CeFF: A FRAMEWORK FOR FORENSICS ENABLED CLOUD INVESTIGATION

MD ABDUL MAJED PRAMANIK

M.Phil.

2017

CeFF: A FRAMEWORK FOR FORENSICS ENABLED CLOUD INVESTIGATION

MD ABDUL MAJED PRAMANIK

A thesis submitted in partial fulfilment of the requirements of the School of Architecture, Computing, and Engineering, University of East London for the degree of Master of Philosophy

August 2017

Declaration

“I hereby certify that this dissertation has been composed by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree. This project was conducted by me at The University of East London towards the fulfillment of the requirements of the University of East London for the degree of MPhil under the supervision of Dr Shareeful Islam.”

Date: 31/08/2017 Signature: Md. Abdul Majed Pramanik

Abstract

Today, cloud computing has developed a transformative model for the organization, business, governments that brings huge potentials and turn into popular for pay as you go, on-demand service, scalability and efficient services. However, cloud computing has made the concern for forensic data because of the architecture of cloud system is not measured appropriately. Due to the distributed nature of the cloud system, many aspects relating to the forensic investigation such as data collection, data storage, crime target, data violation are difficult to achieve. Investigating the incidents in the cloud environment is a challenging task because the forensics investigator still needs to relay on the third party such as cloud service provider for performing their investigation tasks. It makes the overall forensic process difficult to complete with a duration and presented it to the court. Recently, there are some cloud forensics studies to address the challenges such as evidence collection, data acquisition, identifying the incidents and so on. However, still, there is a research gap in terms of consistency of analysing forensic evidence from distributed environment and methodology to analyse the forensic data in the cloud.

This thesis contributes towards the direction of addressing the research gaps. In particular, this work proposes a forensic investigation framework CeFF: A framework for forensics enabled cloud investigation to investigate evidence in the cloud computing environment. The framework includes a set of concepts from organisational, technical and legal perspectives, which gives a holistic view of analysing cybercrime from organisation context where the crime has occurred through technical context and legal impact. The CeFF also includes a systematic process that uses the concept for performing the investigation. The cloud-enabled forensics framework meets all the forensics related requirement such as data collection, examination, presents the report, and identifies the potential risks that can consider while investigating the evidence in the cloud-computing environment. Finally, the proposed CeFF is applied to a real-life example to validate its applicability. The result shows that CeFF supports analysing the forensic data for a crime occurred in cloud-based system in a systematic way.

Dedication

To my wife- Shahida and son- Zoreez

For your unconditional sacrifice and support…

I thank you

Acknowledgement

My experience as a research student at the University of East London has been amazing, and there are many people to thank for that.

I would like to thank my supervisor Dr Shareeful Islam in the School of Architecture, Computing, and Engineering for his encouragement, advise, and valuable hint helped me throughout the time of researching and writing my thesis.

I would like to thank my all university staffs who have directly or indirectly helped me during my study.

Thank you also to Dr Rajib, Mr Shafi and Mrs Fatema for their support during my study.

Finally, I deeply grateful to my wife Shahida and my son Zoreez, for being patient, encouragements, sacrifices and supporting me throughout my study.

Table of contents

Lists of Figures

Abbreviations

CeFF	Cloud Enabled Forensic Framework
CSP	Cloud Service Provider
FMP	Forensic Monitoring Plane
VM	Virtual Machine
TCP	Transmission Control Protocol
RAM	Random Access Memory
API	Application Program Interface
OS	Operating System
DDoS	Distributed Denial of Service
SLA	Service Level Agreement
TET	Transparency Enhancing Technology
MAC	Media Access Control
DBaaS	Database as a Service

Chapter 1

Introduction

1. Introduction

The development of advanced technology such as cloud computing conciliates enormous potentials to fulfil the dream called as “utility computing” for the business, and organisations. It promises a pay-as-go system, on-demand services, scalability, and instance access features for the research community and the business to execute their scientific complex data. In the cloud system, data execution and streaming is constantly on-going process by using the application domains, i.e. healthcare system, embedded system, sensor networks, and financial system. The information that distributed such systems is provided by the heterogeneous sources ranging from other systems to individual system that treated by the number of transitional agents. The diversity of information sources precipitates the significant of data provenance to investigate the forensic data in obtaining the evidence. In this circumstances, data provenance is an effective process to contemplate for evaluating data, particularly in cloud forensics.

On the other hand, cloud forensics is a process to recognise and search digital objects for investigations in order to facilitate in a court or to organizations internal investigation in the cloud environments. In 2001, digital forensics defines by the palmer (Palmer, 2001) in DFRWS as follows: *“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and preservation 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”.* Ruan et al. (Ruan et al., 2011a) proposed that cloud forensic is a interaction between the cloud actors in order to provide the investigations both internally and externally that comprises a hybrid forensic approach in the multitenant situations.

While cloud computing conciliates the enormous potential to the organisations, however, there is a huge risk of depredation due to the unsolidified character of digital information in cloud computing environments. So far, cloud forensics are newly established in the research area. It assists to the forensic investigators to identify, collect and analyse the forensic data on the cloud in order to present in a judicial of law or the company’s internal investigations. However, the cloud forensics investigation process is completely depending on the tools and methods to attain the accurate result of forensic data. The main challenges are conquering the evidence which is not feasible due to the extensive of complex data that is generally unattainable for forensics investigators in the cloud system.

There is an essential requirement for both technical and practical cloud forensics answers as criminals who are using the cloud technology in different ways to expedite the illegal activities such as unauthorised access, system modification and data access. In this research, we develop a comprehensive CeFF (Cloud Enabled Forensics Framework) framework in order to produce efficient and effective forensic data in the cloud.

1.2 Motivation

Today, Cloud computing is emerged into the IT sector along with huge capabilities and potential that modernised to the organisation and government. The development of the cloud system is distributing the IT services efficiently and effectively than before. The radical expansion of such technologies and prolong capabilities; data sharing, distributed computation, collaborations are being offered by W3 (World Wide Web) for science, industry, organisation and society. In the cloud environment, users have exchanged data while communicating with many parties online. Cyber-attacks and malicious activities are taking place constantly. The vulnerable data includes crucial data such as user ID, passwords, account no etc. is the target to the attackers which is security concerns in the cloud system. The cyber-crimes are not limited to any users, organisations or companies. There are many incidents comprised of foreign computer systems which is crucial during the investigation. However, digital evidence is gradually becoming more important to an organization, business and government to keep their resources which can minimise the physical storage. But dealing with digital evidence is very challenging tasks in the cloud system. On the other hand, most of the time, digital evidence can be altered, modified or deleted by the malicious people or inappropriate investigation. Also, cloud computing is a nature of a distributed manner, it is quite difficult to access and obtained digital evidence from a cloud system. Because data is stored in a different country or different data centre which is another challenge in the cloud environment. To examine and analyse digital forensics evidence, the investigators are always dependant on the cloud service provider. Typically, the aspects of forensic investigation in the cloud system is ignored by the research community. Beebe et al. (Beebe, 2009) defines that "[...] *to our knowledge, no research has been published on how cloud computing environments affect digital artefacts, and on acquisition logistics and legal issues related to cloud computing environments"*. Therefore, it is essential an appropriate method that permits the investigators to do the investigation flexibly and formally in the forensic investigation. Processing, collecting evidence is crucial before presenting the report in the court. Therefore, there is a necessity to develop a framework that can meet all the requirement such as data collection, examination and present the report and identify the potential risks that can consider while investigating the evidence.

1.3 Problem statement

Cloud attracts organisation of any size and type, but security and trust are one of the main concerns. Many of the security attacks are novel and unique to clouds. Therefore forensic investigation is necessary not an option for the business using the cloud to meet its objective. Cloud computing and its impact on digital forensics will continue to grow. However, tradition forensic investigation process inadequate for any investigation that necessary for cloud-based infrastructure. NIST (Kent et al., 2006a) and McKemmish (McKemmish, 1999) have introduced forensics framework that emphases the preservation, collection, presentation, and analysis of digital evidence but there are challenges for executing forensics investigation in cloud environments such as:

- Extracting and availability of any evidences for cybercrime within cloud context, in particular in a distributed in a cloud environment. This could be very difficult to obtain forensic evidence.

- Once the evidence are collected, analysing those evidence in the cloud are very difficult because different cloud users have different formats and different applications which are challenging in the cloud context. As a consequence, there is the inconsistency of analysing the evidence.

- The complexity of testimony. All the technical information of the acquisition is almost unlikely to be understood by the court where the jury consists of people with only the basic knowledge in a computer system. Thus the evidence should be presented carefully, and the expert witness testimony should be understood by the jury which is an important issue towards the progress of the trial.

Various researchers (Birk and Wegener, 2011, Ruan et al., 2013, Martini and Choo, 2012, Thethi and Keane, 2014) have offered various frameworks, models, however there is no strong research in cloud forensics to identify and extract the unique digital objects of when, how and where can be found. In a sense cloud computing makes forensic harder. The reasons are users data is controlled by a CSP which is not known to the users, it is hard to get digital evidence and control of the evidences from cloud infrastructure even with a subpoena since the evidence depends on different cloud service models. Moreover, different cloud service providers are followed by different methods in the cloud computing and missing terms in SLA for the user to investigate if there is an incident. It is also difficult to segregate data in a multi-tenancy environment.

1.4 Research Questions

The following research questions have been designated for this research to achieve the objectives in the cloud computing domain. We summarise the following questions:

RQ1. How can a relevant forensics data be collected while conducting a digital forensics investigation in cloud domain?

RQ2. How forensics enabled system can be developed in order to investigate forensic evidence in cloud-based environment?

RQ3. What are the different crimes for the cloud-based system?

1.5 Research Aims and Objectives

It is a challenging task to identify and collect digital evidence from a cloud computing environment. The main aim of our research is to develop a novel comprehensive framework to investigate forensics data in a coherent way which can identify and collect digital evidence from a cloud environment. These aims are further elaborated in the following objectives below. These objectives are based on their relative importance towards achieving the overall research goal.

RO1. Conduct existing frameworks and address the issues related to forensic investigation.

RO2. Develop a conceptual framework and representation to improve the forensic investigation process effectively and efficiently in the cloud environment. The framework will include a number of related concept and process for this purpose.

RO3. To resolve multi-jurisdiction and multi-tenancy complications in collecting forensics data that meet technical and legal requirements for acceptance in court and scales correctly for a cloud computing environment.

RO4. Validate the framework through real-life case studies.

1.6 Research Contributions

In responding to the questions, the research develops a comprehensive framework that effectively and efficiently satisfies those problems while collecting the forensics data in the cloud. The novel contributions of this research are:

RC1. Examine and analyse the cloud forensics challenges, limitations, and problems of state of the art with respect to forensics data in particularly collecting information in the cloud.

RC2. Facilitate the forensics capabilities that collect the information on the cloud that enhances the traceability of events performed by the user in the cloud system.

RC3. Identify all forensics evidence that enhanced with related artefacts from various sources from the cloud computing environment. It could be confirmed and validated evidences that are been collected in forensically sound condition.

RC4. The framework meets technical and legal requirements for acceptance in court and scales correctly for a cloud computing environment.

1.7 Structure of the thesis

The structure of the rest of the report is as follows.

Chapter 1 we concentrated the scope and problem definition, motivation and the main contribution of this research.

Chapter 2 describes the theoretical background & state of the art which provides background information about digital forensics in cloud computing. It explained the digital forensics processes, especially in the cloud domain. Existing framework and models are proposed by other researchers in conducting digital forensics as well as challenges are encountered while conducting digital forensics investigation.

Chapter 3 describes the research methodology. This chapter is articulated an appropriate methodology and framework for the proposed research. This research method is mainly provisioned on descriptive, concepts and process model in order to investigate forensics data and describe how this research evaluate the proposed methodology.

Chapter 4 describes the cybercrime and the legal requirements and also describes the crime challenges in terms of a forensics investigation.

Chapter 5 describes the CeFF framework concepts are presented with Meta-model that shows the relationships between the concepts.

Chapter 6 describes the proposed methodology in particular activities included in the process is described. These understand the crime contexts, understand the evidence, identify the risks and identify the forensics actions.

Chapter 7 describes the evaluation of this research and conducted case studies to validate the proposed framework, in chapter 8, concludes and future directions are discussed.

The below figure 1.1 depicts the thesis organisation.

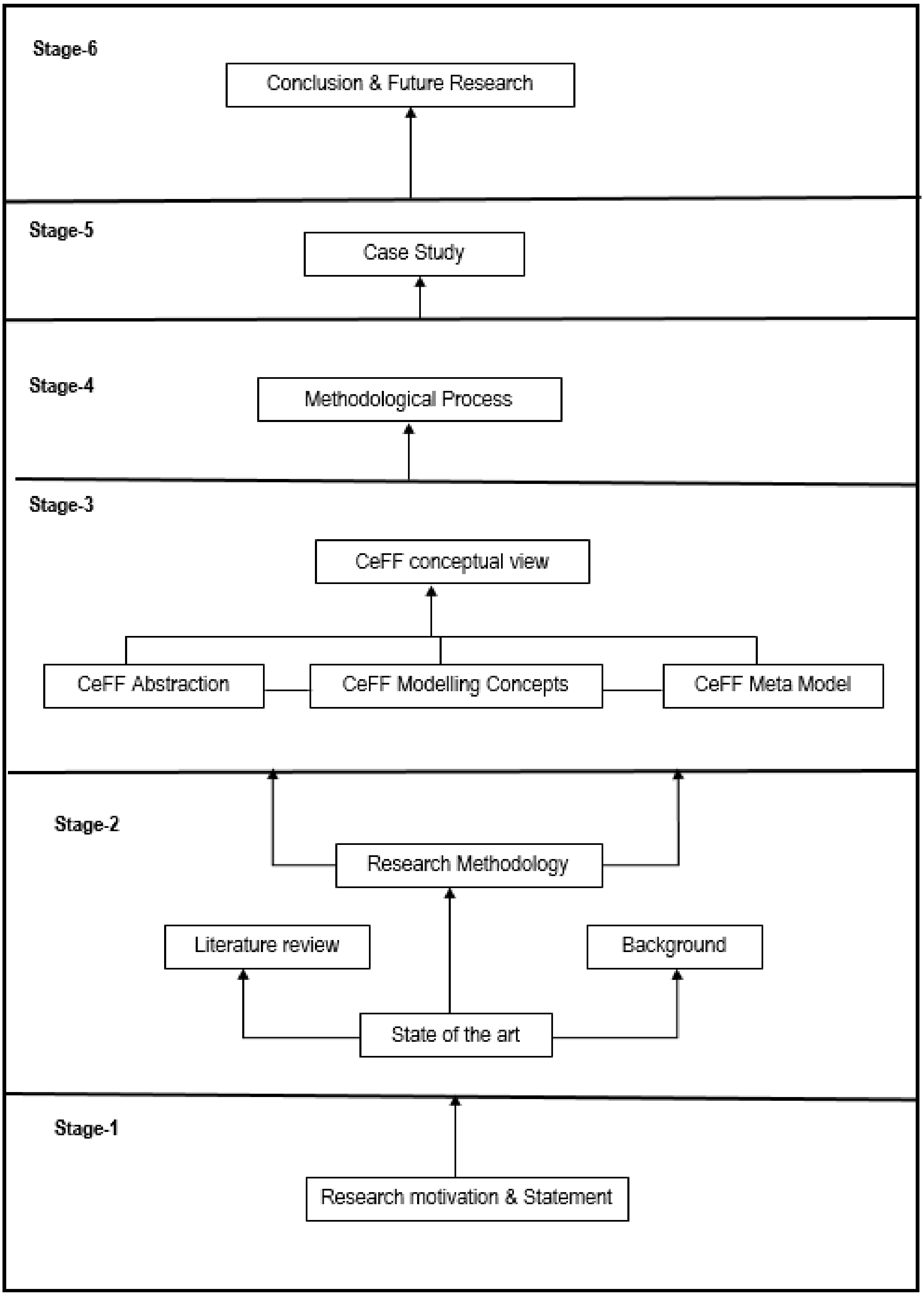


Figure 1.1: Thesis Organisation

Chapter 2

Theoretical Background – State of the art

2. Theoretical Background-Sate of the art

In this chapter, we have reviewed the current state of the art in the area of cloud forensics in the cloud computing environment. In this section, we deliver the theoretical background about cloud computing, forensics and digital forensics, the challenges of forensic investigation and forensics investigation process. To identify relevant literature, a systematic literature review has been conducted using the following search engine such as IEEE Xplorer, ScienceDirect, Google Scholar, ACM digital library.

2.1 Cloud Computing

Cloud is a metaphor for the internet, so cloud computing can be known as using the internet to provide computing services for users and also the abstraction for the complex infrastructure it conceals behind the internet (Scanlon and Wieners, 1999). Gartner, Inc. - the world's foremost company ITRA (information technology research and advisory) conclude cloud system as-

"a style of computing where massively scalable IT-related capabilities are provided „as a service" using Internet Technologies to multiple external customers.(Stevens and Pettey, 2008)".

Cloud computing is based on virtualisation technology to build the abstraction of computer resources. In cloud computing architecture, virtualised server, storage and applications are treated as a pool of resources, which can be allocated on demand. This can be achieved by using virtualisation technology; virtualisation provides functionality that allows multiple virtual servers are running on a single server (Kasemsap, 2015). However, virtualisation technology just provides basic functions and resources for the cloud computing, in order to encapsulate these functions and resources into a single entity, computer clustering is used to allow multiple servers can be treated as a single server (Armbrust et al., 2009). NIST (National Institute of Standards and Technology) (Mell and Grance, 2011b) has defined cloud computing as-

"*a model for enabling 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 provisional and released with minimal management effort or service provider interaction".*

In our pursuit, for the cloud computing definition, we recited articles (Buyya et al., 2008, Vaquero et al., 2008, Wang et al., 2008) and came up our delineation that easy to understand and it is broad to scope. Our delineation is put in words: *Cloud computing is a dynamic development of the system, where the leverage of vast infrastructures like data centre is shared through virtualisation and resource management, which also deliver elastic resources with dynamic provisioning, scaling based on demand, pay-per-use, on demand*

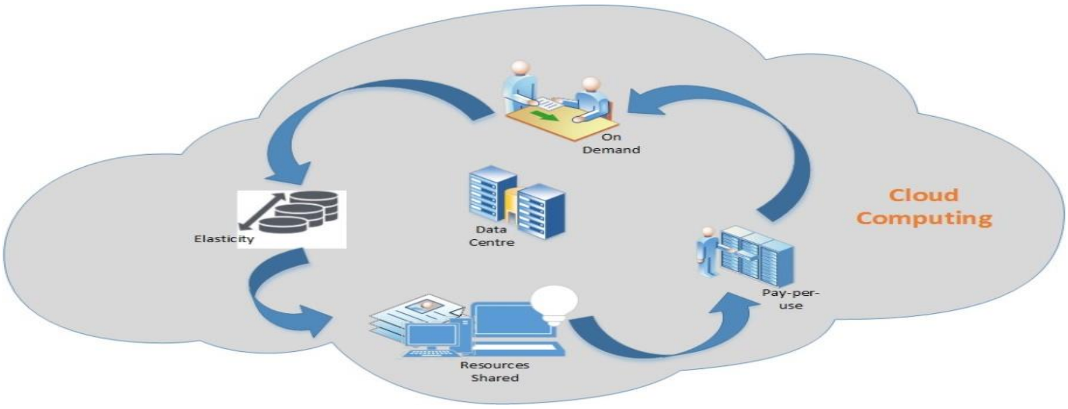


Figure 2.1(a): Schematic Cloud Computing Definition

Services to its clients. A visualised graphical form as described in figure 2.1 (a).

In the period of cloud computing definition, we carefully perceived that some professionals (Subashini and Kavitha, 2011, Heiser, 2009) distinct cloud computing is nothing but “Internet Technology”. However, our clarification does not console to that features imperative because an organisation that has a private cloud does not need any internet service to access cloud services. Resource sharing, pay-per-use, elasticity, virtualisation, on-demand services and instant service are the main features that converted to the data centre into cloud computing. The ‘data centre’ might be restrictive in the sense of common delineation because it could be any IT resources that could be shared using virtualisation techniques. Conversely, if we visit any cloud service providers workplace, we could see a large data centre is used to share resources of cloud systems. In this sense, we can use the phrase ‘data centre’ as our definition to make more relevant to the cloud computing era. Though cloud computing is promised to provide an enhanced utilisation of resources using virtualisation technology, so it brings six advantages (Williams, 2010):

1. Higher utilisation rates: virtualisation can dynamically allocate resources for virtual machines. Thus the server's utilisation rates can be increased and buying any further server capacity could be avoided and deferred.

2. Consolidate of resources: Virtualization technology can consolidate multiple IT resources, such as, server, storage, application infrastructure and so on, which can bring cost saving and efficiency.

3. Lower power usage and cost: By consolidation resources, organisations can minimise the cost of computing hardware, and consequently reduce electricity consumption.

4. Saving physical space: Virtualization technology can run many servers on a single server. Thus physical space can be saved, organisations no longer need to spend money on building rooms for extra servers and related hardware.

5. Disaster recovery and business continuity: By creating VMs on the server, applications and data are encapsulated in its VM environment. So it can increase service-level availability rates and provide new methods for disaster recovery.

6. Reduce operation costs: "Each server in the data centre costs and enterprise on average $10,000 per year to run including provisioning, maintenance, administration, power...(Crosby and Brown, 2006)".

Thus cutting down the number of the servers can greatly reduce operating costs of the organisation.

Though cloud computing is promised to provide an enhanced utilisation of resources using virtualisation technology, and it revolves three service models as listed below:

(a) *IaaS (Infrastructure-as-a-Service):* This is a top layer of the cloud service model. In this model, cloud users can access their VM over the infrastructure of the server. The infrastructure of the server is always isolated to others using hypervisor technology.

(b) *PaaS (Platform-as-a-Service):* This layer is a middle layer of the cloud service model. In this layer, the cloud user can develop their applications without installing and configuring the softwares. In this platform, the cloud service provider delivers the programming platform where users can develop their web-based applications, and they can establish the relationship between application and hardware.

(c) *SaaS (Software-as-a-Service):* This is the bottom layer of the cloud service. In this layer, cloud users need to rely on the cloud service provider.

And, the cloud deployment model can be categorised as:

(a) *Public cloud:* The public cloud is owned and hosted by the cloud service provider. Also, it is known as an external cloud. Cloud service provider is vending their resources to the enterprises, organisations or governments over the internet via web applications or web services.

(b) *Private cloud:* This cloud is completely owned and hosted privately by the owner of the business. Also, it is known as an internal cloud. In this deployment model, clients can take control and operated from their premises. This model is considered a secure and reliable model than other deployment models in the cloud environment. Generally, this model is used in a large business or research firm.

(c) *Hybrid cloud:* This deployment is the composition of two or multiple cloud infrastructures such as public and private cloud service model. The architecture of this model is required both on-premises and off-site such as remote server basis infrastructure.

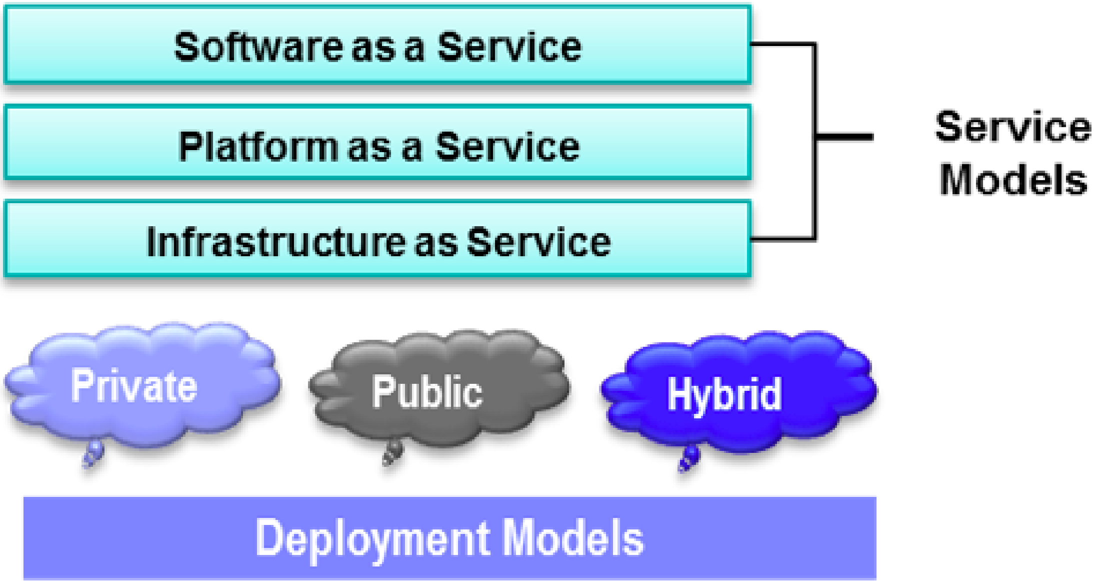


Figure 2.1(b): Cloud computing service and deployment model

2.2 Digital forensics and Cloud forensics

Digital forensics is a method for the preserving, collecting, identifying, validating, analysing, interpreting, documenting and presenting the criminal activities and resources to facilitate and assisting to investigators (Carrier and Spafford, 2004). According to the Wiles (Wiles and Reyes, 2011), digital forensics is "*a methodical series of techniques and procedures for gathering evidence, from computing equipment and various storage devices and digital media, that can be presented in a court of law in a coherent and meaningful format".* The NIST (Grance et al., 2006) also delineates the digital forensics as *"an applied science to identify an incident, collection, examination, and analysis of evidence data".*

On the other hand, cloud forensics is a method of identification. Collection, preservation, examination and analysis, and presentation of the evidence. The cloud forensics is designed for the necessity of digital forensics investigation especially in the cloud computing environment. In the cloud forensics, the forensic investigators have to consider the various level of problems related cloud forensics compared to digital forensics. Due to distributed nature of cloud computing, the evidence are placed in everywhere where identifying the location is a major challenge in these aspects. Also, there are some other challenges such as multi-jurisdiction, multi-tenancy, depends on the cloud service provider during a cloud forensics investigation. The NIST (Group, 2014)delineates cloud forensics is *"the application of scientific principles, technological practices, and derived and proven methods to reconstruct the past cloud computing events through identification, collection, preservation, examination, interpretation, and reporting of the digital evidence".* The process of cloud forensics is differed from the digital forensics and completely depends on the cloud service and deployment model. The challenges of cloud forensics are identifying the evidence from the cloud and the locating the data as well. Cloud forensics investigation process was conducted using some methodologies and tools from digital forensics environment. However, the advancement of new technology such as cloud computing is essential new approaches, methods, tools, frameworks to achieve the digital forensics evidence from a cloud computing environment. Another, challenges in the cloud digital forensics is forensics data cannot be compromised to any third parties like a cloud service provider to submit the report in the court with maintain the chain of custody and confirming the forensics data integrity.

2.3 Cloud enabled Forensics Investigation process

Cloud forensics applies four procedures such as Collection, examination, analysis, and reporting of the evidence data that shows in figure 2.3 (Kent, 2006). A forensic investigator has investigated the facts against suspected crime to prove the criminal evidence. In the digital forensics, process media transforms into the evidence. Through this transformation, three steps are followed:

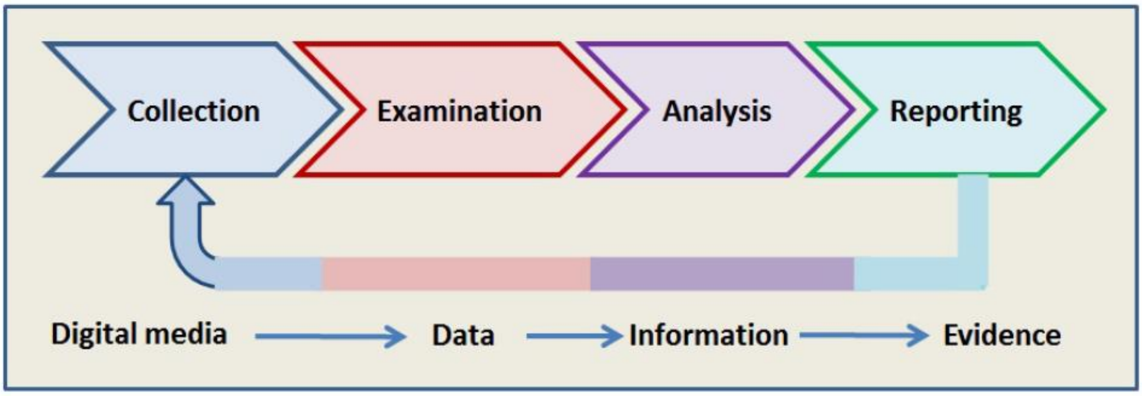


Figure 2.3: cloud enabled digital forensics Phases

Step 1: Collection – Examination: The data is collected in a format where forensic tools can understand data.

Step 2: Examination – Analysis: The relevant data is extracted from the collected data.

Step 3: Analysis – Reporting: The forensic investigator should use various analysis methods to conclude the case under the investigation.

As the cloud has unique characteristics, cloud forensics investigators are defined with new challenges in organisational, technical and legal dimensions due to inevitable of the cloud environment. However, it is necessitated to develop a novel digital forensics framework which enables to investigate digital data in the cloud. For forensic investigation, existing traditional forensics phases and processes have involved in investigating the intricate digital data. Our research has identified that many existing frameworks and models (Gary, 2001, Alex and Kishore, 2017, Kent et al., 2006b) follow similar methods while others are followed in different areas of investigation. However, most of the cases are same because of forensics stages and processes are similar to the same meaning. So it is important to integrate and analyse the missing forensics capabilities into the maturing process of cloud computing. To implement our novel framework, the following stages and processes we consider based on the limitations of existing models:

2.3.1 Digital Data Identification

This stage is the first entry point and is primarily concerned to identify all sources of evidence that may contain potential evidence to determine that the criminal activity took place in the cloud system environment. The sources of evidence might be heterogeneous devices such as mobile, desktop, laptop or data centre from client or cloud provider side which can access cloud services. During the forensic analysis, investigators should identify all connected devices to the cloud system to determine types of crimes and devices through criminal activities. The identification stage is comprised into two phases such as- (a) identification of the incident, and (b) identification of the evidence, that is required to verify the incident. During this stage, all potential evidence must be recorded and documented for taking any actions and investigators should have an action plan to produce the types, format and location of evidence.

2.3.2 Data collection – preservation

This stage emphasises how data is extracted and collected from different types of sources for further forensic investigation. The forensic investigator should ensure proper collection and preservation to maximise its potential use of digital evidence. While collecting digital data, investigators must ensure the data integrity and illegal modifications of data in the cloud environment. On the other hand, the data collection process is depending on the cloud deployment model, and different cloud services are used. It is very important; when investigators collect evidence, they must ensure data must be collected either cloud client side or cloud service provider side as investigation requirements. In client-side data collection, data can be collected from physical memory before shut down device. There are many tools such as LiME, FTK imager etc. to collect memory. When any devices shut down or restart, from that system, evidence collection is critical but using some tools (i.e. Software: TrueBack, EnCase and Hardware: 3p, hardcopy, Tableau forensics duplicator) data can collect during the investigation. All of the above tools are performed forensically sound data acquisition. On the other hand, cloud side data collection can be collected applying remote acquisition approaches to get images from VM. VM can be created provenance where data provenance of the incident not only relays on the virtual image, and malicious attacker uses the virtual machine memory but it is correspondingly produced log files and activities during the investigation. Such logs are categorised as APIs logs, i.e. start, end, events etc. and log hosts such as firewall logs, network activity etc. Data collection can be categorised into two forms –

(a) *Pre-data collection* – can be facilitated forensics investigator before starting an investigation that confirming forensics accuracy. This can be minimised the cost of investigation and reduce the time of investigation as well.

(b) *Post-data collection* – able to receive and retort the evidence when the incident is being discovered. This post-data collection can be distributed to the cloud environment.

2.3.3 Examination and analysis of data

This stage is the ability to examine forensic data after the data is collected and preserved from the sources in the cloud platform. Data examination can include data extraction and data reduction capability. Heterogeneous data from the examination stage should be analysed properly and should be reserved and kept secure data centre and make those evidence available when needed. Through the analysis period, some iterations methods might be applied to authenticate the forensic investigation. On the other hand, data reduction is the ability to reduce the amount of evidence that should be examined and analysed in a forensic cloud investigation. After examining the forensic data, the analysis approach depends on what type of data is collected by the investigator. Investigator can determine the significant amount of data in order to transform them into evidence during analysis.

2.3.4 Presentation of digital evidence

This stage emphases the report to state findings during the analysis of evidence. A well-documented report produces using proficient evidence on the analysis of the evidence. Evidence should be presented in a way where the jury can understand all technical facts on cloud computing. The report should be submitted with all supporting documents concerning the maintaining the evidence of the chain of custody to the court. The well-documented report should include details of findings, types of incident, who’s responsible, the location of the incidents etc.

2.4 Cloud Forensics: Challenges and Solutions

Although cloud computing has been used in the industry for many years, the development of cloud forensics is still in its infancy (Zawoad and Hasan, 2013b). Different problems can be faced by the researchers depending on each of the cloud service models(Sang, 2013). As suggested by different researchers, it would be difficult for them to perform a real-life discovery and investigation in the cloud infrastructure without relying on the cloud service providers (Pătraşcu and Patriciu, 2013, Ruan and Carthy, 2012). They have also suggested numerous conceptual framework to overcome this problem. According to them, there are four key stages in a digital forensic process. Those are identification, collection & preservation, analysis & examination and finally presentation (Poisel et al., 2013). These stages are briefly discussed in the following sections:

2.4.1 The identification stage

In the primary stage, it is required to recognise the machines where illegitimate actions could be carried out and consequently a forensic investigation is required. Several obstacles hinder the investigators to carry out the identification stage as the nature of the cloud infrastructure is very dynamic.

- **Log Evidence Access:**

In the cloud environment, it is difficult to identify evidence through different sources, and it is very challenging as well (Birk and Wegener, 2011, Dykstra and Sherman, 2011, Shah and Malik, 2013). In reality, in specific cases, the investigators do not know the exact location of the data as they are distributed on the cloud and comes from different data centre (Reilly et al., 2011)Cloud service model defines the availability of log files and system statutes. In PaaS and SaaS models it is not feasible as the client has limited access. But it is partially applicable in laaS model where the client has access to virtual machines which behave like the actual system (Birk and Wegener, 2011). Researchers have proposed a number of tools to identify and acquire digital evidence from the cloud (Zawoad and Hasan, 2013b). However, most of them are based on reading the evidence from system logs in order to pinpoint the details of past incidents.

A standard logging mechanism is developed and proposed by Zaferullah et al. that ensures the retention and generation of system logs in conjunction with a log-management system that correlated and collects logs (Anwar and Anwar, 2011). A Eucalyptus cloud environment used to evaluate the approach proposed by Zaferullah. Eucalyptus is a Linux based architecture that implements efficiency-enhancing hybrid and private clouds with an organisation’s current IT infrastructures keeping its configuration. It can also be used to leverage a varied collection of virtualisation within a single cloud, to integrate resources that have already been virtualized. To monitor the behaviour of Eucalyptus system, analysing and monitoring tools were used and all the internal and external interactions were logged. Important information of interest such IP address of attacking machine, type of browsers, HTTP requests and content can be collected from those logs. The number of VMs controlled a by a specific Eucalyptus can also be indemnified. Finally, they have argued on their results that if cloud service providers provide better logging system than cloud forensics would be advanced.

On the other hand Sang also argued for a log-based model that is suitable for PaaS and SaaS models (Sang, 2013). His model suggested to keep a log in client machines and synchronise it that of CSP logs to find out discrepancies. The investigators can check SaaS users' activities without the support from the CSPs. But the CSP ensures the comparability of the log content. Incremental Hash code is used to improve the efficiency in order to guarantee the authenticity of the logged data. A bespoken log module is supplied to both the client and the cloud provider in PaaS. On the other hand Damshenas et al. argued to identify potential evidence from the client side only. For this configuring and designing built-in app logs is necessary to log potential evidence(Damshenas et al., 2012). It can be helpful to implement the feature to check the status of a client's usage and basics logs in a SaaS system. But Damshenas et al. failed to give details on how this built-in the app could be applied.

Marty devises a framework for retrieving logging information during an investigation in a standard manner; what, where and when(Marty, 2011). A synchronised, bandwidth efficient, reliable and encrypted TCP layer is developed to transfer logs from the source to a central log collector after enabling logging on all the components. According to this framework, a few numbers of fields are required to be showed for every log that consists of the time-stamp records, users, session ID, reason, severity and categorisation. This approach assures that the data collected are reliable. Volatile data are not dealt with in this model, and those volatile data may contain important information. In a different paper, researchers (Birk and Wegener, 2011) proposed a logging model that logs data and transmit them to the central system under the supervision of the customers. They suggested that a prevention mechanism is required to prevent the eavesdroppers from changing and view data during transmission. They also talked about read-only API from the CSP to get the necessary logs from cloud service models.

- **Data Volatile:**

Another major problem in the identification process is the data volatility. Volatile data cannot be sustained, when there is a power cut or outage. Similarly, all the data stored in the RAM of VM will be lost if that VM is turned off and there is no backup image. Important data like user id, passwords or encryption key which were stored in RAM can be gone for good. But live data forensics has become significant due to the size and processing power of RAM (Almulla et al., 2014). On the other hand, the current infrastructure of CSPs do not provide persistent storage for the client's data. Volatile storage can be a problem if data are not kept in persistent storage or they are synchronized in persistent storage. Consequently volatile data within virtual environment could be lost when customers restart their machines (Zawoad and Hasan, 2013b, Zawoad and Hasan, 2013a, Reilly et al., 2011, Guo et al., 2012). In that case, only option to conduct an investigation is the live forensic approach (Zawoad and Hasan, 2012). Damshenas et al. recommended a solution to address volatile data issues, and it provides persistent storage for data. This added storage can be used for data recovery, data safety and data collection for the investigators. This storage should be accessible by both CSPs and clients for data consistency. But due cost, it is not common to implement this system in the medium or smaller organisation.

On the other hand, Wengener and Brik proposed a different solution to overcome the problem related to volatile data (Birk and Wegener, 2011). They recommended continuous data synchronisation of the data between persistent storage and virtual machines. But their approach did not provide practical implementation or guidelines for the measures. The lack of control over the systems is another issue when it comes to the investigations of digital forensic procedures (Khan et al., 2016). In fact, customers have limited control and access to the levels of cloud infrastructure and have no clue where their data are kept (Dykstra and Sherman, 2013).

The lack of control over the system poses a number of obstacles to digital investigators when they carry out evidence acquisition (Khan et al., 2016). Indeed, consumers have varied and limited access and control at all levels within the cloud environment and have no knowledge where their data are physically located (Dykstra and Sherman, 2013). For example, an administrator has more control over the IaaS model and his/her control decrease as he/she got towards the SaaS model. This creates an obstacle in the process of physical acquisition of storage and this is required in computer forensic investigation. An investigator has to gain important information from vague resources in order to comprehend the cloud environment that includes cloud hardware, software, file system and hypervisor. But at present day scenario, such information is not available in cloud architecture. Lack of awareness among customer's leads to the loss of important terms regarding the forensic investigation and this is common on all the service models (Sibiya et al., 2012).

2.4.2 Data Collection and Preservation Stage

Collecting data is the core functionality in any digital investigation. Artefacts of digital evidence are collected with supporting material that is considered of potential value. Original after facts are preserved in a way that is complete, reliable, accurate and verified. The investigators face different issues when they are trying to collect and preserved data. In the following section existing literature of those issues will be discussed.

- **Dependence on CSP**

To collect data from a cloud environment both the investigators and customers have to rely on CSP as they have full control over the environment. This creates a serious trust issue in the evidence integrity and the CSP. There are lots of reasons that prevent CSPs to provide the desired evidence that is required for the forensic investigation.

These include but are not limited to :

1. Most CSPs keep limited number backup as they have limited storage.
2. For data movement and replication reasons the CSPs tries to hide data locations from the clients (Sibiya et al., 2012)
3. During any failure, the CSP tries to restore the servers as soon as possible rather than preserving the evidence.
4. The CSPs does not recruit certified investigators to handle cloud-based incidents. This creates a question of integrity (Crosbie, 2012)
5. The response time to an electronic discovery becomes difficult for location uncertainty of the data.

The CSP infrastructures are designed to provide the most effective use of resources in the most economical fashion. Hence it does not consider forensic analysis and acquisition. At present cloud investigators and customers have to rely on CSPs to provide evidence through centralised management and administration (Ko et al., 2011). The trust relationship between CSPs and clients might be affected due to the lack of transparency. A model called TrustCloud is proposed by Ko et al., the model consists of five layers of accountability. These layers are data, system, workflow, regulations and policies (Dykstra and Sherman, 2012). On the other hand, a six layers model was proposed by Sherman and Dykstra for laaS based platform. The layer is a guest operating system, guest apps, host OS, virtualisation, network cloud layer and physical hardware. The less cumulative trust is necessary as the investigator goes further down the stack. For instances, a guest app requires trust from all of the layers (Beckman et al., 2014). On the other hand, a network layer only needs trust in the network. They proposed a cloud management system to be used in the laaS model in a way that investigators and customers can collect important digital data that includes logs, VM images, databases, processes. Ultimately, they recommended a cloud-management plane for use in the IaaS model. But this approach required an added level of trust in the management system. If the CSP does not provide its customers or investigators with applications and tools, the dependency on CSP does not minimise. If a solution is designed with forensic in mind, a better result of investigation can be achieved.

But the industrial point of view does not follow this approach i.e. deigned in align with forensics. This point of view suggests that forensic requirements should not affect the architecture of the cloud environment. However, if such necessities would defend public security, governments might inspire CSPs to set up forensic capabilities while designing cloud architectures(Almulla et al., 2014). Fortunately, the leading cloud provides start to adopt this approach. For instance, Amazon has released logging apps that enable the logs to get utilising AWS portals & delivers logs to an ASSS (S3) (Pichan et al., 2015). This application is primarily designed for security purpose but can be used for forensic data analysis of Amazon users. However this tools is dependent on third-party plugins, and hence more level of trust is still required (Delport et al., 2011).

- **Isolating a cloud instance**

It is important to separate the incident environment in order to prevent any temperament in digital evidence. For this, in any forensic process, the particular instance that is connected with the incident in the cloud needs to be separated. But this is not efficient in a cloud environment due to the data sharing storage with multiple instances. Also a single cloud machine or node may contain many instances, and the nodes have been cleared when investigators are doing their investigation. There are some isolation techniques (Yan, 2011) which can be used to isolate these cloud instances. This will help to prevent any tampering or contamination with the existing evidence during forensic investigations in the cloud environment. If an incident can be stimulated inside the cloud, these techniques require instance relocation. Instance relocation can be done automatically via the operating system or by a cloud administrator. In this instance the request between the node and the user needed to be re-routed by server farming. In the last state, the isolated evidence is paced in Sandbox. A combination of this mentioned procedure can be implemented to get a better result. However, these mechanisms are still theory based.

- **Data provenance in the cloud**

In data forensics within the cloud environment provenance plays an important role. Hence it is required to implement secure provenance. This will help investigators to gain important forensic data from the cloud infrastructure by defining who owns the data at a specific time and who has accessed those data. Also, data provenance keeps the chain of custody as it provides timeline of evidence (Alqahtany et al., 2015). A secure provenance in cloud computing is required that will record the process history of data in the cloud and its corresponding ownership as suggested by Li et al. (Li et al., 2014). They argued that such a mechanism should fulfil conditional privacy preservation. This mechanism also argued for the confidentiality of data in a cloud environment, province tracking and anonymous authentication. The suggested technique by Li et al. will provide trusted evidence. However, their solution is still in theory.

- **Data integrity**

Ensuring the integrity of evidence and preserving the integrity of original data is another challenge for cloud forensic investigators (Crosbie, 2012). Data integrity is an important part of the cloud forensic process (Dykstra and Sherman, 2011). To maintain the integrity, incident related information has been kept in the chain of custody that includes where, how and by whom the evidence was collected, how it was preserved and stored(Damshenas et al., 2012). Failure to do that make the evidence valueless in a court (Khan et al., 2016). There is the possibility of errors as multiple actors are involved in this process(Zawoad and Hasan, 2013b). This poses another challenge for the investigators to prove the data as integrated.

A TPM (Trust Platform Module) was proposed by researchers that aim to preserve the integrity (Birk and Wegener, 2011). By adhering to TPM confidentiality & integrity of the data can be maintained. TPM provides hardware encryption, machine authentication, attestation, secure key storage (Zawoad and Hasan, 2013b). But, due to the possibility of modification of the running process the security of the TPM is questionable (Beckman et al., 2014). The adoption of TPM by the CSPs in the near future is not likely as the current devices are not compatible (Zawoad and Hasan, 2013b).

Besides, multi-factor authentication methods such as VPN can be used with TPM in order to authorise the client to ensure integrity and confidentiality to mitigate data preservation issues (Damshenas et al., 2012). Researchers have suggested an encryption technique as security is an important concern in a cloud infrastructure. This can be advantageous for the investigators though it comes with some complexity. On the other hand, Yan suggested a framework that mirrors the relative files and cords completely (Marangos et al., 2016). Also a freezing mechanism is needed to be kept the CSP on the customer's account to prevent any changes to the data (Zawoad and Hasan, 2012).

- **Time synchronisation**

Time synchronisation is another very important aspects of forensic investigation. It can be used as a source of evidence. But when data comes from multiple instances, the data time's stamps and date stamps can be questionable(Zawoad and Hasan, 2013b). As cloud instances are located globally in different time zones, this can affect the reliability, integrity, admissibility of evidence. At present, the cloud environment is dependent on the VM guest's OS network protocol to synchronise with a network time server. To obtain time from many instances of sever the best strategy is suggested by (Grispos et al., 2013) CSP can use a standard time system for example GMT on all instances of the cloud and this can help to provide a logical time pattern in the way that helps investigators to create analysis based on timeline. This will help them track different instances located in different places (Almulla et al., 2014). Network Timing Protocol can be used to get a consistent time to get time specific evidence.

- **Cloud literacy of investigators**

Lack of training materials that could be used to educate investigators on cloud tech is another problem cloud forensic investigation. Major challenges of the cloud environment are not updated regularly on forensic training materials. Moreover, the investigators with technical expertise are not familiar with legal procedures. Hence it is important to train them on the legal procedures, including networking, programming negotiation and communication with the CSPs (Al Fahdi et al., 2013).

- **Chain of custody**

Chain of custody is another important issue in digital forensic (Zawoad and Hasan, 2013b). How the evidence was gathered, preserved and collected has to be detailed in the chain of custody. This will help to present the data in a court of law inadmissible way (Dykstra and Sherman, 2011).

Due to unique combinations of features of cloud computing, it is hard to verify the data chain of custody. Apart from that multi-layered and distributed infrastructure of cloud environment make it difficult to verify the chain of custody (Ko et al., 2011). Certain specific tasks need to be clarified in order to retain the chain of custody such as the way logs are generated, collected, stored along with ownership of the logs. To do so, CSPs have to recruit qualified and trained specialists.

2.4.3 Examination and Analysis Stage

Due to the sheer volume of resources and a vast number of instances, it is very difficult to perform a proper analysis in the cloud. Also, a standard program to extract forensic as the customers can access data from various devices such as a tablet, PC, laptop, mobile phones. Moreover, there is no standard program for the forensic extraction of data, as the customer can access relevant data from various devices such as a desktop PC, tablet, or mobile phone, and from a wide range of applications. The data extraction depends on the model of a device. As data are sometimes exported in an unstructured way, it becomes difficult for the investigators to analyse the data using standard forensic tools. Hence it is important to build apps that convert native cloud data to a recognisable and readable format (Mell and Grance, 2011a). Crucial and important analysis is produced after the reconstruction of the event of the forensic investigation. This will help to recreate the crime. However, each event related to a crime may occur in different location or countries due to the distributed nature of cloud environment.

In the following section a few challenges faced by the investigators are discussed based on existing literature:

- **Lack of available cloud forensic tools**

The distributed and elastics structures of cloud computing cannot be managed with the available forensic tools, and there are limitations of the tools as well (Sibiya et al., 2012, Reilly et al., 2011). Participants in a survey (Al Fahdi et al., 2013) concluded that there is a lack of forensic tools. Majority of them recommended that automation is needed in digital forensics process to tackle challenges. In addition, the demand of aware forensic tools is very high to conduct a forensic investigation (Sibiya et al., 2012). For this, it is important to build tools that can be utilised for collecting, identifying, and analysing forensic data (Shah and Malik, 2013). To analyse forensic data in a timely fashion a combination of tools are required. To collect active data traditional forensic tools can be used. Data over the network can be collected using network forensic tools (Barolli, 2012). E-discovery can be utilised to conduct offline investigations on a network or a computer. For instances, Encase software has their e-discovery apps although there are multi-jurisdiction problems (Taylor et al., 2010).

Due to technical, cost and legal reasons, it is less likely that CSPS will obey the legal e-discovery obligations (Mell and Grance, 2011a). In addition, the SLA to an e-discovery is challenging due to the uncertain nature of data location (Ko et al., 2011). Stanford University in California has developed an open source software (OWADE). This tools can detect website visited by the users, extract info from the cloud, recreate internet activities and identify online instances users accessed. This software is still in development and is only compatible with Windows XP (Peleg et al., 2003). Due to the high level of trust issue involved, Dykstra et al. do not suggest to use some commercial tools (Beckman et al., 2014). Forensics Open-Stack Tools (FROST) is a tool developed by Dykstra and designed to get forensic data from VMs, logs and firewall logs (Dykstra and Sherman, 2013). It is operated within the cloud management plane. In the IaaS model, FROST is the first forensic tools (Dykstra and Sherman, 2011).

- **Evidence correlation across multiple sources**

As evidence are spread across multiple locations, correlation of evidences can be overwhelming. This creates a problem for the investigators to handle multiple sources as a time.

- **Reconstruction of a crime scene**

In order to understand how illegal activities were done, it is required to reconstruct the crime scene. In a cloud environment, it is a big problem (Zawoad and Hasan, 2013b). Reconstruction of the crime scene is impossible when an adversary shut down his/her virtual instance. A method is proposed by Belorkar and Geethakumari to allow the investigators to replay an even of the attack by using snapshots (Geethakumari and Belorkar, 2012). This will help the investigator to visualise outgoing and income data.

2.4.5 Presentation Stage

Presentation is the final stage of the digital forensic investigation. In the stage, the findings are presented in a court of law in the form of report (Trenwith and Venter, 2013). In the context of a cloud environment, many challenges lie in this step. For example, due to the distributed nature of the cloud environment, it is not clear how to specify the physical location of a cloud-based crime. This creates confusion among the investigators on the legal system to be followed. Moreover, the jury needs to understand technical aspects of the presented case that involve with thousands of VMs. But the jury member is not likely to technically sound (Reilly et al., 2011).

2.5 Existing Framework and Models and Limitations

In our research, we have done various research in details based on the cutting-edge research on digital forensics and cloud forensics. In the past, a number of the researcher has offered numerous frameworks, models in both cloud and digital environment.

DFRW(Gary, 2001)S (Gary, 2001) has defined a process to investigate with digital system and networks. The model has formed with a linear process that involved identification, collection, preservation, examination, analysis, presentation and decision. The limitation of this model is that it is not in details with stages that they followed. Every step the model introduces a list of problems without any clarification.

NIST (Kent et al., 2006b) proposed forensics analysis in 2006 and the forensics process comprises the following stages such as collection, examination, analysis and reporting. This NIST model is used for internal investigation for LEAs or organisational purposes where the forensics process is converted to the media into the evidence. In the initial stage, they collected data from the source, and later they examined. Once the examination is completed, then they extracted evidence from media and converted into the different format that could be processed using the forensics tools. Formerly, the converted data is converted into the information through analysis. Once the analysis is completed, then the information is converted into evidence through the reporting stage. The problem of this model is while converting the evidence into a different format, it lost the data integrity and sometimes it volatile data which cannot be readable.

In 2004, V. Baryamureeba et al. is proposed an EDIP (Enhanced Digital Investigation Process) (Baryamureeba and Tushabe, 2004), model. In this EDIP model separated the crime scene into the two-part for example primary and secondary part. Instead of linear, they describe each phase as an iterative. This model is based on the IDIP model that develops from the deployment stages to physical stages when the primary crime scene is considered during the digital crime scene investigation. The limitation of this model is once all investigations are completed then the investigator can be made the reconstruction.

Beebe NL et al. proposed a hierarchical and objectivities based framework (Beebe and Clark, 2005) for the digital investigation process that includes subj and objective based phases which are related to various layers of abstraction and further any layer can add if needed. The framework comprises the following stages such as preparation, data collection and analysis and presentation with findings. The problem with this framework, while collecting the incident, no proper logs are maintained by when, how and what incident occurred.

In 2019, Edington M Alex et al. have proposed a forensics framework (Alex and Kishore, 2017). The framework is addressed current challenges such as less control in the cloud, data collection physical inaccessibility, multi-tenancy, and logging, the vitality of logs and accessibility of logs. The proposed framework introduced the forensics monitoring plane and forensic server for enhancing cloud forensics where the framework will be mitigating the challenges in particular at one scenario at a time. The main limitation of this framework is if an attack occurs, the framework cannot be checked entire crime and whether their proposed FMP (Forensics Monitoring Plane) could collect all data that related to malicious activities.

In 2018, a cloud forensics logging framework (Pichan et al., 2018) introduced by Ameer Pichan et al. where the frameworks enable the forensic activities such as re-create events, trace the chain of events, separate the CPU logs, acquire the logs, interpret the logs, without affecting other clients. However, there is a limitation on this framework which cannot validate the logs that generated their framework.

Brik et al. (Birk and Wegener, 2011) have recommended the use of application programming interface (API) to enable access log information to customers by read-only API, and the customer can provide information for the forensic investigation. This solution solved the issue of the trusted third party since customers are directly involved in continuous synchronisation. But the dependency of CSP still exists, and the authors have also suggested the encryption of logs before sending to the API for defending external breaches.

B. Martini et al. proposed ICDF (Integrated Conceptual Digital Forensics) framework (Martini and Choo, 2012) that based on the NIST framework. The framework focuses on the differentiation between the collection of data and the preservation of data in the cloud computing environment for forensic purpose. This framework is only conducting the investigations in the cloud computing. The issue of this framework is there is no digital forensics library in terms of cloud platform and the cloud deployment models. Therefore, Law Enforcement Agents must understand the CSP needs the legal bindings of data they can be gather and type of evidence.

Shah JJ et al. in 2014, proposed an approach towards digital forensics frameworks where they underlined the potential malicious activities in the cloud computing environment. Their proposed approach has three layers of architecture where they used tools and techniques for each of the layers. The limitation of this framework is it only working on a private cloud environment.

Belorkar A et al., in 2011 proposed VNsnaps (Belorkar and Geethakumari, 2011) to analyse the cloud attacks through event regeneration. The VNsnaps will take recurrent snapshots of the virtual network environment during the attack that are detecting using the fuzzy clustering techniques. The fuzzy clustering technique is used to determine whether the virtual machine is on safe or unsafe mode. There is no proper direction on how the evidence will present after analysing the forensic evidence in the cloud environment.

Valjarevic A et al. introduced harmonised digital forensics investigation model (Valjarevic and Venter, 2012) that is performed constantly and parallel with several actions to attain efficient investigation and confirm the acceptability of forensic evidence. This model follows the multi-tiered and iterative model where every step comprises a set of sub-steps. All the steps are defined with their scope and function such as planning, incident response and detection, identify the crime, collection, transportation, analysis and presentation. In this model, it consists of additional six steps such as data flow, authorisation, chain of custody, preserving the digital evidence, interaction and documentation; that simultaneously ponders during the forensic investigation process. In the data, flow steps categorise and describe all the data flow. Therefore they can protect from any malicious attack. The main limitations of this model are that evidence accuracy and effectiveness is not certified.

2.6 Framework Comparison

A detailed study has been conducted throughout this research. Therefore, it is concluded a comparison needs to be formed in order to map the methodologies. This research has discovered that some of the existing model and framework follow associated with the same methods and approaches where others are followed by different methods. However, most cases the results are same. In order to make an appropriate comparison, we have considered the limitations of the existing frameworks and models. First of all, we are considering the planning. The planning has many actions which can be measured in the event of incidents. Planning can prepare all the requirements, potential consequences for the incidents, potential risks for the process the investigation. A proper plan can deliver the quality of evidence and minimise the risks. When a crime happens in the cloud system, retort the incident is very challenging because if there is no proper plan. Develop a proper plan can be reduced any types of risks, policies and procedures must be explained clearly if any investigations will be tested. Identification is another concern to identify all potential sources that can have further evidence in a cloud environment. When incidents are identified, the forensic investigators are looking for the type of incident, time of the occurrences, malicious actors etc. In the cloud, there is always target to cloud service provider service or organisation or clients. Most of the malicious people use the CSP services as a normal user to launch their attack. The cloud service provider main concerns are on the users because CSP does not who is malicious user or who is not. In our concept, we have identified some actors such as CSP, internal and external staff, LEA and malicious people. When incidents occur, then it is initiated several goals. On the occasion of the incidents, the investigators start using some services such as forensics, tools, plan, process and procedures to reconcile these issues. The services that could be used into the related people such as technicians, investigators, law enforcement agents and any other people who are working on this case. However, investigators can establish policies in relates to making any decisions based on the planning, identification, preparations. Proper planning and strategies will make the case very effective over the period. A good plan can deliver the quality of evidence and minimise the risks. Initiating the response plan strategy can confirm the all incidents are under examination that considered all potential risks. Policies and procedures must be explained clearly if any investigations will be tested. On the other hand, a forensic investigation team is responsible for any types of aspects during the investigation which should be dealing with which investigators (it might be internal or external staff). Practice and guidance do a vital role in every aspect of the investigation by reducing any errors and risks. Cloud service providers are liable to help all investigators along with all investigation related evidence that available in CSPs infrastructures. Forensics investigators and LEAs must be skilled in handling possible evidence that needs to be preserved with data integrity and continued the chain of custody. Because of the nature of cloud computing, data can be stored in different locations, so this a challenges for LEAs and investigators to identify the location and different countries have different law and legislation. Therefore, forensics investigators and LEAs should conduct with the legal authorities of the country in order to get access location of the evidence, and the evidence must be up to date during the investigations. After identifying, collecting all the evidence, forensic investigators have to find what are the requirements needed in order to solve the problems. Both investigators and LEAs will determine the requirements based on evidence, and all the requirements should be supported by evidence. Requirements determine the right and obligation because right performs certain actions and obligation is a correlate of the right. Documentation is a core component, and data integrity and chain of custody should be retained at all the time. Well documentation must be maintained from beginning to end of the process along with other concepts. Documentation must be maintained following procedures by the investigators. To keep the record up to date, a good documentation is important in order to perform training and risks analysing in the investigation. Any methods that is applied during investigation and tools that is used must be documented to keep the chain of custody correctly. Any modifications in the evidence must be also documented. Besides process and requirements are continually running in parallel because both of them depend on each other. When process complete, then what type of requirements are needed to minimise the risks. The outcome of the documents, investigator make the report in order to present in the court or to inside the organisation.

To verify the applicability of the comparison above framework, we have conducted two case studies in the evaluation chapter. Throughout the case studies, it shows all the concepts and activities of the framework that are identified and described.

2.7 Discussion of Current Solutions in the Cloud

The related research per stage of the digital investigation was taken into consideration when developing the literature. The author has retrieved the paper form well know academic databases including, IEEE Xplore, ACM, Springer , ScienceDirect. Only cloud forensics issues and challenges were discussed on most of the reviewed paper. Solutions are provided in several studies in order to perform proper forensics investigation. Despite this most of the recommendation was only in theory and not tested in a real scenario. The author has found one piece of research that examined and evaluated the current tools used in conducting remote data acquisition. This paper was conducted by Sherman and Dykstra who invented a set of tools discussed earlier as FROST. Despite the difference between traditional computing environments and cloud environment, traditional tools such as FTK and Encase are still common tools. Instead of interacting with the OS inside as guest, FROST operates on the cloud management plane. This tool was the first forensic capable tools in IaaS cloud model. The CSP has deployed FROST. Hence trust is required in the CSP environment. Trust is also required in a cloud environment, host OS, cloud employees, hypervisor. It also assumed that stakeholders in a cloud environment are cooperative and they are actively involved in the investigation. The work consists of conducting three experiments from three different layers namely, the virtual layer, the guest OS and the host OS. A certain amount of trust is necessary for each layer.

To perform the data acquisition, investigators and customers are dependent on the CSPs. To mitigate the issues of dependency, researchers have recommended solutions such as API or cloud management plane. These are provided to the clients in order to get the forensic hard disk. However, there are numerous important data that resides in the CSP. There are many other dependency issues on the CSP which were highlighted by the researchers. But no solution was provided to mitigate the dependency.

In contrary, Amazon, with CloudTrail logging app, has started to deliver services that aim to a forensics investigator. Although this app was designed for security reasons, it may provide prime informative data for Amazon users.

Another major problem faced by the investigators is piecing together a sequence of events. Till today the investigators have not provided an approach to reconstruct the past event with accuracy. From the literature, it is observed that there is a big concern with data acquisition and data integration in the cloud environment. Also, data logging procedures are not simplified. These include log review, timeline, log policy monitoring, log correlation. Due to the lack of proper guidelines and lack of global standard legal procedure, legal issues hinder the forensic investigation process.

It has become important to identify a solution that will overcome current problems, and that will help forensic investigators. It is also important to depend upon on VM images being gathered and stored, while other research has recommended an IaaS solution with credibility being placed on the addition of the CSP as central to the resolution (Dykstra and Sherman, 2013). CSPs usually do not let their customer look behind their virtual curtains (Damshenas et al., 2012). They only listen to the legal order and willing to help when there is a legal requirement. Therefore a starting point is necessary.

2.8 Conclusion

Cloud computing is a recent advance technology wherein IT infrastructure and applications are provided as “services” to end-users. Cloud computing is posing a serious challenge to digital forensics investigations. In the initial of this chapter, we discussed background of cloud computing and its service and deployment model is also presented. We also discussed digital, and cloud forensic that follows to cloud-enabled forensic investigation processes. This thesis is aimed to address the challenges encountered when the digital forensic investigation is conducted. This chapter is also presented the existing research on digital forensics and the current solutions with their limitations in the cloud environment. Based on the findings in this chapter, next chapter proposes a research methodology in order to develop our framework.

Chapter 3

Research Methodology

3. Introduction

In previous chapter 2, we have considered a detailed literature study that is related to our research. In this section, we delineate our profound methodological concepts based on our literature review and the limitations of the current study in cloud forensics investigations. The primary objective of this chapter is to articulate an appropriate methodology and framework for the proposed research. In our research, we have conducted various studies in a similar field, and we have evaluated fully in order to develop our framework. This research method is mainly provisioned on descriptive, concepts and process model in order to investigate, and evaluative in nature. In section 3.1 is considered the descriptive part which involves literature of the existing research that addresses the challenges of digital forensics in the cloud. Also, the literature focuses on forensics investigation processes and techniques. Evaluates existing frameworks are carried out which are used as a benchmark to formulate and develop of the solution in addressing the problems of digital forensics investigations in the cloud environments. In section 3.2, modelling concepts and processes are carried out at a different level. The last part (section 3.3) of the research method is evaluated in order to validate the framework.

3.1 Descriptive (existing research)

In order to develop the research methodology, research studies have been sourced and reviewed. In the previous chapter 2, various theoretical studies took place in order to facilitate the forensic investigation process in the cloud environment. The following research studies have been selected for the forensics investigations in the cloud environment.

3.1.1 Forensics investigation process in the cloud: cloud forensics is a method of identification. Collection, preservation, examination and analysis, and presentation of the evidence. The cloud forensics is designed for the necessity of digital forensics investigation, especially in the cloud computing environment. A forensic investigator has investigated the facts against suspected crime to prove or disprove evidence. As the cloud has unique characteristics, cloud forensics investigators are defined with new challenges in organisational, technical and legal dimensions due to inevitable of the cloud environment. However, it is necessitated to develop a novel digital forensics framework which enables to investigate digital data in the cloud.

In order to implement our novel framework, the following stages and processes such as digital data identification, data collection – preservation, examination and analysis and presentation of digital evidence; we consider based on limitations of existing models.

3.1.2 Cloud forensics challenges and solutions: In the digital cloud forensics, we have identified challenges that hinder the cloud investigators to carry out the investigation. In the following stage: identification stage, there are several obstacles such as log evidence access (difficult to identify through different sources), data volatile (volatile data cannot be sustained); data collection and preservation stage, the issues such as dependence on CSP (as CSP has full control of the environment), isolating a cloud instance (instance that is connected with the incident in the cloud needs to be separated), data provenance (secure provenance is required), data integrity (ensuring data integrity), time synchronization (used as source of evidence), cloud literacy (lack of knowledge), chain of custody (How the evidence was gathered, preserved and collected); examination and analysis stage: the challenges that are faced by the investigators such as lack of available cloud forensics tools, evidence correlation across multiple sources and reconstruction of crime scene; and the last stage is presentation stage where all findings are presented in court of law in the form of report.

3.1.3 Existing Framework, models and limitations: This research has conducted a various study on cloud-enabled forensics framework and model. In the existing framework and model, this research has identified limitations and problems of the existing framework. Therefore, this research has made a comparison in order to map the methodology. To do an appropriate comparison, this research has considered the limitations of all existing framework and models.

3.2 Modelling concepts and process

The next phase to the completion of the methodology is to .develop a .process .based on the .concepts identified and presented in the conceptual model. The framing concepts are constituted from the level of abstraction. The level of abstraction has three levels such as organizational, technical and legal level; that forensics investigators can understand which level they can start an investigation in order to make a successful investigation. The main concepts have been identified that are related requirements and considers evidence to support investigator in the cloud environment. Therefore, the necessary concepts are being applied to following different levels.

3.2.1 Organizational level: The organizational structure defines the fundamental concepts which are to be used in forensics investigation. The necessary concepts such as actor, goal, incident, planning, action and report at organisational level which is implemented at a technical level.

3.2.2 Technical level: The technical level is to support the perception of what are technical measures are required to investigate forensics data in the cloud environment. In the technical level, the following concepts such as evidence, process, requirements, mechanism, provenance, documentation and risks; have been identified to concentrate on the technical procedures during the forensics investigations in the cloud environments.

3.2.3 Legal level: In the legal level the following concepts such as Law Enforcement Agent (LEA), right and obligation; have been identified to represent the evidence in a court through proper documentation.

3.2.4 Process: During the process of investigation, we have introduced four activities in order to take specific actions for investigating the forensic evidence in the cloud environment. The following four activities are presented in CeFF process:

- Crime context- to identify the background of the crime; in particular, crime preparation, investigation strategy and determining the complexity.
- Identify risks- to identify all possible risks to determining the facts of the incident.
- Evidence- to identify all relevant evidence and segregate all evidence accordingly to build the case.
- Identify forensics actions- to identify appropriate actions to resolve the incidents to construct data integrity for forensics investigation.

3.3 Evaluation

To assess the strength and weakness of our proposed methodology, the proposed framework is applied to the real-life case studies. We have evaluated the case study into qualitative and quantitative approaches to develop the test theory. We have conducted the qualitative and quantitative approaches because of the availability of members and using the methodologies with gaining the experience to learn new procedures. This is very constructive for the practitioners to identify the real-life problem with the methodology i.e. missing conditions or ambiguity. We have followed (Verner et al., 2009, Runeson and Höst, 2009, Kitchenham et al., 2002) the following steps to process our case study.

- *Research outline*- defines the objectives of the research such as literature review, objectives, aims and goals etc.
- *Case study plan*- defines the evidence identification, collection, procedures, methods and design the plan step by step.
- *Data collection*- that includes data collection from different sources during the development of the project.
- *Data analysis*- includes the assessment and conclude with respect to the case study.

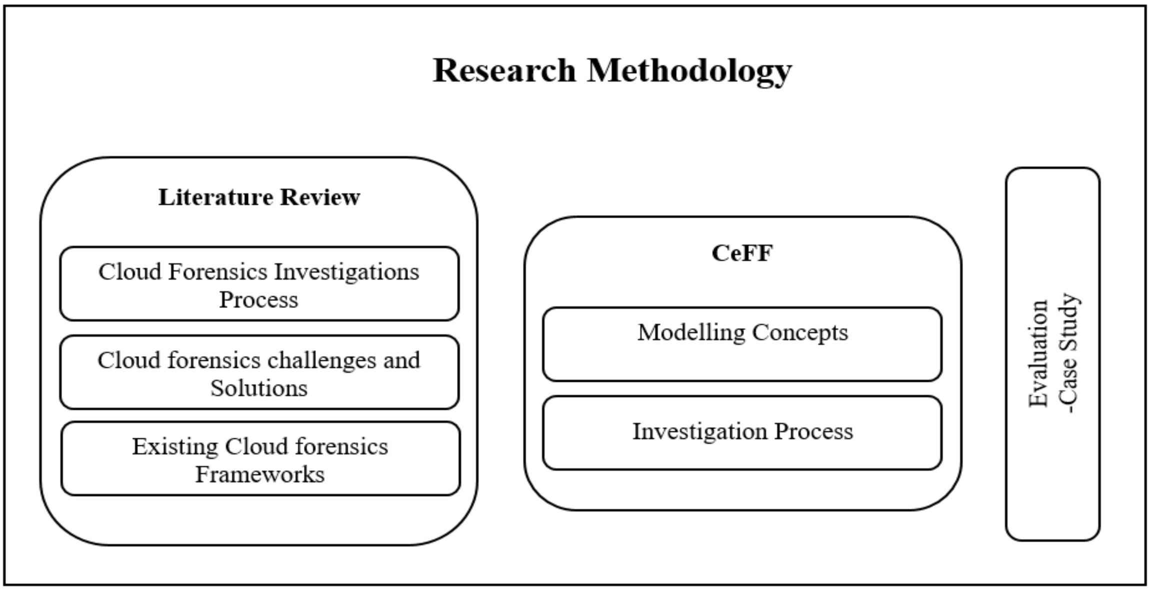

Research Methodology
Literature Review
Cloud Forensics Investigations Process
Cloud forensics challenges and Solutions
Existing Cloud forensics Frameworks
CeFF
Modelling Concepts
Investigation Process
Evaluation
-Case Study

Figure 3.1: Research Methodology

3.4 Conclusion

In this chapter, we have described the research methodology of our proposed framework. We have described the theoretical background where we identified the cloud forensics investigation process, the challenges and solutions with the existing framework. We described the modelling concepts and process which are carried out into the different level. Finally, we describe how we evaluate the proposed methodology. In the next chapter address the challenges of digital forensics cybercrime with its type. It presents legal requirements that are required for forensic investigation.

Chapter 4

Cybercrime and Legal requirements

4. Introduction

With the rise of cloud computing services, cybercriminals discover new and improved ways of conducting cybercrime, using cloud computing services as their instrument of choice. The differences in responsibilities in the service models described earlier allow cybercriminals the opportunity to perform their activities while minimising the required effort. Examples of malicious use of cloud computing services include sending a massive amount of spam (Krebs, 2008), using the reputation of cloud providers to deceive firewalls (Danchev, 2009) and deploying botnet command-and-control servers (Danchev, 2009). Cybercrime itself is well-known and well-researched. However, information on the relation between the use of cloud computing services and cybercrime is scarce, although important for coming to an understanding of the effects of widely-available cloud computing services on modern-day cybercrime. This section will present various types cybercrime that happens in the cloud system and the forensics issues of cybercrime in a cloud environment. And also this section will describe various requirements that consider throughout cloud forensics investigations.

4.1 Types of cybercrime

The properties of cloud computing give way to more and different types of cybercrime to be performed using cloud services. Many of these types of cybercrime existed before they were performed using cloud services. In the case of cloud computing, cybercriminals can abuse these services in two different ways. The first way is to use rented servers, provided by the cloud provider, to perform cyber-attacks. Another way is to compromise or in any other way misuse cloud services rented by others to perform their attack. Both of these methods result in the cybercriminal not being affected by the consequences of using these services for the malicious activities. The only parties affected are the cloud service providers, who own the physical machines (Mell and Grance, 2011b) and the legitimate services users when their machines are compromised or in any other way misused. This section will discuss different types of cybercrime, including examples of real misuse if found during the research.

4.1.1 Malware hosting

Malware hosting is a broad term that entails hosting of malicious programs, exploits and other types of malicious software. Examples of malicious programs are Trojans, hosted through websites promising users useful applications. These websites may dupe users into executing the hosted malware. Another example of malware hosting consists of hosting exploits to attack users without the need for the user knowingly interacting with the malicious website or host. The only thing the user needs to do is connect using a program that is vulnerable to an exploit used by a malicious host. Consider the example of drive-by downloads; these can be classified as an exploit because they make use of vulnerabilities to execute malicious programs (Le et al., 2013). The advantage cloud computing brings to malware-hosting is scalability of the capacity of the host, that is, the amount of data the host can serve. Another advantage, which is not necessarily a general property of cloud computing, is the abuse of reputation of popular cloud service providers. The abuse of the reputation of these cloud service providers can lead to a delayed listing in blacklists and can delude other reputation based system.

4.1.2 Non-malware malicious hosting

Malicious hosting is not restricted to hosting just malware. Malicious hosting also includes hosting of malicious websites that are not meant to infect its visitors. Examples of this type of malicious activity are hosting websites to scam people or phishing websites. The advantages of the use of cloud computing for this type of cybercrime are mostly the same as the advantages described for malware hosting. This is because the technique required is (almost) the same. The attackers need only to host a website or other way of communication a user can connect to (McGrath and Gupta, 2008).

4.1.3 Sending spam

One of the most known types of spam is email spam, which is discussed throughout this paper. Email spam involves sending messages to recipients by email. These emails may contain links sending users to phishing websites or websites hosting malware. Other spam emails may contain malware or unsolicited commercials (Cranor and LaMacchia, 1998). To recognize emails as spam, many email clients and email services utilize so-called spam filters. To a certain degree, these spam filters can filter out the unsolicited messages from incoming email. These spam filters often consist of statistical techniques for filtering (Androutsopoulos et al., 2000), the configuration of user preferences and reputation based filtering methods (Kolthof, 2015). While spam itself is nothing new, the use of cloud computing services for sending spam can provide spammers with some advantages. An advantage of using cloud computing services for sending spam is its scalability. Spammers have the opportunity to scale their spam sending operations using cloud services instantly. Another important factor in choosing to utilise cloud services instead of other infrastructure has nothing to do with the technique of sending spam itself, but with the filtering of spam message by recipients. Attackers can abuse the reputation of cloud service providers, which can delude spam filters. This abuse of reputation can lead to the attacker being able to send more spam message before being detected or blacklisted. An example of misuse of cloud services for spam is the abuse of Amazon‘s Elastic Compute Cloud (EC2) for sending spam. Which led to blocks of IP addresses belonging to Amazon‘s EC2 being blacklisted on multiple spam databases (Krebs, 2008).

4.1.4 Phishing

In the phishing attacks, users are working on a fraudulent side that appears to be a legitimate site. Phishing sites are created to obtain the users credential. The other phishing attack is through the e-mail, where users received the e-mail from the adversaries. E-mail received appears as legitimate mail from the known source. Such emails provide very concise or no information and provide the link to know more about it. Once clicked on the embedded link sent, malware gets installed on the user’s PC. A number of phishing attacks have already occurred in the cloud. Some of them have been discussed below:

- Longline Phishing: Longline phishing is a new type of attack that is occurring in the cloud. In this type of attack, adversaries take advantage of email services and sought personal information from the users. Attackers sent the mail to the cloud user tricking him to click the link (Mell and Grance, 2011a).

- Spear Phish Attack on Raythe: Defense Company Raythe (Raytheon) have also encountered the phishing attack in its cloud. It was a spear phishing attack; an email was sent to the employees to access an application through this e-mail link. However, no damage was reported due to the outgoing filters that were in place.

- Phishing Attack on Microsoft Employees: Recently, some of the phishing attacks occurred on account of Microsoft employee that was maintained on social media and emails (Green, 2013). These accounts were targeted phishing attack. It occurred to obtain the law enforcement information inquiries.

- Phishing Attack on Dropbox: Phishing attack is also uncovered in Dropbox users account by the security firm Approvers (Goscinski and Brock, 2010). This attack phishes victim’s password via bogus email once succeeded then users computers are infected with malware. They send an official appearing mail to reset the password once clicked by the user on the reset button a malware gets installed on the user’s browser.

- Phishing Attack on Amazon and Apple: One of the major data breaches occurred with Apple and Amazon (Mell and Grance, 2011a). In this breach, Honan’s accounts on Apple and Amazon were compromised. In these attacks, the victim has lost all his information stored in his account. Additionally, he has lost the photo and video of his 18 years daughter, which he has not stored anywhere else.
- Phishing Attack on DBaaS: Recent trend is to offer database as a Service. In this model, user can subscribe for the relational database to leverage this cloud offering. Amazon and Microsoft both are offering DBaaS. Users can benefit from these services by subscribing to it and pay for its usage. But a recent report by Imperva highlights that DBaaS is extremely risky and can be exploited by Command and Control (C & C) Server if necessary precautions are not observed (Initiative, 2012). To examine the vulnerabilities, (Initiative, 2012) conducted the research and concluded that cloud subscription is fairly risky because the same database can be shared/ subscribed by the adversaries. This will result in easy access and attack on the database. To support their claim they have carried out a research that revealed that mail sent to a user might lead to execute the malware in his system and connect the user's system to a remote location that is controlled by the adversaries. OLEDB provides the necessary connectivity to connect the database. Also, the report revealed that vulnerabilities existing in the database provide further ground to attack DBaaS.

4.1.5 Distributed Denial of Service (DDoS)

Distributed denial of services is the other category of prominent cyber-attack that is taking place in cloud computing. Distributed denial of services attack is the cyber-attack in which a number of computers are used to attack the single destination. Compromised computer is known as Zombie. Due to DDoS, legitimate users are denied the resources, since they are utilised by non-legitimate users. DDoS exploit the volumetric technique or the amplification technique. In the volumetric technique, huge volume of traffic is directed to the network in order to consume the bandwidth or resource-sapping exhausts. State exhaustion attacks such as TCP SYN flood and idle session attacks are the example of misuse of state nature of TCP and causes the resource exhaustion. In the amplification technique, attackers take the help of the victim to increase the traffic. An amplification technique, the attacker exploits the attacked resource. Attacked botnet sends out a DNS query of about 60 bytes to an open recursive DNS resolver that responds with response message up to 400 bytes, increasing the amount of traffic by more than the factor of 60. The following attacks discussed the major DDoS attacks that have already been caused.

- The attack on Spamhous Spamhous is a spam avoiding company. Recently, DDoS attack took place in spamhous project (Mell and Grance, 2011a). The attack exploited the DNS Servers, open DNS resolver's capability. In this attack, peak attack traffic has reached the capacity of the server. The peak attack traffic has reached the volume of 300 gigabits per second. To handle the issue spamhous released a press note advising the internet community to check the traffic leaving their network to stop spoofed sending addresses is not leaving their network and to lock down any open DNS resolver (Mell and Grance, 2011a).

- Security Breach in Sony: Security breach on Sony has alerted the whole internet community (Singh, 2014). Attack has exposed 100 million account records. Attackers did not remain concentrated on this attack instead an additional attack occurred on Sony's online entertainment that exposed an additional 25 million users. To determine the reasons, a company constituted an investigation team. It was revealed that the attack took place due to the availability of two servers behind the firewall. The two servers were a web server and the application servers. Attacker exploited the vulnerabilities of application servers and attacked the web Server (Singh, 2014).

- DDoS Attack Took Place on Bitbuchet: Bitbuchet is a development company that hosted its infrastructure on the cloud. It has subscribed to Amazon EC2 (Mell and Grance, 2011a). In 2009, all of a sudden this service went down. As a result, the whole production came down. The problem continued for several hours (19 hours approx.) before the services were restored. Once the Amazon pinpointed the problem, and then only it could be put on (Mell and Grance, 2011a).

4.2 Forensics issues of cybercrime

4.2.1 Cybercrime Forensic Issue

Cybercrime is the use of computer technology and network technology to implement high-tech crime (Balkin et al., 2007). Compared to traditional crime, the evolution in computer technology has continued. Computers and other communication systems have become very complicated and better connected through all kinds of networks. In the cloud period, cybercrime techniques have also become more sophisticated and better coordinated. They encompass a broad range of activities. The computer may have been used in the commission of a crime, or it may be the target. Sometimes, criminals try their best to attack the DC and the cloud instead of personal computers. The best characteristic feature of cybercrime is executed without time and area restriction. So the involved computer equipment in the case is distributed more widely. The information service or the user data can be distributed in different locations or even different countries. Therefore, it causes the legal difference and a dispute in information security supervision for the government and increases the forensic period and difficulties. Moreover, the judicial issues between users' physical boundaries are fuzzy, which is caused by virtualized technologies and can not be allowed to be neglected. On the other hand, depending on the cloud plat, the criminal forms involve many domains such as the electronic community, obscene websites, phishing, child pornography, copyright infringement, and e-commerce bilk, etc. There are also problems with privacy when confidential information is lost or intercepted, lawfully or otherwise. Such crimes may threaten a nation's security and financial health. According to the (Cisar et al., 2014) cybercrime is "rapidly growing area of crime because the Internet is global phenomenon criminal have been enabled to commit almost any illegal activity anywhere in the world". It focuses on finding digital evidence after a computer security incident has occurred. Nowadays, cybercrime forensics has become a hot topic to fight network crime and protect the network environment.

4.2.2 Evidence Preservation Issue

The goal of cybercrime forensics is to do a structured investigation and find out exactly what happened on a digital system, and who was responsible for it. There are essentially three phases for recovering evidence from a computer system or storage medium. Those phases are: acquire, analyse, and report. Often, the results of a forensic investigation are used in criminal proceedings. Computer criminals always leave tracks; it's "just" a matter of finding these tracks. But this part is not always easy. The police should be proficient in computer and network technologies, including security technology, in which reconnaissance and ant reconnaissance, anti-hunt chase and the battle will be largely reflected as a technology contest. The network evidence belongs to the electronic evidence. Most evidence, such as log files stored in the cloud services, email records used in e-commerce bilk, or digital signature, cannot prove something by themselves, only when they are analysed and examined by certain authentication. Since the electronic evidence is easy to be tampered with, it is urgent to avoid the various factors that destroy the legal effect in the above three forensic phases. Moreover, internationally, both governmental and non-state actors engage in cybercrimes. Activity crossing international borders and involving the interests of at least one nation-state is sometimes referred to as cyber warfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court (Ophardt, 2010).

4.3 Legal requirements

This section will detail commonly cited legal issues for cloud forensics and will discuss whether or not each issue presents a unique legal challenge concerning the cloud. These legal requirements should be considered throughout cloud forensic investigations.

4.3.1 Multi-Jurisdiction

Multi-jurisdictional issues are consistently noted as the primary issue in cloud forensic investigations, and digital forensic investigations as a whole (Ruan et al., 2011a). The location of data affects the ability to compel production of such data and may, although unlikely under most states' long-arm jurisdiction rules, affect the determination of where a case involving cloud data must be filed/prosecuted.

- ***Criminal Cases:*** Criminal cases involve criminal charges brought by the government under criminal sections of the U.S. Code or state counterparts. The jurisdictional issue for where such a case may be filed usually turns on questions of where the victim is located, where the defendant is located, and where the criminal acts occurred or where their impact was felt. Often jurisdiction is not exclusive, i.e., several states or the federal government and one or more states may each legitimately assert jurisdiction. Subject to double jeopardy limitations prosecution in multiple jurisdictions is possible.

In general, jurisdiction for a case will be in the jurisdiction investigating and filing the case, although this is largely a tautological decision for usually the selection of what jurisdiction will investigate a case is decided by the determination of which jurisdiction may prosecute the case. In cases with multiple possible jurisdictions, so long as the valid statutory jurisdictional requirements are met, the ultimate decision as to which will prosecute is usually a policy question.

For criminal cases, the controlling substantive, procedural and constitutional rules (including the Rules of Evidence) are those of the government asserting jurisdiction and bringing the case.

- ***Civil Cases:*** Cases where one person or entity brings a claim against another person or entity for a failure of a legal duty are considered civil cases. The government can be a party, either as a plaintiff or defendant; the key requirement is that the cause of action is civil. For civil cases, an understanding of jurisdiction is more complicated. When the data and entities involved in the case are in different geographic areas, the primary jurisdictional requirement is that the "forum" state (the state where an action is brought) has "enough connection with a problem to satisfy constitutional and statutory requirements" (Richman et al., 1984). Some courts contend that the location of a server is not sufficient enough to qualify as a connection for jurisdiction decisions.

Issues other than determining jurisdiction can be involved in multi-jurisdictional cases. One significant issue is whose substantive law applies when the parties and evidence are located in different jurisdictions? A large and complex area of law called "Conflict of Law" has been developed to resolve these issues. This body of law is beyond the scope of this article and will not be addressed here.

The most important point to be made for this article is that the issues associated with the multi-jurisdictional nature of cloud-based data storage are not unique. These issues frequently arise in disputes completely outside the realm of cloud storage.

4.3.2 Multi-Tenancy

Multi-Tenancy issues are endemic to cloud forensic investigations due to the shared storage nature of cloud computing. There are two issues, each already discussed in the previous two sections. The first is the validity-of-the-warrant issues relating to establishing probable cause to believe that evidence of a specified crime will be found at the location for which search permission is sought, and the related issue of the need for particularity in the warrant regarding the identification of the place to be searched.

The second issue is authenticity. If data from multiple tenants is stored at the location to be searched, there must be a sufficient basis for claiming that the offered data is that of the defendant and only the defendant.

Where the investigator cannot specify with precision the location of the sought after data, there may be a temptation to seek “cloud-wide” warrants or other compulsory production orders. Such overbroad orders may look to a reviewing court like a fishing expedition. Such overbroad, general warrants are unlawful searches, and the results of such searches will almost certainly be suppressed.

Such a broad warrant, one that does not limit itself to a specific user's data, can be overbroad in two ways. First, such a warrant almost by definition is reaching or has the potential to reach the data from tenants with no involvement in the matter before the court. This could conceivably rise to trespass or invasion of privacy action against the party seeking the evidence. Second, it could involve reaching data of the target outside the scope of the warrant or subpoena. Either of these flaws can lead to suppression.

4.3.3 Service Level Agreements (SLA)

Service level agreements (SLAs) govern the relationship between the customer and the cloud service provider. As such, the terms agreed to within the SLA may provide information on how forensic investigations will be handled. A large majority of cloud forensics survey participants noted that tools, techniques and other information for forensics investigations should be included in SLAs (Ruan and Carthy, 2012). While a review of current SLAs is outside the scope of this chapter, it is important to provide a brief overview of the legal implications of SLAs and how SLAs effect investigations.

Legally, SLAs are almost always binding fall under U.S. contract law. SLAs can be of importance particularly when setting terms for a collection of forensic data. The most common burden SLAs place on the cloud provider is with respect to uptime for the customer, though several have advocated that these agreements include how to be handled (Grobauer and Schreck, 2010), incidents will including the processes for conducting investigations that respect the laws of multiple jurisdictions (Ruan et al., 2011b).

From an investigative standpoint, the SLA dictates the availability of forensic data for the customer that could be collected in the event of an investigation. While much of the focus of this chapter has related to obtaining cloud data in an adverse relationship (i.e., the government seeking the defendant's cloud data), in many instances the cloud data at issue belongs to the victim, and the issue is not how to command such production but rather the rights the user has to her own forensically accurate data. If the SLA does not include notice of what type of process or forensic data will be provided for the customer, then the cloud provider has no contractual duty to provide such information. This does a couple of things legally: 1) it binds access to forensic data that may otherwise be available; 2) lowers quality of best evidence available. The SLA may govern what type of forensic data is collected and the process in which it is stored.

It is important to note that an SLA is only binding between the parties and does not restrict the information that may be sought under a warrant or subpoena. An SLA that denies any provider responsibility to give a user log files is not a shield against a warrant asking for log files. If they exist, they must be produced.

4.3.4 Chain of Custody

A crucial component of the admissibility of evidence in court is whether a well-documented and validated chain of maintained for such evidence (Kuntze et al., 2012). When evidence is "susceptible to alteration by tampering or contamination," then a "substantially more elaborate foundation" may be required (Losavio, 2005). There are many factors that present a chain of custody concerns for cloud forensic investigation that would introduce susceptibility, and thus a more rigorous requirement for a proper chain of evidence.

The first potential failure of the chain is with the cloud provider. At this point, forensic evidence will be obtained by the cloud provider and presented to law enforcement as evidence. With this reality, there is no control on the forensic investigation concerning procedure, process, or person; the collection of evidence is conducted 'behind doors.' While it is allowed under the Fourth Amendment for search and seizure without the presence of law enforcement (Navarro, 2003), diligence must still be conducted for a proper chain of evidence. The burden of documenting the chain of custody rests on the cloud provider, and such documentation is critical to ensuring the chain is maintained. Detailed documentation should include the person conducting the investigation, the steps taken to ensure the evidence has not been modified, and verification through hashes.

With regards to the person—particularly when there are multiple persons—conducting the investigation, a proper chain of evidence must be maintained through logs and comprehensive notes to detail who conducted what elements of the investigation as well as how the evidence was handed off and stored securely. Additionally, establishing the person(s) on the cloud provider side had familiarity with the investigation process used by the company may be a useful step inadmissibility for authentication (Edwards, 2012). This would be in line with authentication through expert witness testimony as previously discussed. Ensuring the evidence has not been modified also must be established. A proper process and inclusion of verification through hashes should be conducted and documented to confirm evidence had not been modified, which will stand as verification in court (Orton et al., 2012). However, this may be a technical problem in cloud forensic investigations where cloud images may not be able to be validated using cryptographic hashes (Dykstra and Sherman, 2012).

Another issue with ensuring a proper chain of evidence is that many cloud providers use proprietary file systems for provided services. This introduces questions of validity and presents a gap in familiar digital forensics practices handling hard drives.

4.4 Conclusion

In cloud computing, security is a most critical issue especially in digital forensic. This chapter presents types of cybercrime that related to digital forensic. While forensics investigation, what are the forensics issues of cybercrime that is faced by forensic investigator also considered. During the preservation of the forensic evidence, what are the issues should consider, that also presented in this chapter. This chapter is well discussed some legal requirements issues with multi-jurisdiction, multi-tenancy, SLAs and chain of custody when an investigation will conduct if evidence is located in other countries.

Chapter-5

CeFF: Cloud-enabled forensics Investigation Framework

5. CeFF methodology

In previous chapter 2, we have considered a detailed literature study that is related to our research. In this section, we delineate our profound methodological concepts based on our literature review and the limitations of the current study in cloud forensics investigations. We describe the concepts in different levels of perspectives such as – organisational, technical and legal. This section is structured as follows: section 5.1 presents the structure of the methodology, section 5.2 describes the different level of abstractions which are associated with a list of concepts, section 5.3 provides all the concepts that are required for forensic investigation through organizational, technical and legal perspective for effective forensic analysis in the cloud environment, section 5.4 describes the conceptual view of CeFF framework. In the last section 5.5, we present a meta-model to rationalise in connection among concepts.

5.1 Structure of the CeFF Methodology

In figure 5.1 describes the complete methodology that we are using in the rest of the thesis. The CeFF methodology comprises a level of abstraction, framing concepts, process and a case study. Consecutively, the CeFF framing concepts are constituted from the level of abstraction and combine all the concepts into a meta-model that defines the relationships among the concepts. The level of abstraction has three levels that forensics investigators can understand which level they can start an investigation in order to make a successful investigation. On the other hand, we consider various concepts that enable forensics investigators to investigate forensic evidence in a correct manner. Also, forensic investigators can able to examine and analyse the evidence in a systematic way. The CeFF process follows various activities that investigators follow the process to investigate. The process describes how investigators collect, examine and analyse the forensic evidence. In the process, we apply a sequential logic which can be evaluated the existing condition and present condition determine the present condition. The reason we use sequential logic, extracting information from digital sources should be mined before the investigation start.

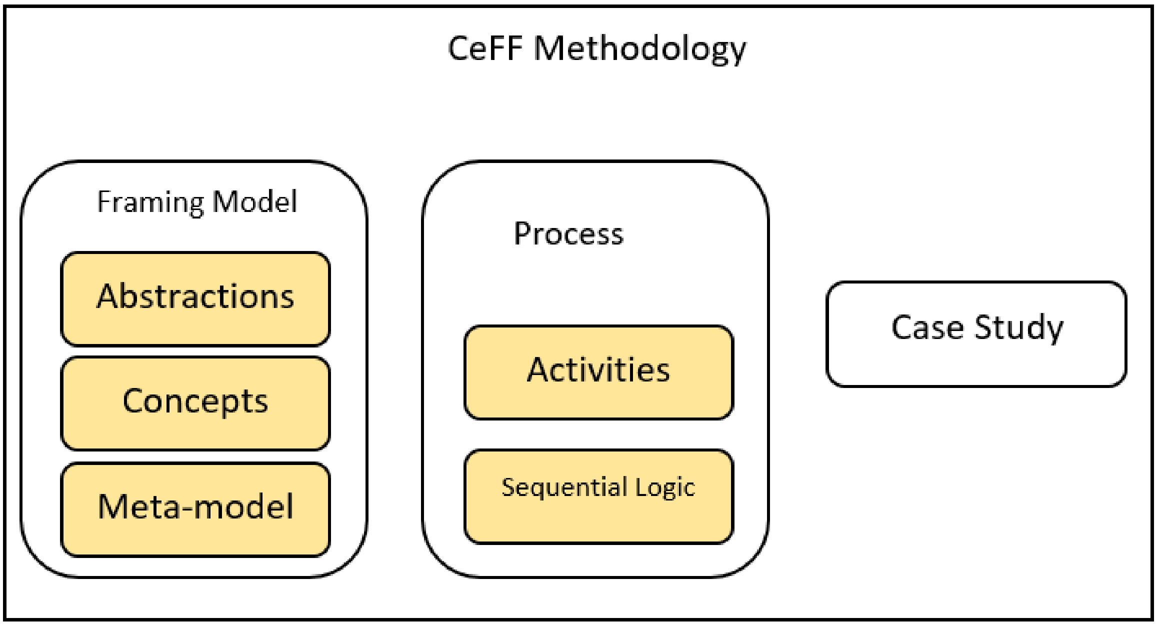
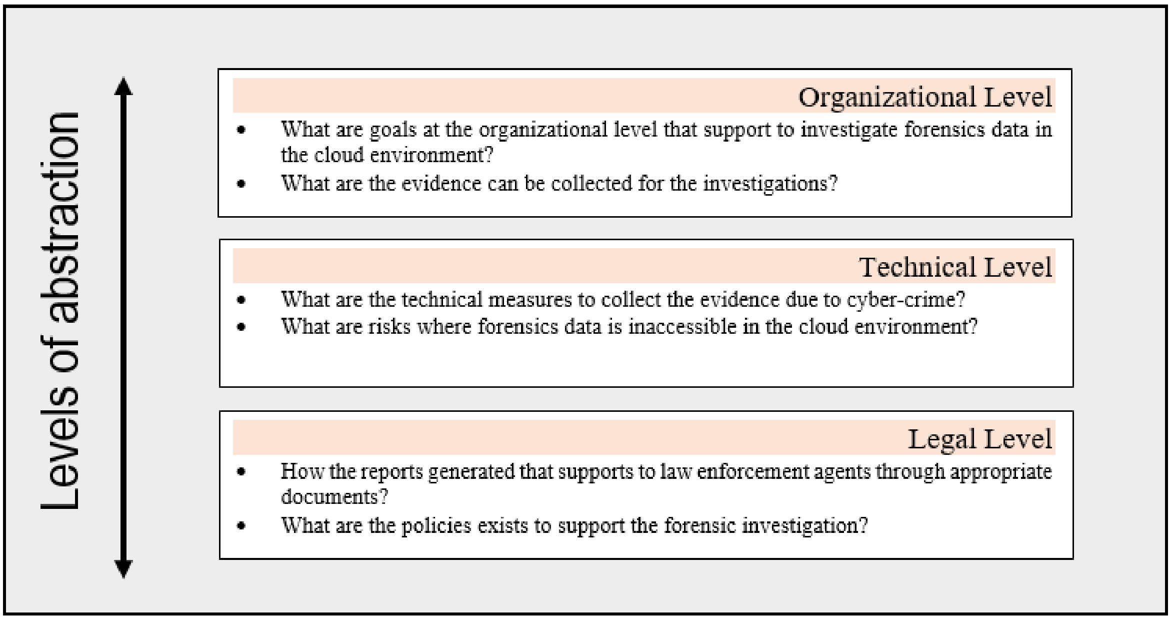


Figure 5.1: Structure of Methodology

5.2 Level of Abstraction

In this section, we describe the different level of abstractions. In our research, we comprise our framework into three different levels of abstractions –organisational, technical and legal level that constitute the concepts for forensics investigation in the cloud. In this section, we demonstrate how all concepts satisfy for a successful forensics investigation in different levels in the context of the cloud system.



Organizational Level

- What are goals at the organizational level that support to investigate forensics data in the cloud environment?
- What are the evidence can be collected for the investigations?

Technical Level

- What are the technical measures to collect the evidence due to cyber-crime?
- What are risks where forensics data is inaccessible in the cloud environment?

Legal Level

- How the reports generated that supports to law enforcement agents through appropriate documents?
- What are the policies exists to support the forensic investigation?

Figure 5.2: Level of Abstraction

5.2.1 Organizational Level

This is defined by the concepts such as actor, goals in order to achieve forensics investigation in the cloud domain. This level involves how actors (i.e. client and CSP) participate in order to achieve the goals during the investigation in particular, who, how and where the evidence is collected for what purpose. Various entities may play certain roles, duties and most cloud applications are depended on the cloud service provider. Because of the multi-tenant nature of cloud computing, cloud users/clients are shared their resources and files which are stored in the cloud platform. The main concern of multi-tenancy is the privacy issue. Because of the privacy problems, any logs or provenance data cannot be delivered to any forensics investigators to investigate the forensic data. However, cloud users, services are mostly dependant on the cloud service providers. In this circumstance, the forensic investigators must determine dependant on either cloud service provider or cloud user. In a cloud environment, dependencies are highly dynamic in following with the chain. Cloud forensic investigations may have to follow each link of chain on the investigation process. In such a situation, any exploitation or interruption in the chain may lead to serious problems on investigations. Also, SLA's and organisational policies enable to communicate and collaborate with the law enforcement agency in forensics activities. Also, law enforcement agency and cloud service provider should liaise with all arbitrators and academics. Arbitrators can help for any forensics auditing and acquiescence. On the other hand, academics can help in technical areas such as cloud system, any tools which can efficiently intensify the forensics investigations. To support forensics investigation in the cloud, the following roles can satisfy the collaboration of users, internal and external members who are delivered by cloud actors.

> -*IT Expert and investigator:* IT expert delivers essential training to forensics investigators that includes cloud system, forensics tools, data collection methods etc. Also, they can help to forensics investigators in retrieving criminal records, carrying out evidence collection in support of forensic investigators. Generally, IT expert can be a cloud system administrator, Network engineer, IT technician, Cloud security manager and so on.
>
> Besides, a forensics investigator is liable for collecting all resources and evidence and, examining and analysing those evidence in an appropriate manner. Forensics investigators are accountable for all forensics data if any criminality is charged

and they should work collaboratively along LEA (law enforcement agent) as required. All forensics investigators should work as a team, and they should be capable of investigating their resources, moreover collaborate with external members during investigations.

-Incident responder: If any incidents are encountered during the investigations, the incident responder must provide response and report the incident immediately to the high authority. Incidents include data violation, data loss, DDoS attack, unauthorised access to data, disclosing data, end user attack, malicious activities, and violation of tenant's data confidentiality. An incident responder must make a plan where he categorises the type of incidents, security level, appropriate solutions of incidents, relevant knowledge of professionals etc.

-Third party: In order to establish forensics tasks effectively, forensics investigators should work collaboratively, and they must build trust on each other. More importantly, forensic investigators must verify the actions if any tasks or activities are performed by third parties and make sure the related rules, strategies, plans and agreements must transparent to relevant members.

-Legal Forensics Advisers: The legal forensics advisers must have knowledge of multi-tenancy and multi-jurisdiction problems especially in cloud domain. The advisers also should have up-to-date knowledge of regulations related to cloud, and they confirm that any activities during the investigation cannot impose laws and legislation and ensure the tenants' data confidentiality which are shared the resources. The actions must be clarified by the SLA's, and internal legal advisers must communicate with SLA's to consider overall jurisdictions. The internal advisers are also accountable to link with external LEA's and investigate forensics data collaborate during investigations.

5.2.2 Technical level

This conducted with a range of concepts such as transparency, evidence, requirements, and incident to determine the methods of collection and preservation of forensic evidence in a technical manner. This level specifies and helps to the forensics investigators where forensics data is inaccessible on the cloud environment and how forensic processes (i.e. data collection, evidence segregation, analysis etc.) are performed during the investigation. Two entities for example clients an CSP forensics data are located in both client-side and CSP side infrastructures. Collecting forensics data thru using tools and techniques from both sides may be different based on the particular model of data responsibility that is in place. Collecting data is a method of identifying the artefacts, categorise, segregate and acquire the forensic evidence. The resources of forensics information can reside into two sides such as the customer side and cloud service provider side. In the customer side, the forensics data could be any client's infrastructure such as mobile, tablets, desktop, laptops etc. on the other hand cloud service providers' side, and forensics data could be CSP data centres or CSPs infrastructures. The methods of collection should be followed with appropriate tools to ensure the forensics data integrity. Therefore, for a successful forensics data collection should ensure data integrity with proper segregation of duties between user and CSP. It shouldn't be compromised and breached any tenant's data where resources are shared. So that proper measures can be facilitated cloud forensics investigation in the cloud. In cloud computing, the rapid elasticity is an important characteristic where data could be provisioned and non-provisioned with on-demand. Consequently, forensics tools should be adaptable with all cases such as recovering volatile data, collecting and acquisition of data, data examinations and analysis. Another significant characteristic of cloud computing is resource pooling where multiple users are pooled resources using a multi-tenant model. In the multi-tenant environment, users can share their resources which can be decreased IT cost. Though, evidence segregation in the cloud is essential to categorise. Therefore, the forensics tools should be developed in order to segregate forensics evidence among multiple users in the cloud service and deployment models.

5.2.3 Legal level

This level defines the concepts -right, obligation, report that ensures the development of regulations and legislation that do not breach laws and regulations in the jurisdictions where forensics data resides. Due to cloud characteristics, it is crucial to conduct evidence acquisition when forensics investigations are considered by a different legal system where different laws and regulations may vary by countries. This level specifies how forensics legislations can make smooth forensic investigation procedures for cloud forensics investigation. And also, it will resolve the transparency issues, for example, SLA can provide right information and regulations between clients and cloud service provider for performing any investigations in a multi-jurisdictional environment without violating any privacy policy, laws and regulations

5.3 CeFF Modelling Concepts

In order to develop new forensic methods on the cloud computing, we have proceeded on finding a number of concepts that are used for forensic investigation at organisational, technical and legal levels. The main concepts have been identified that are related requirements and considers evidence to support investigator in the cloud environment. Therefore, the necessary concepts are being applied to following different levels.

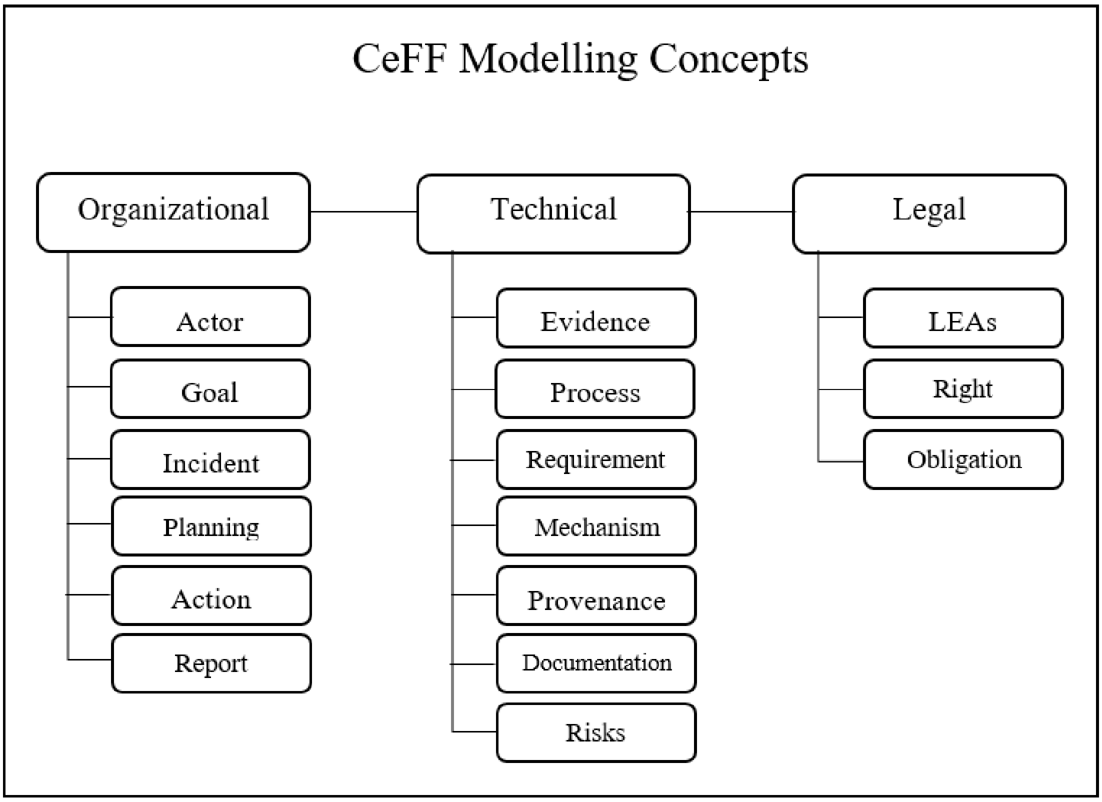


Figure 5.3: CeFF Modelling Concepts

- **Organisational Level**

In order to perform forensic activities effectively and efficiently, an organisational structure is required. The organisational structure defines the fundamental concepts which are to be used in forensic investigation. The following are the necessary concepts at the organizational level which is implemented at the technical level.

- Actor: An actor is an entity such as an individual, a system or an organisation that has goals and intentions within the system or within the organisational setting [Yu, 95]. CSP and data processor are the special actors in our case responsible for managing and processing user data. Any incidents can occur at any time in the cloud service provider (CSP) and their infrastructures. Although, evidence access, transparency, reliance on

CSP/users are linked to cloud service provider. The cloud service provider and investigators can build trust and reduce the dependency of each other. A cloud service provider can give support to forensics investigators by giving the data, evidence that are found in their infrastructures. When forensics investigators have requested any pieces of evidence from CSP, CSP can be provided all the information that has been requested without conceding security and privacy of their occupants. To establish trust and transparency with the consumers, CSP should give the information about their data and the locations where data is stored. Else, trust might be lost from CSP and investigation might produce the complexity. An actor has a specific role for example administrator, company legal advisor, and investigator; depending on the context and also has the right to claim anything and obligation that correlates with the right.

- Goals: Goals are the objectives, expectations and constraints depending on a specific context aiming to preserve the benefits for migrating into the cloud. To attain a system mechanisms, the goal can be a condition. Goals also can be expressed the reasons for a system. Goals can be different types such as functional and non-functional goals. The functional goals can be expressed where a system can be likely to deliver. On the other hand, non-functional goals can be delivered the qualities of systems, i.e. security and privacy, flexibility, system performance and so on. The goal can be hard and soft depending on the level of information disclosed by the user. Hard privacy goal follows data minimisation strategy and emphasises disclosing as little data as possible to avoid trusting other entities. In case of soft privacy goal, data minimisation rule is not strictly followed, and user expects to trust the external entities to manage their data. Identifying the goals is not easy tasks because lots of goals are embedded. So, the process of goal elicitation should be analysed into the present system environment and extract the goals from various sources such as case study, report, documents, policies etc. After identifying the goals, the next phase is to develop them until the goal completely is applied.

- Incidents: This concept is to identify the details of incident and events that occurred in the cloud. Incidents can be identification, security and privacy, permission, instigation etc. Once incidents happen, then the forensics investigations are introduced to identify crimes. The internal team will be informed for the incidents that already occurred, and it continuously observes the system. Besides another team will be established to manage the incidents and attempt to reduce the risks. The main aim is to detect the crime and relevant incident, reduce the risks, try to find as much as information and collect all evidence. Because of the nature of the cloud system, all digital evidence can be stored in different locations and different data centres. In the cloud forensics, this is very critical to retain the digital evidence and the chain of protection for digital evidence. In the cloud platform, identifying the digital data is a challenging method because of various service and deployment models and also is very challenging to access any data where the evidence are stored in virtual devices. To carry out any criminal cases, proper documentation must be formed and presented. In some cases, the relevant criminal records cannot be predictable, because there are high chances that evidence not at all be collected or accomplished. In the meantime, it has been revealed that the evidence does not exist anymore in digital form (i.e. evidence might be deleted, altered or restart the system etc.). In order to identify any pieces of evidence in the cloud environment, the system must be examined and configured in such a way where the location or data centre must be resolute. Technically sound forensics investigators can determine the tools and techniques that should be used in order to investigate the forensic data. Secure data storage and preserve the evidence are the top priority must undertake. The internal team must collaborate with the external members such as academics, third party and cloud service providers. Taking authorisations are other challenges to digital forensics investigation because it delays the investigation processes. There are many types of authorisation which will be delivered by a different agents such as law enforcement agent, internal or external staffs. Usually, incidents are continuing to affect several targets which aiming the goals. A cloud forensics investigation is being started when occurrences take place. To generate or resolve the incidents, all actors use some assets such as methods, plans etc. An actor plays an important role in making the case very productive in the events of the incident by the following planning and organising the steps. Therefore, an actor monitored all activities and informed to the team in order to minimise the risks.

- Planning: The concept planning that is used in both internal and external investigations. Proper planning ensures the investigators to investigate a crime scene if any incident occurs. The planning includes internal and external members, preparations, training, developments, implementations, and SLA (service level agreements). The aim of the concept planning is investigators can make sure any operations that take place with well prepared and to support in case of incidents during the investigations. A good plan can deliver the quality of evidence and minimise the risks. When a crime happens in the cloud system, retort the incident is very challenging because if there is no proper plan. Develop a proper plan can be reduced any types of risks, policies and procedures must be explained clearly if any investigations will be tested. On the other hand, a forensic investigation team is responsible for any types of aspects during the investigation which should be dealing with which investigators (it might be internal or external staff). Moreover, SLAs are responsible how forensics investigation can be dealt between clients and cloud service provider. Strong SLAs must be contemplated to deliver practical and law in details along with all roles and responsibilities among clients and cloud service provider, legal terms and regulations, multi-tenancy and multi-jurisdiction environment, clients data confidentiality, data privacy and security policies.

-Action: An action is an operation performed over a period of time. Generally, an action is performed by an actor and effect on the data. Appropriate actions can be resolved the incidents in order to construct the integrity of evidence for forensic investigations. Appropriate actions satisfy the goals and meet the requirements to resolve the incident. Actors must be identified the potential risks and the type of incidents that may occur before taking any actions. However, risks can be data loss, data breach, illegal data traffic and loss of manpower. Before considering any actions, it should be necessary to ponder the quality and availability of evidence, goals, requirements, privacy policies and legal requirements. For instance, an action can be view, process, transfer, store, delete and retain data and notice, consent to the actor. An action is controlled by the right and obligation.

- Report: This concept emphases the report to state findings during the analysis of evidence. The contrary, report is indistinguishable as of documentation. Typically, the report emphases on the preparation of investigation and presentation of the case in the court or to the organisation. After the examination and analysis of the data need to be converted to report where to report will be presented to the jury. In many instances, the court can make the decision based on the presentation of the report. Therefore, a well-documented report produces using proficient evidence on the analysis of the evidence. Evidence should be presented in a way where the jury can understand all technical facts on cloud computing. The report should be submitted with all supporting documents relating to the evidence where the chain of custody is properly maintained to the court. The well-documented report should include details of findings, types of incident, who's responsible, the location of the incidents etc. The report must be represented by the persons who are having excellent knowledge of law and is not only the person who is technically sound.

- **Technical Level**

The technical level is motivated by the organisational level as concepts on an organizational level to support the perception of what are technical measures are required to investigate forensics data in the cloud environment. The main importance of this level concentrates on the technical procedures during the forensics investigations in cloud forensics systems. Therefore, the researchers has identified the following concepts:

-Evidence: Evidence is defined as collective information about an action by the actors involved within the system. Actors such as user or CSP are responsible for implementing their evidence collection mechanism. The evidence is associated with other entities for collecting different level of information based on the evidence collection mechanism or generation. During the investigation, potential evidence are identified when crime scenes occur. Usually, incidents can be categorised by timestamps, alteration, and deletion of any events. If any data is altered, then it should be considered as corrupted evidence. Identifying and collecting this type of evidence can produce new evidence such clients logged in or out which can be used in court for the report. Under the evidence concepts, some concepts consider such as evidence acquisition, evidence process, and evidence examination and analysis. Where physical access is possible to the crime scene, then forensics data is contemplated for potential evidence which should collect, preserve and store for forensic analysis. On the other hand, the nature of cloud computing, there is physical access limited or not possible. Because of this reason, evidence acquisition is considered at the forensics investigation. After evidence acquisition, evidence must be transported to secure place by the forensic investigation team. Evidence acquisition and transportations mean that evidence are stored in a secured location for investigation. For instance, provenance is a type of evidence generation mechanism. Cloud service and development models are a source of evidence. In IaaS, VM snapshots are a source of evidence, and in SaaS, evidence can be generated from the logging API.

-Process-investigation: The process concepts is to investigate forensic evidence in a cloud computing environment. The process includes methods, investigation, type of data that need to process, data integrity and so on. WG Kruse et al. (Kruse II and Heiser, 2001) describe the forensics methodology into three procedures such as (1) acquisition of evidence without violating the original data (2) recovering the evidence using the authentication methods is same as the original (3) examining and analysing the evidence without altering. The main aim in this concept is maintained the data integrity while preserving the evidence and without manipulating the chain of custody. Generally, the acquisition is a method of producing a duplicate of evidence within evidence. Actors will decide what type of process should use for evidence acquisition. When the acquisition of evidence is stored in the data centre, so that acquisition should materialise through the system is administered and such methods must apply to confirm the tenant's data privacy and effectiveness of the process. First of all, a search strategy must be applied using the mechanisms and forensics tools must be used to collect, extract data in order to confirm data integrity is maintained appropriately. During the forensic investigation, data integrity can ensure whether data has been altered or not from the acquisition period. Evidence transportation can be done after the acquisition. When evidence transport to the data centre or location using the different methods, the result of the evidence transmission must be the same as the original. The same methods can also be applied while evidence is stored. The internal or external team must ensure that evidence cannot be violated and it remains as it is. Analysing any evidence must be in a meaningful and evidence must convert into the feasible form and size. The correct timeline should be maintained in order to response critical enquiries. So that, the reconstruction time zone is challenging in the cloud system because of the different location time zone.

-***Requirement:*** Requirements are the constraints within which specific actions to be taken or restrict the way that actions can be taken. The concepts requirements define the ability to which actors must follow. It can be directly derived from clients requirement. The concepts requirements assign with evidence identification of a potential solution to problems and challenges in digital forensics. According to Ruan (Ruan et al., 2011a), digital forensics is categorised into three dimensions such as- technical, organisational and legal. The technical dimensions typically include issues that relate to technical, i.e. process, tools and methods. The process and methods must be described based on the requirements available into the incidents. The requirements are introduced by forensics investigator, and it must be implemented and well documented for future use. The organisational dimensions define the actors such as CSP, internal and external member, third party etc. In the organisation dimensions, actors will be informed if any incident occurs and then the experienced staff would follow the correct methods to establish data integrity. Legal dimension is dealt with the laws. The distributed nature of cloud computing, evidence may reside in any other country data centres. Different country has different law and legislation. So that multi-jurisdictions have to be considered by the forensic investigators. When a requirement is introduced from the system property such as transparency, further analysis is required to establish if and how that requirement can be satisfied. In our case, goals also introduce the requirements.

-Mechanism: The concepts mechanism is delineated mainly use during technical or non-technical result that satisfies the requirement to achieve the goal. For instance, we consider provenance as a technical mechanism for transparency. Policy document disclosure to the user is also a mechanism to support transparency. Therefore, the mechanism is associated with the evidence.

-Provenance: The concept provenance, in our case, is a Transparency Enhancing Technology (TET) that is realised by the mechanism to satisfy the transparency requirements. We consider provenance from three perspectives, i.e. entity (i.e. data), activity (i.e. action performed on data) and agent (i.e. actors such as data owner, user)(W3Consortium). The provenance produces a chain with various attributes to track actor, data and action necessary for dealing with transparency. Provenance data is immutable and often contains more sensitive information than a traditional log.

-Documentations: A well-documented evidence is carried out significant investigation and is continued simultaneously through the forensic investigation in a cloud computing environment. According to Adam et al. (Adams, 2013) *"Documentation is vital to ensure that a record is kept of all activity associated with the acquisition of the electronic data and subsequent transportation and storage as there is the potential for the whole process to come under scrutiny in court"*. The concepts documentations comprises evidence, investigation process, actors and chain of custody. The goal of this concept is for proper investigation documentation is needed in order to win a case in the court or inside analysis during the investigation. When a crime occurs, investigators must keep the incident in the document for future reference. Also, the investigator must monitor the specific stages according to the occurrences that is happened. These stages must be assigned to in a guide, and all members of staff must follow the manual. At the early stages of incidents, documentation can help keep a record in right track and take all possible actions using the various techniques and tools. To keep the record up to date, a good documentation is important in order to perform training and risks analysing in the investigation. Any methods that is applied during investigation and tools that is used must be documented to keep a chain of custody correctly. Any modifications in the evidence must be also documented.

-Risk: The concepts risks is the main concern in a forensics investigation. The risks may cause to reduce the ability to achieve the goals during the investigations process. Thus, risks identify all possible facts of incidence during collection, preservation and analysis within the forensics process. Throughout the investigation, forensic investigators need to identify all possible problems in determining the facts of the incidents. Also, they need to recognise the nature of risks and determine whether they are prepared to proceed or not. Besides risks can be partly transferred to cloud service provider via SLA but remaining risks still have to be monitored and assessed. Because of multi-tenancy where same infrastructures are used in different users and make it difficult the isolated evidence and concern for data. When forensics investigations are carried out, might any other confidential evidence might be exposed accidentally. This is a high risk in the digital forensics, especially in the cloud environment. Another risk are storing the forensic evidence in the cloud where evidence can be stored in a different location which is making a complexity during the forensic investigation. This is a huge risk for investigators for data identification. The decision includes different issues such as high risks, cost, damage, and availability of resources. Once the risks identified, investigators need to involve all stakeholders in the investigation.

- **Legal Level:**

After identifying all the concepts at an organizational and technical level, the research has conducted some concepts to represent the evidence in a court through proper documents, logs, i.e. who deal the evidence, how was done, whether data integrity maintained or not etc. The following concepts we consider at the level of legal to ensure proper investigation forensics data in the cloud.

-Law Enforcement Agent (LEA): This concept is used to conduct a forensic investigation in the cloud. Without these concepts, the proper investigation cannot be done. The aims of this concepts is to ensure the investigation must perform in an agreement to current law and legislation. The LEAs is always chased the potentially illegal activities. LEAs include customs, police officer or federal agent etc. and they have authority to control in particular jurisdictions. The investigation process, procedures and guidelines are properly maintained by the LEAs. The guidelines stipulate the rules and legislation that all government agent should follow when they are compromising with the forensic investigation. LEA's can ask for the assistance of external consultants to advise them with the process of the investigation if any complexity of incident occurs.

-Right: Right is broadly defined as entitlement to perform certain actions or be in certain states or entitlement that others perform certain actions or be in certain states. For instance, actors can have the right to access the data based on the purpose or identity. Right controls certain actions to be performed by the actor. A right can be a claim which is the entitlement for a person to have something done by another person. It is important to preserve the right of the owner before granting access to other users.

-Obligation*:* Obligation is a correlative of the right. Similar to the right, obligation influences the certain action to be performed by the actor. However, obligation provides the mandatory actions that must be performed for the context. It can be a duty or social responsibility. For instance, cloud provider takes the owner consent as a duty for the secondary use of the data.

5.4 Conceptual View

In the previous section, we describe all the concepts and relationships among the concepts explained for dealing with the investigation. In order to achieve a goal, we need to understand the underlying issues before undertaking certain practice. In the conceptual view, we encapsulate all the concepts which are used in the different levels such as organisational, technical and legal levels for digital forensics investigation.

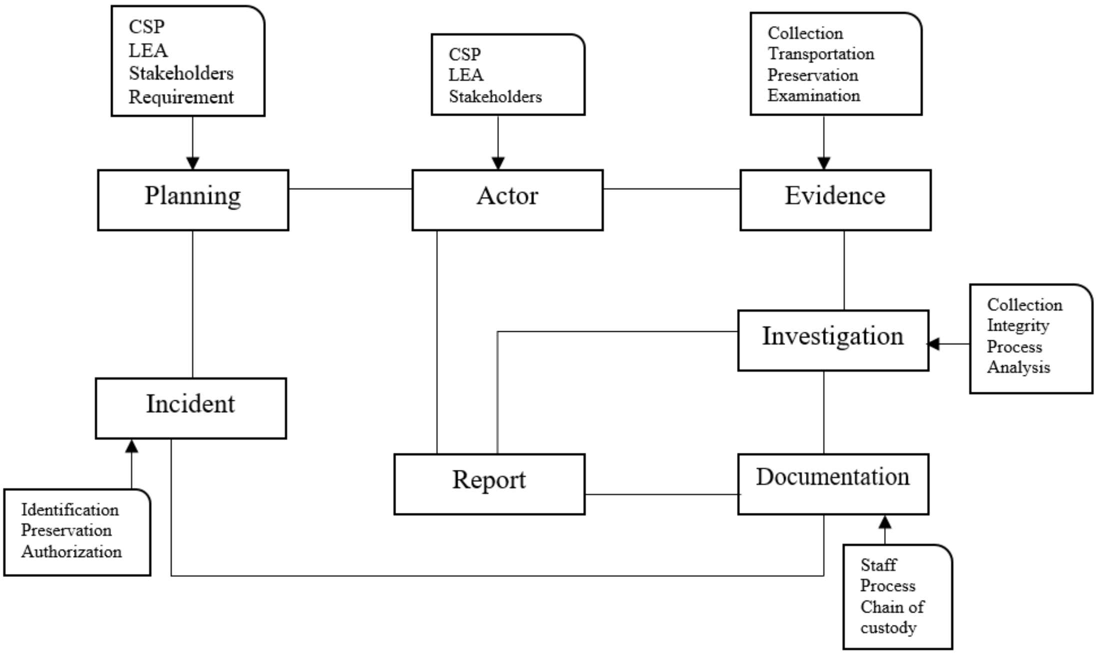


Figure 5.4: Conceptual View of CeFF

Actor includes the following entity such as Cloud service provider, Law enforcement agent, and business stakeholders. All entities are relayed between them to produce effective and efficient investigation in the cloud environment. Each actor has a specific role depending on the context and also has right to claim anything. They must interchange and share the ideas and information with them. Typically, cloud service providers are eager to provide their data to access and help them to carry on the forensic investigation. Finally, CSP, business stakeholder, LEAs are necessitated throughout the process of investigation.

The *planning* concepts have many actions which must be measured in the event of incidents. These concepts have to prepare all the requirements, potential consequences for the incidents, potential risks for the process the investigation. A proper plan can deliver the quality of evidence and minimise the risks. When a crime has happened in the cloud system, retort the incident is very challenging because if there is no proper plan. Develop a proper plan can be reduced any types of risks, policies and procedures must be explained clearly if any investigations will be tested.

In this conceptual model, *documentation* is a core component, and data integrity and chain of custody should be retained at all the time. Well documentation must be maintained from beginning to end of the process along with other concepts. Documentation must be maintained in accordance with procedures by the investigators. To keep the record up to date, a well documentation is important in order to perform training and risks analysing in the investigation. Any methods that are applied during the investigation, and tools that are used must be documented to keep a chain of custody in correct manner. Any modifications in the evidence must also be documented. Besides process and requirements are continually running in parallel because both of them depend on each other. When process complete, then what type of requirements are needed to minimise the risks. The outcome of the documents, investigator make the report in order to present in the court or to inside the organisation.

The aim of the conceptual view is to describe the understanding of all the concepts that have been considered and how each of the concepts plays the role during the forensic investigation in the cloud computing environment. The conceptual view provides what exact relationship each of the entity and how they represent while investigation is. The importance of conceptual view enables to provide a solid background of developments and analysis that can help to develop an effective and accurate framework to the digital forensics investigation in the cloud domain.

5.5 CeFF Meta-model

In the previous section, we describe the conceptual view of the concepts. In this section, we have revised all the concepts and justify the relationship of each concept at a different level of perspectives such as an organizational, technical and legal level. We have identified several concepts in order to constitute the meta-model. A meta-model can help the developers to design the process of all corresponding aspects when developing cloud-enabled forensics system. In this meta-model, we have encapsulated all the critical elements in this model and explained how all the components works and their relationships.

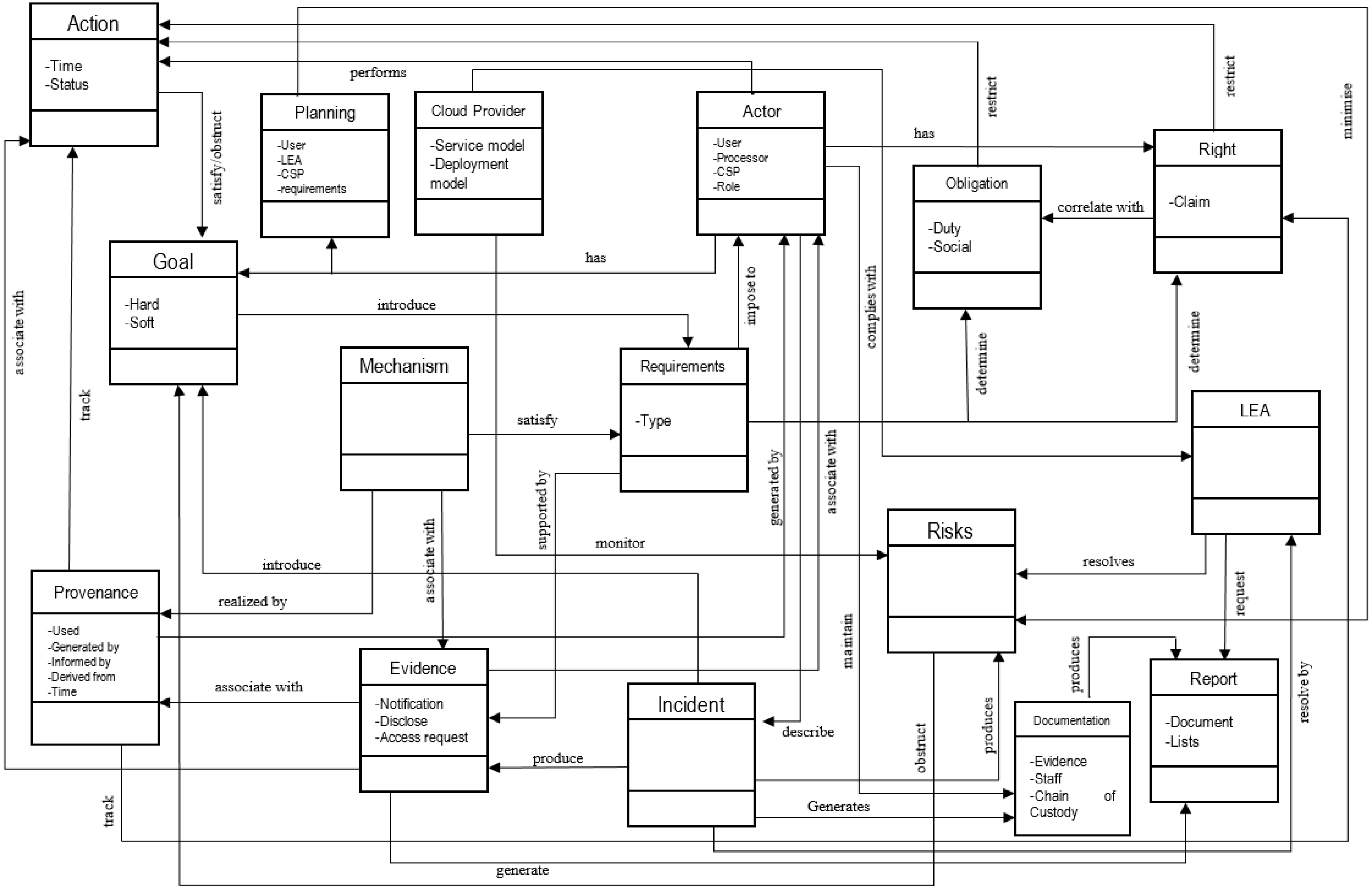


Figure 5.5: CeFF modelling Meta-model

The investigation method begins always when an incident happens. As soon as the incidents are identified, the forensic investigators are looking for the type of incident, time of the occurrences, malicious actors etc. In the cloud, there is always target to cloud service provider service or organisation or clients. Most of the malicious people use the CSP services as a normal user to launch their attack. The cloud service provider main concerns are on the users because CSP does not who is malicious user or who is not. In our concept, we have identified some actors such as CSP, internal and external staff, LEA and malicious people.

In many cases, the malicious actor is always targeted one incident at a time. When incidents occur, then it is initiated several goals. On the occasion of the incidents, the investigators start using some services such as forensics, tools, plan, process and procedures to reconcile these issues. The services that could be used into the related people such as technicians, investigators, law enforcement agents and any other people who are working on this case. However, investigators can establish policies in relates to making any decisions based on the planning, identification, preparations. Proper planning and strategies will make the case very effective in the period. A well plan can deliver the quality of evidence and minimise the risks. Initiating the response plan strategy can confirm the all incidents are under examination that considered all potential risks. Policies and procedures must be explained clearly if any investigations will be tested. On the other hand, a forensic investigation team is responsible for any types of aspects during the investigation which should be dealing with which investigators (it might be internal or external staff). Practice and guidance do a vital role in every aspect of the investigation by reducing any errors and risks. Cloud service providers are responsible for helping all investigators along with all investigation related evidence that available in CSPs infrastructures. It means that all actors have to collaborate with each other for quality investigation. During the investigation, identification of the evidence is crucial because if any violation of data is collected and break the chain of custody. Therefore, forensics investigators and LEAs must be skilled in handling possible evidences that need to be preserved with data integrity and continued the chain of custody. Because of the nature of cloud computing, data can be stored in different locations, so this a challenges for LEAs and investigators to identify the location and different countries have different law and legislation. Therefore, forensics investigators and LEAs should conduct with the legal authorities of the country to get access location of the evidence, and the evidence must be up to date during the investigations.

After identifying, collecting all the evidence, forensic investigators have to find what are the requirements needed in order to solve the problems. Both investigators and LEAs will determine the requirements based on evidence, and all the requirements should be supported by evidences. Requirements determine the right and obligation because right performs certain actions and obligation is a correlate of the right.

Documenting the evidence is an important aspect in the digital forensics investigation. Well maintained documentation provides up to data, integrity and chain of custody that can help to win a case in the court. When an incident happens, forensics investigators begin their investigation from the time of the incident. Therefore, proper documentation can keep a track record of the incident which can reduce the risks. Also, it is important to keep document when any test cases and risks analysis took place during the investigation so that it will help to investigators if any investigations needed in future. Proper documentation can deliver the historical evidence, records during the investigation period. After having a document, the jury needs to present a report in a court to represent the case. A report should be understandable, and all technical phrases must be clearly explained when presenting the report. Therefore, the report must be represented by the persons who are having excellent knowledge of law and is not only the person who is technically sound.

This chapter has delineated the cloud forensics related concepts at different levels such as organisational, technical and legal levels. So that, investigators can distinguish all those concepts. We describe all the concepts and relationships among the concepts explained for dealing with the investigation. Therefore, all the concepts, we encapsulated in the conceptual view. In the meta-model, we have revised all the concepts and justify the relationship of each concept at the different level of perspectives such as an organizational, technical and legal level. We have identified several concepts in order to constitute the meta-model. A meta-model can help the developers to design the process of all corresponding aspects when developing cloud-enabled forensics system. In the next chapter, we will implement those concepts into process, details how the procedures will take place during the forensic investigations.

5.6 Conclusion

This chapter has introduced the concepts and meta-model as the basis of the modelling language. This chapter is also presented the list of concepts in different level such as organisational, technical and legal level which are required during the forensic investigation. Also describes the conceptual view of CeFF framework and a Meta-model to rationalise in connection among concepts. The proposed meta-model allows identifying both direct and indirect relationships with the concepts in a systematic way. The next chapter will focus on the CeFF investigation process.

Chapter 6

CeFF Investigation Process

6. Introduction

In the previous chapter, we have discussed the framing concepts at different levels in the context of cloud computing. In this chapter, we delineate the process of our framework that can considerate forensics investigation process in the cloud environment starting with the crime context analysis and concluding with specific actions for investigating the forensic evidence in an automated manner. During the forensic investigation, some methods will be led by automated whereas some methods will be conducted manually. The process we have designed in such a way that is concentrated automated to manual procedures. In our CeFF investigation process, we have discussed four activities and its steps. The following four activities are introduced in CeFF process:

- **Crime context-** to identify the background of the crime; in particular, crime preparation, investigation strategy and determining the complexity.
- **Identify risks-** to identify all possible risks to determining the facts of the incident.
- **Evidence-** to identify all relevant evidence and segregate all evidence accordingly to build the case.
- **Identify forensics actions-** to identify appropriate actions to resolve the incidents to construct data integrity for forensics investigation.

This chapter will focus on proposed CeFF investigation process model that is integrated with ISO/IEC 27043:2015 forensic investigation standard. In the end, we will summarise the chapter.

6.1 CeFF Investigation Process Model

In this section, we propose cloud forensics investigation process in the context of cloud domain which is integrated with digital forensics standard ISO/IEC 27043:2015. The ISO/IEC forensics standard group categorised forensics investigation process into four processes such as readiness, initialisation, acquisition and investigation. In our thesis, we are not considered the readiness process and the rest of the processes we are contemplated in our CeFF investigation process where investigators can involve dynamically to investigate any crimes that are happened.

In this thesis, the CeFF process consists of four activities such as understanding crime context, identify risks, understanding evidence, and, identify forensics actions.

In the crime context, we consider the following steps: (1) identification of incident, (2) retort of the incident and, (3) plan and preparation for investigation. Crime needs to be identified and modelled with the all relevant resources i.e. information, software etc. to establish the case. In particular, investigators should determine all types of crimes and resources that are used in this activity. Also, investigators need to identify all potential resources, criminals' resources, and cloud service providers and its location of the crimes. When an actor is confirmed crimes, then the investigation team will be involved with relevant skills people such as cloud technicians, legal advisors and law enforcement officers. While identification stage, proper documentation should be maintained in order to plan and deploy their strategy for further investigation in the cloud domain.

Once a crime is identified, potential evidence must be identified and segregated all evidence to build the case. A proper understanding forensics evidence can determine to set up cases and actions accordingly. We consider the following process to understand forensics evidence such as- (1) Collection and acquisition of evidence, (2) examination and analysis of evidence and, (3) transportation and preservation of evidence. The process can perform many times to support forensics investigation in a cloud environment.

After understanding forensics evidence, the main concern is to identify the possible risks during a forensics investigation. The risks identify all possible facts of incidence during collection, analysis and preservation within the forensics process.

The forensic investigator should prepare a document before taking any appropriate actions to resolve the incidents. Appropriate actions satisfy the goals and meet the requirements to resolve the incidents. After all, proper and accurate documentation is important to ensure that the chain of custody and evidence are maintained with the consequences during the investigation process.

To represent our process, we consider sequential logic which can be evaluated the present condition is determined by the existing condition and present condition. The reason we use sequential logic, extracting information from digital sources should be mined before the investigation started. The notation of sequential logic for CeFF process:

CeFF = {{*identify crime* ➔ *forensics evidence investigation* || *crime scene*
investigation ➔*identify risks* ➔*forensics actions: requirements*}
➔*report* || *documentation*} (1)

where

crime = {{ incident ➔ identify ➔ confirm ➔ retort}➔plan & preparation}

where,

plan = {*forensic team*➔*location*➔*evidence sources*}

&preparation = {*assign tasks*➔*policies*➔*operational tasks*
➔*tools selection*}

Forensics evidence investigation = {{*collect*||*acquisition*➔*examine*
➔*analyse*➔*transport*➔*store*}^
➔*identify risks*➔*forensics actions*
||*requirements}*

Report = {*documentation*➔*decision*➔*presentation*

The CeFF process is presented in figure 6.1(a), 6.1 (b) and mutually these depictions will be used in the next section.

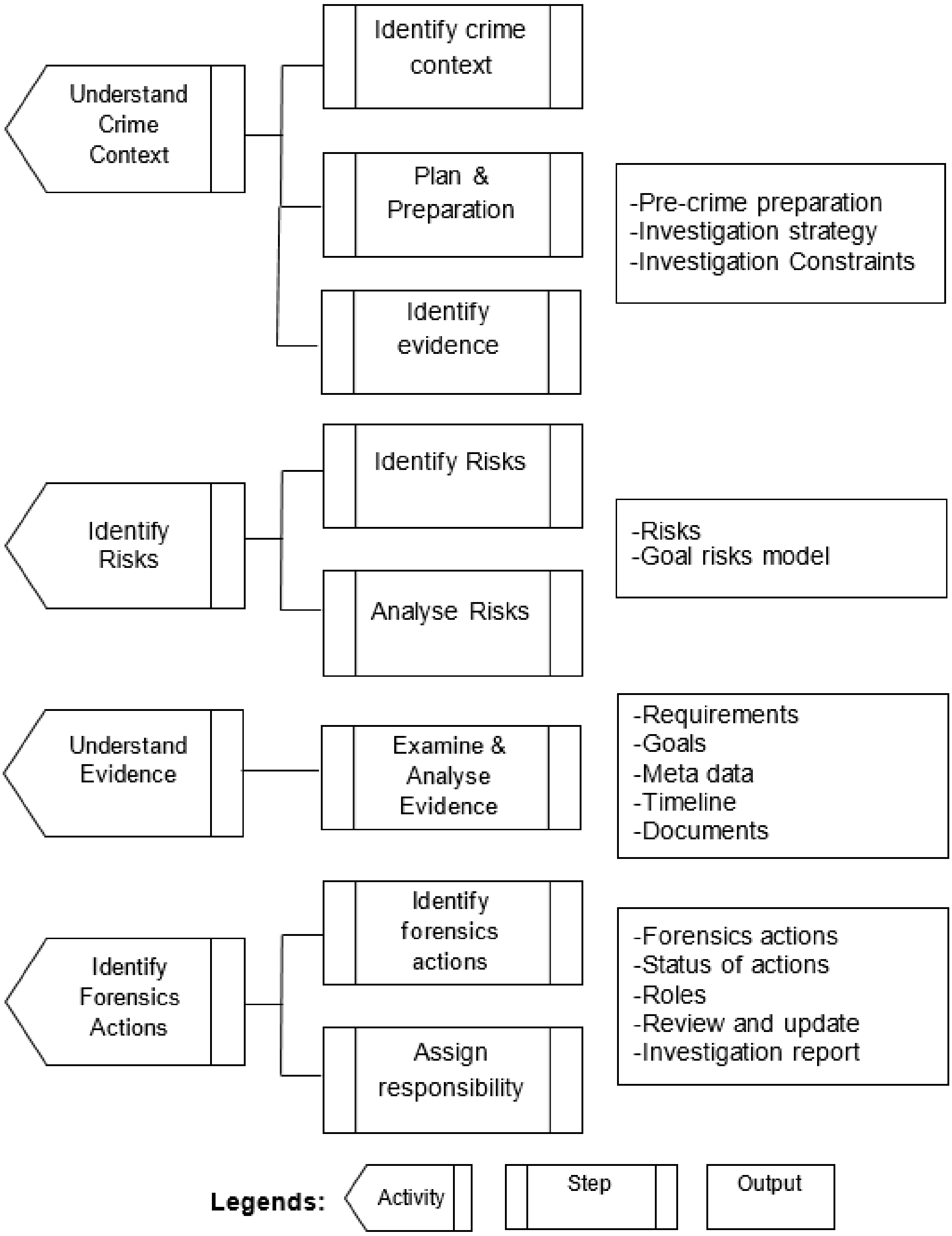


Figure 6.1 (a): Systematic process of CeFF Investigation

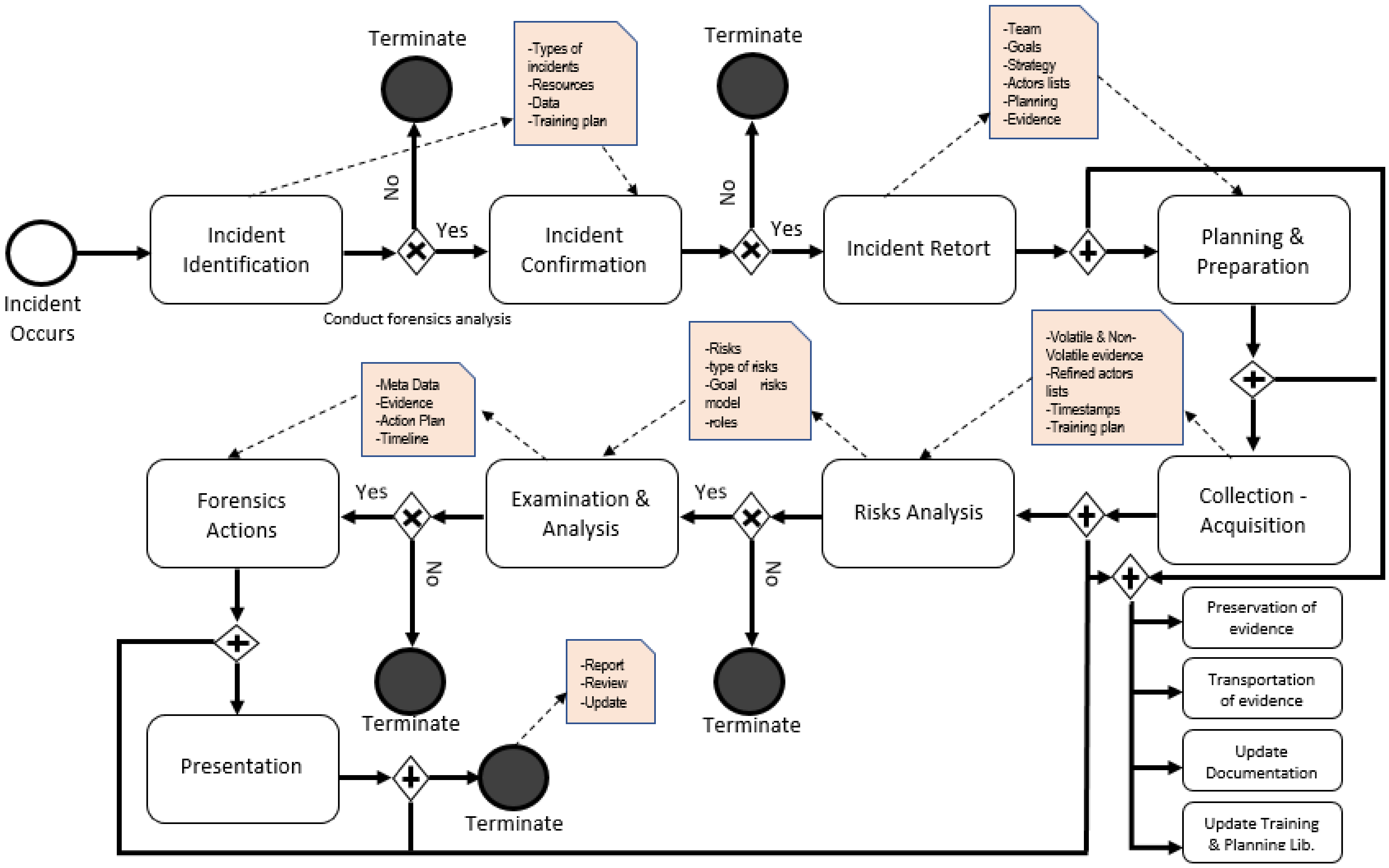


Figure 6.1 (b): Process flow diagram of CeFF

6.1.1 Activity 1: Understanding crime context

The main activity of the proposed process is to understand and initialise crime context from different sources such as actors (external), administrator or automated system for forensic investigation process in the cloud. The crime context follows the following steps: (1) identification of incident, (2) retort of the incident and, (3) plan and preparation for investigation. The figure illustrates the activities of crimes that performed with its steps.

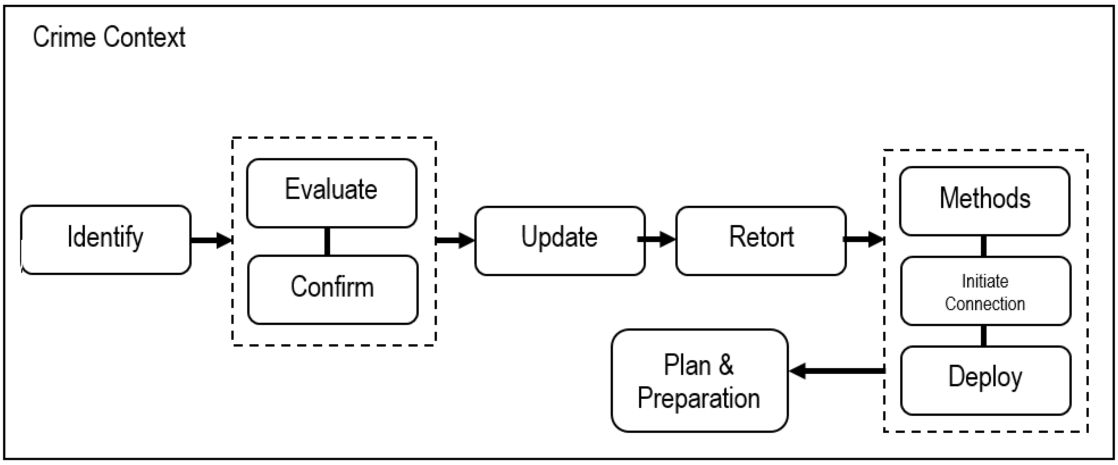


Figure 6.1.1: Crime context process flow

The sequential process of crime is set as:

$$crime = \{\{incident \rightarrow identify \rightarrow confirm \rightarrow retort \rightarrow plan \ \& \ preparation \qquad (1.1)$$

Step 1: Identification of incident

In the first step, crime needs to be identified and modelled with the all relevant resources, i.e. information, software etc. to establish the case. In particular, investigators should determine all types of crimes and resources that are used in this activity. Also, investigators need to identify all potential resources, criminals' resources, and cloud service providers and its location of the crimes. Incidents can be identified by forensics investigators based on a sequence of measures or natures of anonymous events. The identification of incident is a method that instigated the complete forensics process for investigation. Throughout the investigation, forensic investigators can establish a proportional data set which includes types of incidents, timestamps, and findings

When actor is confirmed crimes, then the investigation team will be involved with relevant skills people such as cloud technicians, legal advisors and law enforcement officers.

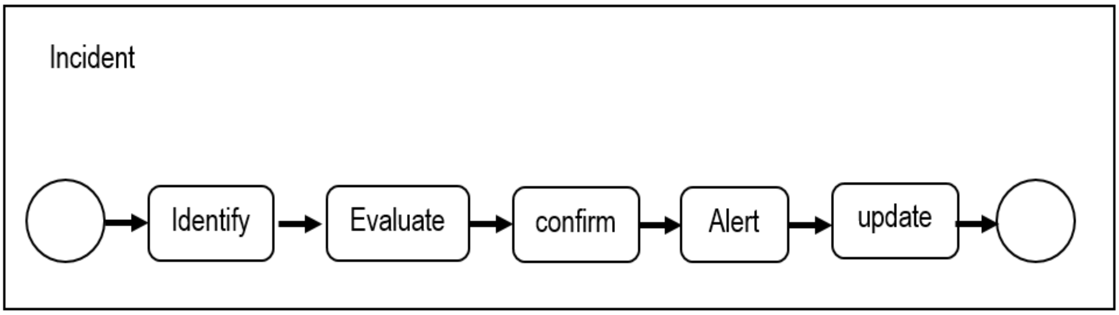


Figure 6.1.1(a): Incident process flow

While identification stage, proper documentation should be maintained in order to plan and deploy their strategy for further investigation in the cloud domain.

The sequential logic of the incident as follows:

$$Incident = \{identify \rightarrow evaluate \rightarrow confirm \rightarrow alert \rightarrow update\} \qquad (1.2)$$

(a) Identify: In the forensics investigation, when an incident is occurred, then the identification process is initiated. This process is always identifying the forensics investigators with the automated forensics tools. The incident identification process is a physical task often complete by the forensics team (not administrator) based on the prior knowledge. The incident identification is also accomplished by scene possessor or cloud service provider. A provisional data set must be created in order to make lists of the type of incidents, incident findings, time of incidents (start and end time), guidelines for the forensic investigation.

(b) Evaluate: After identifying the incident, the forensic investigators and the external forensics team are evaluated using their system. After evaluating the incident, the investigators will decide for appropriate action for their forensics investigation.

(c) Confirm: In the confirmation process, after identifying and evaluating the incident, the actors (i.e. investigators or external advisers) must be confirmed the incident and the make alert to next stage in the incident response. In this confirmation process, the investigators should be conscious of what type of forensic investigation is needed. The forensics staff is accountable for security that necessity to inform another member of staff regarding malicious activities such as DDoS, data loss, breach of confidential information, illegal activity, trafficking malicious data etc. Forensics investigators should always alert for the potential risks that could be happened, and also they have to recognise the nature of the crime. Once they understand the crime, then the can decide whether they can initiate an investigation or not. The decision might be cost, staff availability, dangerous incident, volatile data etc. After confirming the incident by the investigators, then it has to notify to another member of staffs who are involved in the investigation. Proper approval has to be confirmed in order to take the subsequent phase of the investigation.

(d) Alert: A notification must be sent by the investigators to start an investigation, when forensics investigators are verified and confirmed the incidents. The alert notification should be sent to all business stakeholder includes internal and external actors.

(e) Update: Internal investigators are required to update all the incidents once the administrator is confirmed and validate the incidents. This should include types of incidents, locations, time of the incident, lists of incidents, system information etc.

Step-2: Retort of incident

In step -2, the retort of the incident is established, once the incident is updated. In the first, retort is typically encountered when incidents scene is confirmed by the investigator. In the event of the incidents, the investigator has to present physically to determine the type of incident and type of investigation that need to be considered. Well documentation can support for investigation, and in parallel, all resources have to be

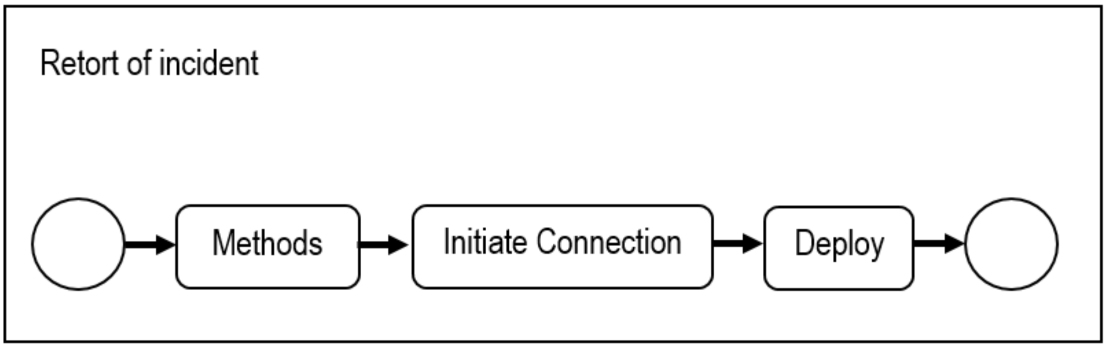


Figure 6.1.1(b): retort process flow

identified in order to response the incidents. The investigator should be settled the team and trained them tools and systems and show the process and procedures. When the team is used to practise the tools to detect the possible evidence, the team must handle with all tools. The primary responder is responsible for maintaining the accurate document and also maintain the chain of custody.

The sequential logic for retort of incident as follows:

$$retort = \{methods \Rightarrow initiate\ connection \Rightarrow deploy\} \qquad (1.3)$$

(a) Methods: Forensics investigators must decide the methods that are going to apply for the investigation. The methods can be constructed after identifying the incidents, resource list, time of the crime etc. The main aim of the methods is to establish a process that maintains the chain of custody which can reduce the potential risks to forensic evidence. The methods can include search (i.e. might be location, type of incident, document, targeted system etc.), seize (i.e. no. of incidents, affected system etc.), transport (i.e. evidence, data), store.

(b) Initiate connection: Initiating the secure connection for the incident to the isolated host (i.e. cloud system) is important because a secure connection can avoid congestion throughout the forensics investigation. Once the secure connection is established, the forensics investigator can transport the confidential evidence.

(c) Deploy: All the processes that already described should deploy in the cloud system in order to detect the incident. In the cloud deployment, an investigator will choose where the process will establish whether in public or private. After determining the deployment model, the forensics investigator must inform to the internal and external team and the LEAs.

Step-3: Plan & preparation

In the last step, once the incident is identified, the preliminary planning can be carried out based on the previous documentation and the policies for how the investigation will be performed. All the methods and procedures should adopt with the investigation team and tools that are used to identify the potential evidence. *"Trust must be managed through detailed Service Level Agreements (SLAs) with clear metrics and monitoring mechanisms and clear delineation of security mechanisms"* (Simpson and Chandersekaran, 2014). To keep and continue the chain of custody, a proper plan must be measured the investigation constraints that includes resource list, team lists (actors), time plan, budgetary restrictions, action plan etc.

(a) Plan: Digital forensics investigation is typically assumed because there is no clear persistence for the particular scene. Determining proper investigation is very difficult. Therefore, a systematic plan can deliver the appropriate solution for the digital investigation. The preliminary forensic investigation plan typically comprises selecting a forensics team, locations and evidence sources.

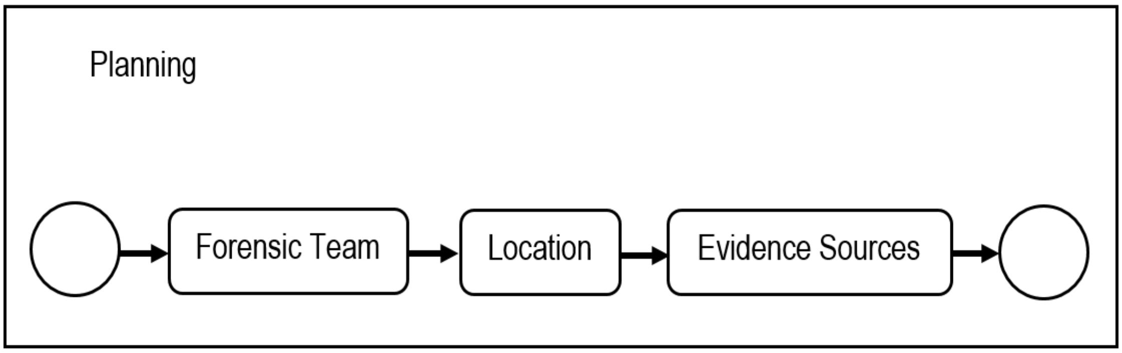


Figure 6.1.1(c): planning process flow

The sequential logic for plan as follows:

plan = {*forensic team*➔*location*➔*evidence sources*} (1.4)

-Forensics Team: The forensic administrator should select the investigation team. The forensics team should have depth knowledge to discourse the problems related to forensic investigation. The team must handle the investigation during any issues may arise. A forensics team must be submitted documents such as reports, incident scene, authorisation, policy, guidelines etc.

-Location: In the digital forensics investigation, location is important to initiate the crime scene. The locations can be include network, physical, virtual, the place, forensics laboratory etc. In the physical system, evidence may be situated in the routers, hardware such as MAC address etc. Also, the unidentified location should be considered in the planning as cloud computing is a distributed.

-Evidence sources: After identifying and collecting all the evidence, the forensics teams must be allocated and mentioned all evidence sources, i.e. location, hardware, applications, virtual or physical devices etc. This could produce a quality investigation in digital forensics.

(b) Preparation: The critical approach in the forensic investigation is preparation. In this process, the stakeholders, investigators will investigate the type of crimes, attacks, malicious activities etc. Before starting an investigation, investigators should need to take preparation the particular type of investigation that will carry on. Preparation method aims to increase the efficiency and effectiveness of the forensic evidence. The preparation method includes assign tasks, policies, operational tasks and tool selections.

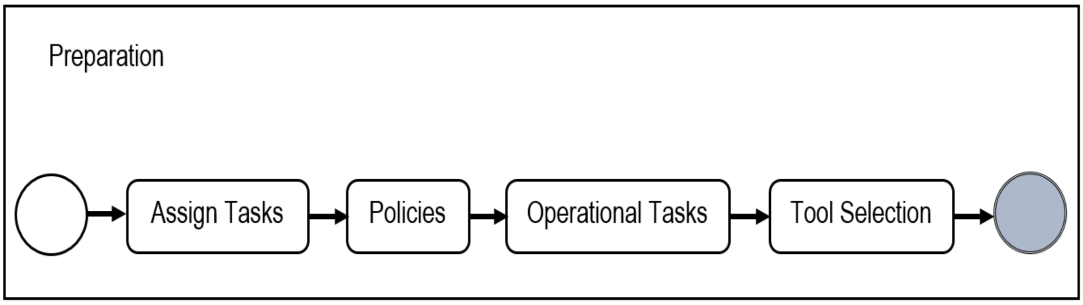


Figure 6.1.1(d): preparation process flow

The sequential logic for preparation as follows:

preparation = {*assign tasks*➔*policies*➔*operational tasks*➔*tools selection*} (1.5)

-Assign tasks: Assign tasks is the process where forensics investigators will allocate tasks to the forensics team. Allocating tasks is very important in order to improve team productivity. The certain team can handle a certain amount of evidence and the certain team can become expert in technically. Therefore, appropriate preparation can produce a quality of the investigation.

-Policies: Before starting the forensics investigations, business stakeholders, investigators must make a draft initial policy and guideline where it should have clear description that how forensics investigation will take place. The policy aims to maintain the integrity of the data throughout forensics investigation. The investigator should be aware of international policy throughout the investigation period.

-Operations tasks: In the forensics investigation, the operational tasks are divided into two aspects such as (i) internal and, (ii) external aspects. The internal aspects include team training, allocating tasks to related member etc. where external aspects include law and legal system, investigation type, liaise with external investigators etc.

-Tool selection: Selection of tools is challenging tasks in the forensic investigation. The tool might be infrastructure level, network level, application level. The investigator should be aware during the selecting the appropriate tool for the digital investigation.

6.1.2 Activity 2: Identify Risks

The third activity of the CeFF process concerns the risks in a forensics investigation. The risks may cause to reduce the ability to achieve the goals during the investigations process. Thus, risks identify all possible facts of incidence during collection, preservation and analysis within the forensics process. Throughout the investigation, forensic investigators need to identify all possible problems in determining the facts of the incidents. Also, they need to recognise the nature of risks and determine whether they are prepared to proceed or not. The decision includes different issues such as high risks, cost, damage, and availability of resources. Once the risks identified, investigators need to involve all stakeholders to do the risk assessment for the forensic investigation.

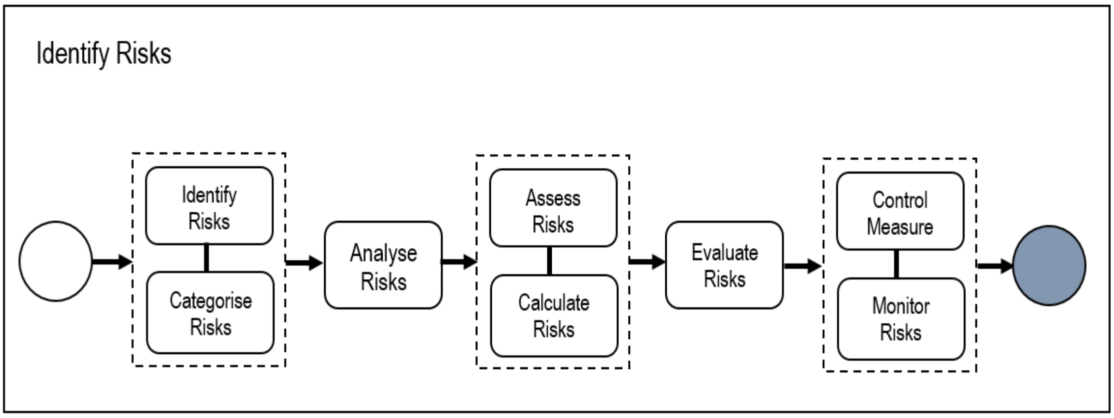


Figure 6.1.2: Risks identification process flow

The sequential logic for risks identification is as follows:

$$Risks = \{identify\ risks \rightarrow analyse\ risks \rightarrow evaluate\ risks\} \qquad (2.1)$$

(a) Risks identification: This process will identify all potential risks and related aspects that can affect the forensic evidence. The related aspects of risks are the principle cause of any risks and managing those risks is a concern of risks administration. The forensics teams who are dealing with only risks factors, they have to find all potential risks. Therefore, the investigators and business stakeholders are knowing about any risks that need to consider for forensics investigations. Risks could be influenced by the factors, and various methods can be applied to find risks such as revising the document, forensics data that already been collected, critical information, taking an interview with skilled members etc. Risks can be concentrating on threats that can be encountered the attain the goals during cloud forensics investigation period. Risks can be any type such as loss of data, leakage of data and sometimes risks can be malicious users, applications, end users etc.

(b) Risks categorisation: The risks can hinder to achieve the goals of the investigation. Any violation of the integrity properties, malicious actors could be tempered the log activities which may not provide an appropriate report for the legal authorities. In this process, we categorised several risks for the forensic investigation. The following risks are:

i. ***Log modification-*** refers modify the logs by any actors such as CSP, investigator, malicious actor etc. Usually, malicious actors are tampered with the log after collecting all the data. Also, a forensics investigator can be modified the logs before submitting the log to the court. Logs are typically contaminated thru false log, deletion of crucial logs and modification of the order of logs(Zawoad et al., 2016).

ii. ***Loss of integrity:*** refers to unauthorised modification by malicious actors. No evidence to prove whether data has been modified or deleted or altered and many copies of data potentially detained by several entities.

iii. ***Loss of availability:*** this concerns if any data is unavailable to the end user and other concerns dealt with if service or server is spoofed, penetrated, suspended in supporting to organisations goals.

iv. ***Privacy violation:*** a malicious user who can have access the log storage, can identify the clients' activities from log storage. This risks might be magnified if malicious actors disclosed the logs activity.

(c) Analysis of Risks: The process of risk analysis could be assisted to produce initial assessment to defend forensic evidence and also restrained from any attack that might be occurred. So that assessment of risks plays an important role in the digital forensic investigation. In the risks analysis, we categorised into two forms such as – (i) assessment of risks and (ii) calculation of risks.

-Assessment of risks: To assess forensic evidence for investigation, the investigator should know what evidence are required to assess. For the risks assessment, we have considered the following terms-

- ***Risks scene:*** that defines any occurrence, incident situation that decreases the ability and capacity of the resources.
- ***Identification of vulnerabilities-*** that defines any defective hardware or system that are used during the investigation. Any faulty system can be exploited the data at any time.
- ***Identification of threats-*** that describes the other risks that can exploit vulnerabilities of systems and devices are recognised. Threats can be obtained from the log files and log activities.
- ***Analysis of event-*** that can be matched a list of vulnerabilities and the threats already identified. From the facts, the event can be analysed.

-Calculation of risks: After assessing the potential risks, the investigators need to differentiate the disastrous and expected risks. This can be done by calculating using the following theory.

$$\mathrm{RA} = \mathrm{PR} \times \mathrm{PI} \qquad (2.2)$$

Where RA = Risk assessment

PR = potential risks

PO = Probability of Incidence

So that, it can be calculated for an individual component within the resources-

$$\mathrm{R} = 1 - \sum_{k=1}^{n}(1 - RA) \qquad (2.3)$$

Where R = 1,2, 3,4,… of individual risks. The composed risks comprise of all risks-

$$\mathrm{Rc} = 1 - (\mathrm{R1}, \mathrm{R2}, \mathrm{R3}\ldots\ldots\ldots\mathrm{Rn}) \qquad (2.4)$$

(d) Evaluation of risks: The evaluation of risks can be done into two forms such as (i) control measures and (ii) monitor risks. In the control measures, the investigators must ask the cloud service provider to deliver their current controls or what to ease the risks that identified. The risks can be measured into three phases-

Phase-1: completion is zero for dealing the risks

Phase-2: completion is partial for dealing the risks

Phase-3: completion is full for dealing the risks.

On the other hand, the process of monitoring risks can confirm that any potential risks are under control and identify if any risks arise. In this process, monitoring can include any incidents, penetration, security, data leakage, mechanisms etc.

6.1.3 Activity 3: Understanding evidence

Once the crime context has been modelled, the next activity is to identify all relevant evidence and segregate those evidence. Because of cloud system nature, many instances running on a single physical machine, it is a challenge for forensic investigators to segregate assets without penetrating privacy that already been shared infrastructure. In this regard, the process involves two categories- examination and analysis. In order to have appropriate evidence, investigators should be examined previous cases and find the patterns that can be facilitated and developed actions plan and reduce the time of examination. Because of the high volume of information and complication of information that is stored on forensic evidence, actors should make decisions that type of tools and approaches will be used to get the appropriate data in a forensic investigation. Also, actors can choose to examine forensics data using automated process and techniques such as filtering, data compression, and de-duplication of data. On the other hand, the analysis is the capability to analyse forensic data to convert into digital data. In order to reconstruct

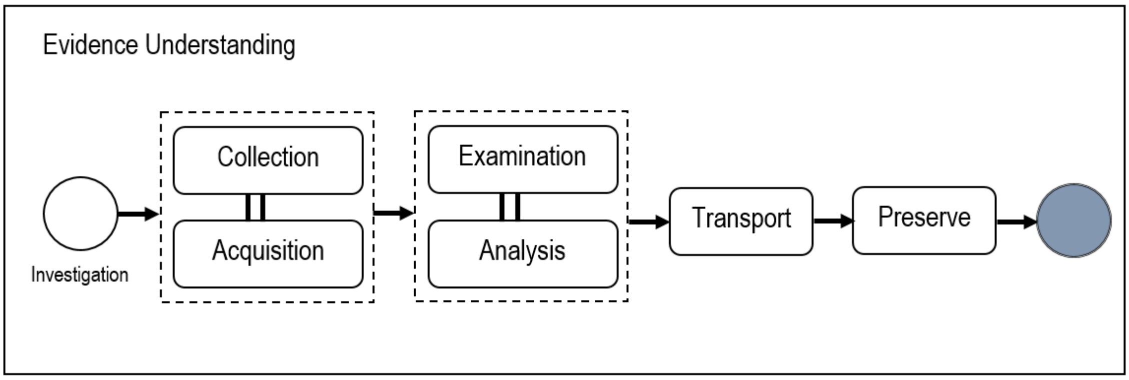


Figure 6.1.3: Investigation process flow

the timeline and potential evidence, encrypted and Meta-data must be analysed and processed from examination phase. All rest of data must keep in a secure place, and it must be accessible and obtainable as demanded. The analysis process can be performed many times to support the forensic investigation in the cloud.

The sequential logic for evidence understanding is as follows:

$$\textit{Forensics evidence investigation} = \{\textit{collect}||\textit{acquisition} \rightarrow \textit{examine} \rightarrow \textit{analyse} \rightarrow \textit{transport} \rightarrow \textit{store}\} \qquad (3.1)$$

(a) **Collect -Acquisition:** This process emphases how data is collected from different types of sources for further forensic investigation. The collection is a process comprising physical resources that include possible evidence. On the other hand, the acquisition is a process producing another copy within the data set. The main objective of this process is to attain possible digital evidence. The forensic investigator should ensure proper collection and acquisition to maximise its potential use of digital evidence. While collecting digital data, investigators must ensure the data integrity and illegal modifications of data in a cloud environment.

On the other hand, the data collection process is depending on the cloud deployment model, and different cloud services are used. It is very important; when investigators collect evidence, they must ensure data must be collected either cloud client side or cloud service provider side as investigation requirements. In client-side data collection, data can be collected from physical memory before shut down device. There are many tools such as LiME, FTK imager etc. to collect memory. When any devices shut down or restart, from that system, evidence collection is critical but using some tools (i.e. Software: TrueBack, EnCase and Hardware: 3p, hardcopy, Tableau forensics duplicator) data can collect during the investigation. All of the above tools are performed forensically sound data acquisition. On the other hand, cloud side data collection can be collected applying remote acquisition approaches to get images from VM.

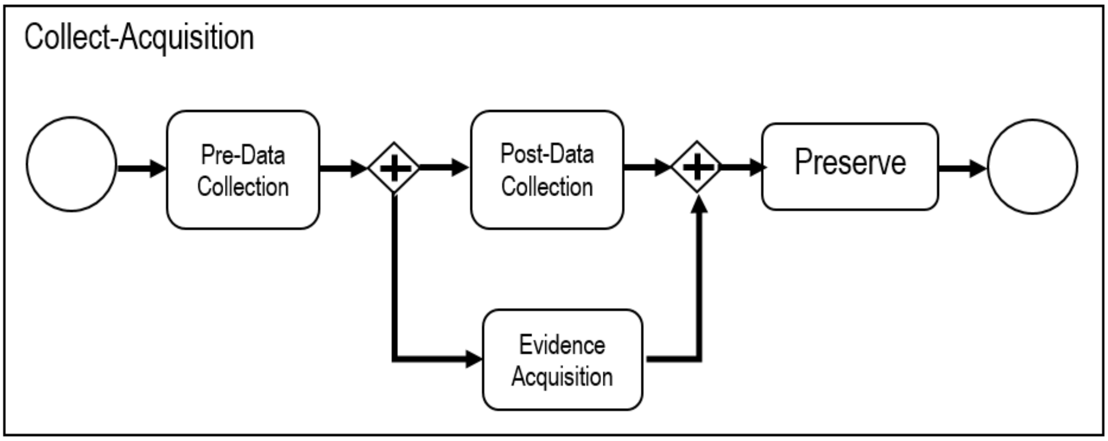


Figure 6.1.3 (a): Collect-acquisition process flow

During the process of collection, data can be collected into two forms- (i) Pre-data collection and, (ii) Post-data collection. In the pre-data-collection process, data can be classified and accumulate into the digital form which is vital for cloud forensics investigation. The pre-data collection can be facilitated forensics investigator before starting an investigation that confirming forensics accuracy. This can be minimised the cost of investigation and reduce the time of investigation as well. On the hand, a collection of post-data is able to receive and retort the evidence when the incident is being discovered. The post-data collection can be distributed manner in the cloud computing environment. Finally, the collected evidence must be documented and patterned for the data integrity to the future use.

(b) Examination & Analysis: Examination is a method that extracted evidence and converted those evidence into an understandable format. Evidence examination can

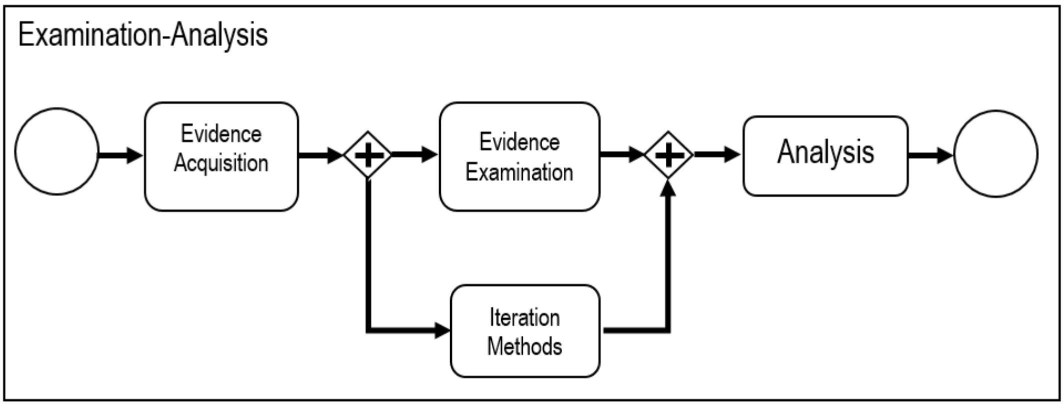


Figure 6.1.3 (b): Examination-Analysis process flow

be included in data extraction and data reduction capability. For quality forensics investigation, investigators need to be processed any altered or modified data by using comprehensive forensics techniques in the cloud system. When collected evidence is preserved in a secure data centres, a number of duplicate copies to the actual data have to deliver where an investigator can be started their investigation on that point. To do the forensic evidence examination, forensics investigator should have a complete overview of all evidence which need to be confirmed before examination is initiated. Else, it may delay which could create issues if any complications are experienced. Although, investigators should do past analysis cases and any plans that already made by previous investigators, which could be provisioned to minimise the forensics examination time and create their new plan for examination. Because of the high volume of evidence and information that stored in the different systems, investigators have to determine what type of tools and approaches are going to be used in order to concentrate on the related information. After examining the forensics evidences, investigators should initiate analysis methods. The analysis approach depends on what type of data is collected and examined by the investigator. So that, the investigator can determine the significant amount of data can be transformed them into evidence. Heterogeneous data from the examination stage, should be analysed properly and should be reserved and kept secure data centre and make those evidences available when needed. Through the analysis period, some iterations methods might be applied to authenticate the forensic investigation.

(c) **Evidence transport:** Transport of evidence is a process where evidence is shifted from the original place to a secure data centre under the supervision of forensics investigator. Evidence might be transferred using external devices or over the internet.

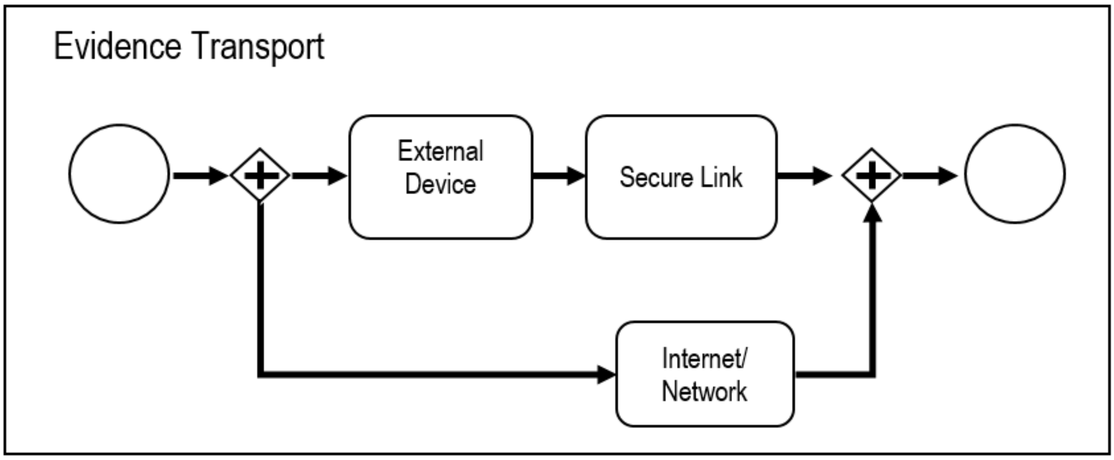


Figure 6.1.3 (c): Evidence Transport process flow

To transfer the evidence over the external device, the conventional methods should be pursued. On the other hand, if evidence transfer over the internet using a network system, the security must be confirmed by the cloud service provider or the investigators. After collecting, examining and analysing all potential evidence have been transferred and accordingly, it should be preserved securely.

(d) Evidence Store: The reason of evidence transportation is data should be stored in a secure place. The evidence also needs to be stored in an adequate secure storage secure place. All storage evidence must check the integrity and well-maintained chain of custody. Forensics investigators have to be considered the following factors such as lost or stolen, natural disaster, malicious attack etc. The forensics evidence can be store in both online and offline storage correspondingly.

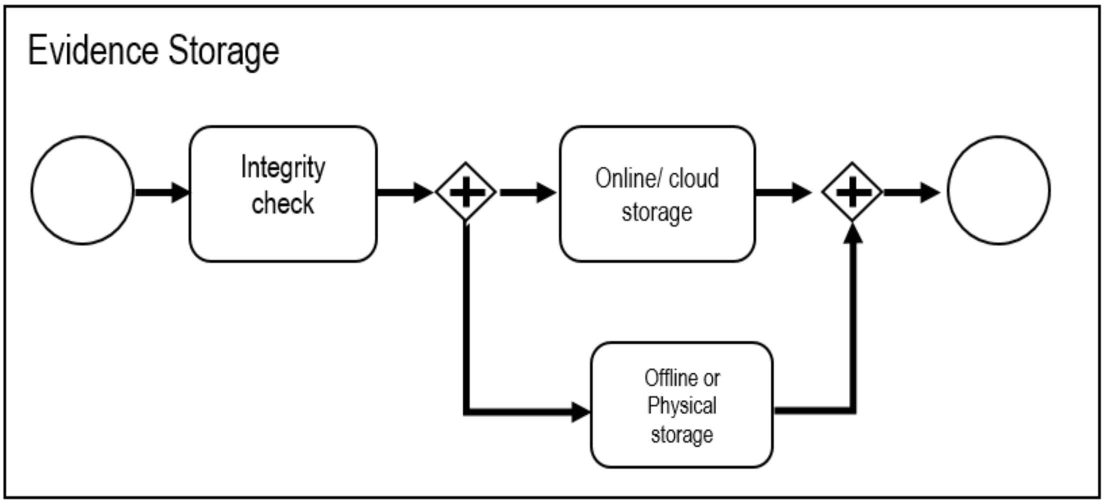


Figure 6.1.3 (d): Evidence Storage process flow

6.1.4 Activity 4: Identify forensics actions

In the final activity of the process is to identify appropriate actions to resolve the incidents in order to construct the integrity of evidence for forensic investigations. Appropriate actions satisfy the goals and meet the requirements in order to resolve the incident. Actors should understand the nature of potential risks and incidents before taking any necessary actions. However, risks can be a financial loss, data loss, loss of manpower, breach on confidential data, DDOS attack, trafficking illegal contents etc. depending on the individual or organisational or public domain. Before considering any actions, it should be necessary to ponder the quality and availability of evidence, goals, requirements, privacy policies and legal regulations. The selected forensic actions should be implemented for the successful completion of the investigation. This step also monitors the effectiveness of the implemented control actions. In order to construct the integrity of evidence for forensic investigations, the following actions can lead to resolving the incidents.

- ***Integrity verification of log:*** to verify the integrity of logs, investigator examine and analyze the data whether the data exists. If data exists, then the investigator proceeds to start the log verification process.
- ***Timestamps verification:*** This action aids to generate timestamps when any files are created, altered and deleted to check the authenticity of the information. Using this action, the investigator can verify the correct time of the files.
- ***Sequence verification:*** This action verifies two consecutive entities. The first entity will be displayed instantly before the second entity in the original sequence of log generation. For example, if the first entity of the log and the second entity of the log represents same, in this case, the investigator should compute the log of chain to verify the appropriate log sequence.
- ***Evidence Creation:*** This action is applied to proof any evidence that already been created for particular information. For example, if one static IP address is created for all logs on the same day, then it is easy to retrieve data if is needed in future. This action saves the time and minimises the cost while investigations particularly in a cloud environment.

The last process is present the report along with all evidence throughout the investigation period. A well- documented report produces using proficient evidence on the analysis of the evidence. Evidence should be presented in a way where the jury can understand all technical facts on cloud computing. The report should be submitted with all supporting documents concerning the chain of custody of evidence to the court. The well-documented report should include details of findings, types of incident, who’s responsible, the location of the incidents etc. After presenting the report, the jury will resolve the case by making decision that the occurrence is imputed to whom. The judgement should be kept in the data centre for the future if it needed.

Above all activities should be followed during the forensic investigation and the well documented must be produced with clear methodologies in order to ensure the data integrity and validity of the evidence. The chain of custody can be preserved all events such as who, when what etc. in order to maintain the quality.

6.2 Conclusion

Cloud computing is distinct due to the distributed and virtualised nature. Traditional procedures cannot be not applicable directly to the cloud environment. Therefore, systematic procedures are required for cloud environments. The digital forensic process is presented in this chapter. These are the procedures that are implemented in this chapter and details on how the procedures can be implemented are discussed in this chapter.

Chapter 7

Evaluation

7. Evaluation

In this research, our proposed framework is applied to the real-life example at ABC Ltd to validate the framework applicability. We have consolidated the case study approach using the concepts that we have demonstrated in the metamodel. Selecting a suitable approach is depending on the various factors such as resource availability that associated with the case study. However, we have evaluated the case study into qualitative and quantitative approaches to develop the test theory. We have conducted the qualitative and quantitative approaches because of the availability of members and using the methodologies with gaining the experience to learn new procedures. This is very constructive for the practitioners to identify the real-life problem with the methodology, i.e. missing conditions or ambiguity. In this case study, we have applied all activities that are performed to understand the investigation necessitated with evidence collection, examining and analysing the forensic evidence during a forensics investigation. In this study, we have considered the following components such as study design, identifying the crime context, understanding the evidence, identify the risks, and the actions. The research completed with the presentation of the report in the framework.

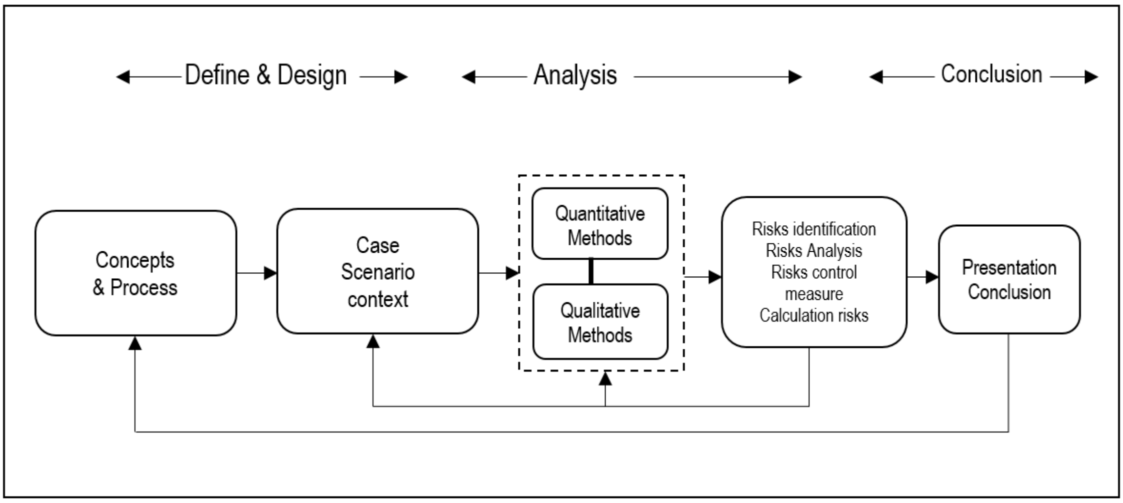


Figure 7: Study Design

During the period of study, we had collected data and selected all data to validate the appropriateness of the CeFF investigation framework. We have followed (Verner et al., 2009, Runeson and Höst, 2009, Kitchenham et al., 2002) the following steps to process our case study.

- ***Research outline***- defines the objectives of the research such as literature review, objectives, aims and goals etc.

- ***Case study plan***- defines the evidence identification, collection, procedures, methods and design the plan step by step.
- ***Data collection***- that includes data collection from different sources during the development of the project.
- ***Data analysis***- includes the assessment and conclude with respect to the case study.

The aims following are of this study-

- To comprehend and practicality of the CeFF framework in helping to ABC Ltd in the investigation.
- To comprehend and support forensics investigation process in the cloud environment.
- To comprehend and identify the risks associated with forensic evidence and the actions need to take.

7.1 Case study 1:

7.1.1 Overview, context

ABC Ltd was established in 2007 and amongst the top vocational training service provider in the UK. ABC Ltd is an independent vocational training provider. It offers various Vocational Learning Programmes and Apprenticeships from level 2 to 6 in Pharmacy Services, Health & Social Care, Child Care, Clinical Health Care, Business Administration and Customer Service. The organisation has already provided more than 5000 learners and offered more than 15 courses. The company is also an affiliated to Pearson VUE examinations centre for major professional training certificate (Vendor qualifications) such as CISCO, and MICROSOFT and recognised by OFSTED to be 'Outstanding' (2014). It also possesses recognitions from bodies such as National Skills Academy, Customer First, MATRIX and Investors in People (Gold). The organisation strives to endure within the top 100 training service providers in the UK. Therefore reputation is the key factor to the organization when promoting itself to the rest of the UK to attract learners. So that Digital forensics investigation is the process that ensures any incidents are effectively and efficiently investigated for the organisation.

In 2016, ABC Ltd had identified an important document that containing a complete new apprenticeships programmes design pattern had been disclosed to a competitor. The file name was "apprenticeships_Programmes.pdf". In the ABC, Mr Bob is a managing lead who managed all credential files, documents etc. for the organization. The company is used cloud services from Microsoft, i.e. Azure. The organisation firstly suspected to Mr Bob because all files and data are managed by him.

Based on the instance, the organisation was raised an investigation case file and was issued to Mr Bob. A warrant was issued by the court, and the court was ordered to seize Mr Bob's PC, laptop, mobile and external devices (USB, hard drive) or cloud services for investigating this allegation. However, a personal laptop was provided to Bob for business purpose and a mobile phone so that the targeted devices are those devices.

In this case study, The main objectives of the investigation were to identify who and when leaked the file and what devices had been used to disclose the file.

We have applied the CeFF methodology to investigate the incident. There already have been discussion CeFF concepts and the processes. Therefore, at this stage, the CeFF methodology can be applied to carry out an effective and efficient investigation.

7.1.2 Activity 1: Understand Crime Context

From the scenario, we identify the actors such as Mr Bob and forensics investigator. In this stage, the investigator will collect all information from all sources such Mr bob's PC, mobile phone etc. In this activity, the process focuses on understanding all possible problems, issues concerning to investigation. Mr Bob is liable for starting the incident because initially he was trafficked the information using his PC or mobile. However, the forensics investigation team is responsible for collecting data and detects all illegal activities to decide whether they are going to proceed with the investigation or not specially classifying any of the information is forged. The investigator can set up a goal and the initial plan to identify any common working pattern using similar previous case.

Step 1: Identification of incident

The primary identification was unsuccessful because of the log files of the OS such as KLN file did not provide any indications. In the time of disclosing file, when Mr Bob trafficked the file, there were no artefacts resulting from connecting any external devices and messenger or webmail services. In this circumstances, the investigator should try to get more evidences from Microsoft cloud storage. Therefore, forensic investigators have to detect Mr Bob's servers where Mr Bob transferred the company's file. In the meantime, the forensics team is responsible to make the incident case and search for a warrant. When a warrant is approved from the court, then the forensics investigator will communicate with the cloud service provider and request for Bob's data that already stored in the cloud. The forensics investigators will follow communication methods where Bob cannot suspect that any activities are going on his cloud account. Simultaneously, Forensics investigators and the team must create some provisional data in order to make lists of the type of incidents, incident findings, time of incidents (start and end time), guidelines for the forensic investigation. The IP address of Bob's is failed to trace because of the proxy server that he has used. With the help of a cloud service provider, the forensics investigator can get more information such as account subscription, log activity, VM and data store etc. In this case, the investigator also maintained properly the policy and guidelines about the data preservation if any external member or cloud service provider is involved during the investigation. Correspondingly, the forensics investigator can start research to identify resources such as any devices mobile, computer and laptop etc. After identifying the potential evidence, the forensics team and investigators have to evaluated using the forensics tools. Once evidence evaluated by the investigators, then they should take decision for appropriate actions for further investigation. Also, data and potential evidence had been documented, investigator could be initiated to implement the acquisition plan and deliver resource list, proper time plan and further action plan. Once the crime identified, the crime unit must be confirmed to administrator and make a decision whether they continue this case or not. During the investigation, the forensics team should be always aware of potential risks that could be happened such as Bob's might delete a file, modify the data etc. The head forensics investigator will informed to the forensics team, the initial plan and procedures to start the next stage of the investigation. Finally, the team is required to update all incidents that include the type of incident, locations, timestamps, lists of incident and system information.

Step 2: Incident retort

In the first response, the forensics team is encountered, when the investigator confirmed Bob's incidents scene. Also, a well documentation has been maintained in order to support the investigation. Now forensics investigators will decide the methods and construct the plan.

Step 3: Plan and preparation

The primary plan is carried out based on the previous documentation and policies for how the investigation will be performed. The initial plan is set up by the administrator. In the proposed plan, the administrator will include the forensics team, log books where details of evidence will log, incidents log, time plan etc. In this case, the forensics team start working on it and make a document including the incident scene, policy and guidelines. Also identifying the location with the help of cloud service provider which are VM, external devices, network etc. The preparation method is critical in this case. In this process, they need to take all Bob's information, scene time, incident, any malicious activities that Bob already done. In the preparation method includes assign tasks, policies, operational tasks and tool selections.

7.1.3 Activity 2: Identify risks

The risks can hinder to achieve the goals of the investigation. Any violation of the integrity properties, malicious actors could be tempered the log activities which may not provide an appropriate report for the legal authorities. In this case study, we categorised several risks in the above scenario. The following risks are:

- ***Log modification-*** refers modify the logs by any actors such as CSP, investigator, malicious actor etc. Usually, malicious actors are tampered with the log after collecting all the data. Also, a forensics investigator can be modified the logs before submitting the log to the court. Logs are typically contaminated thru false log, deletion of crucial logs and modification of the order of logs(Zawoad et al., 2016).
- ***Loss of integrity:*** refers to unauthorised modification by malicious actors. No evidence to prove whether data has been modified or deleted or altered and many copies of data potentially detained by several entities.
- ***Loss of availability:*** this concerns if any data is unavailable to the end user and other concerns dealt with if service or server is spoofed, penetrated, suspended in supporting to organisations goals.
- ***Privacy violation:*** a malicious user who can have access the log storage, can identify the clients' activities from log storage. This risks might be magnified if malicious actors disclosed the logs activity.

Assessing the forensics evidence, the forensics team and ABC staffs have identified some requirements to do the investigation. First of all, they considered identifying the risks scene where occurrences happen. And then they can be considered any vulnerabilities that might be any defective hardware or any other faulty applications that are used during the investigation. After all the forensics investigator considered the threats which can be exploited vulnerabilities of the systems. When the investigator finishes their assessment during the investigation, they can calculate the actual risks.

7.1.4 Activity 3: Understand the evidence

Once the forensics data had completely collected, the investigator needs to examine and analyse all information to ensure the integrity and validity of resources. By using an appropriate existing tool, information had been analysed for other useful information such as logs, IP address, file system and registry etc. At the point, investigator had identified that file is encrypted and it is very crucial at the stages of data retrieving. During the investigation, time is valuable because it is related to the amount of data that is analysed. After through an investigation, the investigator is delivered reports that contain information about the file alteration, the person who was involved, evidence analysis, approach and techniques that followed, relevant findings and technical terms that had been used. When forensics investigator gets all Bob's files from VM and the other information, then new methods are applied to verify the chain of custody and data integrity. The forensics team delivered two duplicates copy to investigate, and from the two duplicates, one copy is stored securely for the future if forensics administrator is needed. The forensics team is used the tools to examine the data, and they found on the file IP addresses, log activities, timestamps etc. with the help of a cloud service provider. At the end, a final report was produced to the legal authorities.

7.1.5 Activity 4: Identify forensics actions

The forensics actions need to be satisfied goals and meet the requirements in order to resolve the incident. In order to construct the integrity of evidence for forensic investigations, the following actions can lead to resolving the incidents.

- ***Integrity verification of log:*** to verify the integrity of logs, investigator examine and analyze the data whether the data exists. If data exists, then the investigator proceeds to start the log verification process.
- ***Timestamps verification:*** This action aids to generate timestamps when any files are created, altered and deleted to check the authenticity of the information. Using this action, the investigator can verify the correct time of the files.
- ***Sequence verification:*** This action verifies two consecutive entities. The first entity will be displayed instantly before the second entity in the original sequence of log generation. For example, if the first entity of the log and the second entity

of the log represents same, in this case, the investigator should compute the log of chain to verify the appropriate log sequence.

- ***Evidence Creation:*** This action is applied to proof any evidence that already been created for particular information. For example, if one static IP address is created for all logs on the same day, then it is easy to retrieve data if is needed in future. This action saves the time and minimise the cost while investigations particularly in a cloud environment.

All the above activities should be followed during the forensic investigation, and A well-documented report produces using proficient evidence on the analysis of the evidence. Evidence should be presented in a way where the jury can understand all technical facts on cloud computing. The report should be submitted with all supporting documents concerning the chain of custody of evidence to the court. The well-documented report should include details of findings, types of incident, who's responsible, the location of the incidents etc. After presenting the report, the jury will resolve the case by deciding that the occurrence is imputed to whom. The judgement should be kept in the data centre for the future if it needed. The chain of custody can be preserved all events such as who, when what etc. in order to maintain the quality.

7.2 Case study-2

7.2.1 Overview and context

A UK based company SIMPLYCAREWORLDWIDE was established in 2018 in the care home sector. The company is a dynamic, fast growing a domiciliary care agency providing a career to both private care company and individuals. Since 2018, the company is expanding comfortably due to their excellent services and clients feedbacks and reviews.

Recently, the company had identified that their company website exploited and there was no company information on their website. The company was made a complaint to the legitimate company who is dealing with this type of problems. Therefore, the legitimate company start looking to solve this issues and investigate the crime that happened with the SIMPLYCAREWORLDWIDE.

The main objectives of this case study were to investigate the crime as well the malicious activities that took place.

This case study is demonstrated all the activities that could happen during the forensic investigation in relation to the proposed concepts.

In this case, let assume that the company SIMPLYCAREWORLDWIDE takes a cloud service as Software-as-a-service providers such as Amazon or Microsoft Azure. In this cloud service model, the cloud service provider has full access to all platforms such as hardware, OS and hosting. In this circumstance, the legitimate company might hire a lawyer to accuse the malicious actor. On the other hand, the attorney can contact with the forensics investigator who was conducted the forensics investigation during the period of the investigation. So that, the forensics investigator develops a plan in order to access the cloud service provider platform remotely through a secure channel using the SIMPLYCAREWORLDWIDE credentials. Finally, the investigator can able retrieve all source file of the website. On the other hand, when source files are retrieved, zero malicious was initiated since the malicious actor was hidden the files from both cloud service provider APIs and the host operating system. In this case, the forensics investigator decides to follow further possible sources that can be found from CSP access log, flow logs and VM server logs.

The prosecuting attorney will conduct to the cloud service provider by order and request all information that is associated with VM forensics data. However, the CSP will take place an internal investigation. In this case, the CSP can decline to produce any confidential data and sources that might be lack of SLAs. The prosecuting attorney can be conducted with the judge that there are possibly have malicious activities inside the CSP side and can be issued a warrant to the CSP. An expert forensic technician can be recruited in order to get the data from CSP infrastructure and to verify the data integrity. With the above information that we carried during the forensic investigation, the forensics investigator can reveal the following:

i. A sequence of events can demonstrate that when the website information has been accessed or edited or modified.

ii. Identify the malicious activities that initiated in the first phase.

iii. Determined how the system was conceded for the website

iv. Examine and analyse the potential data breach to the other system

In the above case, if the host OS and VM server were used to recover the data, then there was still huge doubt whether the retrieve data modified or not. Or there might be having the hidden malicious data. In this instance, if the files and data can be collected appropriately, then there was a high chance to get accurate data. To doing so, forensics investigator needs to determine what data for example meta-data with time logs, can be received from the cloud service provider.

7.2.2 Analysis of the case study

In the cloud environment, forensics investigation is an intensive process and always is restricted by time and budget until and unless clients willingly to support independently. Considering this case study, how we investigate in relation to the proposed concepts.

7.2.2.1 Planning – Before to the incident occurred, this activity will take place. SIMPLYCAREWORLDWIDE has comprehended procedures and appointed a forensics investigator from an external company to investigate the case. The specialised external investigator will be trained to the SIMPLYCAREWORLDWIDE administrator in order to carry out the case. Once the internal administrator is well trained, a team will be set up to monitor and investigate their system with potential scenarios. The administrator will be playing a key role, and the consultant will be playing an assisting role. Also internally a legal officer will be trained for the multi-jurisdictions problems and to assist another team in any other forensics related issues. The company will be equipped with forensics and other related tools, and evidence preservation procedures also will be developed. Before appointing any CSP, SIMPLYCAREWORLDWIDE has conducted market research to find a suitable provider for their needs. Finally both sides such CSP and client will be signed an SLA (service level agreement) of using software-as-a-service (SaaS) and the primary obligations.

7.2.2.2 Incident – when an incident occurs, the administrator will be informed to the team that some data and information are lost from the host and VM server. Their claims will be checked to determine if they are valid and confirmed via system analysis. The secure system between the cloud service provider and SIMPLYCAREWORLDWIDE Company to trace the system log and timestamps in order to detect the malicious activities. Also, an appropriate tool is used to detect and preserve the possible evidence. A proper back up will be activated in order to assess the damage.

7.2.2.3 Stakeholder – The forensics administrator will contact with CSP and set up a secure communication channel between company and CSP. This is open to determine the consequence of issues. Access to provider activity logs and enough information is being asked to know more about the incidents and SLA is originated this stage. The administrator will take any further action if it is required and the consultant will discuss further with various procedures and methods which they might follow. The consultant can be informed by the cloud service provider that incident happened and will ask the IP address where the host server is located. The legal officer is mindful that the cloud service provider depends on the 3rd party for their data storage and will contact to the LEA (Law Enforcement Agents) about the incident and request for assistant in jurisdictional problems.

7.2.2.4 LEAs (Law Enforcement Agents): LEAs also is comprised the incidents and ask for training to their team to learn the procedures and techniques of the cloud forensics. They also learn the regulations and legal issues that related to the cloud forensics. They will employ best technical background forensics investigators and equipped with best forensics tools. After getting a call from the SIMPLYCAREWORLDWIDE legal officer for the incident, then the LEAs will be involved in the forensics investigations to investigate the criminal activity. They have been known that the evidence are stored in different locations and have conducted with the cloud service provider to access the log files. LEAs are collecting all evidence regarding the criminal activities and a search warrant is attained. The search warrant may not cover due to the jurisdiction issues. So that LEAs need to contact law authorities of the country where evidences are stored. LEAs order to place a litigation hold to prevent any further modification of the data.

7.2.2.5 CSPs – CSPs are trained their team on the forensics tools, techniques, procedures and forensics incidents. CSPs can be contacted with third party for their large amount of data and can be signed off to host data into third-party server. Therefore, CSP is approved it employees to corporate with the other stakeholders and LEA. Now, the cloud service provider (CSP) and Law Enforcement Agents (LEAs) are collecting all data and information about the data nature that already kept. After analysing the nature of data, the CSP and LEAs will ask to give the authorisation to access the data for gathering further evidence.

7.2.2.6 Investigation – Once a warrant is accepted and get the authorisation to access the log files then the investigation process is started. The LEA's and the CSP are gathering all log files and evidence and they make if forensically sound by using the forensics tools. They are retained high confidentiality and integrity with other clients' data. Without breaching the integrity of the evidence, they will transfer those evidence securely to the lab for examination. Evidence will be analysed in order to discover and extract any further data. Using IP and NTP (Network Time Protocol), the investigator will be focused on the time logs of the activities during the period of the crime. After analysing the time stamps and log data of the activities, the investigator revealed that the company files and track were initiated.

7.2.2.7 Provenance – Chain of custody was properly maintained to access the data. Through the chain of custody, the administrator considers provenance from three perspectives such as entity data, activity (actioned performed on data) and actor (such as data owner or agents). Therefore, provenance has produced a chain with time logs, actors chain track.

7.2.2.8 Risks – During the forensics investigations, risks are considered to identify all possible facts of incidence throughout collection, preservation and analysis of forensic evidence. Throughout the forensics investigations, the investigators need to identify all potential issues to determine the facts of incidents. Also, they should identify the nature of risks that associated with these incidents. Risks can be CSP or multi-jurisdictions, data alteration or evidence expose accidently.

7.2.2.9 Result – As a result, the legal officer will follow the forensics techniques and procedures. If there was an issue with jurisdiction, then the legal officer will contact with Law Enforcement Agents. However, the LEAs was acquired a warrant to proceed the forensics investigation. To avoid the jurisdiction issues, they conducted with the criminal's country authorities and access was approved. The analysis of the data has revealed that they need more investigation and have decided to do again the investigation process in order to get more information.

7.2.2.10 Documents – During the investigation, a document is generated. Before start investigation, a planning manual was created where all there parties were included with all planning concepts and process, guidelines, case studies to the incidents. The company administrator will access all records and manual for the investigation that all stages take place during the incidents. The same stage is applied to LEAs and cloud service provider (CSP). All the stages are followed to gather information that includes a warrant, collection method, and staff involvement in are documented. It confirmed confidentiality and privacy of other clients' information and data integrity also documented. During the whole investigation, what methods and tools have been used to gather the evidence, it also is documented. The data transportation and evidence that are kept also recorded.

7.2.2.11 Reports – To present the result, reports should be generated when the investigation and results are closed. The investigators will submit the result to the company stakeholders with the investigation report. The report will confirm that during the investigation proper integrity is maintained and the correct procedure was followed.

7.3 Conclusion

In this chapter, we conducted the evaluation of our proposed methodology. The evaluation was based on the two aspects of CeFF: firstly the framing concepts in a different level of perspective which was described in chapter 5 and secondly, CeFF standardised digital forensic process presented in chapter 6. Both aspects are focused on how CeFF satisfied the forensic investigator through the real-life case studies. In the next chapter, concludes the thesis and suggest the future directions of the research.

Chapter 8

Conclusion and Future Directions

8. Conclusion and Future directions

Cyber-crimes are increasingly becoming a rising concern for any industry, and specifically, the attack trends are now very sophisticated and difficult to detect. Furthermore, it is more challenging for cybercrime, which occurred in the cloud-based outsourcing context where the users do not have full control of their data. It is, therefore, necessary to develop a cloud-enabled forensics solution so that evidence relating to cyber-crime are analysed systematically.

This research contributes to moving forward towards the cloud-enabled forensic investigation domain. In our research, we develop a conceptual CeFF framework in order to examine and analysis of forensics data effective and efficient way in the cloud environment. The meta-model of our framework has described the essential concepts identified in cloud forensics stage from a holistic perspective focusing on organisational, technical and legal perspectives. On the other hand, the new systematic framing process for cloud enable forensics investigation that consists of four principal activities to understand the context of crimes and identify all evidence in the cloud system. It is required appropriate actions and operations in order to satisfy the investigative goals.

In this research, we have applied our CeFF framework into two real use case scenarios to demonstrate the applicability of our framework. The case study cases demonstrate that the CeFF framework can support the organisation to investigate their cybercrimes. CeFF able to analyse the evidence not only from technical perspective in terms of victim limitation cause for the attack but also legal and organisational implicated posed by the crime. This helps to provide a comprehensive investigation of the crime. Furthermore, our work also determines the possible risks of not analysing the crime and mitigate it before the actual investigation has undertaken. However, the CeFF framework does not provide a detailed process of technical level for efficient and effective investigation. Moreover, we would like to apply our framework into other case study related to cloud-enable forensics investigation scenario, so that we can generalise our findings more.

The research achieved its objective and addressed the research questions. In particular, RO 1 and RO2 are achieved through developing the CeFF framework including concepts and process. RO 3 is achieved through case studies where we have analysed the evidences from a legal perspective to meet the legal requirements from the multi-jurisdiction context using the concepts considered in CeFF. Finally, RO4 has also achieved through the case studies by demonstrating the applicability of CeFF.

However, we observed limitations, and this allows considering the future direction for the research. Automation of the process is necessary to make the overall investigation effective. Therefore, the development of tool is one of the future directions of the work. Furthermore, a taxonomy and guideline are also necessary to help the forensic investigator how to analyse the crime in a specific crime class. This can be done by developing semantic and ontology modelling of the cyber crime domain. Forecasting crime is always demanding for any industry; the future work can also integrate machine-learning technique to predict the crime for a specific context using various features extracted from the CeFF concepts' properties. Finally, more crime cases are always preferable to demonstrate the applicability and unique findings from different cases.

References

9. References

ADAMS, R. 2013. The emergence of cloud storage and the need for a new digital forensic process model. *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, 79-104.

AL FAHDI, M., CLARKE, N. L. & FURNELL, S. M. Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. Information Security for South Africa, 2013, 2013. IEEE, 1-8.

ALEX, M. E. & KISHORE, R. 2017. Forensics framework for cloud computing. *Computers & Electrical Engineering,* 60**,** 193-205.

ALMULLA, S. A., IRAQI, Y. & JONES, A. 2014. A state-of-the-art review of cloud forensics. *Journal of Digital Forensics, Security and Law,* 9**,** 7-28.

ALQAHTANY, S., CLARKE, N., FURNELL, S. & REICH, C. Cloud forensics: a review of challenges, solutions and open problems. Cloud Computing (ICCC), 2015 International Conference on, 2015. IEEE, 1-9.

ANDROUTSOPOULOS, I., KOUTSIAS, J., CHANDRINOS, K. V., PALIOURAS, G. & SPYROPOULOS, C. D. 2000. An evaluation of naive bayesian anti-spam filtering. *arXiv preprint cs/0006013*.

ANWAR, F. & ANWAR, Z. Digital forensics for eucalyptus. Frontiers of Information Technology (FIT), 2011, 2011. IEEE, 110-116.

ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A. D., KATZ, R. H., KONWINSKI, A., LEE, G., PATTERSON, D. A., RABKIN, A. & STOICA, I. 2009. Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley.

BALKIN, J., GRIMMELMANN, J., KATZ, E., KOZLOVSKI, N., WAGMAN, S. & ZARSKY, T. 2007. *Cybercrime: digital cops in a networked environment*, NYU Press.

BAROLLI, L. EIDWT 2012: Third International Conference on Emerging Intelligent Data and Web Technologies, 19-21 September 2012, Bucharest, Romania. Bucharest, EIDWT. 2012. EIDWT.

BARYAMUREEBA, V. & TUSHABE, F. The enhanced digital investigation process model. Proceedings of the Fourth Digital Forensic Research Workshop, 2004. 1-9.

BECKMAN, J., RIEDLE, M. & VARGAS, H. 2014. Analysis of Amazon S3 Cloud Services.

BEEBE, N. 2009. Digital forensic research: The good, the bad and the unaddressed. *Advances in digital forensics V.* Springer.

BEEBE, N. L. & CLARK, J. G. 2005. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation,* 2**,** 147-167.

BELORKAR, A. & GEETHAKUMARI, G. Regeneration of events using system snapshots for cloud forensic analysis. India Conference (INDICON), 2011 Annual IEEE, 2011. IEEE, 1-4.

BIRK, D. & WEGENER, C. Technical issues of forensic investigations in cloud computing environments. Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on, 2011. IEEE, 1-10.

BUYYA, R., YEO, C. S. & VENUGOPAL, S. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. High Performance Computing and Communications, 2008. HPCC'08. 10th IEEE International Conference on, 2008. Ieee, 5-13.

CARRIER, B. & SPAFFORD, E. H. An event-based digital forensic investigation framework. Digital forensic research workshop, 2004. 11-13.

CISAR, P., CISAR, S. & BOSNJAK, S. 2014. CYBERCRIME AND DIGITAL FORENSICS-TECHNOLOGIES AND APPROACHES. *DAAAM International Scientific Book.*

CRANOR, L. F. & LAMACCHIA, B. A. 1998. Spam! *Communications of the ACM,* 41**,** 74-83.

CROSBIE, M. 2012. Hack the cloud: Ethical hacking and cloud forensics. *Cybercrime and Cloud Forensics: Applications for Investigation, Processes***,** 42-58.

CROSBY, S. & BROWN, D. 2006. The virtualization reality. *Queue,* 4**,** 34-41.

DAMSHENAS, M., DEHGHANTANHA, A., MAHMOUD, R. & BIN SHAMSUDDIN, S. Forensics investigation challenges in cloud computing environments. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, 2012. IEEE, 190-194.

DANCHEV, D. 2009. Zeus crimeware using Amazon's EC2 as command and control server. Récupéré sur ZDNet: http://www. zdnet. com/blog/security/zeus-crimeware-using-amazonsec2-as-command-and-control-server/5110.

DELPORT, W., KÖHN, M. & OLIVIER, M. S. Isolating a cloud instance for a digital forensic investigation. ISSA, 2011.

DYKSTRA, J. & SHERMAN, A. T. Understanding issues in cloud forensics: Two hypothetical case studies. Proceedings of the Conference on Digital Forensics, Security and Law, 2011. Association of Digital Forensics, Security and Law, 45.

DYKSTRA, J. & SHERMAN, A. T. 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation,* 9**,** S90-S98.

DYKSTRA, J. & SHERMAN, A. T. 2013. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation,* 10**,** S87-S95.

EDWARDS, D. C. 2012. Admissions Online: Statements of a Party Opponent in the Internet Age. *Okla. L. Rev.,* 65**,** 533.

GARY, P. A road map for digital forensic research. Digital Forensics Research Workshop, 2001.

GEETHAKUMARI, G. & BELORKAR, A. 2012. Regenerating cloud attack scenarios using LVM2 based system snapshots for forensic analysis. *International Journal of Cloud Computing and Services Science,* 1**,** 134.

GOSCINSKI, A. & BROCK, M. 2010. Toward dynamic and attribute based publication, discovery and selection for cloud computing. *Future generation computer systems,* 26**,** 947-970.

GRANCE, T., CHEVALIER, S., SCARFONE, K. K. & DANG, H. 2006. Guide to integrating forensic techniques into incident response. *Special Publication (NIST SP)-800-86.*

GREEN, C. 2013. Dropbox hit by Zeus phishing attack. Oct.

GRISPOS, G., STORER, T. & GLISSON, W. B. 2013. Calm before the storm: the challenges of cloud. *Emerging digital forensics applications for crime detection, prevention, and security,* 4**,** 28-48.

GROBAUER, B. & SCHRECK, T. Towards incident handling in the cloud: challenges and approaches. Proceedings of the 2010 ACM workshop on Cloud computing security workshop, 2010. ACM, 77-86.

GROUP, N. 2014. Nist cloud computing forensic science challenges. *Draft NISTIR,* 8006.

GUO, H., JIN, B. & SHANG, T. Forensic investigations in cloud environments. Computer Science and Information Processing (CSIP), 2012 International Conference on, 2012. IEEE, 248-251.

HEISER, J. 2009. What you need to know about cloud computing security and compliance. *Gartner, Research, ID.*

INITIATIVE, H. I. 2012. Monthly Trend Report# 14. December.

KASEMSAP, K. 2015. The role of cloud computing adoption in global business. *Delivery and adoption of cloud computing services in contemporary organizations*, 26-55.

KENT, K., CHEVALIER, S., GRANCE, T. & DANG, H. 2006a. Guide to integrating forensic techniques into incident response. *NIST Special Publication*, 800-86.

KENT, K., CHEVALIER, S., GRANCE, T. & DANG, H. 2006b. Guide to integrating forensic techniques into incident response. *NIST Special Publication,* 10**,** 800-86.

KHAN, S., GANI, A., WAHAB, A. W. A., BAGIWA, M. A., SHIRAZ, M., KHAN, S. U., BUYYA, R. & ZOMAYA, A. Y. 2016. Cloud log forensics: foundations, state of the art, and future directions. *ACM Computing Surveys (CSUR),* 49**,** 7.

KITCHENHAM, B. A., PFLEEGER, S. L., PICKARD, L. M., JONES, P. W., HOAGLIN, D. C., EL EMAM, K. & ROSENBERG, J. 2002. Preliminary guidelines for empirical research in software engineering. *IEEE Transactions on software engineering,* 28**,** 721-734.

KO, R. K., JAGADPRAMANA, P., MOWBRAY, M., PEARSON, S., KIRCHBERG, M., LIANG, Q. & LEE, B. S. TrustCloud: A framework for accountability and trust in cloud computing. Services (SERVICES), 2011 IEEE World Congress on, 2011. IEEE, 584-588.

KOLTHOF, D. 2015. Crime in the Cloud: An Analysis of the Use of Cloud Services for Cybercrime.

KREBS, B. 2008. Amazon: Hey spammers, get off my cloud. *Washington Post (July 2008).*

KRUSE II, W. G. & HEISER, J. G. 2001. *Computer forensics: incident response essentials*, Pearson Education.

KUNTZE, N., RUDOLPH, C., ALVA, A., ENDICOTT-POPOVSKY, B., CHRISTIANSEN, J. & KEMMERICH, T. On the creation of reliable digital evidence. Advances in Digital Forensics VIII: 8th IFIP WG 11.9 International Conference on Digital Forensics, Pretoria, South Africa, January 3-5, 2012, Revised Selected Papers, 2012. Springer, 1.

LE, V. L., WELCH, I., GAO, X. & KOMISARCZUK, P. Anatomy of drive-by download attack. Proceedings of the Eleventh Australasian Information Security Conference-Volume 138, 2013. Australian Computer Society, Inc., 49-58.

LI, J., CHEN, X., HUANG, Q. & WONG, D. S. 2014. Digital provenance: Enabling secure data forensics in cloud computing. *Future Generation Computer Systems,* 37**,** 259-266.

LOSAVIO, M. M. The law of possession of digital objects: Dominion and control issues for digital forensics investigations and prosecutions. Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on, 2005. IEEE, 177-183.

MARANGOS, N., RIZOMILIOTIS, P. & MITROU, L. 2016. Time synchronization: pivotal element in cloud forensics. *Security and Communication Networks,* 9**,** 571-582.

MARTINI, B. & CHOO, K.-K. R. 2012. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation,* 9**,** 71-80.

MARTY, R. Cloud application logging for forensics. Proceedings of the 2011 ACM Symposium on Applied Computing, 2011. ACM, 178-184.

MCGRATH, D. K. & GUPTA, M. 2008. Behind Phishing: An Examination of Phisher Modi Operandi. *LEET,* 8**,** 4.

MCKEMMISH, R. 1999. *What is forensic computing?*, Australian Institute of Criminology Canberra.

MELL, P. & GRANCE, T. 2011a. The NIST definition of cloud computing.

MELL, P. M. & GRANCE, T. 2011b. Sp 800-145. the nist definition of cloud computing.

NAVARRO, F. J. 2003. United States v. Bach and the Fourth Amendment in Cyberspace. *Alb. LJ Sci. & Tech.,* 14**,** 245.

OPHARDT, J. A. 2010. Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. *Duke L. & Tech. Rev.***,** i.

ORTON, I., ALVA, A. & ENDICOTT-POPOVSKY, B. 2012. Legal process and requirements for cloud forensic investigations.

PALMER, G. DFRWS technical report: A road map for digital forensic research. Digital forensic research workshop, 2001.

PĂTRAŞCU, A. & PATRICIU, V.-V. Beyond digital forensics. A cloud computing perspective over incident response and reporting. Applied Computational Intelligence and Informatics (SACI), 2013 IEEE 8th International Symposium on, 2013. IEEE, 455-460.

PELEG, M., TU, S., BURY, J., CICCARESE, P., FOX, J., GREENES, R. A., HALL, R., JOHNSON, P. D., JONES, N. & KUMAR, A. 2003. Comparing computerinterpretable guideline models: a case-study approach. *Journal of the American Medical Informatics Association,* 10**,** 52-68.

PICHAN, A., LAZARESCU, M. & SOH, S. T. 2015. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation,* 13**,** 38-57.

PICHAN, A., LAZARESCU, M. & SOH, S. T. 2018. Towards a practical cloud forensics logging framework. *Journal of information security and applications,* 42**,** 18-28.

POISEL, R., MALZER, E. & TJOA, S. 2013. Evidence and Cloud Computing: The Virtual Machine Introspection Approach. *JoWua,* 4**,** 135-152.

RAYTHEON. Available: https://www.raytheon.com/capabilities/missiledefense.

REILLY, D., WREN, C. & BERRY, T. 2011. Cloud computing: Pros and cons for computer forensic investigations. *International Journal Multimedia and Image Processing (IJMIP),* 1**,** 26-34.

RICHMAN, W. M., REYNOLDS, W. L. & WHYTOCK, C. A. 1984. *Understanding conflict of laws*, M. Bender.

RUAN, K. & CARTHY, J. Cloud computing reference architecture and its forensic implications: a preliminary analysis. International Conference on Digital Forensics and Cyber Crime, 2012. Springer, 1-21.

RUAN, K., CARTHY, J. & KECHADI, T. Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis. Proceedings of the Conference on Digital Forensics, Security and Law, 2011a. Association of Digital Forensics, Security and Law, 55.

RUAN, K., CARTHY, J., KECHADI, T. & BAGGILI, I. 2013. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation,* 10**,** 34-43.

RUAN, K., CARTHY, J., KECHADI, T. & CROSBIE, M. Cloud forensics. IFIP International Conference on Digital Forensics, 2011b. Springer, 35-46.

RUNESON, P. & HÖST, M. 2009. Guidelines for conducting and reporting case study research in software engineering. *Empirical software engineering,* 14**,** 131.

SANG, T. A log based approach to make digital forensics easier on cloud computing. Intelligent System Design and Engineering Applications (ISDEA), 2013 Third International Conference on, 2013. IEEE, 91-94.

SCANLON, J. H. & WIENERS, B. 1999. The internet cloud. *The Industry Standard, Tech. Rep.*

SHAH, J. & MALIK, L. G. Cloud forensics: issues and challenges. Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on, 2013. IEEE, 138-139.

SIBIYA, G., VENTER, H. S. & FOGWILL, T. 2012. Digital forensic framework for a cloud environment.

SIMPSON, W. R. & CHANDERSEKARAN, C. 2014. Cloud forensics issues. DTIC Document.

SINGH, J. 2014. Cyber-attacks in cloud computing: A case study. *International Journal of Electronics and Information Engineering,* 1**,** 78-87.

STEVENS, H. & PETTEY, C. 2008. Gartner says cloud computing will be as influential as e-business. *Gartner Newsroom, Online Ed.*

SUBASHINI, S. & KAVITHA, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications,* 34**,** 1-11.

TAYLOR, M., HAGGERTY, J., GRESTY, D. & HEGARTY, R. 2010. Digital evidence in cloud computing systems. *Computer Law & Security Review,* 26**,** 304-308.

THETHI, N. & KEANE, A. Digital forensics investigations in the cloud. Advance Computing Conference (IACC), 2014 IEEE International, 2014. IEEE, 1475-1480.

TRENWITH, P. M. & VENTER, H. S. Digital forensic readiness in the cloud. Information Security for South Africa, 2013, 2013. IEEE, 1-5.

VALJAREVIC, A. & VENTER, H. S. Harmonised digital forensic investigation process model. Information Security for South Africa (ISSA), 2012, 2012. IEEE, 1-10.

VAQUERO, L. M., RODERO-MERINO, L., CACERES, J. & LINDNER, M. 2008. A break in the clouds: towards a cloud definition. *ACM SIGCOMM Computer Communication Review,* 39**,** 50-55.

VERNER, J. M., SAMPSON, J., TOSIC, V., BAKAR, N. A. & KITCHENHAM, B. A. Guidelines for industrially-based multiple case studies in software engineering. Research Challenges in Information Science, 2009. RCIS 2009. Third International Conference on, 2009. IEEE, 313-324.

W3CONSORTIUM. Available: https://www.w3.org/.

WANG, L., TAO, J., KUNZE, M., CASTELLANOS, A. C., KRAMER, D. & KARL, W. Scientific Cloud Computing: Early Definition and Experience. HPCC, 2008. 825-830.

WILES, J. & REYES, A. 2011. *The best damn cybercrime and digital forensics book period*, Syngress.

WILLIAMS, M. I. 2010. *A quick start guide to cloud computing: moving your business into the cloud*, Kogan Page Publishers.

YAN, C. Cybercrime forensic system in cloud computing. Proceedings of 2011 International Conference on Image Analysis and Signal Processing, IASP, 2011. 612-3.

ZAWOAD, S., DUTTA, A. K. & HASAN, R. 2016. Towards building forensics enabled cloud through secure logging-as-a-service. *IEEE Transactions on Dependable and Secure Computing,* 13**,** 148-162.

ZAWOAD, S. & HASAN, R. I have the proof: Providing proofs of past data possession in cloud forensics. Cyber Security (CyberSecurity), 2012 International Conference on, 2012. IEEE, 75-82.

ZAWOAD, S. & HASAN, R. 2013a. Cloud forensics: a meta-study of challenges, approaches, and open problems. *arXiv preprint arXiv:1302.6312*.

ZAWOAD, S. & HASAN, R. 2013b. Digital forensics in the cloud. ALABAMA UNIV IN BIRMINGHAM.