CPU Load	1543397426225	16
Edit Copy Delete	1050	Keyboard	Cloud User1	.	0	Keystroke	1543396568056	10
Edit Copy Delete	1306	Keyboard	Cloud User1	[Shift]	0	Keystroke	1543396592593	12
Edit Copy Delete	1818	RAM	Cloud User1	41	2146930688	Ram usage	1543397426426	16
Edit Copy Delete	1051	CPU	Cloud User1	51	100	CPU Load	1543396568282	10
Edit Copy Delete	1307	Keyboard	Cloud User1	h	0	Keystroke	1543396592907	12
Edit Copy Delete	1819	CPU	Cloud User1	52	100	CPU Load	1543397427229	16

FIGURE 9 Collected digital information

the social networking site facebook.com as shown in Figure 11. This information can prove to be vital in attempts at proving whether a cloud user accessed confidential company information without authorization.

The fact that the user used his/her manager's details to login onto the company's FTP site is proof that the user gained unauthorized access. The user also accessed Facebook, which flouts the company regulations that employees should not access social media sites during working hours (8 AM to 4 PM). The time that the user accessed Facebook can be identified by checking the database from the C&C server to see the timestamps for the captured keystrokes. Figure 12 shows the captured keystrokes as observed from the command and control center database.

Figure 12 shows the results of the captured keystrokes from the cloud user 1. The name column describes the details of the item captured, which is the keyboard. The username column identifies the cloud user while the value column shows the keystrokes captured by the prototype. The observation from the figure is that the total value the user entered is www.facebook.com. The date column shows the timestamp recorded for each keystroke captured. Timestamp is in milliseconds and its translation to a particular date and time. For example, the time when the "**f**" keystroke was captured with timestamp 1 555 395 429 237, would be: Tuesday 16 April, 2019 08:17:09 GMT + 02:00.

The time provides evidence that the user accessed the social media site during working hours. This scenario shows how the prototype can be used to assist forensic investigators in finding out who accessed confidential company information. In addition, the prototype can be used by companies to monitor the sites visited by employees during office hours in order to guard against unproductivity and inactivity during office hours.

The second part of the scenario shows instances where the user downloads malware unknowingly and the impact that this malware has is interfering with the CPU and RAM processes and the deployed prototype could easily monitor this in a forensic readiness approach as is shown in Figure 13 and Figure 14 respectively.

The observation from the RAM usage graph is that there was a sharp increase in the RAM usage at 09:40:54 time stamp (one with arrow). An analysis of the CPU usage graph confirms a corresponding increase in the CPU usage at 09:40:53

rawData	hash	timeReceived	ip
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	93711a99cc4ac1ccdbdec85065b8a124	2018-11-28 13:12:21	196.230.99.3
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	93de39caab9aee79cf8da55a473812e2	2018-11-28 12:37:31	196.230.99.2
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	cfc017a31f967c2b4605a8171f91f127	2018-11-28 13:38:37	196.230.99.4
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	f0100a6577bd301e61af728d35cfac89	2018-11-28 12:41:05	196.230.99.2
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	8c6754070926157c42ca87c538a0c412	2018-11-28 13:26:45	196.230.99.3
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	3bd1b347d8a91b63cbd34da8fbf4fbc7	2018-11-28 06:30:36	196.230.99.2
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	9870c782d3aa646e8920b75fecec80f9	2018-11-28 13:11:23	196.230.99.4
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	a9787097ca7710cbe5f8998c417420d1	2018-11-28 07:11:32	196.230.99.2
eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	58b5bb97edd9894f97f5b7c1da3aeed3	2018-11-28 13:11:43	196.230.99.3

FIGURE 10 Raw hashes

FIGURE 11 Captured user keystrokes

Keyboard

ftp[Shift]://ftp.mycompany.competer[Shift]p[Shift]2sswor[Shift][Shift][Shift]d[Enter]www.facebook.com[Enter]

(one with arrow). This information can assist digital forensic investigators to narrow down the timeframe of malware execution within the cloud instance. Digital forensic investigators can easily focus on the time preceding the increase in the CPU and RAM usage, and the time after the increase.

4 | ISO/IEC 27043: RECOMMENDATIONS/GUIDELINES ON INCIDENTS

As indicated in the previous section, the developed and implemented cloud-based operation monitoring readiness model is benchmarked to the readiness phase of the ISO/IEC 27043. The readiness processes groups of the standard comprise three functional concurrent processes groups which include the planning, implementation, and assessment processes group. In terms of description, the planning processes group focuses on planning-related activities; the implementation processes group, on the other hand, deals with implementation-related consideration concerning the investigation. Lastly, the assessment processes group relates to attempts and approaches that can be used to assess the overall implemented processes. In this section, this study attempts to evaluate the degree of compliance of the developed model with the planning processes group of the standard. This evaluation process is summarized in Table 1.

As clarified in Table 1, the implemented model aligns with the ISO/IEC 27043/2015 standard in the area of forensic readiness. However, three other components of this phase are not considered. These include the planning pre-incident analysis of data representing potential digital evidence process, planning incident detection process, and defining system architecture process. These processes are not considered in this study as involve the identification of specific PDE which can be subjective and context-specific. However, from the result shown in Figures 5-14, the implemented model prototype demonstrated that several instance-types can be collected in a forensically sound manner. A filtration technique can then be applied to the collection process to extract relevant data.

5 | DISCUSSIONS

The continued growth of cloud computing technologies witnessed over the years has led to cyber criminals making use of cloud computing as an environment to launch malicious attacks, and this necessitates the need for CSPs to implement proactive DFR processes to combat such security threats. These DFR processes seek to provide ways to collect digital information, in a cloud platform, which can be utilized in a digital forensic investigation. As a result, this research presents a

	id	name	username	value	total	description	date	logEntryId
Edit Copy Delete	1971	Keyboard	Cloud User 1	w	0	Keystroke	1555395427318	18
Edit Copy Delete	1973	Keyboard	Cloud User 1	w	0	Keystroke	1555395427535	18
Edit Copy Delete	1975	Keyboard	Cloud User 1	w	0	Keystroke	1555395427749	18
Edit Copy Delete	1978	Keyboard	Cloud User 1	.	0	Keystroke	1555395428854	18
Edit Copy Delete	1979	Keyboard	Cloud User 1	f	0	Keystroke	1555395429237	18
Edit Copy Delete	1982	Keyboard	Cloud User 1	a	0	Keystroke	1555395429598	18
Edit Copy Delete	1983	Keyboard	Cloud User 1	c	0	Keystroke	1555395429901	18
Edit Copy Delete	1984	Keyboard	Cloud User 1	e	0	Keystroke	1555395430141	18
Edit Copy Delete	1986	Keyboard	Cloud User 1	b	0	Keystroke	1555395430573	18
Edit Copy Delete	1988	Keyboard	Cloud User 1	o	0	Keystroke	1555395430813	18
Edit Copy Delete	1989	Keyboard	Cloud User 1	o	0	Keystroke	1555395430998	18
Edit Copy Delete	1990	Keyboard	Cloud User 1	k	0	Keystroke	1555395431245	18
Edit Copy Delete	1995	Keyboard	Cloud User 1	.	0	Keystroke	1555395432693	18
Edit Copy Delete	1996	Keyboard	Cloud User 1	c	0	Keystroke	1555395432949	18
Edit Copy Delete	1997	Keyboard	Cloud User 1	o	0	Keystroke	1555395433166	18
Edit Copy Delete	1998	Keyboard	Cloud User 1	m	0	Keystroke	1555395433430	18

FIGURE 12 User captured keystrokes as seen from the database

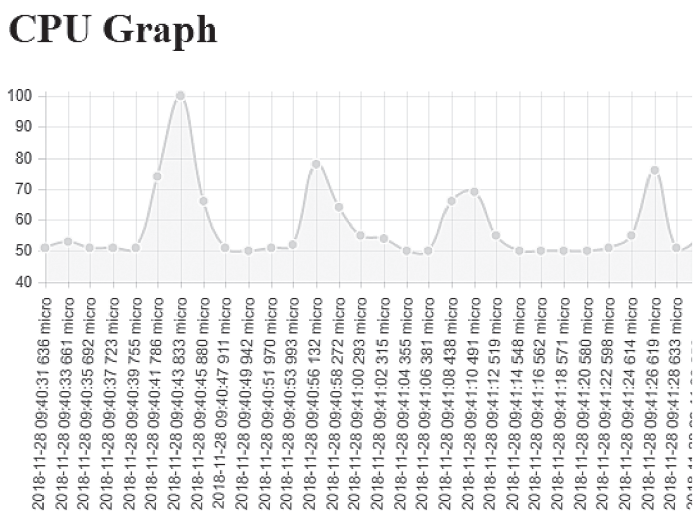


FIGURE 13 Variations of CPU usage as a result of malware

way of attaining DFR in an operational cloud environment through the use of the prototype, which is a modified structure of a botnet that is used as a forensic agent in a non-malicious format. The prototype, was tested in a simulated environment.[26] Hence, this study tested a modified version of the prototype in an operational cloud environment to show that DFR can be attained in an operational cloud environment.

The experiment performed in this paper sought to test the prototype developed by[5,6,17,26] in an operational cloud environment to prove the attainability of DFR in an operational cloud environment. OpenStack provided an operational cloud environment to deploy the prototype based on the scenario that have been discussed in Section 3. The conducted experiments successfully showed that the prototype can be implemented in an operational cloud environment thereby proving the attainability of DFR in the cloud. The observation is that the prototype deployed to three cloud instances was capable of harvesting digital information in each of the cloud instances and forensically storing the digital data in a forensic database. The experiments showed that it is possible to deploy the prototype in three cloud instances. Therefore,

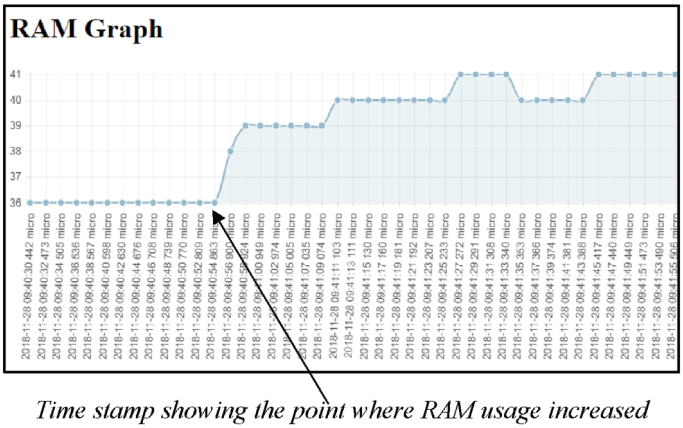


FIGURE 14 Variations of RAM usage as a result of malware

TABLE 1 Degree of compliance with the ISO/IEC 27043

Planning processes group	Evaluation of compliance
Scenario definition	Cloud environment, particularly, instance identification and definition constitute the description of the scenario definition. This study addresses the defining and locating a given instance within the boundary of scenario definition.
Identification of potential digital evidence sources process	The implemented model was able to identify key pieces of potential digital evidences (PDE) as shown in Figure 7. This phase also constitutes the execution and harvesting phases shown in Figure 3.
Planning pre-incident gathering process	The deployment phase as shown in Figure 3 covers this phase of the standardization. More importantly, the implementation result shown in Figure 7 illustrated the potential of the approach presented in this study to gather pre-incident data.
Storage and handling of data representing potential digital evidence process	As shown in Figure 3, the preservation of the PDE aligns fitly with the storage and handling of data in the ISO/IEC 27043/2015 standard and the implemented approach satisfies the requirement of the standard.
Concurrent Processes	While evidence collection activities are being achieved, the concurrent processes may happen concurrently, by mainly focusing on evidence management, chain of custody, digital preservation and obtaining authorization for executing digital investigation processes.

the prototype can be used by organizations that use cloud computing platforms to provide a DFR environment for their cloud computing platforms.

While the authors of this paper note that security monitoring is aimed at addressing the concerns on the protection the system from attacks, it is also important to highlight the need for forensic preparedness, by way of identifying the potential risks by formulating a reliable forensic model that can be leveraged during pre and post-investigation processes as is shown in Figure 15.

From Figure 15, we show risk identification, forensic model formulation and suitable standard identification as an input process. Next, the actual forensic model, its application as a method that leads to the output, which shows the actual guidelines for ISO/IEC 27043 international standard, towards risk management based on security monitoring techniques.

Researchers in[5,6,17,26] note that their prototype complies with the digital investigative readiness processes stipulated in the ISO/IEC 27043 standard. The experiments sought to ensure that these processes were followed throughout the

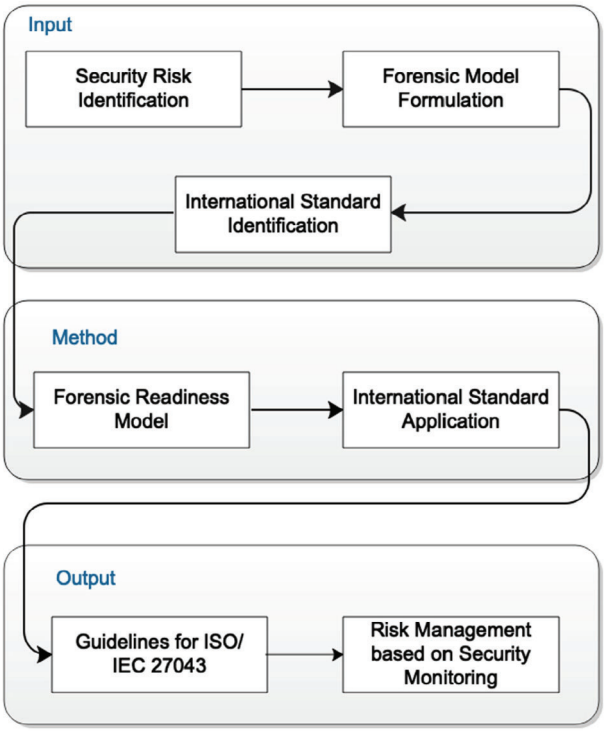


FIGURE 15 Approach towards international standard application

experimentation. Following these processes is essential to make sure that the acquired digital data is admissible in a court of law. Besides, the functionality of the cloud architecture was not changed and this had the advantage of reducing the cost. Consequently, a comparative study of different researches shows other relative works,[35-42] that have addressed the need of incorporating standardization/international standard as a way of addressing digital forensics with respect to standardization as is shown in Table 2.

One of DFR's main advantage is that it decreases the cost of conducting a digital forensic investigation.[43] Now imagine if an organization has about 100 cloud instances running on OpenStack without DFR put in place. It would mean that the DFI would have to forensically image all of the 100 cloud instances and look at the images one by one. This will increase the cost and the time to conduct the forensic investigation. However, in a case where the organization has deployed a DFR, the use of such a prototype becomes seamless. The DFI will be able to isolate specific cloud instances where security incidences were identified and focus on those cloud instances alone.

Generally, digital forensics has the objective of identifying cyber-criminals from a digital environment if a potential security incident is identified. However, the extracted digital information must hold some standards for purposes of admissibility. Generally, the recommendations of ISO/IEC 27043 give general guidelines that are based on idealized processes for digital investigation approaches, data acquisition, and aspects of information security. In this study, ISO/IEC 27043 guidelines have been used as a baseline for achieving readiness in the cloud as was highlighted in Table 1. While research in,[25] has taken steps to highlight different aspects of integration of forensic processes in the cloud as a service through CFRaaS, the authors of this paper emphasized how it reduces the time and the cost that will be incurred in conducting the forensic investigation.[43] In particular, DFR needs to adapt the guidelines that are highlighted in the standard, and this is because the data acquired from the digital environment may have higher chances to qualify as admissible digital evidence during litigation. We also stress the fact that while these processes are conducted, the confidentiality, integrity, and privacy of data and individual is upheld based on the specific cyber and forensic laws of a given jurisdiction.

The authors also posit that, while ISO/IEC guidelines may not be application-specific during the cyber forensic investigation process, it is still important to note that, lack of these processes may easily lead to disregarding potential evidence.[44,45] Notably, important objectives that we present in this paper are as follows: Saving costs by achieving forensic preparedness, forensically sound digital evidence is collected thus the sanctity of this evidence is preserved, the integrity of the collected digital data is also maintained thus increased the chances of admissibility.

TABLE 2 Need for incorporating standardization

Literature	Key aspects on the need for standardization
35,37	Study focuses on the need for standardized forensic processes in computer forensic in general, owing to the maturity of the forensic discipline. Lack of standardization has been identified as a core problem due to difficulties in interpreting and mandating forensic techniques. Also lack of data sets that could be used for research purposes is an issue in this context
37	Focus is mainly on the need for standardizing proactive digital forensics techniques which could culminate in realizing a unified standard that could help in proactive forensic initiatives
38	The need for standardizing a digital forensic laboratory from a technical and managerial perspective so that forensic reports presented by forensic laboratories are accepted by courts
39	Studies mainly focus on standardizing file recovery aspects and authentication approaches, where during cyber investigation, a formalized vocabulary and forensic-based techniques can be used to support validation based on ISO/IEC 27041 and ISO 17025, also supported by European Network of Forensic Science Institutes (ENFSI)
40	Shows the importance of standardizing how forensic reports are generated by utilizing (ISO/IEC 27043) international standard-which can facilitate future automation and text analytics and sharing of reports, including forensic intelligence.
40	Explores techniques of analyzing scenarios and predicting evaluation and monitoring forensic techniques using standardized data based on forensic readiness
42	Research shows how ISO/IEC 17025 has taken competencies on the testing of forensic techniques and has been adapted as a suitable approach for accrediting digital forensic laboratories, which in turn could be useful in standardization approaches.

6 | CONCLUSIONS AND FUTURE WORK

Cloud forensic readiness is the science of forensic planning and preparation for any cyber or digital environment. This involves the extraction of incidental data that may be used to create a forensic hypothesis that can prove a fact if a potential security incident is detected. This paper uses the guidelines mentioned in the ISO/IEC 27043 international standard to conduct digital forensic readiness in the operational cloud. The experiments that have been conducted have proved that it is possible to achieve this and more importantly this could easily be extended to different cloud models. While this research focused on using forensic agents that have the functionality of botnets, future work aims at improving the approaches that have been proposed to a more connected IoT environment.

ORCID

Victor R. Kebande https://orcid.org/0000-0003-4071-4596

REFERENCES

1. De Marco L, Ferrucci F, Kechadi T. Reference architecture for a cloud forensic readiness system. *EAI Endors Trans Secur Saf*. 2014;1(1):1-9.
2. Marston S, Li Z, Bandyopadhyay S, Zhang J, Ghalsasi A. Cloud computing—the business perspective. *Decis Supp Syst*. 2011;51(1):176-189.
3. Popović K, Hocenski Ž. Cloud computing security issues and challenges. *The 33rd International Convention MIPRO*. Opatija, Croatia: IEEE; 2015:344-349.

4. Sen J. Security and privacy issues in cloud computing. *Cloud Technology: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global; 2015:1585-1630.
5. Kebande VR, Venter HS. Novel digital forensic readiness technique in the cloud environment. *Aust J Forensic Sci*. 2018;50(5):552-591.
6. Kebande VR, Venter HS. On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. *Aust J Forensic Sci*. 2018;50(2):209-238.
7. DFRWS, 2001. A road map for digital forensics research-report from the first *Digital Forensics Research Workshop* (DFRWS), Utica, New York.
8. Tan J. *Forensic Readiness*. Cambridge, MA: Stake; 2001:1-23.
9. Adeyemi IR, Razak SA, Azhan NAN. A review of current research in network forensic analysis. *Int J Digit Crime Forensics 5*. 2013;1:1-26. https://doi.org/10.4018/jdcf.2013010101.
10. Kebande VR, Venter HS. Obfuscating a cloud-based botnet towards digital forensic readiness. *ICCWS 2015 – The Proceedings of the 10th International Conference on Cyber Warfare and Security*. England: ACI publishers; 2015:434.
11. Reith M, Carr C, Gunsch G. An examination of digital forensic models. *Int J Dig Evid*. 2002;1(3):1-12.
12. Carrier B, Spafford EH, 2004. An event-based digital forensic investigation framework. In *Digital Forensic Research Workshop* (pp. 11-13).
13. Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. *Dig Investig*. 2005;2(2):147-167.
14. Agarwal A, Gupta M, Gupta S, Gupta SC. Systematic digital forensic investigation model. *Int J Comput Sci Secur (IJCSS)*. 2011;5(1):118-131.
15. Ikuesan AR, Venter HS, 2018. Digital forensic readiness framework based on behavioral-biometrics for user attribution. In *2017 IEEE Conference on Applications, Information and Network Security, AINS*, 2017. https://doi.org/10.1109/AINS.2017.8270424
16. Valjarevic A, Venter HS. Harmonised digital forensic investigation process model. *2012 Information Security for South Africa*. USA: IEEE; 2012:1-10.
17. Kebande VR, Venter HS. A cloud forensic readiness model using a botnet as a service. *The International Conference Digital Forensic and Security*. Czech Republic: Society of Digital and Wireless Network (SDWIC); 2014.
18. ISO/IEC 27043, 2015. Information technology – Security techniques – Incident investigation principles and processes. https://www.iso.org/standard/44407.html. Accessed December 10, 2018.
19. Mell, P., & Grance, T. *The NIST Definition of Cloud Computing*. Gaithersburg, MD: National Computer Security Division, Information Technology Laboratory; 2011.
20. Casey E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Waltham, MA: Elsevier; 2011.
21. Barbara JJ. Cloud computing: another digital forensic challenge. *Digital Forensic Investigator News*. South San Francisco, CA: Forensic-Mag.com. Forensics Magazine; 2009.
22. Alenezi A, Hussein RK, Walters RJ, Wills GB. A framework for cloud forensic readiness in organizations. In *2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*; 2017, pp. 199-204.
23. Kebande VR, Venter HS. Requirements for achieving digital forensic readiness in the cloud environment using an NBM solution. In *ICCWS 2016 11th International Conference on Cyber Warfare and Security*; 2016. pp. 399-406.
24. Kebande VR, Venter HS. CFRaaS: architectural design of a cloud forensic readiness as-a-service model using NMB solution as a forensic agent. *Afr J Sci Technol Innov Dev*. 2019;11(6):749-769. https://doi.org/10.1080/20421338.2019.1585675.
25. Kebande VR, Karie NM, Ikuesan RA, Venter HS. Ontology-driven perspective of CFRaaS. *Wiley Interdiscip Rev: Forensic Sci*. 2020;2(5): e1372.
26. Kebande VR, Venter HS. Architectural design of a cloud forensic readiness as a service (CFRaaS) system using an NMB solution as a forensic agent. *Int J Inf Comput Secur*. 2019;11(6):749–769.
27. Kebande VR, Venter HS. A comparative analysis of digital forensic readiness models using CFRaaS as a baseline. *Wiley Interdiscip Rev: Forensic Sci*. 2019;1(6):e1350.
28. Xie Y, Yu F, Achan K, Panigrahy R, Hulten G, Osipkov I. Spamming botnets: signatures and characteristics. *ACM SIGCOMM Comput Commun Rev*. 2008;38(4):171-182.
29. Yadav S. Comparative study on open source software for cloud computing platform: eucalyptus, OpenStack and OpenNebula. *Res Invent: Int J Eng Sci*. 2013;3(10):51-54.
30. Sefraoui O, Aissaoui M, Eleuldj M. OpenStack: toward an open-source solution for cloud computing. *Int J Comput Appl*. 2012;55:38-42.
31. Kurup LD, Chandawalla C, Parekh Z, Sampat K. Comparative study of eucalyptus, OpenStack and Nimbus. *Int J Soft Comput Eng (IJSCE)*. 2015;4(6):23-27.
32. Dykstra J, Sherman AT. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: exploring and evaluating tools, trust, and techniques. *Dig Investig*. 2012;9:S90-S98.
33. Mónica D, Ribeiro C. 2013. Leveraging honest users: stealth command-and-control of botnets. In *The 7th {USENIX} Workshop on Offensive Technologies*.
34. OpenStack, 2018. OpenStack. https://www.openstack.org/. Accessed December 10, 2018.
35. Meyers M, Rogers M. Computer forensics: the need for standardization and certification. *Int J Dig Evid*. 2004;3(2):1-11.
36. Garfinkel S, Farrell P, Roussev V, Dinolt G. Bringing science to digital forensics with standardized forensic corpora. *Dig Investig*. 2009;6:S2-S11.
37. Mouhtaropoulos A, Li CT, Grobler M. Proactive digital forensics: the ever-increasing need for standardization. *2012 European Intelligence and Security Informatics Conference*. Odense, Denmark: IEEE; 2012:1-289.
38. Chen PS, Tsai LM, Chen YC, Yee G. Standardizing the construction of a digital forensics laboratory. *First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*. Taipei, Taiwan: IEEE; 2005:40-47.

39. Casey E, Nelson A, Hyde J. Standardization of file recovery classification and authentication. *Dig Investig*. 2019;31:100873.
40. Karie NM, Kebande VR, Venter HS, Choo KKR. On the importance of standardising the process of generating digital forensic reports. *Forensic Sci Int: Rep*. 2019;1:100008.
41. Kim J, Son Y, Chung M. A design of evaluation framework for the assets and insolvency prediction depending on the industry type using data standardization based on the forensic readiness. *Int J Multimedia Ubiquitous Eng*. 2015;10:345-354.
42. Alshebel AKS. *Standardization Requirements for Digital Forensic Laboratories: A Document Analysis and Guideline*. Auckland University of Technology: Doctoral dissertation; 2020.
43. Rowlingson R. A ten step process for forensic readiness. *Int J Dig Evid*. 2004;2(3):1-28.
44. Mohlala M, Ikuesan AR, Venter HS. User attribution based on keystroke dynamics in digital forensic readiness process. *2017 IEEE Conference on Applications*. Miri, Malaysia: Information and Network Security, AINS; 2018, 2017:1-6. https://doi.org/10.1109/AINS.2017.8270436.
45. Munkhondya H, Ikuesan A, Venter H. Digital forensic readiness approach for potential evidence preservation in software-defined networks. *14th International Conference on Cyber Warfare and Security*. Stellenbosch: Academic Conferences International Limited; 2019:268-277. https://search.proquest.com/docview/2198531158?accountid=169469.

How to cite this article: Makura S, Venter HS, Kebande VR, Karie NM, Ikuesan RA, Alawadi S. Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring. *Security and Privacy*. 2021;4:e149. https://doi.org/10.1002/spy2.149