

**CLOUD FORENSICS  
(ENTERPRISE CLOUD LOG AUDIT TRAIL FRAMEWORK )**

**BY**

**WILLIAM KIPRUTO LACKTANO**

**REG: 14/00450**

**A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENT FOR THE AWARD OF MASTERS DEGREE IN DATA  
COMMUNICATIONS IN THE FACULTY OF COMPUTING & INFORMATION  
MANAGEMENT AT KCA UNIVERSITY**

**JUNE, 2016**

This research project is available for Library use on the understanding that it is copyright material and that no quotation from the research project may be published without proper acknowledgement.

## DECLARATION

I declare that this Research project is my original work and has not been previously published or submitted elsewhere for award of a degree. I also declare that this Research project contains no material written or published by other people except where due reference is made and author duly acknowledge.

Student Name.....Reg.No.....

Sign.....Date.....

I do here by confirm that I have examined the master's Research project of

WILLIAM KIPRUTO LACKTANO

AND have certified that all revision that the research project panel and examiners recommended

have been adequately addressed

1. SUPERVISOR:DR. GEORGE OKEYO

Sign.....Date.....

2. CO-SUPERVISOR:MR HENRY MWANGI

Sign.....Date.....

## **ACKNOWLEDGEMENTS**

I wish to thank my supervisors Dr. George Okeyo, and Mr. Henry Mwangi for their enormous assistance and guidance, for providing ideas and suggestions for improvement and constant encouragement.. If not for their constant communications and support throughout my research project, and the exciting discussions about cloud forensics and digital forensics I would not have finished my research on time.They provided continual feedback, moral and academic support, editing guidance, and went to great lengths by providing guidance to sources of relevant materials to my research.

## **DEDICATION**

I dedicate this research project to my wife Nellie Lacktano, my daughters Faith, Audrey, Malia and my son Adrian for their patience, understanding, support, academic encouragement, and most of all love, the completion of this work would not have been possible.

<b>List of Figures and Tables.....</b>	<b>iv</b>
Diagram 1-Cloud computing.....	7
Table 1-Cloud forensics main challenges.....	16
Figure 1-Cloud model degree of control.....	20
Figure 2-Computer forensics process flow.....	21
Figure 3-Evidence Handling process.....	24
Diagram 2-Integrated Framework.....	25
Figure 3.1-Framework and prototype.....	27
Figure 3.2-SLA flow.....	27
Diagram 3-Logging for Cloud Forensic Systems.....	30
Figure 3.3-Simulated VM Cloud.....	31
Figure 3.4-acktrack5 Server.....	32
Figure 4- Logic flow diagram.....	35
Figure 4.1-Vm Log File.....	36
Figure 4.2- Data Migration.....	37
Figure 4.3-Logic Audit Trail Framework.....	38
Figure 4.4-Logs and audit trail flow.....	38

## **Acronyms and Abbreviations**

DDF: Digital Forensics

CSP: Cloud service provider

API: Application programming interface

VM: Virtual Machine

MAC: Media Access Control

IP: Internet Protocol

CSA: Cloud Security Alliance

AWS: Amazon Security Services

CSP: Content security provider

DFR: Digital Forensic Readiness

SLA: Service Level Agreement

IAAS: Infrastructure as a service

PAAS: Cloud Platform as a Service

SAAS: Cloud Software as a Service

## Table of Contents

DECLARATION.....	i
ACKNOWLEDGEMENTS.....	ii
DEDICATION.....	iii
List of Figures and Tables.....	iv
Acronyms and Abbreviations.....	v
Table of Contents.....	vi
ABSTRACT.....	1
1.0 CHAPTER ONE.....	3
1.1 INTRODUCTION.....	3
1.2 BACKGROUND.....	8
1.3 Technical dimension.....	10
1.4 Problem Statement.....	11
1.5 Objectives of the research.....	12
1.6 Specific objectives.....	13
1.7 Motivation.....	14
1.8 Justification.....	15
1.9 Scope of research.....	17
2.0 CHAPTER TWO.....	18
2.1 Literature Review.....	18
2.2 Forensics crisis.....	23
3.0 CHAPTER THREE.....	25
3.1 METHODOLOGY.....	25
3.1.1 Live Forensics.....	25
3.1.1 Logging architecture.....	36
3.1.2 Cloud forensics principles.....	27
3.1.3 Framework.....	27
3.1.4 Cloud Forensic process.....	27
3.2.0 Deployment Model.....	29
4.0 CHAPTER FOUR.....	34
4.1 Framework.....	34
4.2 Log in guidelines.....	36
4.3 Framework Model.....	37
4.4 Deployment.....	39
4.5 Tools.....	42

5.0 CHAPTER FIVE.....42  
5.1 RESULTS AND DISCUSSION.....42  
5.2 APPENDIX.....42  
5.3 Output.....50  
  
6.0 CHAPTER SIX.....59  
6.1 CONCLUSION.....59  
6.2 FURTHER WORK.....61  
  
REFERENCES.....63



**CLOUD FORENSICS**  
**(PRIVATE CLOUD LOG AUDIT TRAIL FRAMEWORK)**

**ABSTRACT**

Cloud forensic refers to the digital forensic investigations performed in cloud computing environment.

Cloud related services and data storage migration by organization has resulted to logs trail for digital investigations in computing and any potential crime using the digital forensic evidence from a virtual environment (VM) that is hosting several operating system using various system platform and hardware plates distributed across several locations e.g hypervisor event logs from different applications. It is evidenced that in cloud digital log forensics, work on the forensic reconstruction of evidence on VM hosts system is required to ascertain the activities within the said host ,though with the complexity and heterogeneous involved with a private enterprise cloud, not to mention public cloud distributed environments, there is a possible Web Services-centric approach which may be required for such log supported investigations and which can be achieved through logs audit trail framework. A data cloud log forensics audit trail framework for this type of forensic examination and data comparison needs to allow for the reconstruction of transactions spanning multiple Virtual environment hosts, platforms and applications. This research project paper will explore the requirements of a cloud log forensics framework for performing effective private cloud forensics investigations which will give a lead and can be used in law enforcement. The framework will be important and necessary in order to develop investigative and forensic auditing tools and techniques for use in cloud based log-centric virtual environment through the audit trail logs from the log controller server and web interface.

Cloud computing services is currently one of the most fast growing trans-formative technologies in the history of computing technologies which has revolutionize the world in the current times. Cloud service providers and customers have yet to establish adequate forensic capabilities that can be used to support investigations of criminal activities in the cloud due to the fact that most of the Service Level Agreement are signed with the third parties who are normally not controlled neither by the providers or the customers.

There is need for a growing understanding of how to conduct digital forensic analysis on cloud devices by the providers and clients for proper logs audit trails. However, there is little understanding of how to apply digital forensic methodologies in Cloud computing because of its dynamism, and even less understanding in how to apply forensic methodologies in Cloud investigation by the forensic experts. The aim of this project is to identify the challenges of Cloud computing forensics and come up with a framework to test current cloud computing forensic tools, methodologies and procedures with a clear indicative solution which can be applied across all the platforms universally.

“Both Encryption and cloud computing threaten forensic visibility in much the same way. No matter whichever way critical information is stored in an unidentified server “somewhere in the cloud” or stored on the subject’s hard drive inside a True Crypt volume, these technologies deny investigators access to the case data. While neither technology is invincible, both require time and frequently luck to circumvent” (Casey and Stellatos, 2008). Cloud computing in particular may make it impossible to perform basic forensic steps of data preservation and isolation on systems of forensic interest.

*Keywords: Cloud computing, cloud forensics, virtual environment,hosts ,logs forensics and digital forensic*

## **1.0 CHAPTER ONE**

### **1.1 INTRODUCTION**

The need for Cloud computing forensics arises from the alarming increase in the number of cloud computing crimes(Cybercrimes) that are committed annually due to Technological convergence. After a computer system has been breached and an intrusion has been detected, there is a need for a computer forensics investigation to follow.

Cloud forensics emanates from cloud computing and digital forensics which is a cross discipline, dealing with investigation of meta-data and artifacts of systems. Cloud computing is a shared collection of configurable networked resources where networks, servers, storage, applications and services can be reconfigured with minimal effort, where as cloud forensics is the application of computer science principles using forensics tools to recover electronic evidence in full or partially for presentation in a court of law or to be used for law enforcement.

“Cloud forensics involves various subset of network forensics and data forensics. Network forensics involves forensic investigations of networks devices and connectivity. Cloud computing is depended on wide broad network access which follows various phases of network forensics with techniques tailored to cloud computing environments”(Perry et al., 2009).

Cloud services being provided is radically changing the way how information technology services are created, delivered, accessed and managed.

To ensure service availability and cost-effectiveness, Cloud Service Providers maintain scattered data centers around the world which are being accessed by the clients concurrently. The cutting edge of cloud computing is that there is data replicated at multiple locations virtually to ensure redundancy and business continuity with reduced risk of failure of services accessibility.

Also, the separation and segregation of activities/duties between content security providers and customers in regard to forensic responsibilities differ according to the service models being used and likewise, interactions between multiple tenants that share the same cloud resources differ according to the deployment model being employed.

The default settings for cloud forensics are Multiple jurisdictions and multi-tenancy with different level of access control, which create additional legal challenges. Sophisticated interactions between Cloud Service Providers and customers, resource sharing by multiple integration collaboration between different law enforcement agencies are required in most cloud forensic investigations hence in order to analyze the domain of cloud forensics in a more comprehensive way, there should be emphasis on the fact that cloud forensics is a multi-dimensional issue instead of merely a technical issue, the technical, organizational and legal dimensions of cloud forensics are discussed.

Current state shows that cloud computing services is normally a pay-per-use model where the client/customer chooses the service to pay for, enable availability, convenient, on-demand network access to the shared pool of configurable computing resources provided by the provider e.g. networks, servers, storage, applications, services therefore can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud model promotes availability and is comprised of five **key characteristics**, three **delivery models**, and four **deployment models**.

**(i) Key Characteristics:** *On-demand self-service, Location independent resource pooling. Rapid elasticity, Pay per use.*

**(ii) Delivery Models:** *Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS).*

**(iii) Deployment Models:** *Private cloud, Community cloud, Public cloud. Hybrid cloud.*

In a cloud scenario the need for determining the activity conducted on a network or within a computer would not be necessary, however, the cloud environment is not a perfect world and there are times when it is imperative that the activity of a computer and processes be monitored from a remote location. There should be a way for an individual to observe activities, such as data movement in the cloud space for possible intrusion, misconduct and violation by the third party entrusted with the data thus cloud computing forensic comes an increasingly more important aspect daily.

## Cloud Log Forensics: Foundations, State of the Art, and Future Directions



### Cloud Log Management

Logs are records for capturing various events occurring in a system, network, or process along a specified timeline [Chuvakin et al. 2013]. Each record in the log specifies information related to the sequential steps occurring during the time of system, network, or process execution. The increase in various logs makes organizations adopt log management for the appropriate handling of logs within the existing infrastructure.

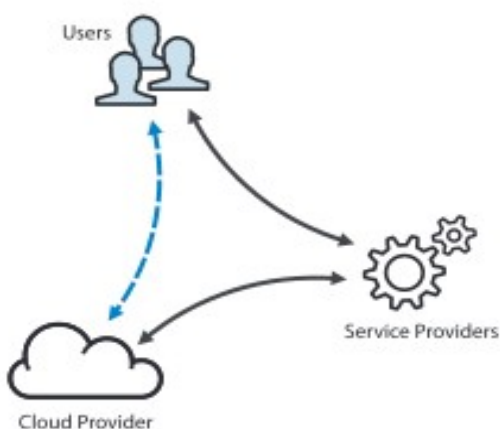
However, the increased size, number, and frequency of logs make it difficult for an organization to manage logs within the context of scarce resources, administrative staff, and security approaches.

The best option to cope with the aforementioned problems is to use the “log-as-a-service” services of cloud computing [Abbadi 2014]. Nowadays, many organizations use the log services of a CSP to simplify their log management. The CSP log-as-a-service assists organizations in managing logs, such as integration of operational log data from various locations, instant log visibility, monitoring of logs in real time, search and filter log data, and much more. Organizations use log-as-a-service services by simply passing different logs to a CSP for managing inside the cloud infrastructure. The log files are transferred to the cloud in different ways depending on log management of the CSP. For instance, Logentries provides customers with multiple options to send their log data to the cloud server, that is, agent-based logging, SYSLOG forwarding, application-based logging, and token-based logging. Agent-based logging contains lightweight agents installed on the client side provided by Logentries to automatically collect and send log files to the cloud servers.



### Why Cloud Forensics?

Many companies are running away from investing on hardware devices, therefore they lease space for services to be hosted by cloud service providers. Due to this the issue of data security comes in place whereby the critical data of the organization needs to be checked so that vital information will not be lost to top competitors hence there is need for logs audit trail to monitor all the operations going on within the set private cloud environment in relation to the service provided by the said cloud provider. The forensics and system relationship overall security is harder to see than the direct relationship between, a firewall and network security. No security system is ideal and presents the suitable and important roles of forensics. Accurate and robust forensic techniques increase the likelihood both of detection of malfeasance and final attribution of the illicit actions to the perpetrator.



There is explicitly trust by users for their data to service provider and the cloud provider that hosts these services or leased services from and to leverage this trust relationship there is a need to

enable users to audit their data directly through the cloud provider and this can be achieved through logs audit trail where the user has autonomy ownership of the data.

## Cloud Service Architecture

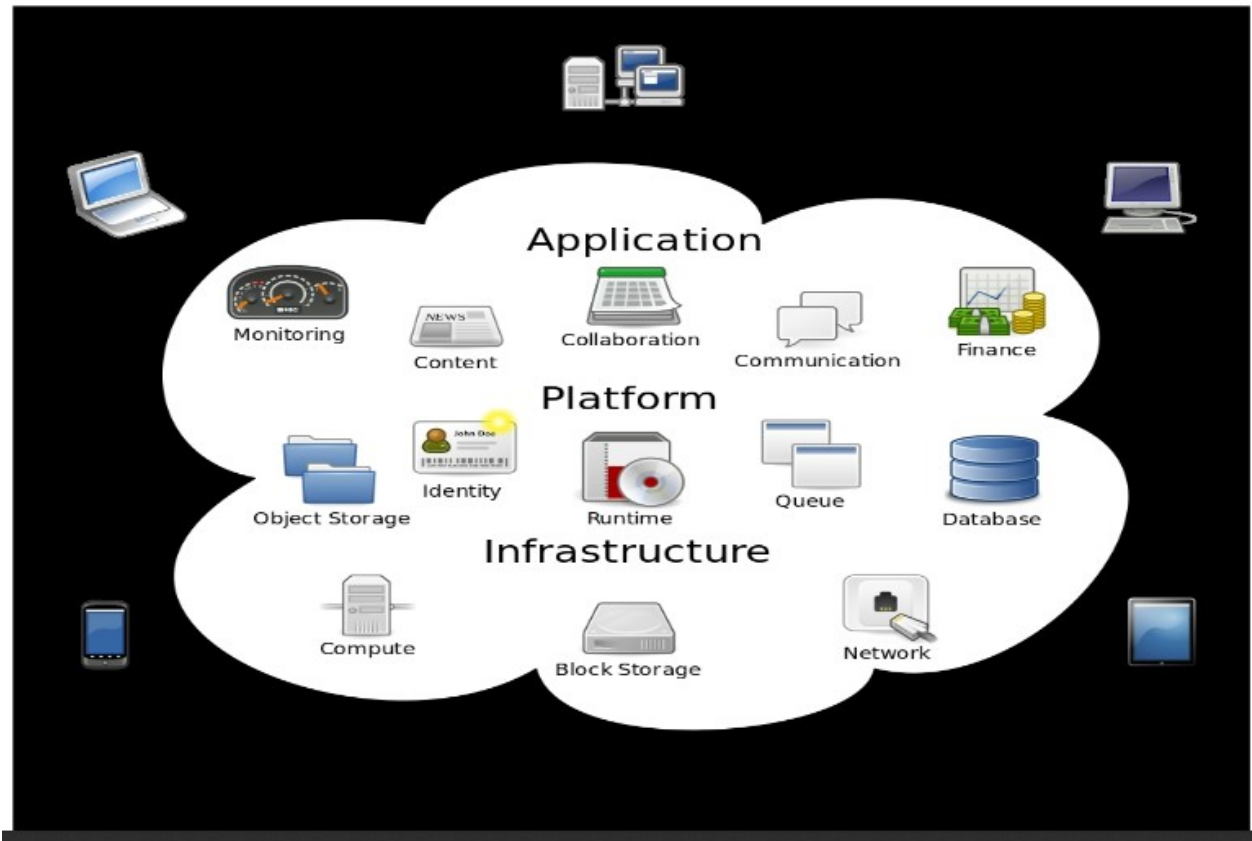


Diagram 1-Cloud computing (NIST SP 500-292, 2014).

From the above architecture, various devices connect to the cloud server to access resources from different locations. In most cases, the owners don't have full ownership of their data hence don't have a clue of what, which and when data is accessed. Due to this there is a need for the client to have a log controller with a web interface which necessitates full-time management of logs from the server.

## 1.2 BACKGROUND

The chosen topic areas for this research project paper consist of an overlap of two new growing information technology areas. The first is cloud forensics and the other is Cloud computing. Specific consideration in the research project will be given to cloud forensics procedures and methodologies. The literature review evaluation will include current trends in Cloud computing technology and cloud forensics tools, methodologies and procedures with comparison with what has been already been done by other researchers on the same.

Cloud Forensics activities involves resolving the difficult issues encountered in conducting digital forensics investigations to cloud computing environment which are virtual other than conventional. The current work addresses interpretative audit analysis for the time-stamped hypervisor virtual machine logs as basis of establishing ground truth forensic evidence, cloud risk assessment modeling, cloud insider threat detection, service level agreements, and privacy preserving auditing but it is a dangerous operation where should anything happens the client will need to deal with third party in trying to unlock the problem and tracing of evidents. Where as this is possible, the time and resource needed for the operation is enormous thus cloud logs audit trail which is an enhancement of digital forensics.

The current nature of cloud environment is multi-tenancy, jurisdiction, data duplication and high degree of virtualization therefore multiple layers of complexity in cloud forensics in the different services are hosted in different environment with different security controls. This is further compounded when the Cloud Service Providers trade service among themselves without the knowledge of their customers they are hosting services for, making it difficult to follow the chain of events when and issue arises i.e data lose through hacking and data stealing. Therefore, the forensics process applicable in non-cloud environment is no more practical in the case of the current cloud environment because of it convergence of application and hardware devices. With the increase use of cloud services, cloud forensics has been categorized into three dimensions: Technical, Organizational and Legal (Ruan et al.,2011), therefore the is need for logs audit trail to mitigate the arising issues being experienced. The various technical dimension encompasses the procedures and tools that are needed to perform the forensic process in a cloud computing



environment whereby most clients doesn't understand how it operates hence just paying for the services to be delivered by the provider. The logs audit trail will help data collection, live forensics, evidence segregation and pro-active measures which can be depicted early enough when monitoring on the logs from the private cloud server. On the other hand, the organizational dimension covers the organizational aspects of the forensics. It includes actors like cloud providers, customers, legal advisers, incident handlers and objects like binding service level agreements (SLAs), policies and guidelines.

The legal dimension for the logs audit trail needs is to cover the regulations setup and agreements to ensure that forensic activities do not breach laws and regulations in the jurisdictions where the data resides or is collected, simultaneously ensuring the confidentiality of co-tenants who share the same infrastructure with other users which is normally the norm with the providers.

The migration of services to cloud resulted to cloud forensics emerging field that requires more attention than standard digital forensics. A large portion of the research done on cloud computing so far has dealt with the increasing legal troubles that law enforcement will face when attempting to seize or retrieve information in the cloud since the procedures to prove to be hard because services are not hosted in the same hardware but virtual with replication across different platforms.

Many organizations that uses cloud services don't consider the legal issues that come with clouds computing. "According to Network World (Messmer, 2013), any business that anticipates using cloud based services should be asking the question: What can my cloud provider do for me in terms of providing digital forensics data in the event of any legal dispute, civil or criminal case, cyber attack, or data breach?" Other studies have compared the actual providers themselves. Each cloud service provider is going to be different; this complicates cloud based forensics because each company will have different rules, guidelines, and requirements. According to the IATAC (Scott Zimmerman, 2011), "to date , there has been very little research done on the current state of the tools, processes, and methodologies to obtain legally defensible digital evidence in the cloud."

### **1.3. Technical Dimension**

The technical dimension encompasses procedures and tools that are needed to perform the forensic process in a cloud computing environment to a standard which its results can be used in law enforcement. It includes collection of data, live forensics, evidence segregation, virtualized environments and proactive measures .

With data collection process it involves identifying, labeling, recording and acquiring forensic data from a source for analysis. Forensic data will include client-side artifacts that reside on client premises (VM) and provider-side artifacts that are located in the provider infrastructure (Cloud). The various procedures and tools used to collect forensic are unique based on the specific model of data responsibility that is in place and the intended function of the artifact. Forensics logs data collection should preserve the integrity and originality of data with clearly defined segregation of duties between the client and provider and also the third party who part of the system. There should be no breach of laws or regulations in the jurisdictions where data is collected, or compromise the confidentiality of other tenants that share the resources. Example, in public clouds, provider side artifacts may require the segregation of tenants, whereas there may be no such need in private clouds since there is ownership.

## 1.4. Problem Statement

With the advent of cloud computing, organizations are now giving up control of their on-premise resources and entrusting a cloud service provider to deliver the service. In this environment, many would agree that logs play an even more important role in security assurance.

Many of the techniques used in computer forensics have not been formally defined. “Computer Forensics is looked at as part art and part science” [HoneyNet Project 2002]. Cloud Forensics has evolve over years into a science as more research and standardized procedures are developed with the expansion of services hosted on cloud to accommodate the user needs and requirements and cope with the dynamic technological trends globally.

Due to the increasing number of cases, forensic analysis increasingly depends on automation to achieve results in a reasonable time which is really a challenge to achieve. Another key challenge that Cloud computer forensics face concerns the credibility of an analysis which is defined by the source of the collected information. Often the credibility of an analysis is mostly based on the credibility of the expert conducting the analysis and software’s used, rather than relating credibility to the methodology applied to investigate the incident.

A cloud provider’s ability to provide specific audit event, log and report information on a per-tenant and application basis is essential. It is apparent that in order to meet these customer expectations, cloud providers must provide standard mechanisms for their tenant customers to self-manage & self-audit application security that includes information about the provider’s hardware, software and network infrastructure used to run specific tenant applications and based on this there is a need for;

(1) Logs audit trail framework to synchronize logs on real time from the private cloud (Virtual Environment) for audit trails hence it is the baseline line of this research paper.

The goal of this research paper is to come up with a framework which can analyze the data from the cloud server on the logs controller on real time. A formal definition of cloud forensics logs audit trail will be given. The paper will look at how intrusion detection systems can be used as a

starting point to a computer forensics investigation. Also, the ways to preserve and recover data during a cloud forensics investigation using open source forensics tools will be explored.

A discussion of how some of various software tools that are used in a Cloud forensics investigation will be included. This paper will explain the rights granted to a company who plans to implement such tool and will provide information on tools currently available for use in cloud forensics. Last, the paper will explore ways that can be used in correspondence with cloud forensics in private virtual environment and in this case the owner of the data will be in full control other than the third party.

### **1.5. Objective of the study**

Cloud computing is an emerging and revolutionary technology that has changed the ways in which data storage and accessing is, and brought with the growing of cloud and related services, security and privacy in the Cloud have become very critical issues in cyber security. The integration of cloud services to existing computing systems and networks changed the security perspectives and measures, consequently affecting how crime related digital evidence is retrieved and handled in this environment.

The main objective of the research is to have :

- i. Cloud Digital Forensics Logs audit trails framework in a private Cloud virtual environment.

## **1.6. Specific Objectives**

1. Identify factors and define
2. Develop a Framework and prototype for Synchronize virtual systems Logs in Enterprise cloud.
3. Test and Validate the framework
4. Implementation of the model

The process outlined by lends itself as a framework for forensic investigation, and is used in the following sections to explore the issues at each stage of the process in relation to forensic analysis in a cloud environment.

## 1.7. Motivation

The rash for cloud computing services, application and data storage necessitated the idea of how well can the customer data be monitored. As digital evidence is becoming more and more relevant in the ever increasingly technology driven world, new challenges arise in handling such evidence. Considering that new technology and new advanced software is released continuously to the market hence keeping up with all developments is a daunting task. In being able to present digital evidence in a court of law, the scientific principles of validity and admissibility have to be met and currently no proper laws governing digital crimes. To be able to do so, there should be general accepted guidelines for testing of the forensics tools used in handling of digital evidence, to be able to say with a reasonable amount of certainty that the results are a cause of one thing, rather than being introduced through the use of a tool or function that the practitioner is unaware of. With the emerging use of different cloud based services for storing and sharing information, there could also be a possible privacy issue.

With the increasing demand for using the power of the Cloud for processing also sensible information and data, enterprises face the issue of Data and Process Provenance in the Cloud. Digital provenance, important meta-data that describes the ancestry or history of a digital object, is a crucial feature for forensic investigations. In combination with a suitable authentication scheme, it provides information about who created and who modified what kind of data in the Cloud. These are essential aspects for digital investigations in distributed environments such as the Cloud which the research project is looking into by introducing logs audit trail framework.

Also the vulnerabilities involve in digital forensic software has widely marketed, the forensic software may lead to defenseless state which might expose the collected information to the third party.

The level of vulnerabilities is unlimited and can be exploited through software architecture, type of file, level of patching and etc. Thus, it is crucial to have a real time logs outside the main server which can be used to extract logs for forensic investigation.

## 1.8. Justification

Different various instances running on a single physical machine are usually isolated from each other via virtualization in the cloud environment since they are using different processing power. The neighbours of an instance have equal access to the host on the Internet. Neighbours behave as if they are on separate hosts but on replication from the core hardware. Customer instances have no actual access to raw disk devices, instead they access virtualized disks. At the physical level, system audit logs of shared resources collect data from multiple tenants. Technologies used for provisioning and de-provisioning resources are constantly being improved therefore in totality the customer's data is handled by third parties of which when there is a crime it is hard to trace and collect the facts needed for investigation.

Most cloud forensic investigations are conducted by traditional digital forensic experts using conventional network forensic procedures and tools. A major challenge is posed by the expertise of technical and legal expertise with respect to cloud forensics. This is exacerbated by the fact that forensic research and laws and regulations are far behind the rapidly-evolving cloud technologies.

The virtual instance currently within the Cloud, where i.e. data is stored or processes are handled, provides potential evidence. In most instances, it is the virtual environment where an incident occurred which provides a potential starting point for a forensic investigation, but with audit log trail, the client has the facts for starting up the forensics. The instance can be accessed by both, the content security providers (CSP) and the customer who is running the instance thus with the Log audit trail controller, the customer will be able to monitor and safeguard all the logs which will fast-track investigation.

Table 1 – Cloud Forensics Main Challenges

Cloud Features CF Challenges	Elasticity	Multiple Locations	VM	Broad Network Access	Third Party Services	Cross-Providers	SLA
Reduced data access	X	X	X				
Lack of physical control	X	X	X				
Lack of standard	X	X	X				
Multiple log formats	X		X				
No timestamps synchronization		X		X			
No routing information		X	X	X			
Lack of expertise		X				X	
Legal measures		X			X	X	X
Multi – tenancy	X						X
Multiple jurisdiction		X					X



## 1.9. Scope of the research

The main aim of this research project is to find key aspects of tracking logs from one virtual box to another for different cloud storage applications to aid forensic investigators and law enforcement. It is important to find any and all relevant artifacts that are created during the applications use, as well as any files or meta-data of files being loaded, whether or not they have been deleted without the knowledge of the client or cloud service provider.

The process of cloud forensics involves various stages which include preservation, identification, extraction, documentation and interpretation of computer data [Kruse II and Heiser 2002], and it is usually used when a crime has been committed or an inappropriate activity has taken place. Some common examples of when computer forensics is used are:

- Testing virtual cloud storage data security.
- To reveal activities and processes taking place within the private cloud server.
- Track logs on real time basis.
- Auditing of logs for security purpose.

Source of data logs to be collected will be captured from;

- (i) Access Logs
- (ii) API Management logs
- (iii) Security Logs (Firewall,IDS,Opensource tools)
- (iv) Metadata-Application
- (v) Netflow, Packet Capture
- (vi) Cloud Data storage
- (vii) Certificate and private Keys

## **2.0 CHAPTER TWO**

### **2.1 Literature Review**

Cloud computing describes a computing concept where software services and the resources they use operate as (and on) a virtualized platform across many different host machines which are connected by the Internet or an organization's internal network. From a business or system user's point of view, the cloud provides, via virtualization, single platform or service collection in which it can operate.

The provided service is utterly economical and expandable. Cloud computing attractive benefits entice huge interest of both business owners and cyber thefts. Consequently, the “computer forensic investigation” step into the play to find evidences against criminals. As a result of the new technology and methods used in cloud computing, the forensic investigation techniques face different types of issues while inspecting the case. The most profound challenges are difficulties to deal with different rulings obliged on variety of data saved in different locations, limited access to obtain evidences from cloud and even the issue of seizing the physical evidence for the sake of integrity validation or evidence presentation.

Challenges for data discovery and evidence collection are experienced due to proliferation of endpoints, especially mobile endpoints, is a. Due to large number of resources connected to the cloud, the impact of a crime and the workload of an investigation can be massive.

The new trends of cloud computing in recent years has produced major technological advancement in the way Information Technology (IT) services are provisioned and deployed. Cloud computing, which can be used by individuals as well as corporations, continues to grow at remarkable rate due to its many favorable features. Among others, adopting cloud computing users can alleviate big capital investments, replacing them with low cost and more flexible operational expenses, while taking advantage of its speed, agility, flexibility, infinite elasticity and more importantly mobility because services can be accessed anytime from anywhere. The offered features have fuelled a phenomenal growth in cloud services market. Independent studies conducted by organizations, such as the European Network and Information Security Agency (ENISA) and Gartner, predicted a sharp increase in the adoption of cloud computing services by corporate organizations,

educational institutions and Government agencies (Gartner,2014; IEEE, 2014). A study by Market Research Media found that the global cloud computing market is expected to grow at a compound annual growth rate of 30% reaching \$270 billion by 2020 (Zawaod and Hasan, 2013). The growth is mainly fuelled by the cost savings and pay per use model offered by cloud computing. A similar case study conducted on cloud migration reported an average cost saving of 37% when organizations move their infrastructures to Amazon EC2 cloud, in addition to potentially eliminating 21% of the support calls, showing compelling reasons to adopt cloud computing (Khajeh Hosseini et al., 2010). A recent study conducted by Right Scale group on the adoption of cloud computing, concluded that cloud adoption reaches ubiquity with 87 percent of the surveyed organizations using public cloud. Amazon Web Services (AWS) leading the cloud adoption at 54 percent (RightScale, 2014).

On the other hand, Cloud Security Alliance (CSA) reported a corresponding growth in cloud vulnerability incidents. Specifically, CSA's report shows that cloud vulnerability incidents between 2009 and 2011 have more than doubled, with top three cloud service providers (CSPs), i.e., Amazon, Google and Microsoft, accounted for 56% of all non-transparent cloud vulnerability incidents.

The report also cited that the number of vulnerability incidents over the past five years has risen considerably (CSA,2013b). The increasing security incidents in the cloud are caused, among others, by easy user account registration provided by CSPs, unfettered accessibility, and virtually unlimited computing power. In essence, attackers can open bogus accounts to the cloud, use them to carry out their acts, terminate the accounts and disappear once their malicious acts have been performed. Easy access and almost unlimited power of the cloud allow the attackers,using cloud as a platform, to perform their powerful attacks from anywhere in short periods.

While it is impossible to prevent all attacks totally, they should be traced back to the attackers. Digital forensics is commonly used to track and bring criminals into justice in a non-cloud (traditional) computing environment. However, traditional digital forensics cannot be directly used in cloud systems. In particular, distributed processing and multi-tenancy nature of cloud computing, as well as its highly virtualized and dynamic environment, make digital evidence identification, preservation and collection, needed for forensics, difficult. Note that cloud systems have been hardly designed with digital forensics and evidence integrity in mind, and thus forensics

investigators face very challenging technical, legal and logistical issues.

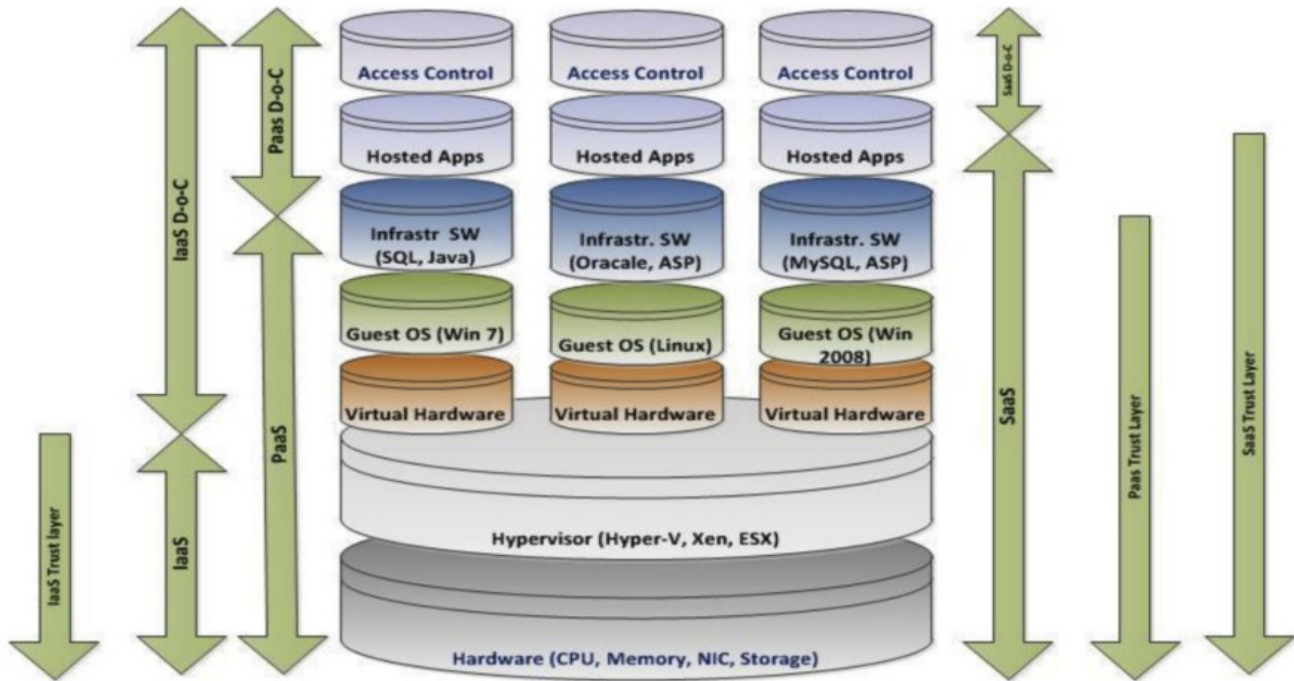


Fig. 1. Cloud model, Degree of Control (D-o-C) and trust layer.

Professional organizations, i.e CSA and National Institute of Standards and Technology (NIST), and researchers have published papers related to cloud computing in areas such as cloud governance, security and risk assessment (CSA, 2011; Iorga and Badger, 2012; Jansen and Grance, 2011). However, only very little work has been done to develop the theory and practice of cloud forensics (Casey, 2012; Zawaod and Hasan, 2013); some have argued that cloud forensics is still in its infancy (Zawaod and Hasan, 2013).therefore there is more to be done on cloud forensics.

Recently, several researchers have addressed cloud forensic challenges and issues, and proposed solutions to address the challenges (Damshenas et al., 2012; Daryabar et al., 2013; Grispos et al., 2013; Reilly et al., 2011; Taylor et al., 2011; Zawaod and Hasan, 2013). Since then there has been many advancement in the cloud forensic area. In particular, NIST has formed cloud forensics working group and produced draft publications in July 2014 (NIST, 2014a), and CSPs have started

delivering services which supports forensics, e.g., Amazon's security suite of products (AWS Security Centre, 2014) and cloud trail used for logging in the AWS Cloud (AWS Security Centre, 2013a).

Marty's (2011) work tells about a logging framework and guidelines that provide a fore-handed approach to logging to ensure that the data needed for forensic investigations has been generated and collected. The standardized frame work in Marty's work eliminates the need for logging stakeholders to reinvent their own standards

Currently there do not appear to be any published guidelines that specifically address the conduct of computer forensic investigations of cloud computing systems. In order to understand and analyze evidence within this environment, computer forensics examiners will require a broader range of technical knowledge across multiple hardware platforms and operating systems. Dr Mark Taylor *et al* examine the issues concerning the forensic investigation of cloud systems.

Constructing the time-line of an event requires accurate time synchronization in real time which is complicated because the data of interest resides on multiple physical machines in multiple geographical regions, or the data may be in flow between the cloud infrastructure and remote endpoint clients as shown below,

Fig 2-Computer forensics process flow.

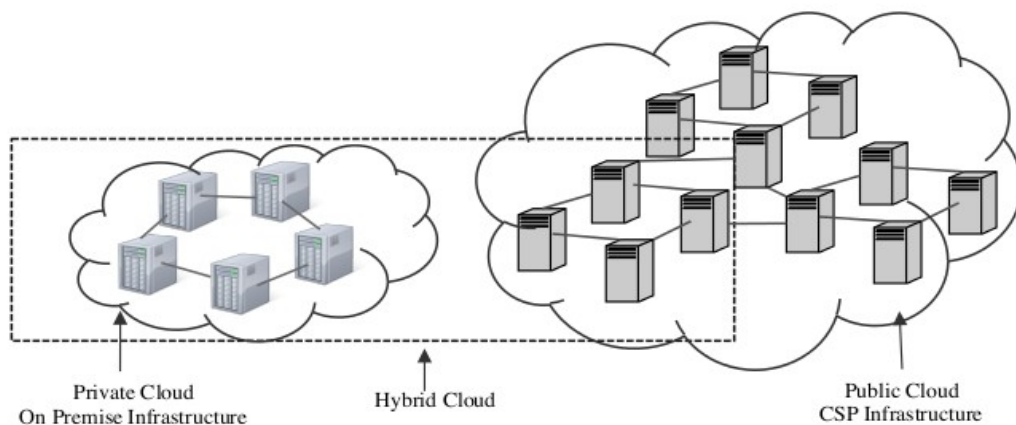


Figure 2. Three different cloud deployment models



Extensive literature review on the current state of forensic research (more so to digital forensics) and the identification of urgent challenges that need to be solved, Prototype implementation for proof of concepts like new data extraction techniques or analyzation methods and Empirical analysis of feature predominance and assessment of expected information increase in forensic examinations.

The purpose of any cloud forensic investigation is to locate identify and preserve evidence data on which a judgment or conclusion can be based and are admissible, authentic, complete, reliable and believable.

Cloud computing is pushing the frontiers of cloud computing forensics. There are various integration involved; technological, organizational and legal challenges. Several of these challenges, such as data replication, location transparency and multi-tenancy, are unique to cloud forensics.

This research project paper suggests a simple yet very useful solution to conquer the aforementioned issues in forensic investigation of cloud systems. Event tracker, Logs synchronization, implementing multi-factor authentication and updating the cloud service provider policy to provide persistent storage devices, are some of the recommended solutions. Utilizing the proposed solutions, the cloud service will be compatible to the current digital forensic investigation practices; alongside it brings the great advantage of being investigated and consequently the trust of the client.

The Digital Forensic Readiness (DFR) is a very active research field that attracted many researchers. DFR combines forensic expertise, hardware, and software engineering. The initial idea of DFR was proposed in 2001 . A DFR system has two objectives: maximizing an environment's ability to collect credible digital evidences, and minimizing the cost of Forensics in an incident response. DFR includes data collection activities that concern some components such as RAM, registers, raw disks logs.

Other related factors have been also analysed, such as, how the logs will be recorded, what is actually logged, how the Forensic Acquisition actually happens, and what are the procedures to be used for Evidence Handling.

Waterloo, Ontario-May 22nd, 2012-Internet Evidence Finder (IEF), the market leading computer forensics solution, now supports the recovery of evidence from Cloud services. IEF v5.5 supports the recovery of cloud-based evidence from computer hard drives and live memory. Initial support includes popular cloud storage services Dropbox, Google Docs, Google Drive, Skydrive, and Flickr. Additional cloud storage services will be supported throughout the summer.

“Cloud storage usage has exploded as people want to share & access their files wherever they are around the world. The positive news for investigators is that there is a wealth of evidence left behind on a hard drive and in RAM when using these cloud services.

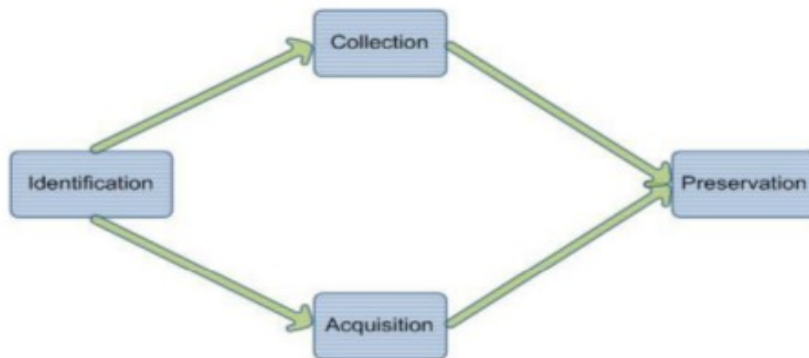
## **2.2 Forensics crisis**

With the technological dynamism, much of the last decade’s progress is quickly becoming irrelevant. Digital Forensics is facing a lot of challenges and in a crisis. Hard-won capabilities are in jeopardy of being diminished or even lost as the result of advances and fundamental changes in the computer industry:

- The storage devices size is growing therefore there is frequently insufficient time to create a forensic image of a subject device, or to process all of the data once it is found.
- Increased prevalence of embedded flash storage and the proliferation of hardware interfaces means that storage devices can no longer be readily removed or imaged.
- Due to proliferation of operating systems and file formats there is dramatically increasing in requirements and complexity of data exploitation tools and the cost of tool development.
- Previously cases were limited to the analysis of a single device, increasingly cases require the analysis of multiple devices followed by the correlation of the found evidence.
- Pervasive encryption (Casey and Stellatos, 2008) means that even when data can be recovered, it frequently cannot be processed.
- With the current use of the “cloud” for remote processing and storage, and to split a single data structure into elements, means that frequently data or code cannot even be found.
- Malware that is not written to persistent storage necessitates the need for expensive RAM forensics.

## Key Issues in Cloud Forensics

1. Acquisition of data is more difficult
2. Cooperation from cloud providers is paramount.
3. Cloud data may lack key forensic attributes.
4. Current forensic tools are unprepared to process cloud data.
5. Chain of custody is more complex



**Fig. 3.** Evidence Handling process according ISO 27037 (CSA, 2013a).

Legal challenges increasingly limit the scope of forensic investigations. New and advanced systems should be able to reason with and about forensic information in much the same way that analysts do today. Programs should be able to detect and present outliers and other data elements that seem out of place. These systems will be able to construct detailed base-lines that are more than simply a list of registry entries and hash codes for resident files.

Realistically, the only way that DF researchers and practitioners can cope with the challenges posed by the increasing diversity and size of forensic collections is to create more powerful abstractions that allow for the easier manipulation of data and the composition of forensic processing elements.



### 3.0 CHAPTER THREE

#### 3.1 METHODOLOGY

##### 3.1.1 Live Forensics

The converged and proliferation of computing endpoints, especially mobile endpoints and roaming devices, is a challenge for data discovery and evidence collection. Because of the large number of resources connected to the cloud, the impact of a crime and the workload of an investigation can be massive.

Constructing the time line of an event requires accurate time synchronization but its because the data of interest resides on multiple physical machines in multiple geographical regions, or the data may be in flow between the cloud infrastructure and remote endpoint clients. Extensive literature review on the current state of forensic research(more so to digital forensics) and the identification of urgent challenges that need to be solved,Prototype implementation for proof of concepts like new data extraction techniques or analyzation methods and Empirical analysis of feature predominance and assessment of expected information increase in forensic examinations as shown below;

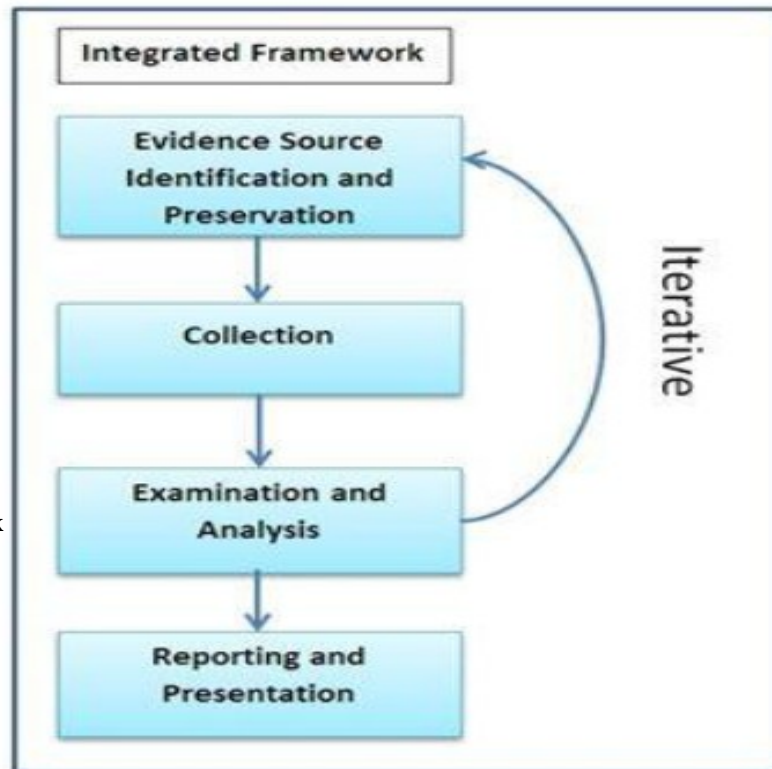


Diagram 2- Integrated Framework

An important source of evidence in traditional digital forensics is deleted data, but with the current trends logs give a lead and make the source of information. In the cloud, the customer who created a data volume often maintains the right to alter and delete the data “Amazon, AWS Security Center, Seattle, Washington (aws.amazon.com/security)”. When the customer deletes a data item, the removal of the mapping in the domain begins immediately and is typically completed in seconds. Remote access to the deleted data is not possible without the mapping. Also, the storage space occupied by the deleted data is made available for write operations and is overwritten by new data. Nevertheless, some deleted data may still be present in a memory snapshot “Amazon, AWS Security Center, Seattle, Washington (aws.amazon.com/security)”. Main challenges in forensics are to recover the deleted data from the source, identify the ownership of the deleted data, and use the deleted data for event reconstruction in the cloud.

### **3.1.1 (a) Logging Architecture**

For cloud forensics to give results, a log management system is the basis to enable log analysis to solving the goals introduced in this research project paper by setting up a logging framework which will involve the following;

- (i) Enable logging in each infrastructure and application component across the different platforms.
- (ii) Setup and configuring log transport Synchronized clocks across the two servers with secured controls.
- (iii) Tuning logging configurations to meet point two expectation

### 3.1.2. Cloud forensic Principles

Digital Evidence	Digital Investigation Process (Collection & identification, Storage, preservation, and transportation, Presentation)
Desired Properties: Integrity, authenticity, complete, reliable, non-repudiation, etc	Desired Properties: Reproducibility, Real-time, Confidence interval, Reliable and believable,

### 3.1.3. Framework and Prototype implementation for proof.

- Simulation will be used to test the data artifacts.
- Use of forensics free source tools and softwares

### 3.1.4. Cloud Forensic Process

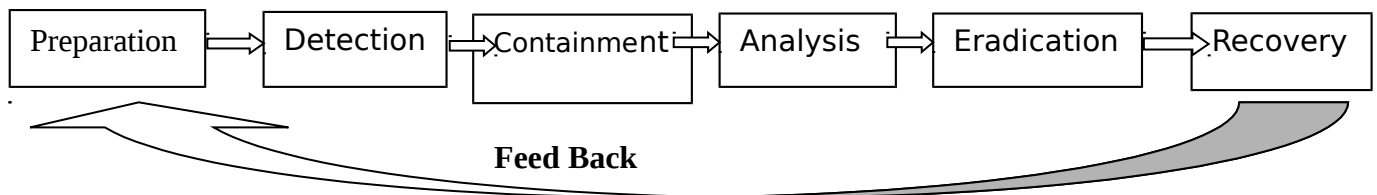


Figure 3.1 Cloud process

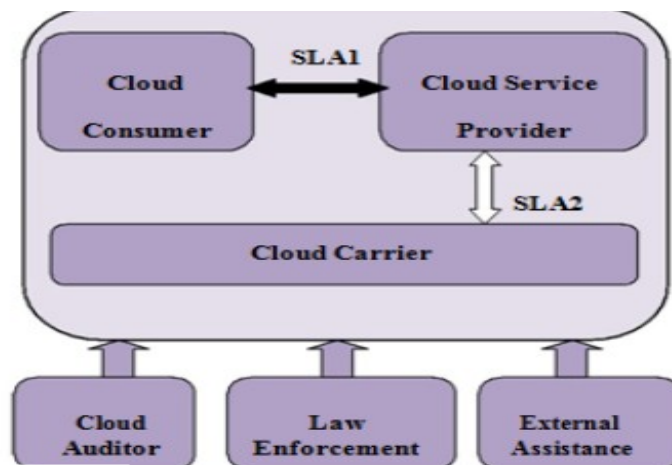


Figure 3.2

Cloud Actors interaction scenario 1

Some of the basic and traditional definitions that are used in the area of cloud forensics research was borrowed digital forensics. Digital data are data represented in a numerical form.

With modern computers systems, it is common for the data to be internally represented in a binary encoding, but this is not a requirement. A digital object is a discrete collection of digital data, which could be a file, a hard disk sector, a network IP address packet, a machine (MAC) address, a memory page, or even a process. By analogy the Digital Object is also equivalent to that of our VM Data Object, hence the VM data object is nothing more than a meta digital data object.

Computer networks keep track of activity on the network but what happens when the network is disconnected and logs are erased by intruders to the system?, For example the network will record information about when, where and who accessed a computer system, including the exact date and time and there is need to track this logs from a different location. System based Log-ins and passwords facilitate detailed record keeping about a computer system and therefore to enhance this, log audit trail comes in place to enable the data owner to be able to be informed on what is happening. Not only does the network record access, it also will contain security-related information, including unauthorized attempts to gain access. The network will remember and identify documents created, stored, accessed or deleted on a system.

## **3.2.0 Deployment Model**

### **3.2.1 Private cloud:enterprise owned or leased**

A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate. As with other cloud models, private clouds will provide computing power as a service within a virtualized environment using an underlying pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organisation providing with greater control and privacy.

A simulated virtual machine (VM) for each of the three cloud services should be created.

- i. Simulated virtual cloud Environment.
- ii. Create a 20GB Linux VM for each cloud service
- iii. Logs audit trail API Framework
- iv. Sysinternals Process Monitor to record any and all changes/additions that the cloud services made during their use, from the installation to when the services were Uninstalled.
- v. logwatch logs analyzer tool.
- vi. Rsyslog open source tool.

The open source tools will be used for reporting purposes and it will be installed and configured in the simulated private cloud and logs controller server environment.

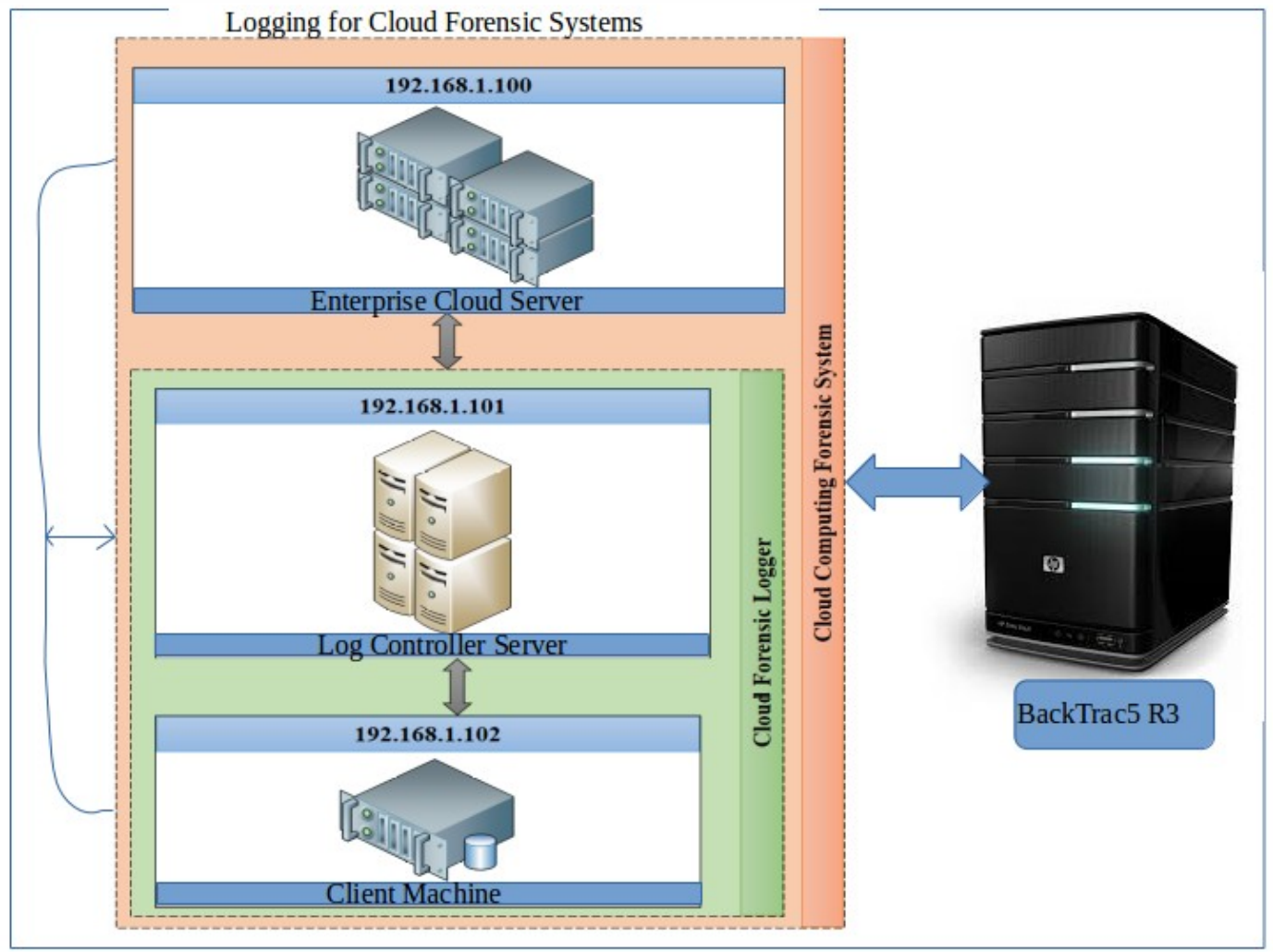


Diagram 3-Cloud Forensics Systems

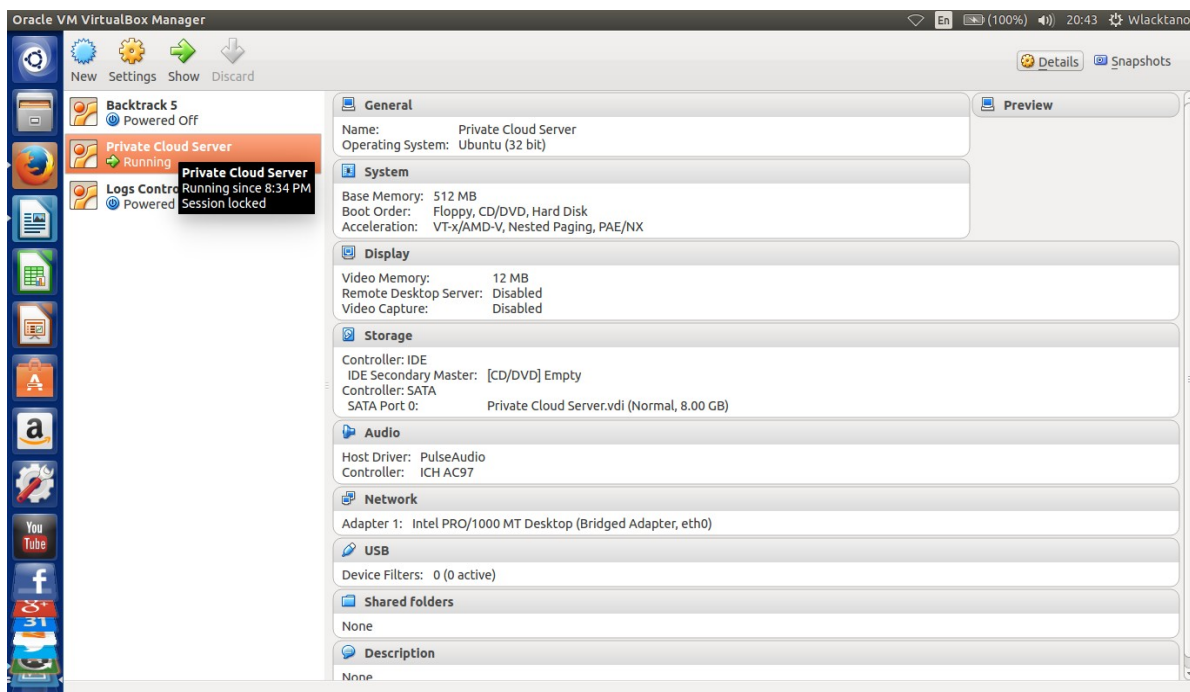
### 3.2 Report API Login Activity Report

The login activity report will involve three servers which uses a real time log audit synchronized mode for the purpose of trailing of logs on the cloud server synchronized to logs controller. Management of the logs will be done through a web interface

#### a) Private Cloud server

This is a dedicated storage in the cloud where services are stored. Private cloud servers work in the same way as physical servers but the functions they provide can be very different and in thus the entire server is dedicated to them with no other clients sharing it. In some instances the client may utilise multiple servers which are all dedicated to their use. Dedicated servers allow for full control over hosting. The downside is that the required capacity needs to be predicted, with enough resource and processing power to cope with expected traffic levels. Most of this private cloud servers are managed by the owners other than the providers therefore there is need for logs audit for security controls.

Figure 3.3 Simlated Vm Cloud



## b) Backtrack5 server with Metasploit framework

Backtrack5 is an information gathering and vulnerability analysis Platform for Metasploit and in technical terms, it is a script-able red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. It saves time and is very powerful in commencing Metasploit attacks.



Figure 3.4-Backtrack5 Server



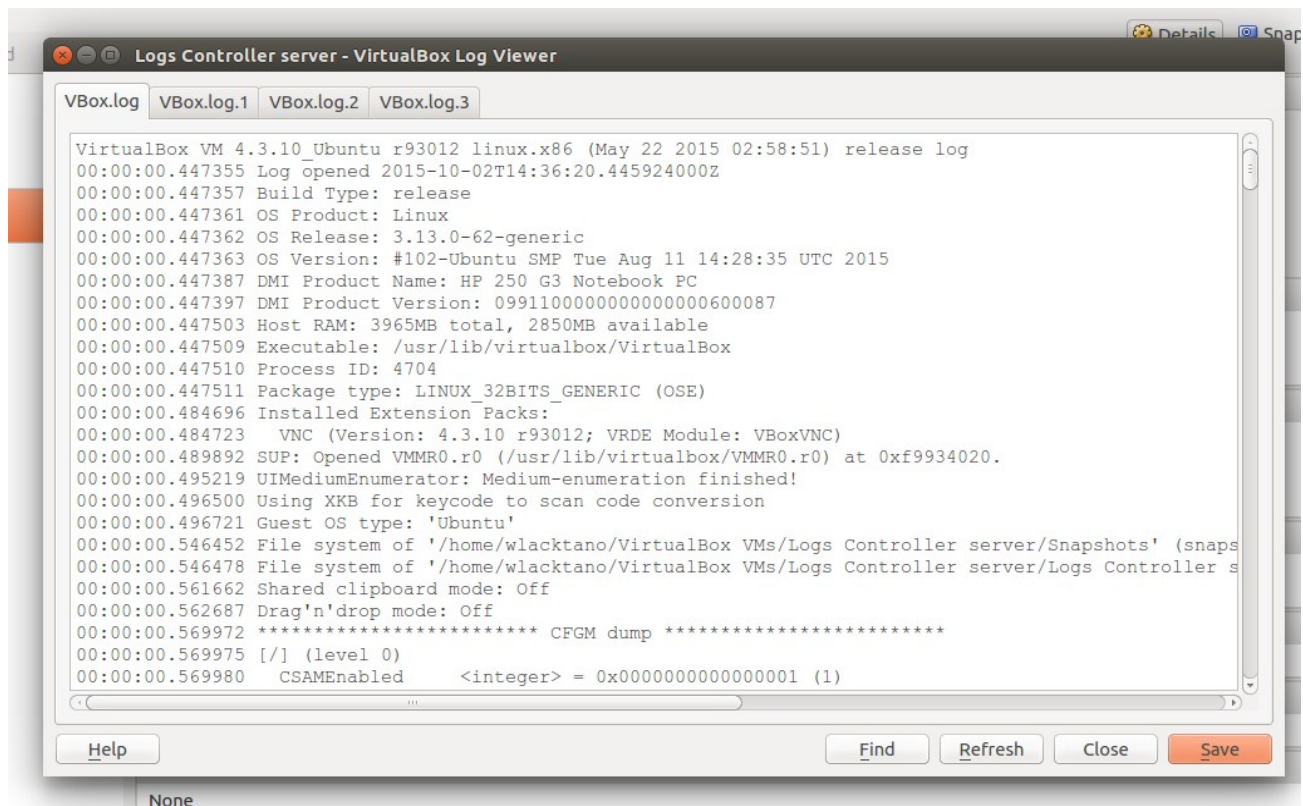
### c) Log controller server

When an investigator wants to investigate an incident, he will first gather the required log either by calling log API or from the cloud management console. While presenting the evidence to the court, he needs to provide the collected logs and also the proof of the logs.

There will be two steps to verify the provided logs. In the first step, the auditor will verify the integrity of the proof and the individual log entry. In the next step, he will verify the order of the log. In this project the function of the Log controller is to pull all the logs of the private cloud server for ease of audit trails when the attacker erases the evidence.

As CSPs have control over generating the logs and the proofs, they can always tamper with the logs. After acquiring logs through API or management console, investigators can also alter the logs before presenting it to court.

The logs audit trail is not only to be used for court case situation but for user ownership and security controls on the data accessibility.



## **4.0 CHAPTER FOUR**

### **4.1 FRAMEWORK**

The cloud forensic system provides various methods and system for generating instances from a client cloud computing environment, where the instance is generated without affecting the integrity of the client cloud computing environment or generating a baseline of the client cloud computing environment thus benchmarking the instance based on comparison of the instance to the baseline, verifying the benchmark based on a client policy and retiring the instance if the benchmark is verified to the accepted standard baseline.

Forensic auditors, Network and database Administrators are always in need of more information and insights from their log data which is normally generated for the source. There are times when an IT administrator would identify some log information which is useful and would like to have it indexed automatically as a new field. Having more fields being indexed makes your log data more useful while conducting log forensics analysis and creating network security reports.

No log management solution vendor will provide out-of-box log collection and reporting functionality for your custom in-house/proprietary applications. With field extraction capability, Log Analyzer allows you to index custom fields and generate reports for any human readable logs collected from your in-house/proprietary applications.

Without a good framework, this cannot be achieved and therefore with log audit trail framework will enable both the cloud forensic auditor and the customer to be in control of their data without going to the third party for storage. The data output format also determine how data will be interpreted and preserved,

System log (Syslog) management is an important need in almost all enterprises. System administrators look at syslogs as a critical source to troubleshoot performance problems on syslog supported systems & devices across the network. The need for a complete sys-log monitoring solution is often underestimated; leading to long hours spent sifting through tons of syslogs to troubleshoot a single problem. Efficient event log syslog analysis reduces system downtime, increases network performance, and helps tighten security policies in the enterprise. To facilitate a more comprehensive mechanism, the developed log audit trail frames will enhance the process of

data collection, analysis, presentation and analysis which is a core factor in forensics field.

If log analysis is the solution to many of our needs in cloud application development and delivery, we need to have a closer look at the challenges that are associated with it.

Common and most challenges associated with cloud based log analysis and forensics are:

- Decentralization of logs
- Volatility of logs

### LOGIC DATAFLOW DIAGRAM

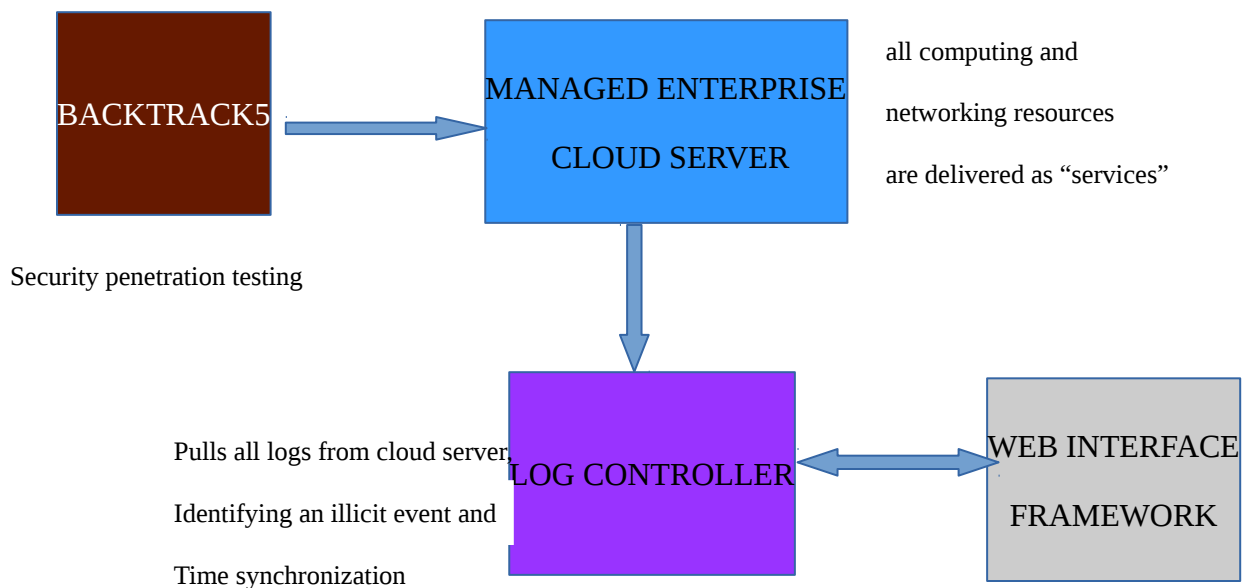


Figure 4-Logic Flow Diagram

## 4.2 Logging Guidelines

To address the challenges associated with the information in log records, the need to establish a set of guidelines and need to have our applications instrumented to follow these guidelines. These guidelines were developed based on existing logging standards and research conducted at a number of log management companies and developed framework can be used to at any level for auditing or law enforcement.

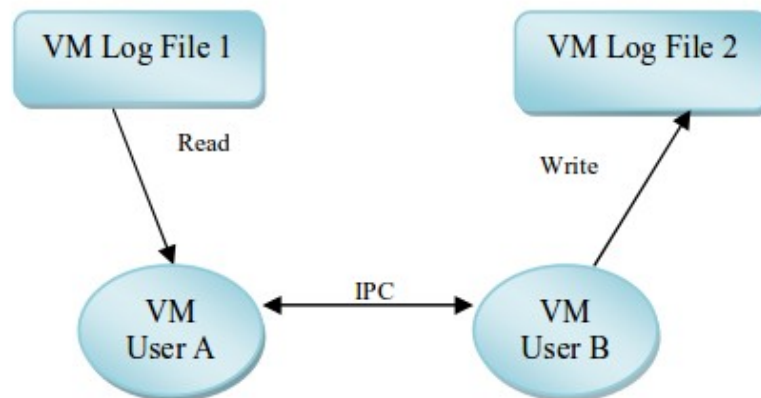


Figure 4.1 The contents of VM Log File 2 are influenced by VM User A

### 4.3 FRAMEWORK MODEL

A cloud computing forensics investigation is to identify the evidences, preserve those evidences, extract them, document each and every process, and validate those evidences and to analyze them by finding the root cause and provide the recommendations or solutions.



Figure 4.2-Data Migration

“There is no single digital forensic investigation model that has been universally accepted. However, it was generally accepted that the digital forensic model framework must be flexible, so that it can support any type of incidents and new technologies” (Adam, R., 2012).

Kent, K., et.al, (2006) developed a basic digital forensic investigation model called the Four Step Forensics Process (FSFP) with the idea of Venter (2006) that digital forensics investigation can be conducted by even non-technical persons and based on this the same was applied when developing the log audit trail framework because this model gives more flexibility than any other model so that an organization can adopt the most suitable model based on the situations that occurred and the reason why the model was chosen was because it will contain below four basic processes has indicated by the diagrams below;

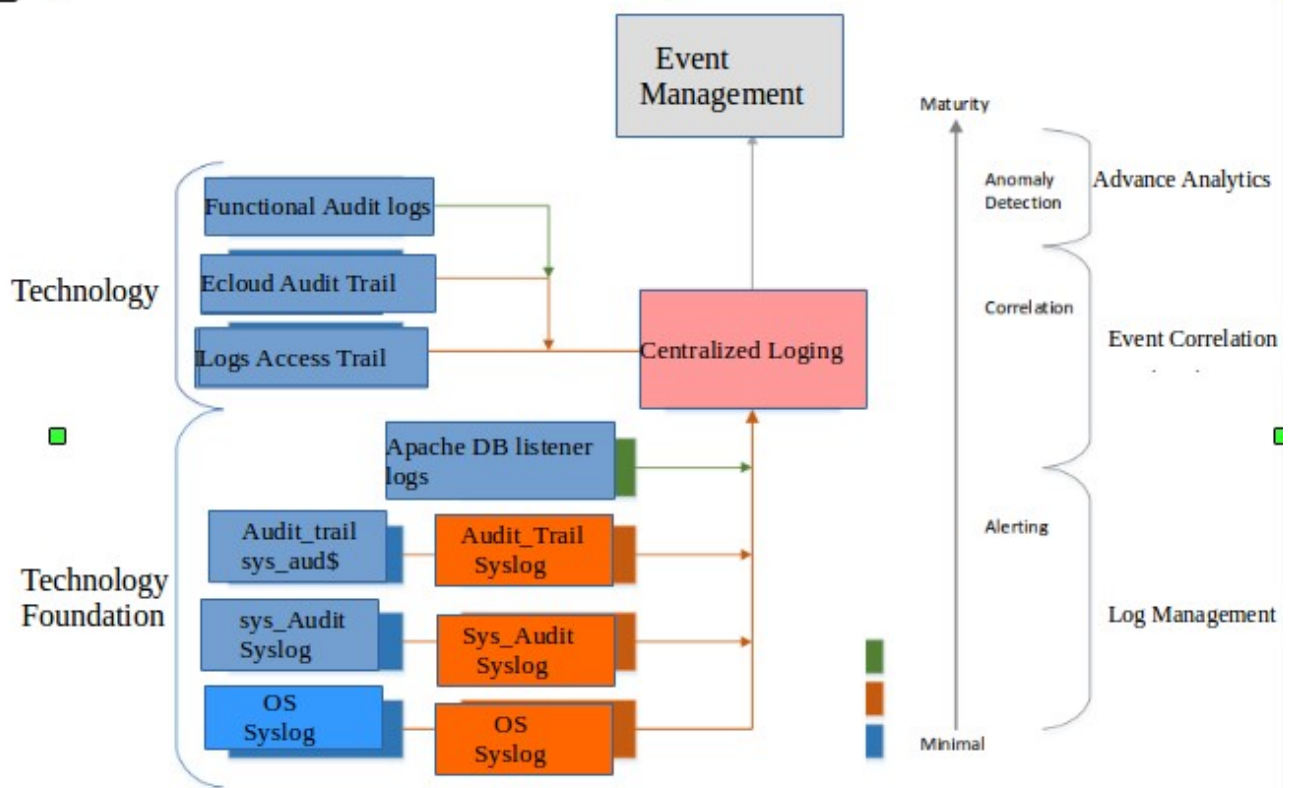


Figure 4.3 Logs Audit Trail Framework



Figure 4.3-Logs audit trail flow

Log audit trail provides for automatic retrieval of your cloud audit logs. You can then route your logs to a centralized server. Backed by an embedded database, it is able to keep track of logs it has already downloaded and logs that have not been sent to the target yet the retrieval and sending of logs to a target is done asynchronously.

In order to do forensics in the cloud, the investigator must log in to different virtual servers and retrieve logs in different formats. Having a unified interface to conduct forensics, across multiple environment and platforms would greatly enhance the ability of the forensic investigator.

#### **4.4 Deploying API**

The application can be deployed to an Oracle WebLogic, virtualBox Server using any of the following tools: the Oracle WebLogic Server Administration Console, Oracle Enterprise Manager Fusion Middleware Control, or Oracle JDeveloper.

The tool recommended to deploy it depends on the application type and whether the application is in the developing phase or in a post-development phase.

#### **4.5 Migrating Logs Audit Policies**

To migrate audit policies, use the export and import operations as explained next.

First, export the audit configuration from a test environment to a file using one of the following tools:

- Logs Audit trail Control: navigate to Domain > Security > Audit Policy, and then click Export.
- The logs command `exportAuditConfig`;  
`wls:/mydomain/serverConfig>exportAuditConfig(fileName='/tmp/auditconfig')`
- Then, import that file into the production environment using one of the following tools:
- Log Audit trail Control: navigate to Domain > Security > Audit Policy, and then click Import.

**Table 2:Logs Types and application**

Types of log	Description	Examples
Application log	Logs that are recorded by an application or program. Application developers are responsible to specify what, when, and how to log through an application execution on a system.	Web applications, Database programs.
System log	System logs are generated by an operating system which are pre-defined and contain information regarding system events, operation, drivers, device change, and various more.	Syslog-ng, Log & Event Manager
Security log	Logs contain security related information to determine malicious behavior found in the system or network. For instance, malware detection, file quarantines, time of malicious detection, and various others.	Event Log Analyzer, Control case Security Event Logging and Monitoring services
Setup log	Setup logs capture the events occur during performing the installation of an application.	Msiexec.exe
Network log	Network log is a log file that contains network related events, that is, description of the event, priority, time occurrence and much more.	Splunk, Log4j2
Web-server log	Web-server log records all events occur on the web-server such as access time, IP address, date & time, request method, and object volume (bytes).	Nihuo Web Log Analyzer
Audit log	Audit log contains user unauthorized access to the system and network for inspecting its responsibilities. It includes destination addresses, user login information, and timestamp.	WP Security Audit Log, auditpol.exe
Virtual machine logs	A file that contains records of each event performed on a virtual machine.	Virtual Machine Log Auditor, JVM controller

application logs, system logs, security logs, setup logs, network logs, web-server logs, audit logs, VM logs, and so on. Each of aforementioned log types is briefly described in



## **4.6 Tools for Audit Trail Analysis**

Many types of tools have been developed to help to reduce the amount of information contained in audit records, as well as to distill useful information from the raw data. Especially on larger systems, audit trail software can create very large files, which can be extremely difficult to analyze manually. The use of automated tools is likely to be the difference between unused audit trail data and a robust program.

Some of the types of tools include:

Audit reduction tools are preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. (This alone may cut in half the number of records in the audit trail.) These tools generally remove records generated by specified classes of events, such as records generated by nightly backups might be removed.

Trends/variance-detection tools look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations. For example, if a user typically logs in at 9 a.m., but appears at 4:30 a.m. one morning, this may indicate a security problem that may need to be investigated.

## 5.0 CHAPTER FIVE

### 5.1 RESULTS AND DISCUSSION

### 5.2 APPENDIX

```
/****** DEVELOPMENT SETTINGS *****/

#Description
#Get a list of the Audit Log entries
#uri - /box/srv/1.1/admin/auditlog/listlogs
#method - POST | GET

/**X-FH-AUTH-SESSION: "<sessionId_returned_from_fh.auth_call>"**/

{
  "userId": "<unique user guid>",
  "storeItemGuid": "<store_item_global_unique_id>",
  "storeItemBinaryType": "ios | iphone | ipad | android",
  "limit": "10 | 100 | 1000"
}

/*****Success*****/

{
  "status": "ok",
  "list": [{
    "deviceId": "<device_global_unique_id>",
    "domain": "<domain name>",
    "guid": "<audit_log_entry_global_unique_id>_RA2E11wCdS",
    "ipAddress": "<downloading host ip address>",
    "storeItemBinaryGuid": "<store item binary guid>",
    "storeItemBinaryType": "<store item binary type>",
    "storeItemBinaryVersion": < store item binary version > ,
    "storeItemGuid": "<store_item_global_unique_id>",
    "storeItemTitle": "<store item title>",
    "sysCreated": "<audit log creation time>",
    "sysVersion": < version > ,
    "userGuid": "<user guid>",
    "userId": "<user_friendly_id>"
  }],
  /* ... */
}
```

```

}

/*****error*****/
{
  "status": "error",
  "message": "<error_message>"
}

$app->configureMode('dev', function () use ($app, $public_path, $srv_public_root) {

    $app->config([

        'log.enable' => true,

        'debug' => false,

        'base.path' => __DIR__,

        'templates.path' => __DIR__ . '/templates', // This will be overridden anyway
        by the default theme.

        'themes.path' => __DIR__ . '/templates/themes',

        'plugins.path' => __DIR__ . '/plugins',

        'schema.path' => __DIR__ . '/schema',

        'locales.path' => __DIR__ . '/locale',

        'log.path' => __DIR__ . '/log',

```

```
'public.path' => $public_path,  
  
'js.path' => $public_path . "/js",  
  
'css.path' => $public_path . "/css",  
  
'db'      => [  
  
    'db_host' => 'localhost',  
  
    'db_name' => 'userfrosting',  
  
    'db_user' => 'Lack5',  
  
    'db_pass' => '12345',  
  
    'db_prefix'=> 'uf_'  
  
],  
  
'mail' => 'smtp',  
  
'smtp' => [  
  
    'host' => 'mail.example.com',  
  
    'port' => 465,
```

```
'auth' => true,

'secure' => 'ssl',

'user' => 'lack5@example.com',

'pass' => 'password'

],

'uri' => [

    'public' => $uri_public_root,

    'js' => $uri_public_root . "/js/",

    'css' => $uri_public_root . "/css/",

    'favicon' => $uri_public_root . "/css/favicon.ico",

    'image' => $uri_public_root . "/images/"

],

'user_id_guest' => 0,

'user_id_master' => 1

]);

});
```



```
Applications ▾ Places ▾ Iceweasel ▾ Fri 10:54 1
http://localhost/forensics/public/logs.php - Iceweasel
Cloud Forensics | Server... x http://localhost/forensics... x +
view-source:http://localhost/forensics/public/logs.php Search ☆
Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

1 <br />
2 <b>Notice</b>: Use of undefined constant E_NONE - assumed 'E_NONE' in <b>/opt/lampp/htdocs/forensics/public/logs.php</b> on line <b>13</b>
3 <!DOCTYPE html>
4 <html lang="en">
5 <head>
6 <meta charset="utf-8">
7 <meta name="viewport" content="width=device-width, initial-scale=1.0">
8 <meta name="description" content="{page.description}">
9 <meta name="author" content="{site.author}">
10
11 <title>Cloud Forensics | Server Logs</title>
12
13 <!-- Favicon -->
14 <link rel="icon" type="image/x-icon" href="{site.uri.favicon}" />
15
16 <!-- Page stylesheets -->
17 <link rel="stylesheet" href="http://localhost/forensics/public/css/font-awesome-4.3.0.css" type="text/css" >
18 <link rel="stylesheet" href="http://localhost/forensics/public/css/font-starcraft.css" type="text/css" >
19 <link rel="stylesheet" href="http://localhost/forensics/public/css/bootstrap-3.3.2.css" type="text/css" >
20 <link rel="stylesheet" href="http://localhost/forensics/public/css/bootstrap-modal-bs3patch.css" type="text/css" >
21 <link rel="stylesheet" href="http://localhost/forensics/public/css/bootstrap-modal.css" type="text/css" >
22 <link rel="stylesheet" href="http://localhost/forensics/public/css/lib/metisMenu.css" type="text/css" >
23 <link rel="stylesheet" href="http://localhost/forensics/public/css/bootstrap-custom.css" type="text/css" >
24 <link rel="stylesheet" href="http://localhost/forensics/public/css/bootstrap-switch.css" type="text/css" >
25 <link rel="stylesheet" href="http://localhost/forensics/public/css/formValidation/formValidation.css" type="text/css" >
26 <link rel="stylesheet" href="http://localhost/forensics/public/css/tablesorter/theme.bootstrap.css" type="text/css" >
27 <link rel="stylesheet" href="http://localhost/forensics/public/css/tablesorter/jquery.tablesorter.pager.css" type="text/css" >
28 <link rel="stylesheet" href="http://localhost/forensics/public/css/select2/select2.css" type="text/css" >
29 <link rel="stylesheet" href="http://localhost/forensics/public/css/select2/select2-bootstrap.css" type="text/css" >
30 <link rel="stylesheet" href="http://localhost/forensics/public/css/bootstrapradio.css" type="text/css" >
31 <!-- Theme stylesheet -->
32 <link rel="stylesheet" href="http://localhost/forensics/public/css/theme.css?user=1" type="text/css" >
33
34 <!-- HTML5 Shim and Respond.js IE8 support of HTML5 elements and media queries -->
35 <!-- WARNING: Respond.js doesn't work if you view the page via file:// -->
36 <!--[if lt IE 9]>
37 <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
38 <script src="https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js"></script>
39 <![endif]-->
40
41 <!-- Header javascript (not recommended) -->
42 </head>
```

\*\*\*\*\*Logging Patterns\*\*\*\*\*

```
import play.Logger;
import play.Logger.ALogger;
import play.mvc.Action;
import play.mvc.Controller;
import play.mvc.Http;
import play.mvc.Http.Request;
import play.mvc.Result;
import play.mvc.With;
import java.util.concurrent.CompletionStage;

public class Application extends Controller {

    private static final ALogger logger = Logger.of(Application.class);

    @With(AccessLoggingAction.class)
    public Result index() {
        try {
            final int result = riskyCalculation();
            return ok("Result=" + result);
        } catch (Throwable t) {
            logger.error("Exception with riskyCalculation", t);
            return internalServerError("Error in calculation: " + t.getMessage());
        }
    }

    private static int riskyCalculation() {
        return 10 / (new java.util.Random()).nextInt(2);
    }
}

class AccessLoggingAction extends Action.Simple {

    private ALogger accessLogger = Logger.of("access");

    public CompletionStage<Result> call(Http.Context ctx) {
        final Request request = ctx.request();
        accessLogger.info("method={} uri={} remote-address={}", request.method(),
            request.uri(), request.remoteAddress());

        return delegate.call(ctx);
    }
}
```



```

#####Configuration#####
<!--
  ~ Copyright (C)2016 Logcontroller----
  -->
<!-- The default logback configuration that Play uses if no other configuration
is provided -->
<configuration>

  <conversionRule conversionWord="coloredLevel"
converterClass="play.api.libs.logback.ColoredLevel" />

  <appender name="FILE" class="ch.qos.logback.core.FileAppender">
    <file>${application.home:-.}/logs/application.log</file>
    <encoder>
      <pattern>%date [%level] from %logger in %thread - %message%n
%xException</pattern>
    </encoder>
  </appender>

  <appender name="STDOUT" class="ch.qos.logback.core.ConsoleAppender">
    <encoder>
      <pattern>%coloredLevel %logger{15} - %message%n%xException{10}</pattern>
    </encoder>
  </appender>

  <appender name="ASYNCFILE" class="ch.qos.logback.classic.AsyncAppender">
    <appender-ref ref="FILE" />
  </appender>

  <appender name="ASYNCSTDOUT" class="ch.qos.logback.classic.AsyncAppender">
    <appender-ref ref="STDOUT" />
  </appender>

  <logger name="play" level="INFO" />
  <logger name="application" level="INFO" />

  <logger name="com.gargoylesoftware.htmlunit.javascript" level="OFF" />

  <root level="WARN">
    <appender-ref ref="ASYNCFILE" />
    <appender-ref ref="ASYNCSTDOUT" />
  </root>

</configuration>

```

```
/***http integration***/
```

```
<filter>
```

```
<filter-name>auditFilter</filter-name>
```

```
<filter-class>org.audit4j.intregation.http.AuditFilter</filter-class>
```

```
</filter>
```

```
<filter-mapping>
```

```
<filter-name>auditFilter</filter-name>
```

```
<url-pattern>/*</url-pattern>
```

```
</filter-mapping>
```

```
/***rsyslog configuration***/
```

Cloud Forensics

Home

Login

# Welcome to Cloud Forensics LC!

Login

[Forgot your password?](#)

[Resend activation email](#)

```

module(load="imfile" mode="inotify")
input(type="imfile"
      file="/path/to/file1-*.log"
      tag="app1")

input(type="imfile"
      file="/path/to/file2-*.log"
      tag="app2")

$template App1Template,"TOKEN_1 %HOSTNAME% %syslogtag%%msg%\n"
$template App2Template,"TOKEN_2 %HOSTNAME% %syslogtag%%msg%\n"

if $programname == 'app1' then @@data.logentries.com:80;App1Template
& ~

if $programname == 'app2' then @@data.logentries.com:80;App2Template
& ~

```

Enter or modify a SOQL query below:

```

SELECT EventDate, CreatedDate
FROM LoginEvent
Limit 10

```

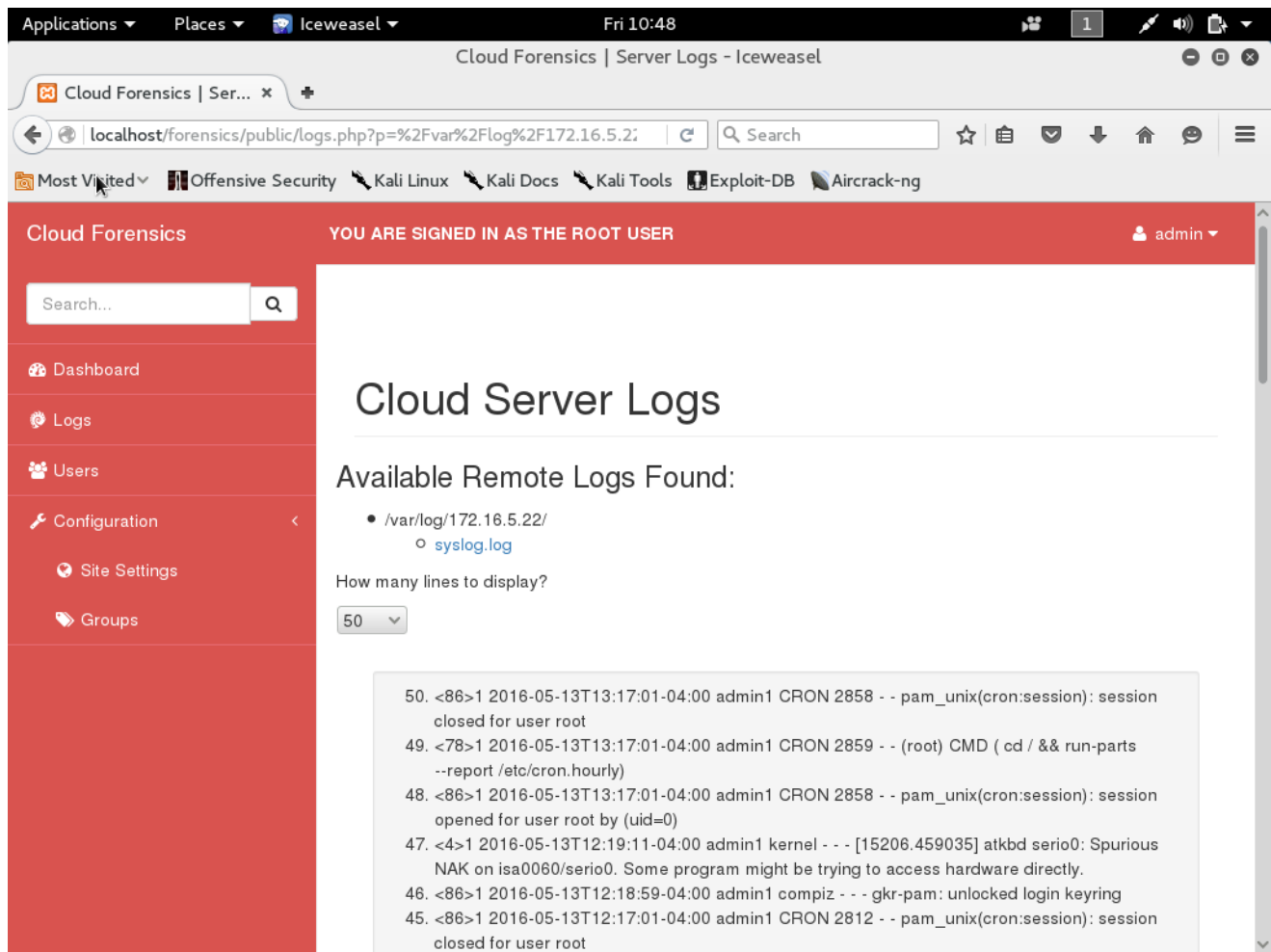
Query

### Query Results

Returned records 1 - 10 of 10 total records in 0.371 seconds:

	EventDate	CreatedDate	
1	2016-01-29T18:29:05.000Z	2016-01-29T18:29:07.708Z	← 2 seconds
2	2016-01-29T18:26:39.000Z	2016-01-29T18:26:46.538Z	
3	2016-01-29T18:25:46.000Z	2016-01-29T18:25:46.536Z	
4	2016-01-29T18:25:46.000Z	2016-01-29T18:25:48.673Z	← 2 seconds
5	2016-01-29T18:25:40.000Z	2016-01-29T18:25:49.349Z	
6	2016-01-29T18:25:33.000Z	2016-01-29T18:25:37.705Z	
7	2016-01-29T18:24:51.000Z	2016-01-29T18:24:57.705Z	
8	2016-01-29T18:24:23.000Z	2016-01-29T18:24:33.145Z	← 10 seconds
9	2016-01-29T18:23:16.000Z	2016-01-29T18:23:17.700Z	
10	2016-01-29T18:21:33.000Z	2016-01-29T18:21:39.335Z	

## 5.3 Login Form



The screenshot shows a web browser window with the following details:

- Browser: Iceweasel
- Page Title: Cloud Forensics | Server Logs - Iceweasel
- URL: localhost/forensics/public/logs.php?p=%2Fvar%2Flog%2F172.16.5.22
- Navigation Bar: Cloud Forensics, YOU ARE SIGNED IN AS THE ROOT USER, admin
- Search Bar: Search...
- Left Sidebar (Navigation): Dashboard, Logs, Users, Configuration, Site Settings, Groups
- Main Content: Cloud Server Logs
- Section: Available Remote Logs Found:
  - /var/log/172.16.5.22/
    - [syslog.log](#)
- Control: How many lines to display? (50)
- Log Output (Code Block):

```
50. <86>1 2016-05-13T13:17:01-04:00 admin1 CRON 2858 - - pam_unix(cron:session): session closed for user root
49. <78>1 2016-05-13T13:17:01-04:00 admin1 CRON 2859 - - (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
48. <86>1 2016-05-13T13:17:01-04:00 admin1 CRON 2858 - - pam_unix(cron:session): session opened for user root by (uid=0)
47. <4>1 2016-05-13T12:19:11-04:00 admin1 kernel - - [15206.459035] atkbd serio0: Spurious NAK on isa0060/serio0. Some program might be trying to access hardware directly.
46. <86>1 2016-05-13T12:18:59-04:00 admin1 compiz - - gkr-pam: unlocked login keyring
45. <86>1 2016-05-13T12:17:01-04:00 admin1 CRON 2812 - - pam_unix(cron:session): session closed for user root
```

## 5.4 Logs report

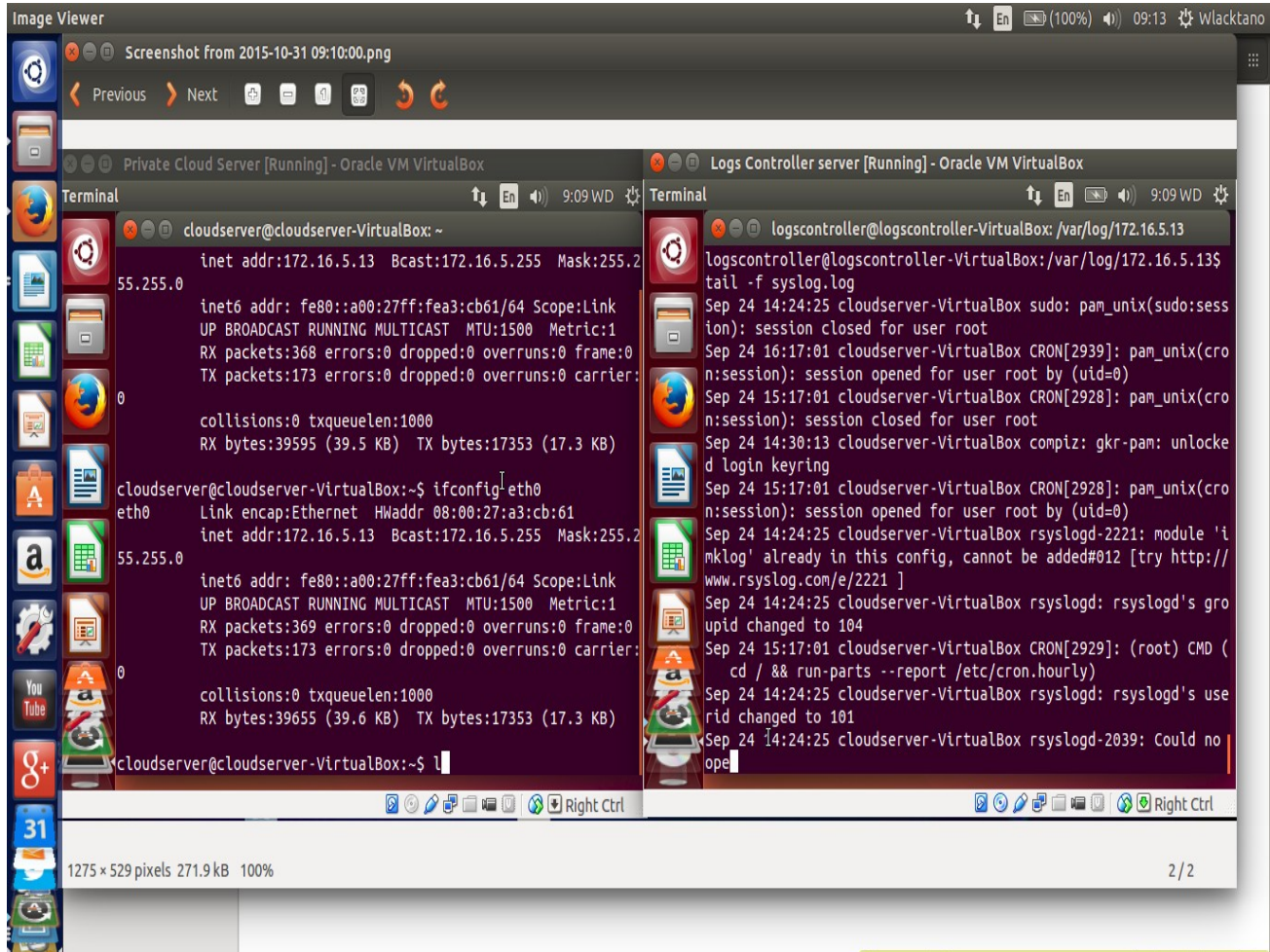


Image Viewer

Desktop

VirtualBox\_Log Controller Server\_14\_05\_2016\_10\_34\_03.png

Applications Places Terminal Fri 10:13

```
root@kali:~#
StButton.app_window_running!last-child first-child] which is not in the stage
<14>1 2016-05-13T18:11:28.717245-04:00 kali gnome-session 913 - - (gnome-shell:
1040): St-CRITICAL **: st_widget_get_theme_node called on the widget [0x828c840
StWidget:last-child first-child] which is not in the stage.
<14>1 2016-05-13T18:11:28.718062-04:00 kali gnome-session 913 - - (gnome-shell:
1040): St-CRITICAL **: st_widget_get_theme_node called on the widget [0x3504c10
StBin:overview-icon:last-child] which is not in the stage.
<14>1 2016-05-13T18:11:28.718378-04:00 kali gnome-session 913 - - (gnome-shell:
1040): St-CRITICAL **: st_widget_get_theme_node called on the widget [0x72d4e50
ShellGenericContainer:last-child first-child] which is not in the stage.
<12>1 2016-05-13T18:11:31.540976-04:00 kali org.gnome.Shell.CalendarServer 899 -
- (gnome-shell-calendar-server:1857): ShellCalendarServer-WARNING **: Error op
ening calendar system-calendar: Cannot open calendar: Cannot parse ISC file '/ro
ot/.local/share/evolution/calendar/system/calendar.ics'
<27>1 2016-05-13T18:11:35.044257-04:00 kali arptwatch - - - 08:d0:9f:9e:c8:45 se
nt bad hardware format 0x2
<27>1 2016-05-13T18:11:45.505673-04:00 kali arptwatch - - - 08:d0:9f:9e:81:c1 se
nt bad hardware format 0x2
<27>1 2016-05-13T18:11:45.903936-04:00 kali arptwatch - - - 08:d0:9f:9e:80:c5 se
nt bad hardware format 0x2
<27>1 2016-05-13T18:11:46.522181-04:00 kali arptwatch - - - 08:d0:9f:9e:c0:d3 se
nt bad hardware format 0x2
root@kali:~#
```

Size	Type	Modified
12.2 kB	Image	Feb 24
15.1 kB	Image	Mar 4
2.9 GB	Unknown	Mar 22
4.9 kB	Image	Apr 1
39.2 MB	Program	Feb 9
6.1 kB	Spreadsheet	Apr 23
15.4 kB	Document	Feb 3
7.7 kB	Spreadsheet	Mar 11
40.1 kB	Image	Mar 3
1.7 GB	Video	Apr 2
12.8 kB	Document	Apr 14
17.9 kB	Spreadsheet	Feb 18
1.0 GB	Unknown	Apr 22 2014
34.2 MB	Archive	Feb 3
(1.6 MB)	Image	10:34

Right Ctrl

## 5.5 Report Properties

The screenshot shows the 'Report Properties' dialog box. On the left is a tree view under the 'Report' tab, listing various report types and parameters. The main area is titled 'Report Properties' and contains a 'General Settings' section. The 'Report Name' is 'CustomAllEvents'. The 'Description' field contains HTML code: `<BODY>`, followed by text: 'This report displays all audit events. You can filter them by event type and date-time range. For a list of components that can generate audit events, see'. The 'Default Data Source' is set to 'Audit' with a 'Refresh Data Source List' link. The 'Parameters per line' is set to '1'. The 'Properties' section includes several checked options: 'Run report online', 'Show Controls', 'Open Links in New Window', and 'Auto Run'. Two unchecked options are 'Enable document cache' and 'Debug Mode'.

**Report**

New Delete ^ v

**Report**

- Data Model
- Generic
- List of Values
  - Users
  - Time Range
  - Application Name
  - ComponentName
  - Event Types
  - Sort By
  - Order
- Parameters
  - userid
  - startDate
  - endDate
  - timeRange
  - componentName
  - appName

**Report Properties**

**General Settings**

Report Name: CustomAllEvents

Description: `<BODY>`  
This report displays all audit events. You can filter them by event type and date-time range.  
For a list of components that can generate audit events, see

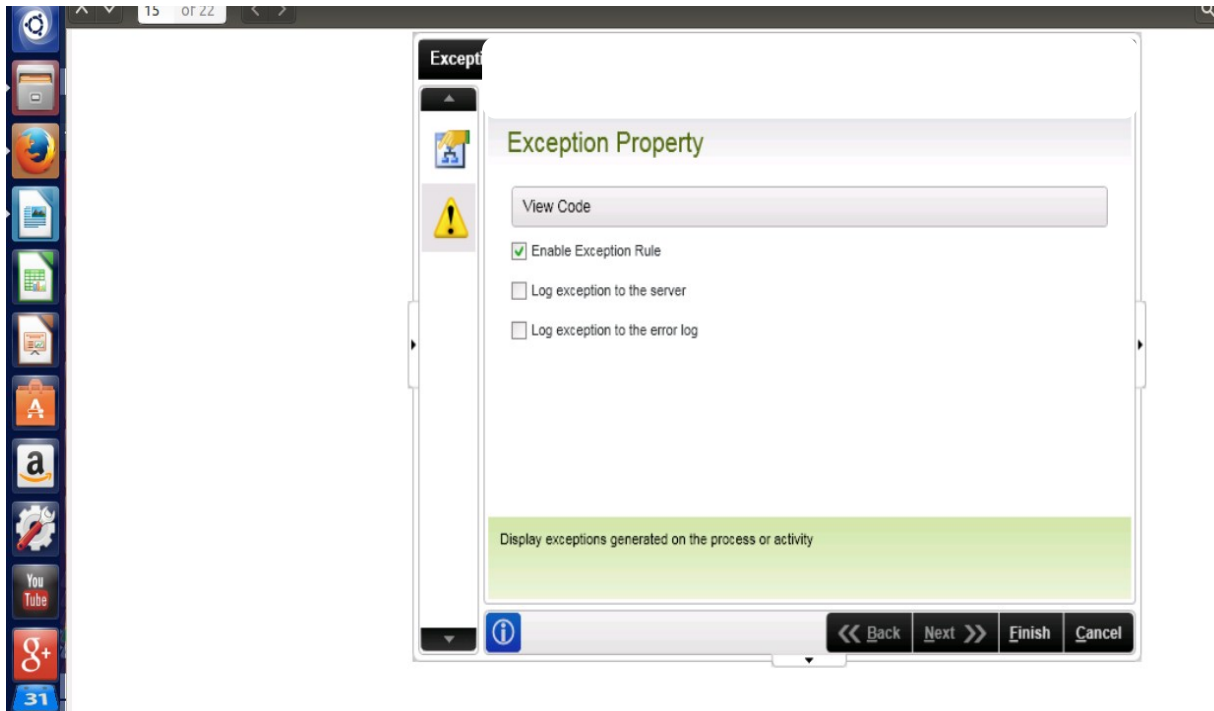
Default Data Source: Audit [Refresh Data Source List](#)

Parameters per line: 1

Properties:

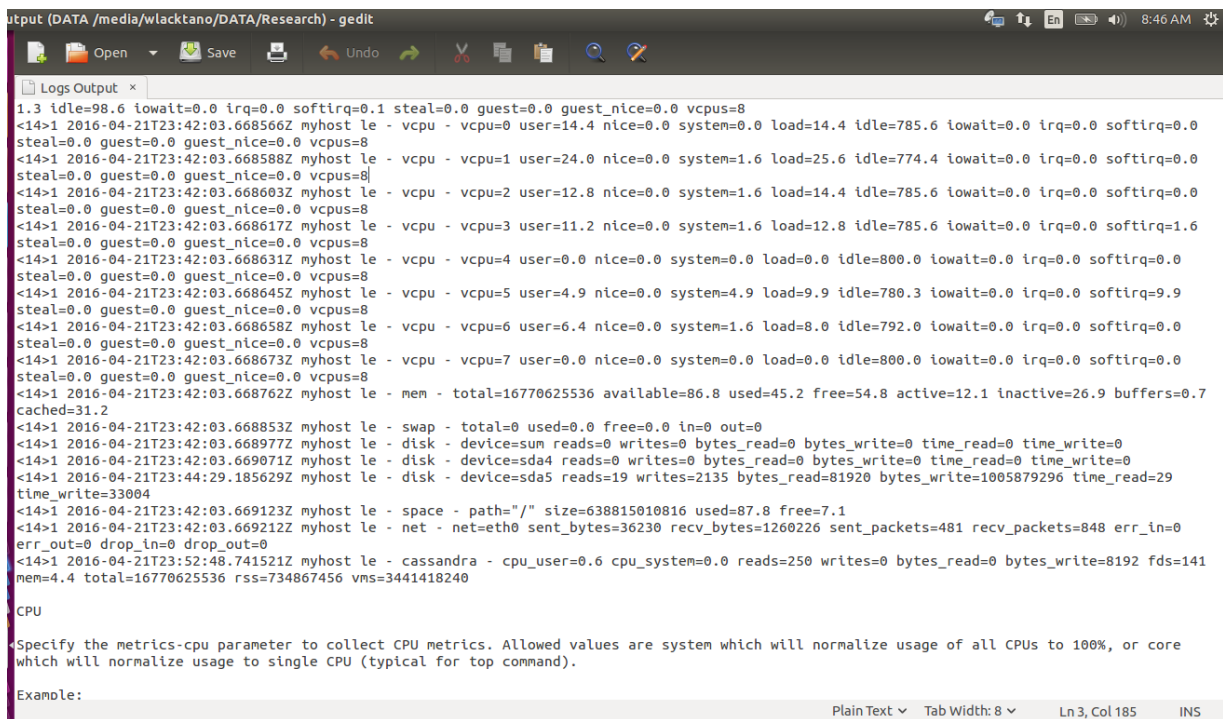
- Run report online
- Show Controls
- Open Links in New Window
- Auto Run
- Enable document cache
- Debug Mode

## 5.6 Report error





## 5.7 Output Sample



```
Output (DATA /media/wlactano/DATA/Research) - gedit
Logs Output x
1.3 idle=98.6 iowait=0.0 irq=0.0 softirq=0.1 steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668566Z myhost le - vcpu - vcpu=0 user=14.4 nice=0.0 system=0.0 load=14.4 idle=785.6 iowait=0.0 irq=0.0 softirq=0.0
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668588Z myhost le - vcpu - vcpu=1 user=24.0 nice=0.0 system=1.6 load=25.6 idle=774.4 iowait=0.0 irq=0.0 softirq=0.0
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668603Z myhost le - vcpu - vcpu=2 user=12.8 nice=0.0 system=1.6 load=14.4 idle=785.6 iowait=0.0 irq=0.0 softirq=0.0
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668617Z myhost le - vcpu - vcpu=3 user=11.2 nice=0.0 system=1.6 load=12.8 idle=785.6 iowait=0.0 irq=0.0 softirq=1.6
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668631Z myhost le - vcpu - vcpu=4 user=0.0 nice=0.0 system=0.0 load=0.0 idle=800.0 iowait=0.0 irq=0.0 softirq=0.0
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668645Z myhost le - vcpu - vcpu=5 user=4.9 nice=0.0 system=4.9 load=9.9 idle=780.3 iowait=0.0 irq=0.0 softirq=9.9
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668658Z myhost le - vcpu - vcpu=6 user=6.4 nice=0.0 system=1.6 load=8.0 idle=792.0 iowait=0.0 irq=0.0 softirq=0.0
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668673Z myhost le - vcpu - vcpu=7 user=0.0 nice=0.0 system=0.0 load=0.0 idle=800.0 iowait=0.0 irq=0.0 softirq=0.0
steal=0.0 guest=0.0 guest_nice=0.0 vcpus=8
<14>1 2016-04-21T23:42:03.668762Z myhost le - mem - total=16770625536 available=86.8 used=45.2 free=54.8 active=12.1 inactive=26.9 buffers=0.7
cached=31.2
<14>1 2016-04-21T23:42:03.668853Z myhost le - swap - total=0 used=0.0 free=0.0 in=0 out=0
<14>1 2016-04-21T23:42:03.668977Z myhost le - disk - device=sum reads=0 writes=0 bytes_read=0 bytes_write=0 time_read=0 time_write=0
<14>1 2016-04-21T23:42:03.669071Z myhost le - disk - device=sda4 reads=0 writes=0 bytes_read=0 bytes_write=0 time_read=0 time_write=0
<14>1 2016-04-21T23:44:29.185629Z myhost le - disk - device=sda5 reads=19 writes=2135 bytes_read=81920 bytes_write=1005879296 time_read=29
time_write=33004
<14>1 2016-04-21T23:42:03.669123Z myhost le - space - path="/" size=638815010816 used=87.8 free=7.1
<14>1 2016-04-21T23:42:03.669212Z myhost le - net - net=eth0 sent_bytes=36230 rcv_bytes=1260226 sent_packets=481 rcv_packets=848 err_in=0
err_out=0 drop_in=0 drop_out=0
<14>1 2016-04-21T23:52:48.741521Z myhost le - cassandra - cpu_user=0.6 cpu_system=0.0 reads=250 writes=0 bytes_read=0 bytes_write=8192 fds=141
mem=4.4 total=16770625536 rss=734867456 vms=3441418240

CPU

Specify the metrics-cpu parameter to collect CPU metrics. Allowed values are system which will normalize usage of all CPUs to 100%, or core
which will normalize usage to single CPU (typical for top command).

Example:
```

## Log set output

## 5.8 Log fields interpretation

For log field interpretation, the following fields will be used to determine which system metrics are gathered by the agent:

- **Metrics-cpu** Collects CPU metrics. Values allowed are system which will normalize usage 100% of system usage, or core normalization usage to single CPU.
- **Metrics-vcpu** Collects metrics for each individual log. The only allowed value is core, which will normalize log usage to a single CPU.
- **metrics-swap** Collects swap area metrics of the different applications running. The only allowed value is system
- **metrics-net** Collects metrics for specified target interfaces and server. Allowed values are interface IDs (e.g. eth0, kernel, devices etc). Special interfaces are:
  - all which instructs the agent to follow all interfaces (including lo)
  - select which will follow selected interfaces such as eth0 and wlan
  - sum which aggregates usages of all interfaces in the system
- **metrics-disk** Collects disk IO metrics. Allowed values are device IDs (e.g. sda4) and all, which instructs the agent to collect metrics for all devices.
- **metrics-space** Collects disk space metrics. Allowed values are device IDs (e.g. sda4)
- **metrics-process** Collects metrics for a specific process. This parameter should be specified in a separate section as shown below:

# Logs Audit real time Results

The screenshot displays the Logentries interface for a real-time log audit. The browser address bar shows the URL: `https://logentries.com/app/210cd517#/log/85aa8764/?last=Last 20 Mins&log_q=`. The interface includes a sidebar on the left with navigation options: Log Sets (+ Add New), All, None, Tags & Alerts, Create Tag, Create Anomaly Alert, and Create Inactivity Alert. A 'HAVE UI FEEDBACK?' button is located at the bottom of the sidebar.

The main content area is titled '/ Log Sets / DemoSet / Usage\_trail' and features tabs for Entries, Tags & Alerts, Settings, and Graphs. The 'Entries' tab is active, showing a search bar and a 'Last 20 Mins' filter. A bar chart above the log stream shows activity peaks, with a tooltip for 'Thursday, Apr 21, 09:20:25' indicating an 'Absolute count 3' and a 'Rate (s): 0.6'. Below the chart are controls for 'Live Tail', 'Table View', and 'Options'.

The log stream displays 11 entries, all from '21 Apr 2016 09:20:xx' with IP '41.139.249.186' and user 'w.lactano@gmail.com'. The log entries are as follows:

- » 21 Apr 2016 09:17:32.707 41.139.249.186 q6dtmceo INFO User='w.lactano@gmail.com' Account=210cd517 msg='Calling callback function' log\_
- » 21 Apr 2016 09:20:11.843 41.139.249.186 q6dtmceo INFO User='w.lactano@gmail.com' Account=210cd517 clicked=click\_btn\_Finished id='.btn-
- » 21 Apr 2016 09:20:24.042 41.139.249.186 q6dtmceo INFO User='w.lactano@gmail.com' Account=210cd517 clicked='account-tab' tab-title='Log
- » 21 Apr 2016 09:20:25.640 41.139.249.186 q6dtmceo INFO User='w.lactano@gmail.com' Account=210cd517 clicked=SideBarHost id='menu-itemtyp
- » 21 Apr 2016 09:20:28.439 41.139.249.186 q6dtmceo INFO User='w.lactano@gmail.com' Account=210cd517 msg='User switches mode in saved sea
- » 21 Apr 2016 09:20:29.895 41.139.249.186 q6dtmceo INFO User='w.lactano@gmail.com' Account=210cd517 clicked=SideBarHost id='menu-itemtyp
- » 21 Apr 2016 09:20:32.657 41.139.249.186 q6dtmceo INFO User='w.lactano@gmail.com' Account=210cd517 msg='User switches mode in saved sea
- » 21 Apr 2016 09:20:34.832 41.139.249.186 q6dtmceo ERROR error='Script error.' line=0 location='https://d2rqpywgsppga97.cloudfront.net/sta
- » 21 Apr 2016 09:20:35.047 41.139.249.186 q6dtmceo ERROR error='Script error.' line=0 location='https://d2rqpywgsppga97.cloudfront.net/sta
- » 21 Apr 2016 09:20:35.489 41.139.249.186 q6dtmceo ERROR error='Script error.' line=0 location='https://d2rqpywgsppga97.cloudfront.net/sta
- » 21 Apr 2016 09:20:41.588 41.139.249.186 q6dtmceo ERROR error='Script error.' line=0 location='https://d2rqpywgsppga97.cloudfront.net/sta

## 6.0 CHAPTER SIX

### 6.1 CONCLUSION AND FURTHER WORK

The report proposed a cloud forensic log audit trail framework to investigation, locate, identify and preserve evidence data on which a judgment or conclusion can be based and are admissible, authentic, complete, reliable and believable.

The current cloud computing trends has pushed the frontiers of cloud computing forensics to a high level thus there is need to leverage the data access and control through client based systems with the integrated cloud technological, organizational and legal challenges of which a number of these challenges, such as data replication, location transparency and multi-tenancy, are unique to cloud forensics and client-el needs hence ,There are unique opportunities that can significantly advance the efficacy and speed of forensic investigations with the advanced right tools and expertise to the standards of facts collection brought by cloud forensics.

The concept of security as a service has been emerging in cloud computing tremendously with new data storage and security needs. This research project paper demonstrated the advantages of user ownership of logs for audit thus they are able to be in control of all activities going on withing their server private cloud .

Security/service providers and vendors are continuously changing their delivery methods to include cloud services, and some companies are providing security as a cloud service. Likewise, forensics as a cloud service could leverage the massive computing power of the cloud to support cyber crime investigations at all levels.

The main conclusions drawn from the report are:

- Despite considerable efforts from the international organizations and market actors (e.g. CSP's) the level of adoption of logs audit trail framework is still low. Some have already defined a Cloud strategy, some others show a tactical or opportunistic adoption of Cloud forensics logs audit trail, but very few have defined and implemented an organizational Cloud strategy framework to be able tract activities within their private network. This framework will be one more reason to support the systematic adoption of Cloud security strategies and actual deployment.

- From the consideration of change-management practice in cloud, all the use cases portend mechanisms for the continuous improvement of the implemented logs audit trail frameworks (policies, mechanisms and deployment).
- The logs audit trail framework proposed in this report (a) encompasses the analyzed captured logs on the logs controller from Clouds server, and (b) is projected to be flexible for extension and adaptation to new users needs and requirements from others. This will be demonstrated by its empirical validation through the three simulated servers. This framework is also meant to be used during the design phase of new Cloud users, as it contains guidance related to different logs features/best-practices that should be taken into account by practitioners and Cloud security architects. On the other hand, the framework can be used by existing private Cloud users as a baseline for analyzing side-by-side different logs audit from their virtual environment.

## **6.2 FURTHER WORK**

In summary, the framework for logs audit trail should become part of the cloud administrations' toolbox when planning migration to the Cloud, and when assessing the effectiveness of the deployed security controls and procedures. Based on this cloud forensics needs further research to be done to enhance how clients (Customers) can control their data flow and in a secured way.

Also further research should be done to enhance the framework so that logs based on device connection,time,type and location can be captured on real time from the various platforms in different virtual environment. This should include all the various models of cloud environment and what forensic investigation tools and cloud provider staff training are in place for logging and preserving evidence of an alleged violation

.

## References

1. C. Furlani, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud," National Institute of Standards and Technologies (NIST), US, 2010
2. K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics: An overview," in Proc. of the 7th IFIP International Conference on Digital Forensics, 2011.
3. J. Dykstra and A. T. Sherman, "Understanding issues in cloud computing: Two hypothetical case studies," Digital Investigation, vol. 3, no. 1, pp. Pages: 19-31, 2011
4. Amazon, AWS Security Center, Seattle, Washington (aws.amazon.com/security).
5. V. Roussev, L. Wang, G. Richard and L. Marziale, A cloud computing platform for large-scale forensic computing, in Advances in Digital Forensics V, G. Peterson and S. Sheno (Eds.), Springer, Heidelberg, Germany, pp. 201–214, 2009.
6. N. Beebe, Digital forensic research: The good, the bad and the unaddressed, in Advances in Digital Forensics V, G. Peterson and S. Sheno (Eds.), Springer, Heidelberg, Germany, pp. 17–36, 2009.
7. J. Oberheide, E. Cooke and F. Jahanian, CloudAV: N-version antivirus in the network cloud, Proceedings of the Seventeenth USENIX Security Conference, pp. 91–106, 2008.
8. <http://www.sciencedirect.com/science/article>
9. Amazon, AWS Security Center, Seattle, Washington (aws.amazon.com/security)
10. T. Parker, E. Shaw, et al. (2004). Cyber Adversary Characterization Auditing the HackerMind. Rockland, Syngress Publishing Inc.
11. Linux/UNIX Audit Logs, <http://raffy.ch/blog/2006/07/24/linux-unix-audit-logs>
12. F. Gens, IT cloud services forecast– 2008 to 2012: A key driver of new growth (blogs.idc.com/ie/?p=224), October 8, 2008.
13. K.-K. Muniswamy-Reddy and M. Seltzer. Provenance asrst class cloud data. SIGOPS Oper. Syst. Rev., 43(4):11{16, 2010
14. Ruan K. (2013) 'Cybercrime and Cloud Forensics: Applications for Investigation Processes'

(pp.1-348), IGI Global, December 2012, doi:10.4018/978-1-4666-2662-1 (Edited Book)

15. Ruan K., Carthy, J. (2013) 'Cloud Forensics Definitions and Critical Criteria for Cloud Forensic Capability: an Overview of Survey Results', *Digital Investigation*, Elsevier, pp34-43
16. NIST Special Publication 500-299 (2013) Cloud Computing Security Reference Architecture, NIST Cloud Computing Security Working Group, NIST Cloud Computing Program, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, May 2013 (public review)
17. Zargari, S., Benford, D.(2012) Cloud Forensics: Concepts, Issues, and Challenges. In Proceedings of the 3rd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), Bucharest, September 19-21, pp. 236-243.
18. S. D. Wolthusen, "Overcast: forensic discovery in cloud environments," in Proceedings of the 5th International Conference on IT Security Incident Management and IT Forensics (IMF '09), pp. 3–9, IEEE, September 2009.
19. M. Taylor, J. Haggerty, D. Gresty, and R. Hegarty, "Digital evidence in cloud computing systems," *Computer Law & Security Review*, vol. 26, no. 3, pp. 304–308, 2010.
20. A. C. Kim, W. H. Park, and D. H. Lee, "A study on the live forensic techniques for anomaly detection in user terminals," *International Journal of Security and Its Applications*, vol. 7, no. 1, pp. 181–188, 2013.