Novel digital forensic readiness technique in the cloud environment

[1,2]Victor R. Kebande[*], [1]H.S.Venter[†].

Department of Computer Science, University of Pretoria,

Private Bag X20, Hatfield 0028, Pretoria, South Africa.

Email:vickkebande@gmail.com[*], hventer@cs.up.ac.za[†]

This paper examines the design and implementation of a feasible technique for performing Digital Forensic Readiness (DFR) in cloud computing environments. The approach employs a modified obfuscated Non-Malicious Botnet (NMB) whose functionality operates as a distributed forensic Agent-Based Solution (ABS) in a cloud environment with capabilities of performing forensic logging for DFR purposes. Under basic Service Level Agreements (SLAs), this proactive technique allows any organisation to perform DFR in the cloud without interfering with operations and functionalities of the existing cloud architecture or infrastructure and the collected file metadata. Based on the evaluation discussed, the effectiveness of our approach is presented as the easiest way of conducting DFR in the cloud environment as stipulated in the ISO/IEC 27043: 2015 international standard which is a standard of information technology, security techniques and incident investigation principles and processes. Through this technique, digital forensic analysts are able to maximize the potential use of digital evidence while minimizing the cost of conducting DFR. As a result of this process, the time and cost needed to conduct a Digital Forensic Investigation (DFI) is saved. As a consequence, the technique helps the law enforcement, forensic analysts and Digital Forensic Investigators (DFIs) during post-event response and in a court of law to develop a hypothesis in order to prove or disprove a fact during an investigative process, if there is an occurrence of a security incident. Experimental results of the developed prototype are described which conclude that the technique is effective in improving the planning and preparation of pre-incident detection during digital crime investigations. In spite of that, a comparison with other existing forensic readiness models has been conducted to show the effectiveness of the previously proposed Cloud Forensic Readiness as a Service (CFRaaS) model.

Keywords: Digital forensics readiness; cloud; non-malicious botnet; agent-based solution; digital evidence.

1. Introduction

The advent of Information Communication Technologies (ICT) infrastructures has changed the way information is being disseminated across the world through the creation of global networks that seems to be dominating every individuals' lifestyle through the interoperability of devices. Moreover, ICT has played an important role in the global sphere with regard to how a majority of organisations conduct their daily businesses through reduced physical activities and improved communication and information management. These claims can be backed by International Data Corporation (IDC)'s[1] top 10 technology predictions, for 2016 which highlights that ICT will be the main theme for the forecast that will see its spending grow by 3.8% with a target that is projected to be more than $3.8 trillion[1]. As a result of these advances, a majority of modern infrastructures are now being built on cloud computing infrastructures which have allowed applications and data to be operated from distributed data centers under flexible cloud technologies.

Despite the above-mentioned benefits, this proliferation of digital devices and advances in these technologies have given room to a number of undesirable adversaries who have found ways of performing illegitimate activities in cloud computing environments. Nevertheless, issues like management and control, legislations, regulations, disaster recovery and lack of standardisation are some of the concerns that have been experienced within the cloud environment. Normally this happens because the Cloud Service Providers (CSPs) control the IT infrastructure and the cloud clients do not have direct access to the resources in the cloud. As a result, this has prompted a lot of concerns with regard to how sensitive data is handled for fears of leakage, breach, and other cyber-related attacks.

According to the survey by the USA's State of Cyber Security (USCS)[2], "cyber threats have become so persistent and the attacks have become so pervasive, that organisations and their leaders have essentially become inured to the ever-increasing threats". Additionally, the USCS[2] highlights that cyber-crime threats in the environment have become increasingly pervasive and very hostile and it is being embedded as a routine for business. Based on this survey, it is evident that there are a number of unwanted digital crimes within the cyber-space, consequently resulting in increased security risks, and reduced readiness.

The cloud provides a new model for provisioning and sharing resources over the internet, however, during Incident Response Procedures (IRP), a digital forensic investigator should be able to create a hypothesis based on the existing Potential Digital Evidence (PDE) that will prove or disprove in a court of law if a particular security event occurred. Nevertheless, cyber-crimes that target the cloud can go unforeseen if there are no sufficient techniques that may allow forensic evidence to be collected proactively before incident identification.

Digital Forensics (DF) plays a significant role through the provision of a scientific way of uncovering and interpreting evidence from digital sources that can be used in criminal, civil or corporate cases. It is mainly concerned with the legal aspect of computer investigations of crimes that are manifested by digital evidence. Furthermore, these aspects can only be conducted for purposes of law enforcement through Digital Forensic Investigations (DFIs).

On the same note, digital investigations on cloud-related crimes rely on a number of existing tools like Forensic Toolkit (FTK), EnCase, Internet Evidence Finder (IEF) and the Sleuth Kit but according to Dykstra and Sherman[3], these tools cannot be given a complete trust without a provision of new techniques and alternatives. This can only be attributed to the prevailing characteristics of the cloud. For instance, there can be a lack of physical evidence as opposed to traditional computing systems according to Zawoad and Hassan[4].

According to the standard of ISO/IEC 27043[5], Digital Forensic Readiness (DFR) has been presented as, a proactive process that occurs before incident identification. ISO/IEC 27043 is an umbrella standard for high-level digital investigation concepts that deal with information technology, security techniques, incident investigation principles, and processes. Therefore, in this paper, the cloud has been used as a target for achieving DFR because given the open nature of the cloud; it's easy for adversaries to use it to commit digital crimes without being detected. Nevertheless, we evaluate the possibility of conducting DFR without tampering with the functionalities of the existing cloud architecture or infrastructure. To bring out the problem that is addressed by this paper, the authors consider the following hypothetical case scenario on information security breach and identity theft:

It is common within a corporate environment to find adversaries with malicious intent, who can make an organisation a target of identity and information theft through unauthorized login. Adversaries do this by planting a malware that is able to collect the administrator's details and reports back to the adversaries which eventually helps them to access confidential information. The researcher considers the following consumer-provider investigative scenario that has been described in the next section.

The scenario involves a company that was able to gather and store its customer's information without protecting the information thereby putting the privacy of all the customers at risk. Nax.com was a cloud service provider (CSP) that offered private cloud services to various clients in Company ABC. ABC, on the other hand, is a company that had approximately 5000 employees who were in possession of the company's credit cards and debit cards. The company was using unprotected Wi-Fi and had not encrypted the client's credit card information and transactions which were stored in the company ABC's central database.

For a given period of time, there were no signs of any suspicious activity within ABC, which could warrant any digital forensic investigation until a number of clients raised issues that were related to the following: Jamming credit transactions as a result of exhaustion, debit card transactions that returned the following: unauthorized transactions; contact your bank and lack of sufficient amount of the debit cards. One client officially lodged a complaint that addressed the following issues:

1. *When he tried to withdraw some amount he realized that the amount was below what he expected and the statement showed 10 consecutive withdrawals that he had not made.*
2. *Each withdrawal was done between 12:00 midnight and 12:01am the next day in a span of one week.*
3. *The monthly statement also showed a number of unauthorized purchases that was made in country X and the client had never travelled to country X.*

ABC later suspected that there was a possibility of a potential security breach or an intrusion in its computer systems. Firstly, the CEO of ABC thought it was an inside job. However, he was not sure and without taking chances ABC decided to hire computer security consultants and digital forensic investigators. The CEO also involved the Law Enforcement Agencies (LEA) and financial bodies like banks that had contracted the credit cards, on the possible security intrusion. Furthermore, ABC chose not to disclose this potential security breach to the public to avoid unnecessary lawsuits until the digital investigations were complete because there was no proactive monitoring of event data in the database and daily transactions.

ABC decided to file for protection as per the law, ABC presented the number of cards affected as 2000. The contracting banks and financial institutions, however, sued ABC and they put the affected cards at 4500. This discrepancy highlighted that ABC and Nax.com did not have any forensic log data that could be used for forensic analysis.

Therefore, as substantiated above, a digital forensic investigation should be triggered by the presence of these incidents. A more significant doubt that DFIs and the LEA should be concerned about in this hypothetical case scenario would be, the identification of the perpetrators responsible for the security attacks, where the attacks originating from, and how they could be prevented in future.

The contributions of this work are as follows:

- Present an extension of previously proposed concepts.
- Present a cloud forensic readiness as a service (CFRaaS) model.
- Present requirements needed in order for the cloud to be forensically ready.
- Present a prototype implementation for the DFR technique in the cloud environment.
- Present a contextual evaluation of the proposed concepts based on the jurisdictional requirements.

As for the remainder of this paper, Section 2 presents reviews on the background. Section 3 presents related work. Thereafter, Section 4 presents the previous work while Section 5 presents the design of a cloud forensic readiness as a Service (CFRaaS) model. This is then followed by Section 6 that presents the requirements in order to achieve DFR in the cloud environment. After this Section 7 presents a CFRaaS prototype that is used as a proof of concept. Next, Section 8 gives a discussion on the functionalities of CFRaaS prototype. Section 9 presents a comparison between the CFRaaS and other existing forensic readiness models. Section 10 provides a critical evaluation of the proposed techniques. Section 11 concludes the work and mentions a possible future work.

2. Background

This section presents the background of the study on the following: Digital Forensics (DF), DFR, readiness process class in ISO/IEC 27043: 2015 international standard, digital evidence, cloud computing aspects, and botnets. The aforementioned parameters are considered because of the following reasons: DF is discussed to show how the science of investigation can help in the excavation of digital evidence using scientifically proven methods. DFR which is a proactive process is conducted inside the cloud environment. Botnets have been discussed because of their capabilities of capturing information over the network. The cloud, on the other hand, is discussed because all the concepts are based within the cloud environment.

2.1. Digital forensics

Digital Forensics (DF) as a science is concerned with the process of discovering evidential fragments, acquisition, examination and analysis of digital evidence[6]. Additionally, the existence of DF can be traced in early 1984 when the Federal Bureau of Investigations (FBI)[7] formed the Computer Analysis and Response Team (CART) to give aid in forensic examinations and technical support during forensic investigations. Nevertheless, since inception, the field has surfaced as the fastest investigative field in computing and law. In a technical report for a roadmap for DF research at the first Digital Forensic Research Workshop (DFRWS) held in Utica, New York in 2001, Palmer[7] gave a definition for DF as, the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

By revisiting the DFRWS definition, it is evident from Politt[8] that DF is focussed on all digital devices with many tasks and processes. Additionally, based on the DFRWS[7] definition, Carrier[9] singles out identification and analysis phases of DF as very important phases and further identifies the goal as, “to identify digital evidence using scientifically derived and proven methods to facilitate reconstruction of events”. The intuition presented by

Carrier[9] tries to show that all the data that has to be presented as digital forensic evidence has to be analysed and identified through acceptable means.

2.2. Digital forensic readiness

Digital Forensic Readiness (DFR) is a proactive process that is used to manage security incidents before they can occur. Security incidents are risks that are considered vulnerable to any organisation. Consequently, DFR plays a role in preventing or detecting the possibility of security incidents. Concepts of DFR were first proposed by Tan[10] and Rowlingson[11] as having two objectives: Maximizing the environment's ability to collect credible digital evidence whilst minimizing the cost of conducting forensic in incident response. Additionally, the most relevant and important forensic readiness technical aspects that Tan[10] identified include: how logging is done; what is logged, intrusion detection systems (IDS), forensic acquisition and how evidence is handled. Nevertheless, Beebe and Clark[12] proposed the Hierarchical, Objectives Based Framework for the Digital Investigations Process, which includes a preparation phase. Beebe and Clark[12] include a preparation phase in their model that encompasses activities that are aimed at fulfilling the aims of DFR. The preparation phase by Beebe and Clark[12] had a goal that was aimed at maximizing digital evidence availability through response, detection and deterrence, which was actually presented as a readiness phase. The authors further illustrate that this phase has activities that help in assessing risks, information retention, training and development of a post-incident plan which are the key aspects of DFR in an organisation. Therefore, it is worth noting that this research is inclined towards Tan's[10] objectives.

2.3. Readiness process class in ISO/IEC 27043: 2015

The readiness process class (RPC) has been defined in ISO/IEC 27043: 2015[5]. Furthermore, it has been mapped with other digital investigation processes to form a forensic RPC. ISO/IEC 27043 considers DFR as an integral process of Digital Forensic Investigation Process (DFIP) which means that DFR has to be contained in the digital investigation process. Additionally, the RPC deals with the process of pre-incident investigation processes. Note that the focus of this paper is to implement DFR process and not the DFIP processes that has been mentioned. Figure 1 represents the various classes of digital investigation processes which consist of the following entities: RPC, Initialization Process Class (IPC), Acquisitive Process Class (APC) and investigative process class. As stated in Section 2.2, this research is inclined towards objectives highlighted by Tan[10]. Therefore, the authors will consider the RPC that is shown in Figure 1.

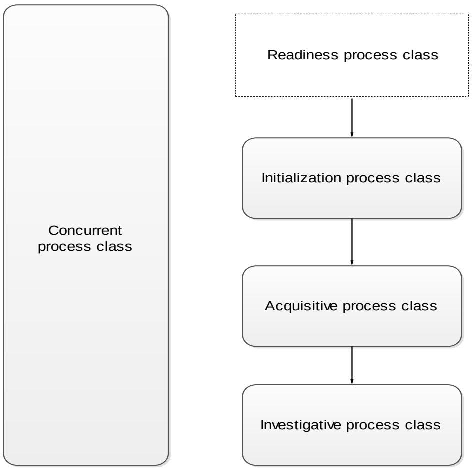

Concurrent process class
Readiness process class
Initialization process class
Acquisitive process class
Investigative process class

Figure 1. Classes of digital investigation process[5]

Based on the ISO/IEC 27043[5] processes, an RPC covers the following aspects: Scenario definition, identification of PDE sources, planning pre-incident gathering, storage and handling of data representing PDE, planning pre-incident analysis of data representing PDE, planning incident detection, defining system architecture, implementing system architecture, implementing pre-incident gathering, storage and handling of data representing PDE, implementing pre-incident analysis of data representing PDE, implementing incident detection, assessment of implementation and assessment of results[5]. While an RPC is a proactive process IPC, an APC and investigative process class represent the reactive process of digital forensic investigation. The concurrent process class are processes that happen in tandem with the proactive and the reactive process. Having looked at the RPC, in the next section the reader is introduced to digital evidence.

2.4. On Digital evidence

Different views have been put across with regard to what is digital evidence, and why it has increasingly been used in judicial proceedings. Firstly, Casey[13] presents digital evidence as "data that is stored or may be transmitted using a computer that may be used to support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or an alibi". Moreover, Casey[13] argues that it goes as further as representing data that has a link between a crime and a victim. Secondly, the Standard Working Group on Digital evidence (SWGDE) [14] presents it as information that has a probative value which is transmitted in a digital manner. Thirdly, Carrier and Spafford[15] view it from the perspective of security incidents, they present it in a generic definition as; digital data that can either support or refute a hypothesis about digital events. Lastly, the Association of Chief Police Officers (ACPO) [16] on digital evidence defines it as, stored data and information of investigative value that can be transmitted by the computer. Based on these views, digital evidence should be extracted from forensic targets so that its characteristics can help to provide the link between the suspect and the crime for possible admissibility in a court of law. In the context of this research paper, the cloud environment has been used as a target for extracting PDE. As a result of the aforementioned views, in the next section, the reader is introduced to cloud computing which is the target of this study.

2.5. Cloud computing concepts

Cloud computing has emerged as the most talked technologies when it comes to business in recent times and this has led enterprises to shift their focus to the benefits and cost effectiveness that the cloud offers. Gartner's[17] survey on cloud computing for business highlights that cloud computing has promised economic advantages, speed, agility, innovation, and elasticity. Moreover, Gartner[17] predicts that by 2016, 20% of all the services offered by the cloud services will be consumed by internal and external brokerages. Furthermore, Gartner predicts that by 2016 public cloud market is forecasted to reach $204 Billion. According to Almorsy et al.,[18], the cloud represents a new paradigm shift in internet-based services that delivers highly scalable distributed computing platforms in which computational resources are offered as a service. Cloud computing delivers hosted services over the internet through the following categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Additionally, the National Institute of Standards and Technology (NIST)[19] defines it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[19]". The focus of this paper is to show comprehensively how the cloud can be made forensically ready for DFIs.

2.6. ***On botnets***

According to Kebande and Venter[20], botnet or robot network is a generic term that describes a set of scripts written to perform systematic pre-defined functions that are written in a form of scripts. The bot itself is derived from "ro-bot", in this perspective bot represents the commands which are actually a collection of bot clients, which works under the command of a botnet operator. Botnets have always been attributed to crime-ware syndicates and they are considered as the dark side of computing[21]. Banday et al., [22] highlights that botnets are able to perform illegal activities ranging from information theft, spamming to Distributed Denial of service (DDoS). They perform these through searching for a vulnerable computer for initial infection, after this, the bot is distributed to clients (target), and then finally they can connect to the botnet operator for more instructions. In the context of this research, the functionality of the initially considered botnets is being modified to have a positive connotation. In the next section, the reader is introduced to work that is somewhat used as related work.

3. Related Work

Previous studies on the techniques of conducting DFR have shown the usefulness of the methods that have been used to collect digital data in a forensic readiness approach. However, most of their focus and scope is hardly targeted to the cloud environment. Based on that premise, the authors describe some prioritized studies on DFR as follows:

Quite a number of comprehensive DF tools have been used by industries in the quest to acquire digital evidence, for example, EnCase[23] and the Forensic Tool Kit (FTK)[24] have in many cases been used during acquisition of digital data from cloud environment. These tools are able to collect, process, search, analyse and report on methods of acquiring forensically-sound evidence. Moreover, a number of artifacts from the cloud have sometimes been recovered using the Internet Evidence Finder (IEF)[25] which at some point substitutes the FTK and Encase. While the certification and effectiveness of these tools can be measured by National Institute of Standards (NIST) Computer Forensic Tool Testing (CFTT)[26], none of them has complied with the standardised forensic readiness highlighted in the ISO/IEC 27043[5].

A research paper published by Reddy and Venter[27] propose architecture for managing DFR in organisations which did demonstrate some aspects of feasibility using a prototype. While this framework was very useful for a DFR system, the proposed system was intuitive and none of them used standardised processes. Nevertheless, Gummadi et al.,[28] published an article that addressed a way of improving service availability in the face of botnet attacks, Not-A-Bot (NAB). In that article, the authors cited that, using a trusted software component which could run on the client machine, it was possible to approximately identify and certify some human-generated activity. The trusted software was implemented with Xen hypervisor and the remote entity could send and receive requests from mouse and keyboard activity. Although this work was novel, the focus of the authors was never targeted to the cloud environment.

Garfinkel et al.,[29] points out Virtual Machine introspection (VMI)-based intrusion detection architecture that allowed the leveraging of the Virtual Machine Monitor (VMM) by allowing the Intrusion Detection System (IDS) to directly inspect the hardware of the VM. Nevertheless, Quick and Choo[30] have demonstrated methodologies of collecting and preserving data from the cloud without changing the metadata of files. The methods ensured that integrity of data was maintained through the use of MD5 and SHA-1 hash values and the originally written timestamps.

Next, Martini and Choo[31] proposed an iterative conceptual digital forensic framework for cloud computing. The framework had four phases as follows: Evidence source identification and preservation; collection; examination and analysis; reporting and presentation. Additionally, Dykstra and Sherman[32] proposed FROST, a design, and implementation of a digital forensic tool for OpenStack cloud computing platform. They presented a user-driven tool in infrastructure-as–a service (IaaS) platform that could do a forensic acquisition of APIs, virtual disks and guest firewall logs. Through this implementation, the authors are able to obtain forensically sound data. Other relevant works on the cloud include Quick and Choo[33], Quick and Choo[34], Martini and Choo[35], Martini and Choo[36], Rahman and Choo[37], Wen et al.,[38] and Westphal et al.,[39]. Nevertheless, a Virtual Machine Forensic Artefact Collector (VMFAC) prototype by Ahmad et al., [40] has been developed to conduct electronic crime investigation in the virtualised environment. The VMFAC prototype has been presented as a proactive approach where it is capable of collecting forensic artefacts. The artefacts that are able to be collected by the VMFAC include: VM network information like IP address, subnet masks and Media Access Control (MAC) address. Also, the log files, windows registry and the history are collected by the VMFAC. Through the VMFAC prototype artefacts are excavated from the VM with minimal traces for forensic investigation purposes[40].

An integrated incident handling model that has been proposed by Ab Rahman, Cahyani and Choo[41] has been designed to allow digital forensics to aid in handling incidental activities. Additionally, this model has been able to incorporate forensic readiness as a practice when handling incidents. The main phases in this model include readiness, identification, assessment, monitoring, recovery and evaluation. Nevertheless, forensic acquisition method from the cloud by Cahyani, Martini, Choo, and Al-Azhar[41] that targeted Windows phone has shown that logical acquisition of data is more suitable than physical acquisition. Also, a case study for cloud forensic storage by Daryabar, Dehghantanha and Choo[43] has been able to identify a number of artefacts that arise form user activities. In this research paper, the authors have identified timestamp modification, login, sharing of files uploads and downloads. Other similar literature that is focused on the cloud forensic investigations and evidence extraction has been highlighted by Daryabar, Dehghantanha, Eterovic-Soric and Choo[43], Shariati, Dehghantanha and Choo[45]. Also, research on the collection of digital information from the cloud-based applications by Martini, Do and Choo[46] and digital evidence in client machines by Shariati, Dehghantanha, Martini and Choo[47].

Currently, there exist quite a number of relevant researches that are focused on the cloud, however, neither of these works nor the ones that have been cited in the references of this paper have presented the technique of modifying a botnets' functionality to achieve forensic readiness in the cloud environment the way we have presented it. Nonetheless, the authors highly acknowledge the aforementioned work that has been done by other researchers. This work has given the authors a broad insight on CFRaaS model. Therefore, in the next section, the reader is introduced to the design of a CFRaaS model.

4. Previous work

In this section, we present preliminary work that has been proposed by the author. A Digital Forensic Evidence Collecting Prototype (DFECP) has been presented as a system that has a botnet whose functionalities have been modified to operate in a non-malicious approach. DFECP is able to collect digital data from a constantly changing environment in the cloud. The processes used to conduct this process all comply with the ISO/IEC 27043 processes on incidental planning and preparation as well as ISO/IEC 27037: 2012 on digital evidence preservation as highlighted by Kebande and Venter[48]. A proposal to add event reconstruction to a digital forensic readiness model that optimises botnets with a focus in the cloud has proposed the following event reconstruction processes: Retrieval of digitally preserved data, clustering of digital data, searching for security events from clusters, checking the similarity measure and reporting the events as shown by kebande and Venter[49]. Nevertheless a proposed Functional Architecture (FA) for computing large-scale potential evidence in the cloud environment by Kebande and Venter[50] operates in a distributed fashion using low-commodity cluster hardware. The structure of the FA is represented using four layers namely: Cloud layer, forensic layer, digital forensic readiness layer and incident response layer. The FA has been used as a building block to successful digital forensic readiness approach in the cloud environment. Additionally, research issues and challenges have been documented by Kebande and Venter[51] with proposed high-level solution when an agent-based solution (ABS) is used to conduct DFR in the cloud environment. In this research, the authors are able to propose a contribution through the assessment of possible solutions that has been viewed from a general, technical and operational point of view. In spite of that, research on characterizing potential evidence in the cloud by Kebande and Venter[52] has presented a Potential Digital Evidence Characterization Model (PDECM) in the cloud environment for forensic readiness purposes. This model is able to characterize evidence based on what is relevant and what is not relevant by observing the following processes: Clustering, activity analysis, event reconstruction and forensic reporting. Other relevant work include obfuscating the Non-Malicious Botnet (NMB) in the cloud environment to prevent tampering or take down during forensic logging process[53] and the requirements for achieving the proactive process have been focused on the legal, technical and operational point of view[54].

5. A cloud forensic readiness as a service model

5.1.Overview

In this section, we present a Cloud Forensic Readiness as a Service (CFRaaS) model. The model depicts a typical approach to DFR in the cloud environment. The model is presented using a high-level diagram of the CFRaaS that is shown in Figure 2. A formalization of the Cloud Model (CM) is first presented in section 5.2 which is then followed by the high-level model in Section 5.3. Each of the constituting parts of the model is discussed in subsequent sections.

5.2.Formalization of the Cloud Model

We use the formalism that is based on the actions that are provided between the Cloud Service Providers (*CSPs*) and the cloud clients (*Cls*) to logically model a formal cloud where the CFRaaS model is based. In the cloud environment, there exist interactions between the *Cls*, and the *CSP*. Logically, the underlying infrastructure between these cloud-based technologies *between the CSP and the Cls* is able to be separated through the concept of virtualization, which is represented as loose coupling according to Gong et al.,[55]. Loose coupling allows different components in a system to interconnect for purposes of interdependence. In this context, the services and applications are offered by the *CSP* and the *Cls* is able to interact with the cloud servers and the data centers, having in mind that the cloud operates on the client-server architecture. Consequently, the *Cls* does not have any control of the data in the cloud. To present a formal logic model of the interactions between the *CSP* and the *Cls* that support the CFRaaS model, the researcher describes a Cloud Model (*CM*) that is represented by a *Cls* and CSPs as shown in equation 1.

$$CM = \{CSP_1, CSP_2 .... CSP_m\}, [m \geq 1] \qquad 1$$

and

$$CSP = \{Cl_1, Cl_2 .... Cl_p\}, [p > 0] \qquad 2$$

Based on equation (1) and (2) of the *CM*, Gong et al.,[55] has highlighted that coupling between entities can be represented as a set. It can be seen from equation (1) that the *CM* is made up of m number of *CSPs*, which implies that in every *CM* there should exist $m \geq 1$. This means at least one *CSP* should exist in a *CM*. From equation (1) and (2) the *Cls* and *CSP* are represented as a set as shown in equation (3).

$$Set(Cl_i, CSP_n) \qquad 3$$

This is then followed by showing the independence of the *Cls* and the *CSPs* which is as shown in equation (4) and (5) respectively.

$$Cl_i \cap Cl_n = \varphi, (0 \leq i, n \leq p, i \neq n) \qquad 4$$

$$CSP_i \cap CSP_n = \varphi, (0 \leq i, n \leq p, i \neq n) \qquad 5$$

This implies the sets of *Cls* and the *CSP* are independent among *n* number of clients and *n* number of *CSPs*, however when they are loosely coupled the *Cls* are able to connect to the *CSPs* as shown in equation (5). Therefore, the interconnection between the *Cls* and the CSPs that shows how independent each entity is, this is shown in equation 6).

$$Set(Cl_{i1}, CSP_{n1}) \cap Set(Cl_{i2}, CSP_{n2}) = \varphi, [0 \leq i, n \leq p, i \neq n] \qquad 6$$

This shows that the *Cls* of the cloud are able to get access to the multiple provisioned services in the cloud at the same time, however, the data centers remain to be independent irrespective of the cloud deployment model. Based on the formalisms that have been highlighted above, it is evident that in the *CMs'* logic plays a big part during the separation of the infrastructure during the process of virtualization. Additionally, the cloud platform is represented as an abstract layer that is capable of separating a variety of applications that runs in the *CM*. In spite of that, once the *Cls* are loosely connected to the *CSPs*, the *Cls* gets no control of the data.

5.3. High-level view of the CFRaaS model

The high-level CFRaaS model is divided into nine distinct processes as shown in Figure 2 which enables seamless communication between the other processes. The uppermost process that is labeled 1, in Figure 2, represents the *CFRaaS Approach Strategy* for preparing the cloud for digital investigations. Next, the process labeled 2 represents the *digital evidence collection* mechanism that is used to collect PDE that can be used as admissible evidence in a court of law. This is done by employing a forensic agent; in this context, the researcher has employed a botnet with modified functionalities.

The process that is labeled 3 is represented as *incident detection*, which mainly shows a possibility of identifying a security incident from the collected PDE. *Incident detection* is concerned with instituting guidelines that allow detection of security incident through notification procedures. Moreover, it involves classifying and describing a security incident that is capable of triggering the DFI process. The process of the high-level model labeled 4 is *pre-incident analysis*, which represents reviewing in detail the compromised digital evidence with the aim of reconstructing the causality of the security incident. Next, this is followed by *event reconstruction* and *forensic readiness report* in the processes labeled 5 and 6 respectively.

The process labeled 7 addresses the *requirements* that have to be satisfied in order for DFR to be achieved. A number of these requirements have previously been discussed in Section 5. The processes labeled 8 represent forensic readiness policy. The main objective of employing forensic readiness policy in a CFRaaS is to ensure that there is a legal premise on how PDE, that is deemed admissible, may be extracted and presented in a legal process. Consequently, process 7, 8 and 9 are meant to run in parallel, i.e. concurrently with the other processes. The reason for this parallelism will become apparent when discussed later.

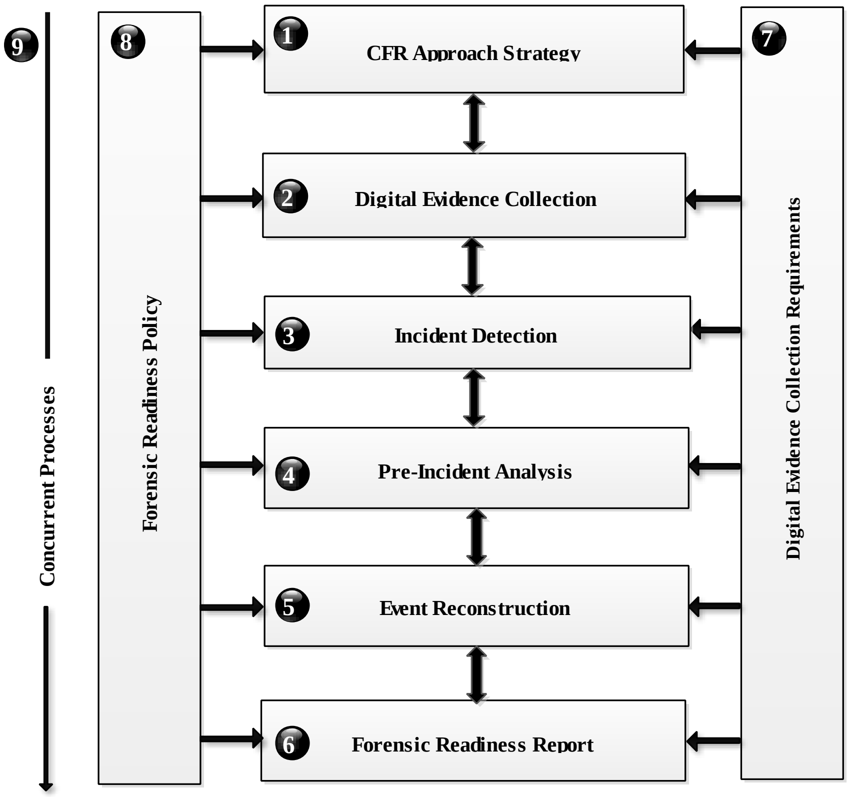

9
Concurrent Processes
8
Forensic Readiness Policy
1
CFR Approach Strategy
2
Digital Evidence Collection
3
Incident Detection
4
Pre-Incident Analysis
5
Event Reconstruction
6
Forensic Readiness Report
7
Digital Evidence Collection Requirements

Figure 2. High-Level Overview of the Model

5.3.1 *CFRaaS approach strategy*

To begin with, the process labeled 1, which is presented as *CFRaaS Approach Strategy* in Figure 2, consist of the following sub-processes: *planning and preparation, scenario identification* and the *Non-Malicious Botnet (NMB) deployment* as a forensic agent. The *CFRaaS Approach Strategy* provides an ideal approach that enables definition of activities that deals with the pre-incident collection of potential evidence in a manner that will make the cloud ready for digital investigations. Additionally, the approach identifies the risks that might identify vulnerabilities and threats, scenarios and techniques of gathering PDE in the cloud. Note that each process previously shown in Figure 2 is further subdivided into sub-processes as shown in Figure 3 and subsequent figures later on.

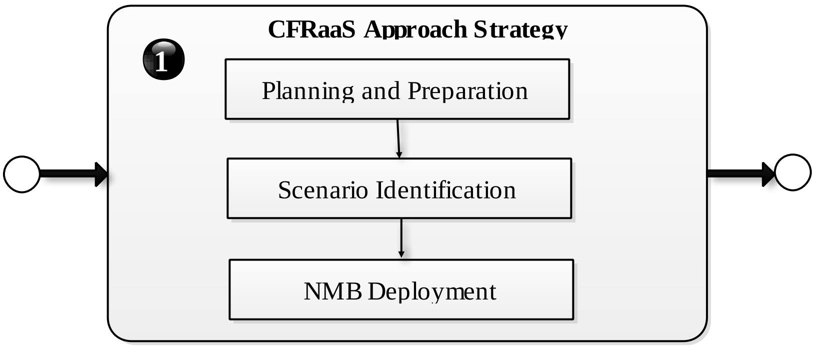


Figure 3. CFRaaS Approach Strategy

Planning and Preparation mainly is a collection of processes that are concerned with the day to day operations in an organisation. This involves processes that are able to formulate the procedures that an organisation will follow if the unexpected is experienced. Actually, this process is used to prepare any organisation before security incidents can occur. In this context, the main focus of *Planning and Preparation* is to plan for major risks that an organisation is likely to experience. After this, organisational functions are protected in a manner that, should a security incident occur, the necessary requirements will be in place to aid investigators with minimal disruption of business processes.

Nonetheless, it is essential to have a comprehensive plan that shows how activities, that are related to forensic readiness, are to be handled. This plan should cover all aspects that deal with *Planning and Preparation* activities. Nevertheless, all the organisational critical functions, security events, the people that are involved, the technology that is going to be used and the resources that are to be employed are all defined in this phase. Rowlingson[11] highlights that incident preparedness can be targeted to be a corporate goal when implementing a forensic readiness approach. An example of technology that may be employed in *Planning and Preparation* includes implementation of intrusion-based techniques. Additionally, this has been defined in the readiness process groups in the ISO/IEC 27043[5] international standard.

We refer to the hypothetical case scenarios that were discussed in Section 1 where client's personal information for company ABC was compromised. In this case scenario, there were no proper planning strategies on how a proactive process could have monitored potential security events. The security breach that was experienced in ABC could have been prevented if intrusion-detection systems that are able to monitor traffic were in place. Another factor is the discrepancy that was highlighted between the CSP, Nax.com, and ABC. In this case, Nax.com had not enforced proper *Planning and Preparation* procedures before these particular incidents could occur. Due to lack of incident preparedness, it is going to be hard for ABC to recover without disruptions because the post-event response mechanism is likely to be costly because of insufficient Planning and Preparing before security events could occur.

The next phase is *Scenario identification*, which involves an assessment of potential risks that enables identification of environments, threats, and vulnerabilities that can act as prerequisites for achieving DFR within a given organisation. At a given time, different organisations will experience different threats.

Due to this, the risk equation highlights an instance, where threats are likely to correspond to threat levels and the cost that is incurred by a given organisation[56]. The main goal, in this case, is to set procedures for identifying, evaluating and mitigating risks that may arise in a business environment. Therefore, in the context of this paper, the existence of potential risks can be defined as shown in Equation (7)[56].

$$Potential\ \_Risks = Org[P\_Threats] \times Org[P\_Vu\ln erabilitie\,s] \times Org[Cost] \qquad 7$$

where *Org [P_Threats]* is the organisation potential threat value and *Org [P_Vulnerabilities]*. Finally, *Org [Cost]* denotes the cost incurred by an organisation based on the potential attack.

The last process of the CFRaaS approach strategy is the *NMB deployment* process. The process is conducted by the CSPs for purposes of forensically monitoring the client's activities (*Ac* as shown in equation 8) within a cloud environment. In this process, botnets with modified functionalities that acts as forensic agents are deployed in the cloud environment, to forensically collect digital information that may be used as admissible evidence in a court of law. Firstly a domain that represents a CSP is defined. The CSP provides services to clients that are represented as a set of activities *Ac*. This can be represented by the following equation:

$$CSP = \{Ac_1, Ac_2 ....Ac_n\} \qquad 8$$

Based on the CSP and client formulation, legally admissible PDE collection from clients is presented in the next section.

5.3.2 Digital evidence collection

The process labelled 2 named *digital evidence collection* consist of the following sub-processes: *forensic clients*, *forensic logging process* and *digital preservation* of forensically collected evidence. Digital evidence that can be used to develop a hypothesis in a court of law is collected in this phase. According to Rowlingson[11], the techniques for gathering digital evidence for DFR purposes should be done through Intrusion Detection Systems (IDS) so as to target major security incidents. In this process (the process labelled 2), monitoring of potential evidence sources is employed in the cloud environment as shown in Figure 4. At this stage, a technique of retaining digital evidence through gathering, preserving and storing is defined. Figure 4 shows forensic clients that basically contains the execution of the NMB in the Virtual Machines (VMs). The underlying assumption in this model is that there are *n* numbers of VMs in the cloud environment through which a modified form of a botnet that acts as a forensic agent, are executed. Through this process, sensitive and critical information can be gathered in a forensic logging approach from the cloud from the *n* number of VMs (see Figure 4).

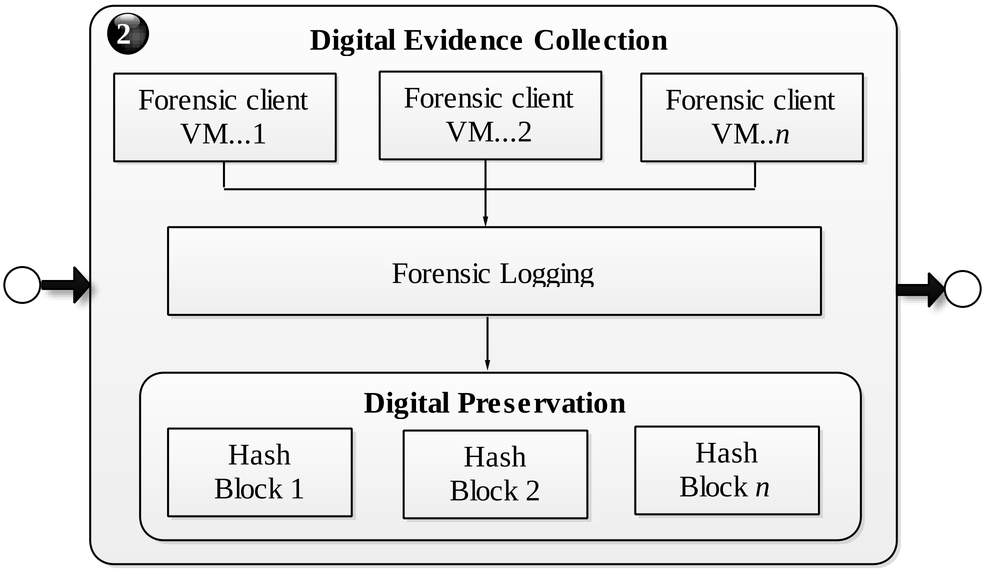


Figure 4. Digital Evidence Collection

The captured potential evidence that is in the form of logs is digitally preserved and then stored in the forensic database. Hashing is performed as a block of hashes to potential evidence in order to maintain the integrity of the data. This is shown using *Block 1, Block 2….Block n*, where in this context, a block of hash represents a set of captured forensic logs. A comparison of cryptographic hash functions is performed on the logged data to ensure that its integrity is maintained. The significance of *digital preservation* is to ensure changes are not made to the gathered potential evidence. Potential evidence that is to be used for DFR purposes has to be retained in its original form without contamination or modification. This is because, the collected digital evidence may satisfy admissibility, which in the long run may be used to make some formal conclusions in a court of law or during court proceedings.

A reflection of the hypothetical case scenario that is highlighted in Section 1 on information security breach and identity theft shows the following: when ABC initially suspects a possible break in their systems, a decision to keep the incidents from the public was reached out of their own interests. Even though there existed no legal provision that necessitated ABC to report the incident, it was evident that the provider, Nax.com had not taken effective security measures for *planning and preparing* before *incident detection* and this complacency was, in one or some ways going to cause ABC a fortune while investigating. This is mainly because of the ineffectiveness of Nax.com, which eventually had a great impact on the security standpoint of the clients. Notwithstanding these anomalies, the clients' influence on the actions that Nax.com could have taken towards security were also limited

Consequently, based on the aforementioned case scenario, there is a higher impact emanating from lack of sufficient proactive process that could help prove a fact in a court of law. It is possible that these vulnerabilities and breaches that allowed intrusions, framing and theft could have been noticed. This could have been possible if Nax.com had performed forensic logging which according to Rowlingson[11] could point to the following:

- Forensic logging could be evidence that could have been gathered in order to act for the company's defense if there was a lawsuit.
- Forensic logging approach could be used as a digital evidence collection method that could deter insider threats.
- Lack of forensic logging approach could help to cover a cyber-criminal track.
- Forensic logging could have reduced the cost and time that could have been required to conduct an internal investigation.

Forensic logs that exist as PDE are collected based on the timeline of activities. It is essential to perform analysis on forensic logs that exist as digital evidence when they are collected from different cloud sources before a DFI is conducted. Therefore, forensic log files can be represented with their respective tag names and the time the activity occurs. A tag name is an identifier that is used to identify a forensic log file. This can be represented using the following equation:

$$< (Lt_1, To_1), (Lt_2,To_2)\ldots(Lt_n,To_n) \qquad 9$$

where L_{ti} is used to denote the identifier of the forensic log or the tag name and To_i denotes the number of times that L_{ti} occurs. This is the actual occurrence of a particular forensic log file. This implies that in each particular activity that *Ac* generates, one or more forensic log file can be used as PDE. This is represented by the following equation:

$$Ac_i=\{L_{ti1},L_{ti2}\ldots L_{tip}\}, i\,\varepsilon\ [1,n] \qquad 10$$

Whenever PDE is collected from a client *Ac* in a given environment, *i* will represent the origin or the source that the forensic log is extracted from. Additionally, a series of Possible Potential Security Events (PPSE) with different attributes may be registered within the forensic logs. Attributes in this context might be the time of occurrence, frequency of occurrence, the size of the log, source or destination of the log. Furthermore, the existence of these PPSE may be represented by the following equation:

$$L_{tij}=\{e_{ij1}, e_{ij2,}\ldots e_{ijm}\}, i\,\varepsilon\ [1,n], j\,\varepsilon\ [1,p] \qquad 11$$

where, e_{ij} is a PPSE that may occur under specific collected forensic log. The attributes *at* for an event *ei* may be represented by varying records that may include: timestamp (t), occurrence (*X*) and size (s) of the log. This is represented by the following:

$$e_{ijq}=\{at_{ijq1},at_{ijq2,}\ldots at_{ijqk}\}, i\,\varepsilon\ [1,n],\ j\,\varepsilon\ [1,p), k\,\varepsilon\ [1,m] \qquad 12$$

Based on the formulations that have been represented it Equation 8, 9, 10, 11 and 12, the components of the CFRaaS model of Figure 2 have been formalized. Therefore, the equation representing the CFRaaS model when process 1 and process 2 are formalized is represented as follows:

$$CSP=\{Ac\{L_t\{e_{ij}\{at_{ij}\}\}\}\}\Leftrightarrow dp \qquad 13$$

where *Ac* represents set of monitored activities, L_t represents identifier or tag name, e_{ij} represents PPSE, *at* represents the attributes while *dp* has been used to represent the process of digital preservation.

5.3.3 Incident detection

An incident has a possibility of occurring if a suspect performs an unlawful action on a computer or over the network. The process labelled 3 represents *incident detection*. It comprises of the following sub-processes: *Incident Detection Rate* (IDR), *incident classification* and *Incident Response Mechanism* (IRM). Consequently, *incident detection* is a process that has a capability of triggering a digital forensic investigation. Incidents can be any potential security threats that have capabilities of exploiting vulnerabilities of any system. In this context *incident detection* has been portrayed as a technique that is used to identify intrusions that may trigger a DFI. Basically, with the availability of DFR, *incident detection* enables efficient discovery, notification and reporting of threats and attacks, which have the potential of compromising any system. According to ISO/IEC 27043, *incident detection* has been presented as a process that deals with detection of potential incidents.

Additionally, incidents are normally related to security threats or attacks that have a possibility of jeopardizing the business processes of any running organization. This can be intrusions, target breach, subverting, system exploitation or an intruder leveraging unauthorized access. These subsequent intrusions happen as a result of adversarial breaches and the threshold of these intrusions ends up costing a given organisation a fortune if DFR is not enforced. Once an incident is reported, information regarding the incident like the time, date, kind of incident, network, host, and how it was detected, should be documented for proper post-incident response mechanism. Figure 5 shows the sub-processes in the incident detection process.

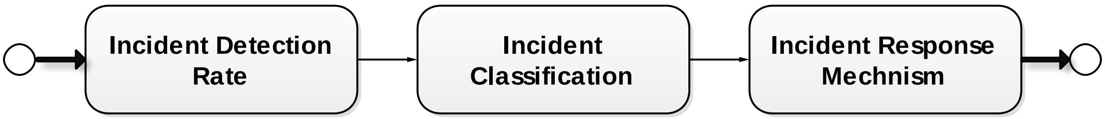


Figure 5. Incident Detection

The tasks represented by incident detection as shown in Figure 5 include *Incident Detection Rate (IDR)*, *incident classification* and *Incident Response Mechanism (IRM)*. IDR is used to estimate the actual frequency that security incidents occur. Therefore, in the context of this paper, IDR is computed as follows:

$$IDR = \frac{Number\_of\_Incidents\_Detected}{Number\_of\ \mathrm{Re}al\_Incidents} + \{False\_Alarms\} \qquad 14$$

Once a potential incident is detected, it will naturally lead to an IRM; however an incident classification is done first to show the type of incident through a description of the actual incident as shown in Figure 5. A team that comprises of personnel with some technical and legal expertise called Computer Security Incident Response Team (CSIRT)[57] is normally responsible for handling with handling incidents. IRM is used to review all information that is related to security incident; therefore, in this paper, we can compute IRM as follows:

$$IRM = IDR + \{Incident\_Description\} \qquad 15$$

Classification of incident allows proper identification of the type of incidents and based on incidental information gathered at this level a DFI can be triggered.

If we refer to the hypothetical case scenario shown in Section 1, it is evident that a number of security incidents were pointed out even though they were not proactively detected. It is evident that sufficient historical data was missing that could have helped ABC to detect suspicious activities. Nevertheless, Nax.com is not going to make appropriate event logs to digital investigators due to lack of forensic readiness.

5.3.4 *Pre-incident analysis*

In this process, a careful examination and assessment of PDE is done for possible detection of incidents. *Pre-incident analysis* is a process that reviews the compromised evidence and compromised hosts with the main aim of conducting a reconstruction of security incidents. *Pre-incident analysis* consists of the following sub-processes: *Pre-incident planning, incident description, PDE assessment, relevant-PDE, non-relevant-PDE* and *pre-incident analysis report*. In this phase (see Process 4) of Figure 2, examination and assessment of PDE is conducted for possible detection of security incidents.

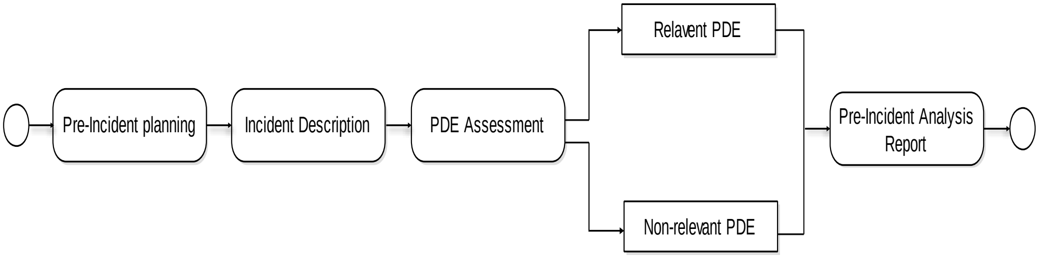


Figure 6. Pre-incident analysis

The output of this process should highlight the security incidents experienced as a result of the incident detection process as shown in process 3 of Figure 2. On the other hand, Figure 6 shows an overview of pre-incident analysis processes of the CFRaaS model.

Pre-incident planning defines activities that should be performed on the collected and digitally preserved PDE by enabling a given organisation to manage security incidents in a manner that allows effective and fast response measures. *Incident description,* on the other hand, provides information on the type or nature of the incident that is detected as previously highlighted in section 4.4. *PDE assessment* is done to check if PDE is relevant or not. PDE is said to be relevant if it has a potential of containing suspicious activities otherwise it is non-relevant. Finally, *pre-incident analysis* defines the procedures for analysing data that represents PDE. This is done for easy detection of actual security incidents through examination and assessment of the aforementioned processes.

Equation 7 presented a formulated equation for the process (labeled 1) and process (labeled 2) of the CFRaaS model as follows: $CSP=\{Ac\{Lt\{e_{ij}\{at_{ij}\}\}\}\} \Leftrightarrow dp$ where *dp* is the preserved PDE. Based on Equation 7, the collected and digitally preserved PDE *dp* is represented as an object or a target while *pre-incident planning* (*pp*), *incident description* (*id*), *PDE assessment* (*pa*) and *pre-incident analysis* (*pi_a*) are presented as activities that are performed on the object *dp*. In this context, the object qualifies to be a digital file or a forensic log, software or hardware. If DP is a set of objects then $dp \in DP$ where DP is given by the following:

$$DP=\{dp_1,dp_2,dp_3\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots dp_i\},\ i \in N \qquad 16$$

Nevertheless, $dp \in DP$ is considered to have a number of properties. These properties can be represented using the following:

$$DP=\{p \in P_o|dp\alpha_o p\} \qquad 17$$

where, p_o represents the properties that give a description of the target. The properties may include: Forensic log name, timestamp, the size of the log and the overall file metadata. α_o provides a relationship that is able to merge the target $dp \in DP$ to the property $p \in P_o$. The activities *pp, id, pa* and *pi_a* are operations that have to be executed after the collected digital information from the cloud environment is stored as PDE. If $\{ppUidUpaUpi\_a\}=A_t$=set of activities then, $at \in A_t$ where

$$A_t=\{at_1,at_2,at_3\ldots\ldots\ldots\ldots\ldots at_j\}, j \in N \qquad 18$$

The aforementioned activities are represented as general operations that occur at the digital location that the target is stored. Following Figure 7.5, the overall activities are represented as

$$\{ppUidUpaUpi\_a\}=A_t \Leftrightarrow \{R\_PDE, NR\_PDE\} \qquad 19$$

Where, *R_PDE* and *NR_PDE* are represented as possible relevant and non-relevant PDE that may contain potential security events e_i. Events e_i are represented as activities *Ac* registered within the forensic logs.

Based on the hypothetical case scenario, potential security incidents could have been detected if there was an availability of proactive process. A preliminary evidence assessment could have been a solution that could have helped to unearth the intruder's suspicious activities.

It is, therefore, paramount to know how to pull the plug when Security incidents are detected in any business setting. Firstly, the main way of managing post-event response after an incident has been detected is to ensure there exist proactive measures in a given business setting. Secondly, it is essential to detect the exact incident efficiently, which should be then followed by responding to the incident and thirdly is to perform a DFI effectively.

5.3.5 Event reconstruction

Event Reconstruction (ER) analyses and examines PDE in order to identify why it holds certain characteristics[49]. This helps in identifying the causality of the possible security event and also helps to build a hypothesis before a DFI is done. The first step when performing an ER procedure is evidence collection and examination, which helps to seek the truth. Afterward, according to Gardmer and Bevel[58], there exist creation and sequencing of event segments from the evidence.

This involves a discrete collection of digital data, which may be examined for possible potential evidence with regard to the occurrence of a security incident. Consequently, ER tends to question why digital evidence has certain properties and characteristics. Additionally, the existing analogies show that during ER, evidence analysis, and examination is conducted to show the exact causes of the characteristics and properties that digital evidence poses. ER (labeled 5) in Figure 2, allows a study of the characteristics of PDE, consists of the following sub-processes: *Retrieval of relevant PDE, clustering of relevant*

PDE, searching events, performing similarity measure and generation of *causality report*. This has been shown in Figure 7.

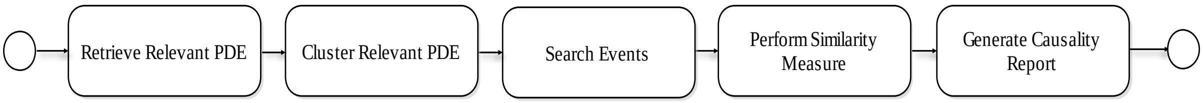


Figure 7. Event Reconstruction

In spite of that, while reconstructing digital events in a forensically ready environment we have to revisit the characteristics and sequence of digital events in a proactive process and check whether the collected PDE satisfies admissibility[49]. For the sake of this paper, ER has been represented in Figure 7. Each of the sub-processes of Figure 7 is explained next.

The mechanism of ER provides a thorough examination and analysis of all the events by revisiting the characteristics and the sequence of events and making sure that PDE is in an acceptable form when an incident is detected. This is done by means of checking if the gathered PDE satisfies admissibility and why that particular evidence must be considered to be evidence. This helps to identify if a causal relationship exists between the sequences of events. Moreover, ER in a CFRaaS model has been presented by Kebande and Venter[49] as a process that is able to distinguish events, discover the structure of events, distinguish one event from the other by focusing on the relationship that exists between the events and predicts the behaviour of events. On the same note, Carrier and Spafford[59] highlight that ER questions why PDE which is treated as an object has some properties and where those properties originate from. It is, therefore, the authors' opinion that every reconstructed event should have a cause and correlation of the potential events that should help in identifying the causality.

Digital events are reconstructed based on the following steps according to Kebande and Venter[49]: PDE retrieval, clustering, event search, similarity measure and event reporting. PDE retrieval entails getting access to the collected digital evidence. Clusters help in grouping events based on possible occurrences of events and later based on their similarity. This is followed by a search function that performs a look-up for possible detection of events. The similarity measure is performed by checking the distance between events using the distance metric[49]. The distance between events can be achieved using the following equation:

$$d^{MD}(w_{1t}, w_{2t}) = \sqrt[p]{\sum_{i=1}^{n} | w_{1t} - w_{2t} |^{p}} \qquad 20$$

where *[p=1, 2….n]* for the distance function of an event w_{1t} and w_{2t}, d^{MD} (w_{1t}, w_{2t}) is the distance between event w_{1t} and event w_{2t}. The similarity, behaviour, and pattern of the events e_i can be calculated using the distance function d^{MD} (w_{1t}, w_{2t}). On the same note, if we consider attributes like time, occurrence and size, we can then test these attributes when *[p=1, p=2 and when p>2 to* ∞ *]* using *Eqn 20*. As a result, when *p=1* in *Eqn 14*, we find the absolute difference between the pair of event attributes by examining the absolute value distance. This is given by the following equation

$$d(w_{ij}) = \sum_{k=1}^{n} |w_{ik} - w_{jk}| \qquad 21$$

When *p=2* in *Eqn 20*, we find the root of square differences between the set of event attributes by examining the distance metric. This is given by the following

$$d(w_{1t}, w_{2t}) = \sqrt{\sum_{i=1}^{n} (w_{it} - w_{2t})^{2}} \qquad 22$$

When *p>2 to* ∞ in *Eqn 20* the maximum value distance is checked by examining the absolute difference in magnitude between the set of event attributes. The distance metric is given by

$$d(w_{1t}, w_{2t}) = \max_{i} | w_{1ti} - w_{2ti} | \qquad 23$$

The distance metric between the events is computed to help with the following:

- Predict the next behavior of events[49].
- Distinguish how one event differs from the other considering their relationship. Kebande and Venter[49].
- To discover how the structure of events is. Kebande and Venter[49].
- Distinguishing one event from another during event reconstruction process. Kebande and Venter[49].

5.3.6 Forensic readiness report

Forensic readiness report represented with the process labeled 6 in Figure 2 is an integral part the DFR process that typically contains information and descriptions of all the steps taken towards digital evidence examination, classification and how ER process is formulated. It consists of two sub-processes namely: *Examination notes* and *causality*.

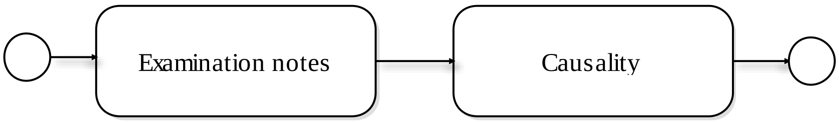


Figure 8. Forensic readiness report

Examination notes show how the DFR process is conducted in the cloud whereas the *causality* shows the potential cause of security incidents. Moreover, ISO/IEC 27043[5] international standard describes this as results from digital evidence interpretation process. At this stage, the roadmap of the readiness process and the security event properties is interpreted and presented to DFI and law enforcement agencies. Reporting is aimed at generating an audit record that shows the scope, occurrence and the characteristics of the events[5].

5.3.7 Digital evidence collection requirements

Digital evidence collection requirements labeled 7 of Figure 2 allow the implementation of DFR processes. The CFRaaS model requirements that have previously been discussed in Section 5 institutes different parameters that guide the successful execution of forensic readiness from a technical, operational and legal point of view.

5.3.8 Forensic readiness policy

Forensic readiness policy that is shown in the process labeled 8 of Figure 2 governs different procedures for collecting, storing and handling PDE. The policy outlines the standardized methods of conducting DFR. It also provides a channel that acts as a legal basis for collecting digital evidence that can satisfy admissibility in a court of law, when required for a legal process. Furthermore, the broad effect of this policy is to reflect different procedures of maximizing the use of PDE when needed. Furthermore, this helps while minimizing the cost and security effects of potential incidents in an organisation. Nevertheless, while conducting a DFI, a forensic readiness policy helps to safeguard the interests of an organisation at the same time. Additionally, the policy also outlines an organisations' capability to conduct proactive forensic monitoring through the collection of admissible digital evidence, examination of digital evidence and presentation for legal purposes.

5.3.9 *Concurrent processes*

The last process labeled 9 of Figure 2 that is shown using an arrow pointing downwards is the *concurrent processes*; this has previously been described in the ISO/IEC 27043[5]. The concurrent processes are executed alongside the other processes. They provide a proper method of handling of digital evidence to enable a holistic approach to digital forensic investigations. The main aim of these processes according to Valjarevic and Venter[60] is to ensure admissibility of digital evidence, that has a potential of being admitted in a legal system (ISO/IEC 27043) and also to follow DF principles.

The tasks involved in concurrent processes according to ISO/IEC 27043 include: Documentation, managing information flow, obtaining authorization, preservation of chain of custody and digital evidence. Documentation is a mechanism of taking examination notes based on the outcome of the digital investigation process while information flow allows automation of on-going processes.

Next, obtaining authorization after a security incident has been detected allows an interaction that can enable a forensic administrator to perform activities dealing with physical investigations. Chain of custody as a process shows the roadmap of preservation of digital evidence. It shows how each and every form of evidence is collected even when changes are made. Digital preservation of the collected evidence is done through hashing to maintain evidence in its original form.

6. Requirements in order to achieve DFR in the cloud

This section provides a discussion of the proposed requirements as a contribution to how a modified botnet that acts as an ABS can be used to conduct DFR in the cloud environment. The primary objective of the requirements is to portray a relationship between the ABS and the different jurisdictions that govern different cloud models. The requirements provided in this section have been used to analyse and specify the CFRaaS model[54]. The requirements are aimed at allowing the ABS to be deployed in a scalable environment to collect PDE. Furthermore, they will ensure that there exists a functional relationship between the structural components of the model. A summary of the requirements has been given in Table 1 and explanations are given thereafter.

Table 1. Requirements in order for a cloud to be forensically ready when using an ABS[53]

	Requirement	Summary
1	**Forensic logging capability and management**	Forensic logs to be used as digital evidence should be collected in a virtualised environment by an ABS.
		It is important to know how logging is done, what is logged and when to log using the ABS.
2	**Integrity and authenticity**	The retained digital evidence should be digitally preserved.
		Verification authenticity should be possible if there is a

		need for a digital forensic investigation.
3	**Timestamping**	Each log should have a timestamp to in order to prove its integrity.
		All events and activities should have timestamp representation.
4	**Digital evidence characterization**	Digital evidence should be grouped respective file format for possible incident identification.
		Activity analysis should be conducted to isolate potential security incidents.
5	**Non-modification of existing cloud architecture or infrastructure**	Functionalities of existing cloud architecture are not modified or tampered with.
		Activities like computation of evidence and analysis are conducted outside the cloud environment.
6	**Security implementation**	The ABS should be protected other malicious activities.
		ABS should be deployed in a trusted environment
7	**Obfuscation**	ABS's patterns are changed in a nonsensical manner to deter surveillance.
		Obfuscation is enforced for privacy reasons
8	**Event reconstruction**	A hypothesis that should prove a fact in a court of law should be developed based on events.
		Structure and occurrence of events should be easily distinguished.
9	**Legal requirements**	The legal perspective and provisions across diverse jurisdictions should be known prior to a digital forensic investigation.
10	**Forensic reporting**	A readiness report that shows the interpretation process as a result of digital evidence retention should be generated.

Table 1 has shown a summary of the proposed requirements that should be taken into consideration in order to achieve DFR in the cloud when an ABS is used. Forensic logging allows the CFRaaS model to collect and manage PDE, hashing is done to the collected digital evidence to maintain integrity. All events and forensic logs should have a timestamp for easy identification of the evidence. Characterization, as described by Kebande and Venter[49], allows one to isolate PDE based on the causality and characteristics during DFR approach. After characterization, forensic activities like manipulation and computations of PDE happens outside the cloud which renders the functionality of existing architecture hard to modify thus saving cost and time needed to reprogram the infrastructure. The ABS is protected from other malicious activities through encryption. It is then deployment in a cloud environment. Deterrence of the ABS is done through obfuscation; this has been highlighted by Kebande and Venter[50, 53] as changing the ABS's pattern to nonsensical pattern so that its purpose cannot be defeated. Event reconstruction has been presented in CFRaaS model as a way of reconstructing events based on similarity measure[49]. This approach should be sensitive to the local laws of a given jurisdiction and law enforcement requirements. Finally reporting provides examination notes through interpretation of what requirements have been achieved in the model. Having highlighted a list of the requirements, in the next section, the we provide the prototype. In order to achieve readiness, the prototype must incorporate the aforementioned requirements.

7. CFRaaS prototype Implementation

In this section, the reader is introduced to the prototype for achieving DFR in the cloud environment namely Cloud Forensic Readiness Prototype (CFRaaSP), its benefits and its uses. The prototype exists as a software application with the functionalities of a modified form of a botnet that acts as an ABS. The functionalities of the prototype are as follows: The first functionality is for the prototype to act as a forensic agent that is able to collect PDE in a constantly changing environment. The next functionality allows implementation of DFR process through successful forensic logging and a final functionality is to uphold integrity through digital preservation of the collected PDE. The prototype would help an organisation to implement DFR as a standardized process defined in the ISO/IEC 27043 so as to ensure the gathered PDE satisfies admissibility.

7.1. Design guidance of the CFRaaSP

In this section, we describe the design guidance of CFRaaSP which is implemented as SaaS in the cloud environment. The aim of the CFRaaSP is to collect, digitally preserve and reconstruct PDE in a legally acceptable manner. Additionally, the proposed CFRaaSP adheres to the requirements that have been presented in section 5. Implementation has been done in a Window-based cloud environment. The task includes building a software prototype with the functionality of a modified botnet that acts in a non-malicious fashion so that it can collect PDE that can be used as admissible evidence in a court of law. To ensure that that PDE will exist in a legally acceptable manner we set the following design goals for the DFRP and they are explained as follows:

7.1.1. Technical goals

In order to find PDE that can link a suspect to a crime in the cloud environment, intruder's footprints are basically examined based on the system content and log files which in most cases require a change in the existing cloud architecture. Furthermore, with the existence of big data, this proposition might be impossible when it comes to tracking the source of potential attacks because while filtering logs using manual forensics you might remove that which you are looking for without noticing. In fact, since these processes are implemented separately. In that case, it might be tedious to reconstruct the sequence of events in order to create a hypothesis that can be used in a court of law for digital investigations.

The above-mentioned limitations can be overcome using the CFRaaSP that the authors have developed. The prototype focuses on the following technical goals: Monitors activities in the cloud environment using an ABS that acts as a distributed forensic client. Next, the digital information gathered in this process is digitally preserved then transmitted to a centralized forensic database for secure analysis. These processes are able to monitor the CPU usage in case a malware is utilizing the processing power that is allocated to each client computer, as well as the RAM processes and the keystrokes with respective timestamps. It is worth noting also that there is no modification or tampering with the cloud architecture since the collected evidence is isolated from the cloud. Lastly, all events are reconstructed for easy detection of any potential security incident.

7.1.2. Deployment environment

CFRaaSP is deployed in the cloud environment which enables forensic logging and monitoring. Additionally, it becomes a challenge to collect digital evidence for DFR purposes in the cloud because cloud instances are easily destroyed as easily they are created. As a result, the ABS is deployed to the host to "infect" and gather digital information which is then sent to a centralized server for analysis. This helps in planning and preparing for possible security incidents. Martini and Choo[36] have pointed out that data that is generated by the CSPs is important in the analysis of the evidence. It is on this premise that the authors think information from cloud instances can be monitored.

The cloud operating system (OS) acts as an intermediary between the Virtual Machines (VMs) and the physical resources. Hence, the botnet can "infect" the instances to gather digital information. It is worth noting that "infection" carries a positive connotation in this context which is actually collecting PDE for DFR purposes. Physical resources represent application servers, storage or data centers. The authors used a Windows-based environment to conduct this experiment that was connected as a client and a server with Intel® processor Core™ i7 with 3.40GHz with 8.0 GB memory. Windows 8 platform that runs in Intel X86 PC desktop was used and the ABS was developed in a high-level language. C++ was the most preferred language for this environment because of the capacity that it has over networks, components, managing memory, protocols and the efficiency of the CPU. PHP a server side scripting language was used with MySQL as a forensic database.

7.1.3. *Functionality modifications*

In this section, the author revisits the cloud-based botnet in which its functionality has been changed to act as an ABS. The modified functionality allows it to be deployed in the VM in Windows OS of the system, gathers digital information and sends it back to the Command and Control (C&C) server and it periodically checks additional commands from the server. Importantly, the collected information is digitally preserved and used for DFR purposes. The modified botnet that acts as an ABS has the following components: main thread, installer thread, ping thread, key-logging thread, update thread, delete the thread and send data thread. Figure 9 shows the components flow (labeled 1-7) of the modified botnet that runs as an ABS in a single diagram.

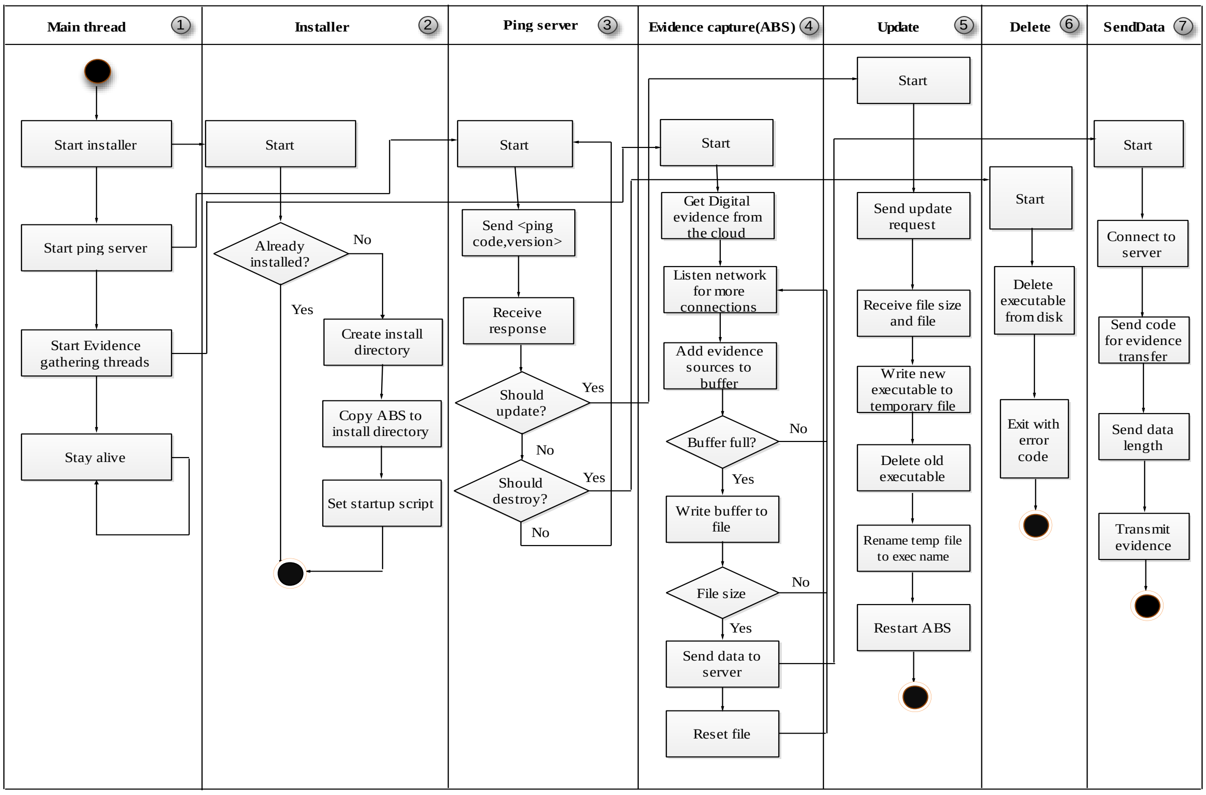


Figure 9. Operational flow of the Agent-Based System[52]

Table 2 shows a summary of each component and its respective description that has been highlighted in Figure 9. The following components that have been labeled from 1-7 have been considered: Main thread, installer, ping server, evidence capture (ABS), update, delete, and sendData.

Table 2. A description of Operation flow components of an evidence gathering ABS[52]

	Component	**Description**
1	**Main Thread**	Starts other threads and keeps the information collecting ABS alive throughout potential evidence collection process.
2	**Installer thread**	Checks if the infection vectors have installed the ABS. If not it installs itself and makes system changes that are needed when the operating system starts up.
3	**Ping thread**	The thread works on a timer which implies that in every *n* minutes the thread contacts the server. When the command is received from the server the ping is able to dispatch to the correct handler for the command sent by the server.
4	**Evidence Capture(ABS)**	The thread starts up when the ABS starts, connects to the network and listens to evidence channels then logs them to a file. After logging and after file reaches a given size the data is transmitted to the server. Thereafter, the file is reset.
5	**Update thread**	Thread starts when the ping is able to receive the update command from the server. It downloads the new version of the ABS, installs it and then it is able to restart itself.
6	**Delete thread**	Starts whenever the ping thread receives the destroy command. This command is able to remove the executable from the disk and kill the ABS by exiting with an error code.
7	**SendData thread**	Responsible for transmitting data gathered by other modules to the server. As a parameter, the thread takes in the data length and a pointer to a byte array of data. It transmits the data length followed by the data to the C&C.

7.1.4. CFRaaSP components

The CFRaaSPs' solution consists of three main parameters namely: Command and Control (C&C) server, the ABS and the execution vector. The C&C is used as a point of issuing commands to the ABS. The ABS in this context constitutes commands that are used to collect digital forensic information. Execution vectors are tasked with deploying the ABS to the target. After "infection" has taken place, the ABS is executed to the host and then initiates communication with the server. Each of the aforementioned parameters has been discussed below.

7.1.4.1. Execution vector

It consists of a bootstrap program that is able to execute inside a host and then installs an executable into the target without the need of modifying the hypervisor thereby the functionality of existing cloud architecture is neither reprogrammed nor modified. It is worth noting that the collected PDE is isolated for secure analysis. The main purpose of executing the ABS is to collect PDE in a forensic readiness approach.

7.1.4.2. Agent-based solution

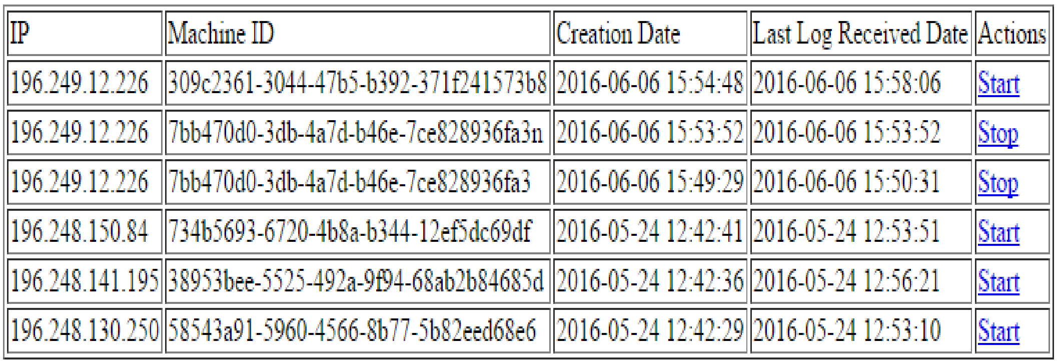
The ABS operates in a non-malicious fashion as an ABS that is used to gather digital information on a specific host. The ABS is propagated to the host by execution vectors via different vulnerabilities. The ABS is able to ping the C&C server periodically for more commands. Nevertheless, during this time, any collected digital information is sent back to the server. Furthermore, the ABS has been built to allow additional information collection modules. As a result, the CFRaaSP implementation is able to handle the power of extensibility multithreading and sharing of resources. Moreover, the ABS is able to maintain other functionality namely: update, get, post and extensibility. All the functionalities are shown in Table 3.

Table 3. Functionality of the ABS[52]

	ABS functionality	Description of functionality
1	**Update**	The ABS is able to update itself via the C&C server when a command is dispatched. This allows the botnet operator to add a new functionality to the ABS.
2	**Get**	The ABS is able to digest digital forensic information through gathering and sends through a post.
3	**Post**	It sends collected digital information back to the server. The structure of interaction depends on the specified information collecting module.
4	**Extensibility**	Allows ease of adding a new functionality to the ABS. The cloud-based ABS should allow the addition of new modules.

7.1.4.3. Command and control server

Once the ABS has been deployed, the C&C is used to listen for incoming connections from ABS that has already been executed in the systems (active ABS). At this instance, the C&C operator issues new commands for execution or saves the PDE that the ABS is sending after collection. In spite of that, the server should be optimised to allow multithreading. Figure 10 shows a C&C server that is used to control the agents. Through the C&C the forensic agents are able to be given more instructions to start harvesting digital forensic information. Figure 10 shows different IP addresses, machine IDs, the day the agents are dispatched and the action. The action is used to start and to stop the "infection" process.



IP	Machine ID	Creation Date	Last Log Received Date	Actions
196.249.12.226	309c2361-3044-47b5-b392-371f241573b8	2016-06-06 15:54:48	2016-06-06 15:58:06	Start
196.249.12.226	7bb470d0-3db-4a7d-b46e-7ce828936fa3n	2016-06-06 15:53:52	2016-06-06 15:53:52	Stop
196.249.12.226	7bb470d0-3db-4a7d-b46e-7ce828936fa3	2016-06-06 15:49:29	2016-06-06 15:50:31	Stop
196.248.150.84	734b5693-6720-4b8a-b344-12ef5dc69df	2016-05-24 12:42:41	2016-05-24 12:53:51	Start
196.248.141.195	38953bee-5525-492a-9f94-68ab2b84685d	2016-05-24 12:42:36	2016-05-24 12:56:21	Start
196.248.130.250	58543a91-5960-4566-8b77-5b82eed68e6	2016-05-24 12:42:29	2016-05-24 12:53:10	Start

Figure 10. Command and Control server

The C&C server comprises of two main threads: The main server thread and the receiver thread. The main server thread listens for incoming connections and then passes them to receiver thread. Whenever an ABS is able to ping the server, the server is able to give relevant commands to the ABS which may be updating, deleting or acknowledging the request. On the other hand, the receiver thread performs operations like reading the ABS requests and checking whether the ABS is able to ping the server. Figure 10 shows the sample C& C control point of the prototype. The main thread server functionalities and the receiver threads are shown in Figure 11.

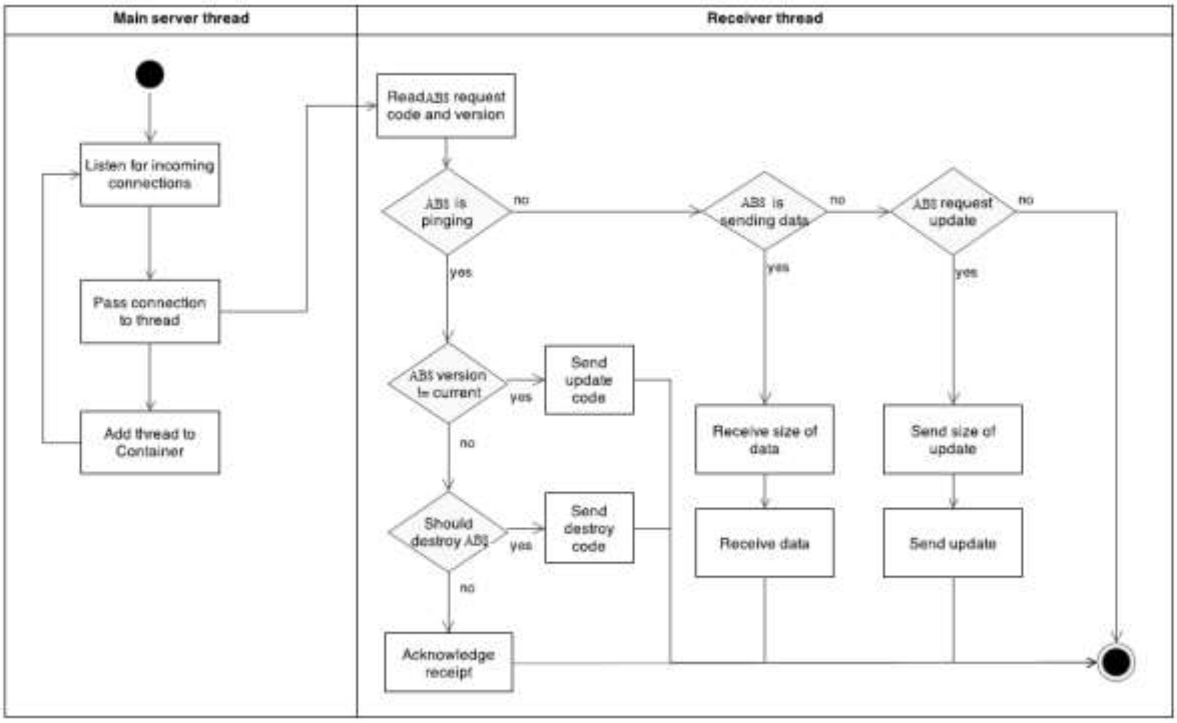


Figure 11. Command and Control server operation flow[52]

7.2. Architecture of the CFRaaSP

The CFRaaSP uses a client-server architecture where the ABS acts as a forensic client. C&C server is used to distribute commands, receive information and to store information. Information is gathered from a virtualized environment where the ABS gathers information that is used as forensic evidence. Figure 12 shows a high-level interaction on how the components in the ABS interact.

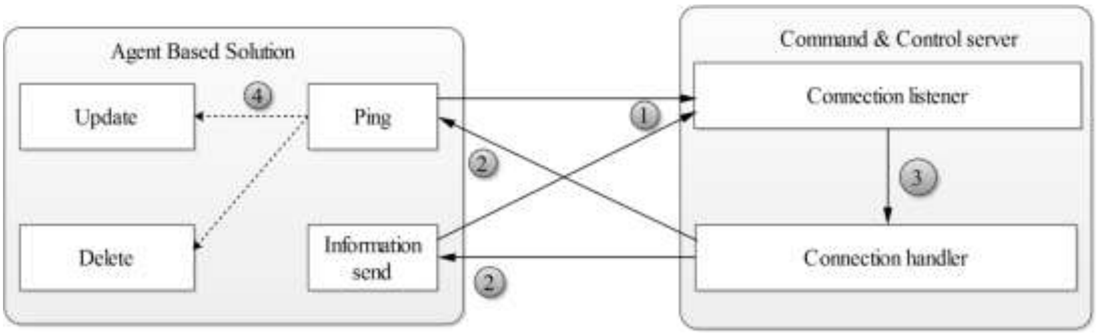


Figure 12. Architecture for CFRaaSP

In the part labelled 1 the ABS connects to the server, once the server receives the connection it passes it to a separate thread that can handle the part labelled 3. After this, the thread is able to dispatch necessary information to the ABS in a form of commands. Thereafter, the ABS component that receives this information is able to pass it to another component. This component may be component labelled 4 if necessary or the delete. For a simple implementation of the CFRaaSP, it is advisable to use third party libraries that provide this functionality.

7.3. Laboratory environment

Various components were availed to set-up an environment for deploying the ABS: A forensic server as a database, C&C center, and physical target clients[52]. This has been shown in Table 4.

Table 4. Experimental set-up

No	Component	Description
	Server	Comprise of a Window-based environment on which the operator uses to send the ABS to harvest digital information periodically. The forensic server is directly connected to the internet.
1	**Forensic Database**	A database is used to receive collected digital information that is being passed by the ABS. This information is passed as possible PDE.
2	**Virtual target**	This is a Linux or Window based VM where the ABS command is executed to collect PDE.
3	**Command & Control**	C&C consist of connection handler and connection listener. It is used to pass commands for infection.
4	**Physical target**	A physical computer where the ABS is simulated as an infection.

To facilitate analysis and management of the processes, events the CFRaaSP is able to perform the following functions:

- Deploy the executable
- Collect PDE
- Transmits collected evidence using openP2P
- Record timestamps
- Hash the collected information
- Posts it back to the server
- Updates the ABS frequently

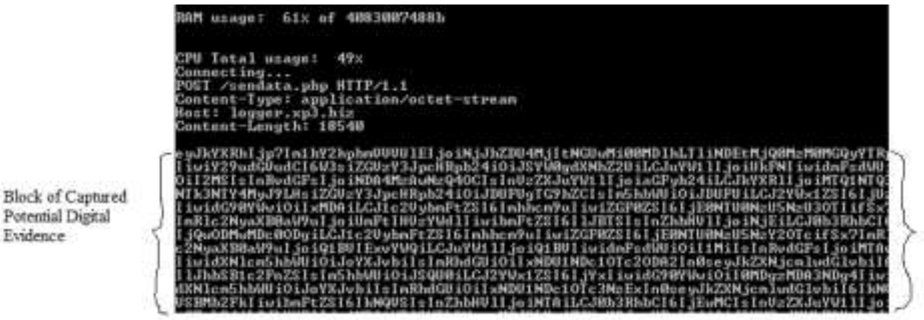
In the next section, the reader is introduced to an overview of the CFRaaSP that is in the discussion.

7.4. CFRaaSP implementation

CFRaaSP is represented as a botnet with modified functionalities that operates as an ABS through the collection of vital digital information for DFR purposes. CFRaaSP is able to monitor activities by recognizing the CPU usage periodically, RAM usage, key-logging and processes. All these processes have been developed in order to help the cloud to be prepared forensically for DFI. It is worth noting that these processes comply with forensic readiness processes that have been highlighted in the ISO/IEC 27043 standard. The CFRaaSP will monitor data in motion and give reports periodically that show respective timestamps. The process is invoked by a forensic administrator and all the collected activities that are associated with digital crimes to enable reconstruction of events that can link a suspect to a given crime.

7.5.Experimental results

Our approach focuses on how digital forensic evidence can be gathered from the cloud environment. The idea behind this experiment is to prepare the cloud forensically for digital investigations. Experimental results presented in this section show that DFR can be achieved in the cloud when an ABS is employed. This could only be achieved through the collection of forensic logs in a proactive process that could monitor the CPU usage, RAM usage, keystrokes and their respective timestamps. These experimental results presented reasonable performances because our implementation and design represented a practical mechanism.



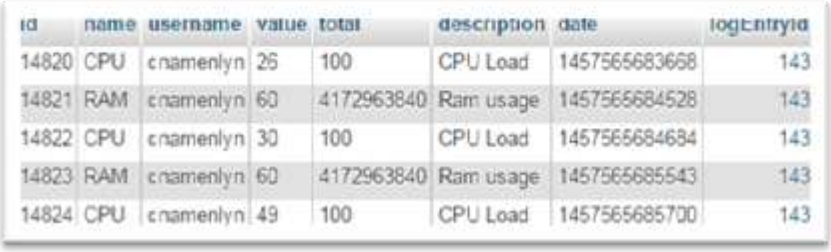
```
RAM usage:  61% of 4083007488b

CPU Total usage:  49%
Connecting...
POST /sendata.php HTTP/1.1
Content-Type: application/octet-stream
Host: logger.xp3.biz
Content-Length: 18540
```

```
eyJkYXRhIjp7Im1hY2hpbmUUUU1EIjoiNjJhZDU4MjItMGUwMi00MDlhLTI1NDEtMjQ0MzM0MGQyYTR
IiwiY29udGUudCI6W3siZGVzY3JpcHRpb24iOiJSYW0gdXNhZ2UiLCJuYW1lIjoiUkFNIiwidmFsdWU
OiI2MSIsInRvdGFsIjoiNDA4MzAwNzQ4OCIsInVzZXJuYW1lIjoiaGFyb24iLCJkYXRlIjoiMTQ1NTQ
NTk3NTY4MyJ9LHsiZGVzY3JpcHRpb24iOiJDUFUgTG9hZCIsIm5hbWUiOiJDUFUiLCJ2YWx1ZSI6IjU
IiwidG90YWwiOiIxMDAiLCJ1c2VybmFtZSI6Imhhcm9uIiwiZGF0ZSI6IjE0NTU0NzU5NzU3OTIifSx
ImRlc2NyaXB0aW9uIjoiUmFtIHVzYWdlIiwibmFtZSI6IlJBTSIsInZhbHVlIjoiNjEiLCJ0b3RhbCI
IjQwODMwMDc0ODgiLCJ1c2VybmFtZSI6Imhhcm9uIiwiZGF0ZSI6IjE0NTU0NzU5NzY2OTcifSx7ImR
c2NyaXB0aW9uIjoiQ1BVIExvYWQiLCJuYW1lIjoiQ1BVIiwidmFsdWUiOiI1MiIsInRvdGFsIjoiMTA
IiwidXNlcm5hbWUiOiJoYXJvbiIsImRhdGUiOiIxNDU1NDc1OTc2ODA2In0seyJkZXNjcmlwdGlvbiI
IlJhbSB1c2FnZSIsIm5hbWUiOiJSQU0iLCJ2YWx1ZSI6IjYxIiwidG90YWwiOiI0MDgzMDA3NDg4Iiw
dXNlcm5hbWUiOiJoYXJvbiIsImRhdGUiOiIxNDU1NDc1OTc3NzExIn0seyJkZXNjcmlwdGlvbiI6IkN
USBMb2FkIiwibmFtZSI6IkNQVSIsInZhbHVlIjoiNTAiLCJ0b3RhbCI6IjEwMCIsInVzZXJuYW1lIjo
```

Figure 13. A block of captured PDE.

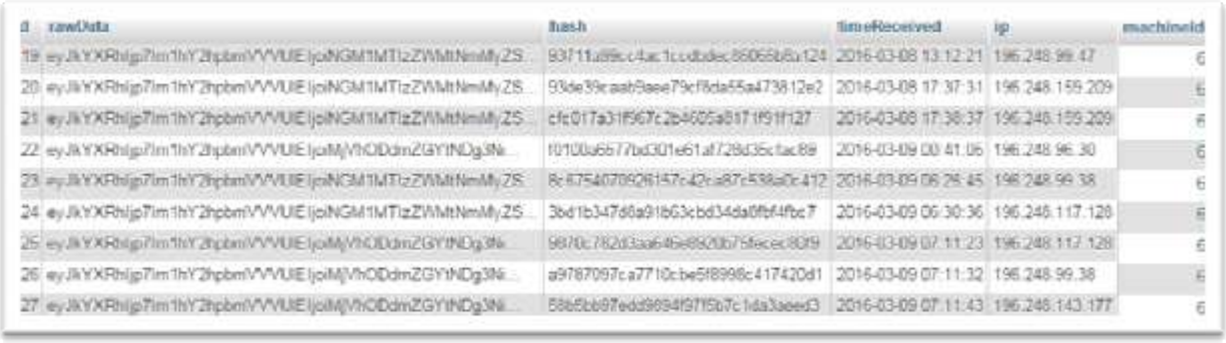
On the one hand, Figure 13 shows a block of PDE that is captured when the ABS is executed. The figure shows the total CPU and RAM usage as captured and any form of replication that may occur. After evidence is captured, it is posted the database using the POST/sendata.php HTTP/1.1 request that is shown in Figure 13 for possible anomaly detection.



id	name	username	value	total	description	date	logEntryId
14820	CPU	cnamenlyn	26	100	CPU Load	1457565683668	143
14821	RAM	cnamenlyn	60	4172963840	Ram usage	1457565684528	143
14822	CPU	cnamenlyn	30	100	CPU Load	1457565684684	143
14823	RAM	cnamenlyn	60	4172963840	Ram usage	1457565685543	143
14824	CPU	cnamenlyn	49	100	CPU Load	1457565685700	143

Figure 14. CPU, RAM and timestamp usage logs posted to the forensic database by the ABS

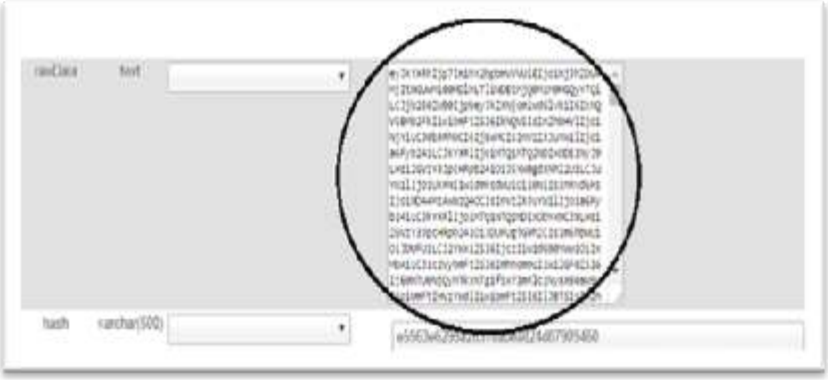
Figure 14, on the other hand, shows a block of log data stored in MySQL database. Also shown is the hash created as a mode of digitally preserving the log, the timestamp, IP address of the forensic client and machine ID.



d	rawData	hash	timeReceived	ip	machineid
19	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	93711a99cc4ac1ccdbdec86066b8a124	2016-03-08 13:12:21	196.248.99.47	6
20	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	93de39caab9aee79cf8da55a473812e2	2016-03-08 17:37:31	196.248.159.209	6
21	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	cfc017a31f967c2b4605a8171f91f127	2016-03-08 17:38:37	196.248.159.209	6
22	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	f0100a6677bd301e61af728d35cfac89	2016-03-09 00:41:06	196.248.96.30	6
23	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	8c6754070926147c42ca87c538a0c412	2016-03-09 06:26:45	196.248.99.38	6
24	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiNGM1MTIzZWMtNmMyZS...	3bd1b347d8a91b63cbd34da0fbf4fbc7	2016-03-09 06:30:36	196.248.117.128	6
25	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	9870c782d3aa646e8920b75fecec8019	2016-03-09 07:11:23	196.248.117.128	6
26	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	a9787097ca7710cbe5f8998c417420d1	2016-03-09 07:11:32	196.248.99.38	6
27	eyJkYXRhIjp7Im1hY2hpbmVVVUlEIjoiMjVhODdmZGYtNDg3Ni...	58b5bb97edd9894f9715b7c1da3aeed3	2016-03-09 07:11:43	196.248.143.177	6

Figure 15. Hash, timestamp, Machine IP address, Machine ID for stored Potential evidence

The raw data that is shown in Figure 15 represents the block of captured PDE that has been posted to the forensic database. This can fully be seen inside a circle of Figure 16 that shows the entire log that can be used as PDE in a DFR approach.

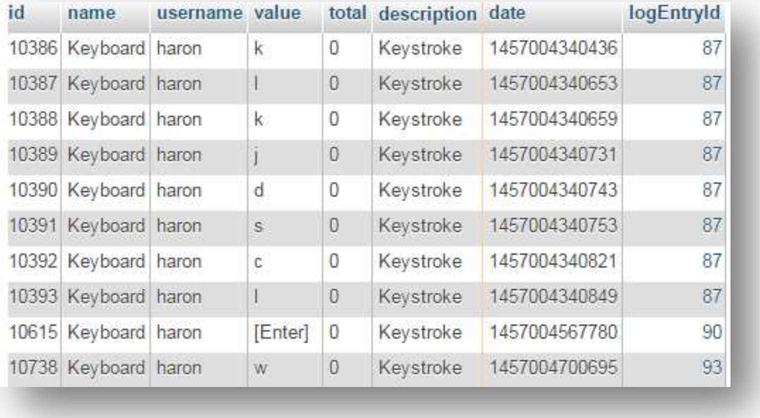


rawData text [illegible]

hash varchar(500) e5563e6299[illegible]2487905450

Figure 16. Sample potential evidence represented as rawData in the database

Notwithstanding that, Figure 16 shows collected PDE after running the ABS solution on a set of clients in the cloud environment when the block of PDE is posted to the forensic database. The timestamp recorded from the report shows 2016-03-13 13.12.21, with IP address 196.248.99.47 which is the IP stored in the forensic database as shown previously in Figure 15. Other system IP addresses that are collected include: 196.248.159.209, 196.248.96.30, 196.248.99.38 and 196.248.117.128 respectively. The report can either be generated using the computer username or IP address as shown in Figure 15. For the sake of this paper, we have generated the report using the computer name, which displays the IP address. Nevertheless, PDE can be extracted based on the date. We used a start date of 2016-02-14 ant time 09:36:00 and an end date as 2016-02-14 12:54:00 and the result are shown using the CPU usage graph.



id	name	username	value	total	description	date	logEntryId
10386	Keyboard	haron	k	0	Keystroke	1457004340436	87
10387	Keyboard	haron	l	0	Keystroke	1457004340653	87
10388	Keyboard	haron	k	0	Keystroke	1457004340659	87
10389	Keyboard	haron	j	0	Keystroke	1457004340731	87
10390	Keyboard	haron	d	0	Keystroke	1457004340743	87
10391	Keyboard	haron	s	0	Keystroke	1457004340753	87
10392	Keyboard	haron	c	0	Keystroke	1457004340821	87
10393	Keyboard	haron	l	0	Keystroke	1457004340849	87
10615	Keyboard	haron	[Enter]	0	Keystroke	1457004567780	90
10738	Keyboard	haron	w	0	Keystroke	1457004700695	93

Figure 17. Forensically captured keystrokes in a readiness approach

Figure 17 highlights the system username; values representing the keys entered representing keystrokes and the timestamp that were collected. Also shown is the log entry ID of the logs that were posted. RAM usage also monitored as a block of digital data, is posted to the forensic database. The RAM graph in Figure 18 has been generated based on the digital data that was previously pushed to the database as shown in Figure 15.

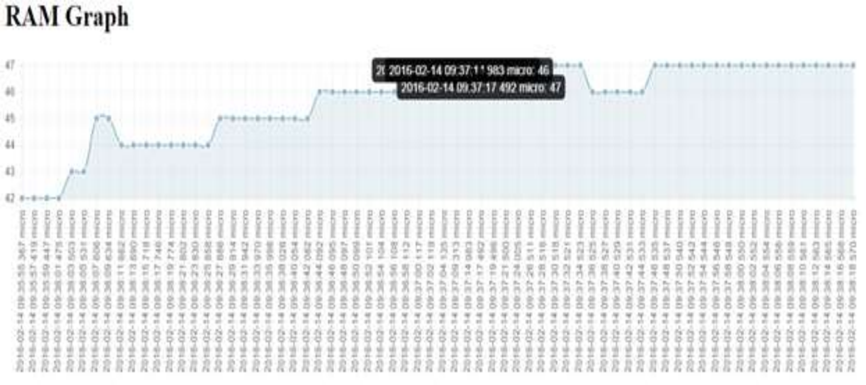
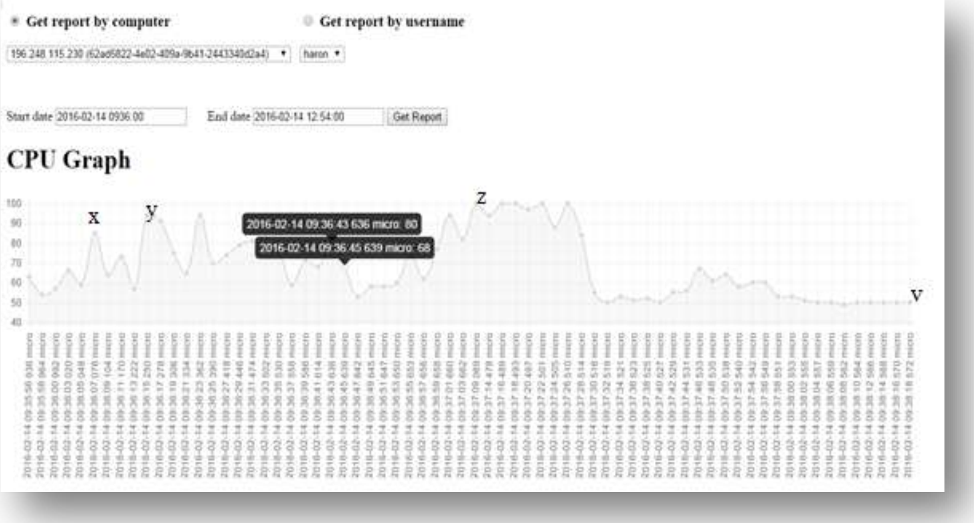


Figure 18. RAM utilization graph

The importance of the graphs that have been presented in Figure 18 and 19 are to monitor if there is any unusual activity that might consume the processor or memory while gathering digital evidence. Respective timestamps are shown in the graph of Figure 19 which shows CPU utilization, this are labeled X, Y, Z, V. For example, the following parameters according to Shropshire [69] might create anomalies in the CPU energy consumption rate: CPU load, memory consumed, network packets received, network packets transmitted, disk reads and disk writes. Based on this premise Figure 18 shows the RAM usage graph report.



● Get report by computer ○ Get report by username

196.248.115.230 (62ad6822-4e02-409a-9b41-2443340d2a4) ▾ haron ▾

Start date 2016-02-14 0936:00 End date 2016-02-14 12:54:00 Get Report

CPU Graph

2016-02-14 09:36:43 636 micro: 80

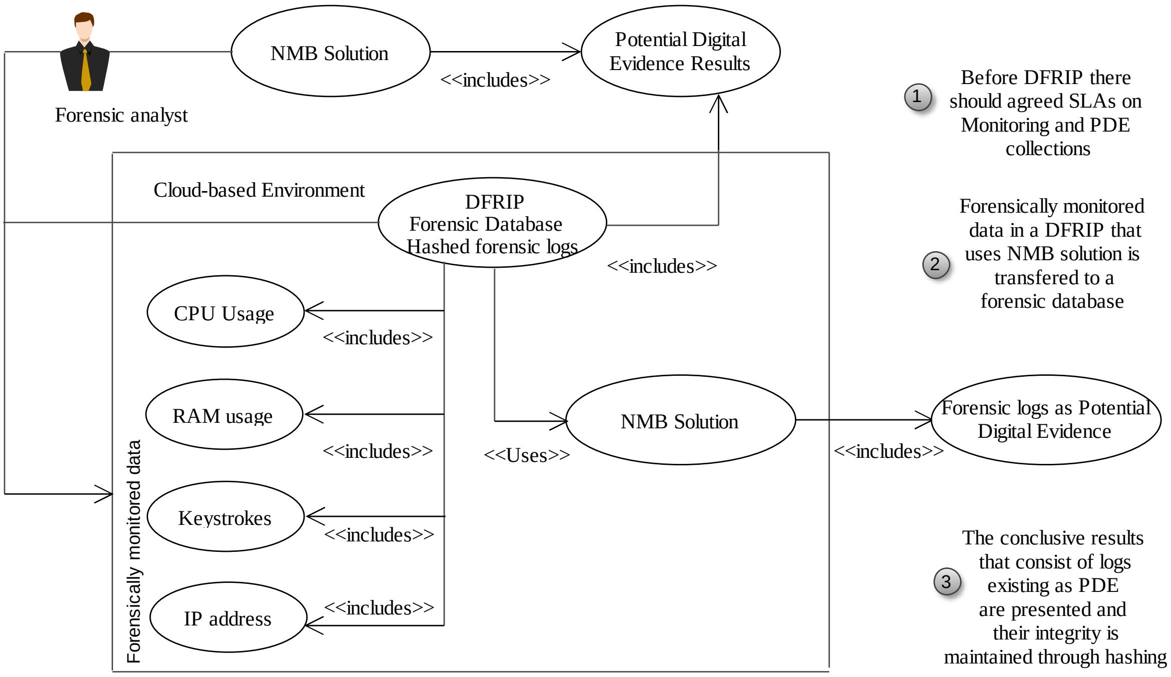
2016-02-14 09:36:45 639 micro: 68

Figure 19. CPU utilization with timestamps graph collected by an ABS solution.

The reader has been introduced to a practical forensic gathering prototype that is able to make the cloud forensically ready for DFI as per the processes that have been defined in ISO/IEC 27043 standard. After collecting PDE, the authors monitored the CPU and RAM overheads that the prototype uses to gather digital evidence from various forensic clients and post it to the forensic database. Also monitored in this aspect is the effect of the tremendous amount of data that is taken into the forensic database after the POST.

8. CFRaaSP Functionalities

In this section, the functionalities of the CFRaaSP that is able to support DFR process in the cloud environment are presented.



Forensic analyst
NMB Solution
<<includes>>
Potential Digital Evidence Results
1
Before DFRIP there should agreed SLAs on Monitoring and PDE collections
Cloud-based Environment
DFRIP
Forensic Database
Hashed forensic logs
<<includes>>
2
Forensically monitored data in a DFRIP that uses NMB solution is transfered to a forensic database
CPU Usage
<<includes>>
RAM usage
<<includes>>
<<Uses>>
NMB Solution
<<includes>>
Forensic logs as Potential Digital Evidence
Keystrokes
<<includes>>
IP address
<<includes>>
Forensically monitored data
3
The conclusive results that consist of logs existing as PDE are presented and their integrity is maintained through hashing

Figure 20. Use-case that shows the functionalities of the CFRaaSP

Currently, CFRaaSP's main focus is to proactively collect digital forensic logs that can be used as PDE in a DFR approach as highlighted in ISO/IEC 27043. The CFRaaSP functionality shows that the inclusivity of other functionalities is possible based on its structure. This has also been described in Section 6 which has discussed extensibility. From Figure 20, before a DFR process can commence there should be a SLA regarding monitoring of personal information for forensic purposes as highlighted in the part labelled 1 on the right- hand side of the CFRaaSP. Digital Forensic Readiness Investigation Process (DFRIP) starts by deploying the ABS to the cloud environment which is then able to collect forensic logs as PDE which consist of the following: CPU usage, RAM usage, keystrokes and user IP address, this data is transferred into a forensic database which is thereafter isolated from the cloud to prevent modifying the functionality of existing cloud architecture this is shown in the part labelled 2. In the final part, the collected PDE's integrity is maintained by creating a block of hashes that can be verified later on during PDE examination and analysis, this is shown in the part labelled 3 of Figure 20.

9. Comparing the CFRaaS Model with existing forensic readiness models

In this section, the authors provide a comparison between the CFRaaS model and existing forensic readiness models. The comparison is aimed at identifying the effectiveness and enhancements through mapping to other existing models. The results of the summary have been presented in Table 5.

Table 5. Comparison of existing models with readiness phases with the proposed Model

	Proposed Model	ISO/IEC 27043:2015[5]	Beebe and Clark[13]	Carrier and Spafford[10]	Baryamureeba & Tushabe[61]
1	**Planning**	Incident detection	Preparation phase	Readiness	Readiness
		First response			
		Planning			
2	**Preparation**	Preparation			
3	**Potential evidence Identification**	Incident scene documentation			
		Identification			
4	**Collection**	Collection	Data collection		
5	**Digital preservation**	Preservation			
6	**Storage**	Evidence storage			
7	**Pre-incident Detection**			Deployment phase	Deployment phase
8	**Pre-Analysis**	Digital evidence analysis	Data analysis	Physical crime investigation	Traceback and Dynamite
9	**Event Reconstruction**				
10	**Forensic Report**	Reporting	Incident	Review	Review Phase

			closure	phase	

Based on the previously proposed models, none of them incorporates all the processes that have been defined in the CFRaaS model. Additionally, at the time of writing this paper, none of the models are focused on the cloud environment. The shaded part of Table 5 shows processes that are not included in the proposed CFRaaS model. ISO/IEC 27043 incorporates most of the CFRaaS processes apart from pre-incident detection and event reconstruction. Beebe and Clarks[13] model has only four processes that are mapped to the CFRaaS. These include Preparation as Planning, Data collection, Data analysis and Incident closure. The CFRaaS model has been mapped to Carrier and Spaffords[10] framework using the following processes: Readiness, deployment phase, Physical crime investigation and Review phase. Lastly, the CFRaaS has been mapped to Baryamureeba and Tushabe's[61] model using the following processes: Readiness, Deployment phase, Traceback and Dynamite and Review phase.

A number of the processes in the CFRaaS model comply with the ISO/IEC 27043 international standard processes although ISO/IEC 27043 is not focused in the cloud either. Furthermore, the authors have introduced event reconstruction process which is hardly mapped to any of the previous models. The role of event reconstruction is to enhance detection process by studying the characteristics of potential evidence. Since there exist no cloud forensic readiness model at the time of writing this paper, the author believes that the order of the processes provided is suitable for supporting future investigative technologies in DFR in the cloud environment. In the next section, the reader is introduced to the critical evaluation of the proposed concept.

10. Critical evaluation of the proposed concepts

Based on the hypothetical scenario presented in Section 1, it is the authors' opinion that if an organisation that lacks adequate forensic readiness policies or methodologies they might not be able to enforce proper post-event response effectively. Furthermore, this might even lead to a compromise in the process of digital investigation. It is, therefore, essential for any organisation to enforce and develop an appropriate forensic readiness approach with a post-incident response process. Having this in place will help in identification of potential incidents and prepare for proper digital investigation process.

The breach experienced in the hypothetical case scenario has shown that Nax.com had vastly insufficient proactive forensic logging, and lack of log correlation methodologies that could help link the suspect to a given crime. The presence of this could have saved company ABC's time and money needed to conduct a digital forensic investigation. Additionally, for proper prosecution in a court of law the provider could have established forensic logging and digital preservation according to the requirements highlighted in ISO/IEC 27043[5], ISO/IEC 23037:2012 [62]and ISO/IEC 10118-2: 2010[63]. On the same note, all systems could have been configured to monitor, record right events and maintain sufficient historical through which digital evidence could have been excavated from.

The CFRaaSP was installed to four target clients each running Windows 8 Operating System and one forensic server as a database. The CFRaaSP had the functionalities of a modified form of a botnet, this allowed collection of digital forensic information as PDE in a constantly changing environment. The CFRaaSP was able to collect a different kind of logs but the main logs were (User IP address, User activities, timestamps, Keystrokes, CPU usage and RAM usage).

The collected PDE is digitally preserved through hashing which is then stored in the database in a sequence that shows the system User IP, processes, User Activities, Timestamps, CPU usage and RAM usage periodically. CPU and RAM usage can be used to monitor anomalous usage of processing power, memory, and a huge amount of data that may be pushed to the cloud. After this process, the collected data is hashed to preserve its integrity. Finally, events are reconstructed as highlighted by Kebande and Venter[52] through correlating evidence that may be ordered by system IP address, time or the process ID's. It is worth noting that the processes employed in this prototype comply with the forensic readiness processes that have been highlighted in the standard of ISO/IEC 27043.

The authors also give a comparison of the approach suggested in this paper with an adversary model for mobile devices that has been proposed by Do, Martini and Choo[64]. In this model the authors are able to construct an adversary model that has physical access to mobile devices using cloud applications. Additionally, the model is able to exploit vulnerabilities by obtaining confidential data from the device (target) with forensic soundness constraint. One capability that appears similar to our approach is corrupting (Target device) and forensic examination (target device, target data). Corrupt which allows an adversary to be able to take the target can be linked to the “infection” of the Non-malicious Botnet (NMB) that acts as an Agent-Based Solution (ABS). Forensic examination (target device)on the other hand that allows locating of artefacts like username, emails, cached files and file metadata is linked with the forensic capturing of potential evidence by the NMB. The NMB is also able to collect, CPU usage processes, RAM usage processes, and keystrokes.

Similarly another adversary model[65] has a root (device) that allows the adversary to be able to get the root access, an intercept (device) for intercepting communication, inject device that allows data to be pushed to the target device. The similarity with our study is that this adversary model has a functionality of conducting forensic analysis that allows forensic examination of a forensic image in order to recover data that is needed[66].Other relevant works that are mapped to our suggested approach include a model for incident handling in the cloud by Ab Rahman and Choo[67] and cloud incident handling and forensic that is focused to mobile networks and applications.

To ensure legal compliance with regard to monitoring and admissibility of digital forensic evidence, a number of Acts have been proposed. For example in the USA, Rule 702 of the federal Rule of Evidence provides a requirement for introducing the expert witness testimony. Additionally, Rule 702 was amended in response to Daubert v. Merrel Dow Pharmaceuticals, Inc. It states that “If scientific, technical or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training or education, may testify thereto in the form of an opinion or otherwise[68]”. On the same note, research on jurisdiction has shown that it is important for the Law Enforcement Agencies (LEA) to have harmonious laws that can assist them across diverse jurisdiction according to Hooper, Martini, and Choo[71]. Nevertheless, on regulation and governance, Choo[72] has highlighted that it is important to determine the law of jurisdiction where the SLA exists. Additionally, at a given time if there is matters of interest like “national security” the CSPs may be obliged to monitor, search and report on these data depending on the law of jurisdiction where the physical machine lies[73].

Our pictured approach has some drawbacks; firstly, implementing the CFRaaSP prototype is faced by a huge, complex and tremendous size of data that jets in large volumes. Even though the back-end storage is able to create a relational database to cater for this data, lack of enough storage might affect the provenance of the data object. To add to that since our study is based on a hypothetical scenario, the study may also be limited to a private cloud environment and to an evaluation based on the fictitious scenario that has been highlighted previously (see Section 1).

Based on the proactive forensic readiness approach that has been proposed in the CFRaaS model the cost of performing a DFI is minimized. Nevertheless, availability and quality of PDE is enhanced. These aspects correspond to the objectives of forensic readiness as highlighted by Tan[11]. Having provided the critical evaluation in the next section a conclusion and future work is presented.

11. Conclusion and Future Work

The main aim of this paper was to propose DFR techniques in the cloud environment that an organisation can undertake in order to prepare for post-event response process. The results that have been portrayed in Figure 9-20 have illustrated that the CFRP successfully performed forensic logging. Furthermore, in this paper, we have presented a development, implementation, and evaluation of forensic readiness techniques. The most significant findings identified include: The CPU graph and RAM graph could change depending on the activity being conducted in the system and this could help in anomaly detection. The authors presented a high-level model of the CFRaaS model which was then followed by the requirements needed in order to achieve DFR in the cloud environment. Thereafter, the design guidance was given and a prototype that demonstrated different ways through which digital forensic data may be gathered from the cloud environment.

The all newly proposed DFR techniques have consistently been able to collect digital forensic information that could be used for forensic readiness purposes. Consequently, based on the test data that was used to perform the attack tests, a number of results we able to be streamed in as shown in the CPU and RAM utilization graphs. The ability of the ABS to track system processes in real-time enables a proper understanding of new computer network attacks. Additionally, a CFRaaSP was introduced which was able to capture digital information in a forensic readiness approach. Furthermore the ability to hastily establish which processes and forensic logs that are affected will reduce the time needed to perform a DFI if a security incident is detected. This allows quicker post-event response processes.

Since our prototype only stores course-grained PDE, in future, we would like to develop a mechanism that can allow the storage of fine-grained digital evidence and also to develop computation mechanism that may solve the drawback of the collection of enormous forensic data.

Acknowledgement

Firstly, many thanks go to the editor for the important feedback. Secondly, the constructive feedback given by the anonymous reviewers is highly acknowledged. We gratefully acknowledge the support of Department of Computer Science, and the Information and Computer Security Architectures (ICSA) Research group, University of Pretoria, South Africa. It is worth noting that any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of NRF or any organization that the authors are associated with.

Disclosure statement

No potential conflict of interest was reported by the authors

Funding

The work was supported by National Research Foundation [Grant number UID85794]

References

1. IDC(2015). IDC's Top 10 Technology Predictions for 2015. http://sdtimes.com/idcs-top-10-technology-predictions-2015/
2. UC(2014). US Cybercrime: Rising risks, reduced readiness key finding from the 2014 US State of Cybercrime Survey.
3. Dykstra J, Sherman, AT. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, *9*, 2012; S90-S98.
4. Zawoad S, Hasan R.. I have the proof: Providing proofs of past data possession in cloud forensics. In *Cyber Security (CyberSecurity), 2012 International Conference on* 2012; (pp. 75-82). IEEE.
5. ISO/IEC 27043: Information technology -- Security techniques -- Incident investigation principles and processes.[online]-Accessed at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44407**.** 2015.
6. FBI(1984), Computer Analysis and Response Team (CART), Available from: https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf
7. Palmer G. A Road Map for Digital Forensic Research. Technical Report DTRT0010-01, DFRWS. Report for the First Digital Forensic Research Workshop (DFRWS). 2001.
8. Politt MM. Six blind men from Indostan. Digital forensics research workshop (DFRWS); 2004.
9. Carrier B, Spafford EH. Getting physical with the digital investigation process. International Journal of digital evidence. 2003 Sep;2(2):1-20.
10. Tan J. Forensic readiness. Cambridge, MA:@ Stake. 2001 Jul 17:1-23.
11. Rowlingson R. A ten step process for forensic readiness. International Journal of Digital Evidence. 2004; 2(3):1-28.
12. Beebe NL, Clark JG. A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation. 2005 Jun 30;2(2):147-67.
13. Casey E. Digital evidence and computer crime. San Diego, Calif. 2000:207-29.
14. SWGDE. Scientific Working Group on Digital Evidence. Available from: http://www.oas.org/juridico/spanish/cyb_best_pract.pdf, 2006.
15. Carrier BD, Spafford EH. Categories of digital investigation analysis techniques based on the computer history model. digital investigation. 2006 Sep 30;3:121-30.
16. ACPO. Association of Chief Police Officers. ACPO Good Practice Guide for Digital Evidence. Available from: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf. 2012.
17. Gartner Gartner prediction. Available from: http://www.gartner.com/newsroom/id/3188817. 2016.
18. Almorsy M, Grundy J, Ibrahim AS. Collaboration-based cloud computing security management framework. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on* 2011; pp. 364-371. IEEE.

19. Mell P, Tim G. The NIST definition of cloud computing. (2011): 20-23.
20. Kebande VR, Venter HS. A cognitive approach for botnet detection using Artificial Immune System in the cloud. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2014a Third International Conference on*, 2014; p. 52-57. IEEE.
21. Kebande VR, Venter HS. A Cloud Forensic Readiness Model Using a Botnet as a Service. In *The International Conference on Digital Security and Forensics (DigitalSec2014)* 2014b; p. 23-32. The Society of Digital Information and Wireless Communication.
22. Banday M, Tariq JA, Qadri, Nisar AS. Study of Botnets and their threats to Internet Security." *Working Papers on Information Security* (2009).
23. EnCase Forensic v7, "“Guidance software," 2015[online]. Available: https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
24. AccessData: Forensic Toolkit(2015): Recognized around the World as the Standard Digital Forensic Investigation Solution [online]: Available: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk.
25. Internet Evidence Finder, 2015.[online].Available: http://www.magnetforensics.com/internet-evidence-finder
26. NIST Information Technology Laboratory Computer Forensic Tool Testing Program. Available from: http://www.cftt.nist.gov/
27. Reddy K, Venter HS. The architecture of a digital forensic readiness management system. *Computers & Security*, *32*, 2013; pp73-89.
28. Gummadi R, Balakrishnan H, Maniatis P, Ratnasamy S. Not-a-Bot: Improving Service Availability in the Face of Botnet Attacks. In *NSDI* Vol. 9, 2009; p. 307-320.
29. Garfinkel T, Pfaff B, Chow J, Rosenblum M, Boneh D. Terra: A virtual machine-based platform for trusted computing. In *ACM SIGOPS Operating Systems Review* Vol. 37, No. 5, 2003; p. 193-206. ACM.
30. Quick D, Choo KKR. Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?. *Digital Investigation*, *10*(3), 2013; p. 266-277.
31. Martini B, Choo KKR. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, *9*(2), 2012; p. 71-80.
32. Dykstra J, Sherman AT. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, *10*, 2013; S87-S95.
33. Quick D, Choo K-K R. Google Drive: Forensic analysis of data remnants. Journal of Network and Computer Applications, 40, 2014; p.179-193.
34. Quick D, Choo K-K R. Impacts of increasing volume of digital forensic data: A survey and future research challenges. Digital Investigation,11(4), 2014; p 273-294.
35. Martini B, Choo K-K R. Remote programmatic vCloud forensics: a six-step collection process and a proof of concept. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on 2014; p. 935-942). IEEE.
36. Martini B, Choo KKR. Cloud storage forensics: ownCloud as a case study. *Digital Investigation*, *10*(4), 2013; p. 287-299.
37. Rahman ANH, Choo KKR. A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 2015; p. 45-69.
38. Wen Y, Man X, Le K, Shi W. Forensics-as-a-service (faas): computer forensic workflow management and processing using cloud. In *The Fifth International Conferences on Pervasive Patterns and Applications*, 2013; (pp. 1-7).

39. Westphal F, Axelsson S, Neuhaus C, Polze A. VMI-PL: A monitoring language for virtual platforms using virtual machine introspection. *Digital Investigation*, *11*, 2014; S85-S94.
40. Ahmad I, Abbas H, Asad Raza, Choo K.K.K , Sajid A, Pasha M & Aslam F.K (2016): Electronic crime investigations in a virtualised environment: a forensic process and prototype for evidence collection and analysis, Australian Journal of Forensic Sciences.
41. Ab Rahman, N. H, Cahyani, N. D. W, & Choo, K-K R. Cloud incident handling and forensic-by-design: cloud storage as a case study, 2016; *Concurrency and Computation: Practice and Experience*.
42. Cahyani, N. D. W., Martini, B., Choo, K-K R and Al-Azhar, A.K.B.P. Forensic data acquisition from cloud-of-things devices: windows Smartphones as a case study, 2016; *Concurrency and Computation: Practice and Experience*.
43. Daryabar, F., Dehghantanha, A., & Choo, K-K. R. Cloud storage forensics: MEGA as a case study, 2016; *Australian Journal of Forensic Sciences*, 1-14.
44. Daryabar D, Dehghantanha A, Eterovic-Soric B and Choo K-K R 2016. Forensic Investigation of OneDrive, Box, GoogleDrive and Dropbox Applications on Android and iOS Devices. Australian Journal of Forensic Sciences 48(6): 615–642 .
45. Shariati M, Dehghantanha A, and Choo K-K R. SugarSync forensic analysis. *Australian Journal of Forensic Sciences*, 2016; *48*(1), 95-117.
46. Martini B, Do Q and Choo K-K R 2015. Mobile cloud forensics: An analysis of seven popular Android apps. In Ko R and Choo K-K R, editors, Cloud Security Ecosystem, pp. 309–345, Syngress, an Imprint of Elsevier
47. Shariati M, Dehghantanha A, Martini B and Choo K-K R 2015. Ubuntu One Investigation: Detecting Evidences on Client Machines. In Ko R and Choo K-K R, editors, Cloud Security Ecosystem, pp. 429–446, Syngress, an Imprint of Elsevier.
48. Kebande, V, Ntsamo, H. S, & Venter, H. S. Towards a Prototype for Achieving Digital Forensic Readiness in the Cloud Using a Distributed NMB Solution. In *ECCWS2016-Proceedings for the 15th European Conference on Cyber Warfare and Security* (p. 369), 2016; Academic Conferences and publishing limited.
49. Kebande VR, Venter HS. Adding event reconstruction to a Cloud Forensic Readiness model. In Information Security for South Africa (ISSA), 2015a Aug 12 (pp. 1-9). IEEE.
50. Kebande VR, Venter HS. A Functional Architecture for Cloud Forensic Readiness Large-scale Potential Digital Evidence Analysis. In *Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015* (p. 373). Academic Conferences Limited, 2015c.
51. Kebande VR, Venter HS. On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges. *Australian Journal of Forensic Sciences*-(2016b):1-30.
52. Kebande VR, Venter HS. Towards a Model for Characterizing Potential Digital Evidence in the Cloud Environment during Digital Forensic Readiness Process. In *Iccsm 2015d-The Proceedings of the 3rd International Conference on Cloud Security and Management*. Academic Conferences Limited, 2015b.
53. Kebande VR, Venter HS. Obfuscating a Cloud-Based Botnet Towards Digital Forensic Readiness. In *Iccws 2015c-The Proceedings of the 10th International Conference on Cyber Warfare and Security* (p. 434). Academic Conferences Limited, 2015.
54. Kebande VR, Venter HS. Requirements for Achieving Digital Forensic Readiness in the Cloud Environment Using an NMB Solution. In11th International Conference on

Cyber Warfare and Security: ICCWS2016 2016a Jan 1 (p. 399). Academic Conferences and publishing limited.

55. Gong, C., Liu, J., Zhang, Q., Chen, H., & Gong, Z. (2010, September). The characteristics of cloud computing. In *2010 39th International Conference on Parallel Processing Workshops* (pp. 275-279). IEEE.
56. Risk equation. International Charter: Available from: http://www.icharter.org/articles/risk_equation.html
57. CSIRT. Computer Security Incident Response Team.Available from: https://www.csirt.org/
58. Bevel T, Gardner RM. Bloodstain pattern analysis with an introduction to crime scene reconstruction. CRC Press; 2008 Apr 8.
59. Carrier BD, Spafford EH. Defining event reconstruction of digital crime scenes. Journal of Forensic Science. 2004 Nov 1;49(6):JFS2004127-8.
60. Valjarevic A, Venter HS. Introduction of concurrent processes into the digital forensic investigation process. Australian Journal of Forensic Sciences (2015): 1-19.
61. Baryamureeba V, Tushabe F. The enhanced digital investigation process model. InProceedings of the Fourth Digital Forensic Research Workshop 2004 Aug 7 (pp. 1-9).
62. ISO/IEC 27037:(2012). Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.[online], Accessed at http://www.iso.org/iso/catalogue_detail?csnumber=44381
63. ISO/IEC 10118-2□2010)Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher.[online]-Available from:
64. Do, Q., Martini, B., & Choo, K. K. R. (2015). A forensically sound adversary model for mobile devices. *PloS one*, *10*(9), e0138449.
65. Azfar, A., Choo, K. K. R., & Liu, L. (2016, January). An Android Social App Forensics Adversary Model. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5597-5606). IEEE.
66. Ab Rahman N H and Choo K-K R 2015. Integrating digital forensic practices in cloud incident handling: A conceptual cloud incident handling model. In Ko R and Choo K-K R, editors, Cloud Security Ecosystem, pp. 383–400, Syngress, an Imprint of Elsevier
67. Cahyani N D W, Ab Rahman N H, Glisson W B and Choo K-K R. Cloud incident handling and forensic-by-design: Cloud storage as a case study. Mobile Networks and Applications[In Press]
68. Feldman, Elliott R., and Esquire Cozen O'Connor. *Criteria for admissibility of expert opinion testimony under daubert and its progeny*. Tech. rep, Cozen OConnor, 2001.
69. Shropshire J. Securing Cloud Infrastructure: Unobtrusive Techniques for Detecting Hypervisor Compromise. InICCSM2015-3rd International Conference on Cloud Security and Management: ICCSM2015 2015 Oct 1 (p. 86). Academic Conferences and publishing limited.
70. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44737
71. Hooper, C., Martini, B., & Choo, K. K. R. (2013). Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, *29*(2), 152-163.
72. Choo, K. K. R. (2010). Cloud computing: challenges and future directions. *Trends and Issues in Crime and Criminal justice*, (400), 1.

73. Gellman R., (2009). Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf