UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

A PERSISTENT CLOUD FORENSICS MODEL FOR RELIABLE DIGITAL FORENSICS BY INVESTIGATIVE AGENCIES IN KENYA

JOHN DECHE MWATSUMA

P53/34055/2019

Supervisor

Dr. Andrew Mwaura Kahonge

A Research Project Report Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Distributed Computing Technology, School of Computing and Informatics, University of Nairobi.

August, 2021

DECLARATION

This research project is my original work and has not been submitted for examination in any other university.

Signature:... .... Date:.............24-08-2021.............

John D. Mwatsuma

P53/34055/2019

This research project has been submitted in partial fulfillment of the requirements for the award of Master of Science in Distributed Computing Technology of the School of Computing and Informatics of the University of Nairobi, with my approval as the University supervisor.

Signature:.... .... Date:......24-Aug-2021..................

Dr. Andrew M. Kahonge

DEDICATION

To my wife, Kayaja and son, Mwatsuma for persevering my absence and lonely hours as I was engrossed in this project. I am so incredibly grateful.

ACKNOWLEDGEMENT

First and foremost, I wish to express a deep sense of gratitude to God the Almighty, for the blessing of progressing this far.

Secondly, to my supervisor Dr. Andrew Mwaura Kahonge for your guidance, instruction and the much-needed advice throughout the project, I will forever be grateful.

To my colleagues, Keter, Ouma and Robert. Thank you for your honest feedback, critique and words of encouragement. Your ideas meaningfully contributed to this accomplishment.

ABSTRACT

The rapid growth of cloud computing and the ever increasing demand for computing resources is gradually driving the migration from the traditional on-premise ICT infrastructure to the Cloud Computing Space. As the trend continues, adoption of cloud solutions by public sector institutions will continue to gain traction as well. It is therefore paramount that mechanisms are put in place to ensure safety and security of both enterprise Systems and data that significantly falls under the control of cloud service providers and could easily be exposed to the risks of cyber crime and Fraud.

Traditional digital forensics techniques are often challenged by the nature and environments presented by cloud architectures where, infrastructure is largely distributed, computing resources are shared among subscribers especially in multi-tenancy arrangements and location of provisioning systems is often unreachable.

This study focuses on the Infrastructure as a Service model and identifies the required needs of overcoming the challenges mentioned. Further, the study proposes the persistent cloud forensics framework to aid in the carrying out of digital forensics for public sector institutions where involvement of cloud service providers is avoided in carrying out cloud forensics.

This study advances a framework where cloud resources can autonomously transmit evidentiary logs of system and user transactions that are securely stored in a remote repository and are made available to investigative agencies mandated to prosecute crimes perpetrated through the cloud resources. The proposed framework provides a form of autonomous log aggregation that is devoid of any intervention from service providers and cloud users, while providing a solution on investigative issues such as collusion, chain of custody, privacy where cloud infrastructure is shared, conflicting laws where hardware and systems provisioning cloud services are distributed and the admissibility of acquired evidence.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

API	Application Programming Interface
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
EC2	Elastic Cloud 2
IaaS	Infrastructure as a Service
I.T	Information Technology
LAMP	Linux Apache MySQL and Php
OCF	Open Cloud Format
PaaS	Platform as a Service
PC	Personal Computing
QoS	Quality of Service
RSYSLOG	Rocket Fast System for Log Processing
SecLaaS	Secure Logging as a Service
SaaS	Software as a Service
VM	Virtual Machine
NC	Node Controller
NIST	National Institute for Standards and Technology

LIST OF FIGURES

LIST OF TABLES

1.1 CHAPTER ONE: INTRODUCTION

1.2 BACKGROUND

Cloud computing according to (Bhatia & Saggi, 2015) can be described as a variety of services accessed over the internet by an assortment of systems. Such systems comprise of an array of low-cost Servers, Storage hardware, Personal Computers (PCs), among other computing resources that are organized to provision on-demand computing services according to particular models or strategies, while offering computing services to clients.

The widely accepted description of the cloud by United States Nation Institute for Standards and Technology (NIST) advances the view of cloud computing as a model for providing wide-scale on-demand access to computing resources that are shareable, in an unattended manner or with minimal supervision (Mell & Grance 2011).

According to (Zwattendorfer & Tauber, 2013), despite the existing complex government procedures and reluctance to innovate, public administrations had began to embrace the use of the cloud or had shown the willingness to subscribe to the services. While explaining the benefits that governments stand to gain, the authors opine that, the public sector would benefit immensely in cost savings through the efficiency of enhanced systems.

The authors affirmed that, governments can reduce capital expenditure spending occasioned by on-premise installations such as physical servers

The authors affirmed that, governments can reduce capital expenditure spending on I.T equipment, by migrating to cloud-based solutions where, the public sector only pays for services on demand. The cloud therefore, has the potential to enhance the implementation of e-governance, which can lead to cost effective service delivery (Microsoft, 2017).

As the adoption of Cloud computing solutions advances, (Zawoad et al., 2015) argued that, there have been reported cases of malicious users have leveraged on the immense computing power proved by cloud platforms to engage in cyber crime. The authors explained for instance that, attackers could initiate Distributed Denial of Service attacks (DDoS) by installing Trojans in Virtual Machines (VMs) provided on Amazon’s cloud platform.

The allure of cloud computing benefits notwithstanding, (Wall, 2017) opined that, the cloud and associated technologies had created an environment that led to an upsurge of cyber crime and that cyber criminals with the ability to exploit the traditional I.T environments were also gaining a foothold and engaging in wide-scale crime on the cloud environments as well, where it is challenging to carryout investigative, preventive and prosecutorial processes.

As the demand for Cloud computing solutions continue, adoption of cloud services by public sector institutions currently relying on on-premise infrastructure will become inevitable. This therefore necessitates the provision of a framework for reliable digital forensics in cloud environments, to aid government investigative agencies in carrying out investigations where cyber-crimes among other incidents are committed on cloud environments.

1.3 THE RESEARCH PROBLEM

According to Marinescu, 2017) a cloud model consists of distinct attributes namely; on-demand self-service, broadband network access, measured or metered services, resource pools and rapid elasticity. The author also explains that database as service is the recent addition to the widely known three service delivery models; platform as a service (PaaS), software as a service (SaaS) and infrastructure as a service (IaaS). The widely accepted deployment models are; the private, community and hybrid clouds. The author further explains that, the advent of the cloud and related services has brought about fundamental change in the management of I.T infrastructure such that, users cede significant control of systems and underlying data to service providers.

In their perspective of the role of cloud service providers while carrying out computer forensics, (Zawoad et al., and 2015) argued that, the traditional set up of I.T infrastructure accorded investigators total control of evidentiary data reposed in routers, event logs and storage hardware while there was less access on evidentiary data on cloud platforms. This consequently leads to the dependency of service providers who may not be truthful, in carrying out reliable digital forensics on the cloud.

As (Simou et al., 2014) explain, acquiring evidence from cloud environments is challenging due to the complexities of associated services, deployment models and the restrictions of seizing physical devices with evidentiary data. This, according to the authors requires that more effective methods and tools are employed to carryout cloud forensics.

The provision of on-demand services by cloud providers does not allow for the support of storing terminated virtual resources such as virtual machines persistently (Zawoad et al., 2015). The data stored in terminated cloud resources therefore, becomes unavailable upon termination making it impossible for investigators to carryout digital forensics to acquire reliable evidence whenever cyber crimes committed are aided by the terminated resources.

In their research on ‘An Open Cloud Forensics Architecture’ the authors argued that, issues of physical location of cloud-services provisioning hardware and privacy where such hardware is used in multi-tenant clouds prevents investigators from seizing of the physical hardware for evidence extraction, due to the potential to violate privacy laws. Further, such evidence would not pass the reliability test since its integrity would be questioned. The authors also caution that cloud service providers could also be compromised into colluding with both the perpetrators and forensic investigators to cover-up cyber crimes.

Activity logs can clearly reveal the actions taken by users as they interact with enterprise systems both on the cloud and on on-premise installations hence, they can be relied upon in prosecuting legal suits. Acquiring the said logs however, is significantly dependent on cloud service providers who control the infrastructure while users and forensics investigators have little or no control. Additionally, acquiring logs from terminated cloud resources in practically impossible.

In view of the concerns aforementioned, the prevailing challenges of carrying out cloud forensics and the inevitable adoption of cloud solutions by public sector institutions to accommodate growing demands for computing resources, there is a need to provide a reliable framework for digital forensics support in cloud infrastructures to aid investigative agencies in Kenya.

1.4 OBJECTIVES OF THE STUDY

1.3.1 OVERALL OBJECTIVE

Provide a framework for acquiring admissible digital forensics evidence from cloud platforms on the Infrastructure as a Service model, to aid in the performance of reliable digital forensics by mandated investigative agencies in Kenya.

1.3.2 SPECIFIC OBJECTIVES

i. Provide a framework for retaining digital forensics evidence by adversaries after virtual computing resources are terminated on cloud platforms.

ii. Provide a framework for acquiring digital forensics evidence from Enterprise Systems hosted on multi-tenant cloud platforms.

iii. Develop a prototype to validate the proposed framework

1.3.3 THE RESEARCH QUESTIONS

The proposed research seeks to answer the following questions?

i) What solutions can be used to acquire evidence for digital forensics from terminated virtual machines on cloud computing platforms?

ii) What mechanisms can be used to acquire digital evidence from virtual computing resources on cloud computing platforms through a persistent digital forensics process?

iii) What solutions can be implemented to ensure verifiable digital evidence from cloud computing platforms is acquired without direct intervention by Cloud Service Providers (CSPs)?

2.1 CHAPTER TWO: LITERATURE REVIEW

2.2 INTRODUCTION

The dawn of Cloud Computing has led to new ways of meeting users' computing demands by providing unlimited and convenient on-demand computing resource and cost-effective solutions. It was predicted that, the cloud computing global market would cross $1 Trillion by 2025, according to research by (Market Research Media, 2021). While the benefits of cloud computing are plentiful, (Balduzzi et al., 2012) cautioned that, both users and service providers of public cloud resources are susceptible to security risks such as; hacking, malware attacks and loss of valuable data. Additionally, investigators in the field of computer forensics face challenges related to the loss of control caused by the nature of cloud environments and vendors (Birk et al 2011).

According to (Zawoad et al., 2015), investigating attacks and incidents on cloud platforms requires that investigators should perform elaborate procedures of digital forensics to establish all facts about the occurrence of reported incidents unfortunately, traditional methods of digital forensics cannot be applied on cloud platforms.

2.3 THE CLOUD ARCHITECTURE

In their research while carrying out a survey on cloud computing security, (Ramachandra et al., 2017) highlight on the need to understand the architecture and the definition of the cloud while analyzing security issues on cloud environments. Understanding the two (cloud definition and architecture) is equally important inorder to appreciate the challenges of carrying out forensics investigations on cloud platforms (cloud forensics) and the validity of the proposed framework in this research.

According to the NIST Cloud Computing Reference Model illustrated below as explained by (Liu et al., 2011), cloud computing is influenced by 5 actors or are in turn impacted by it together with its security connotations.

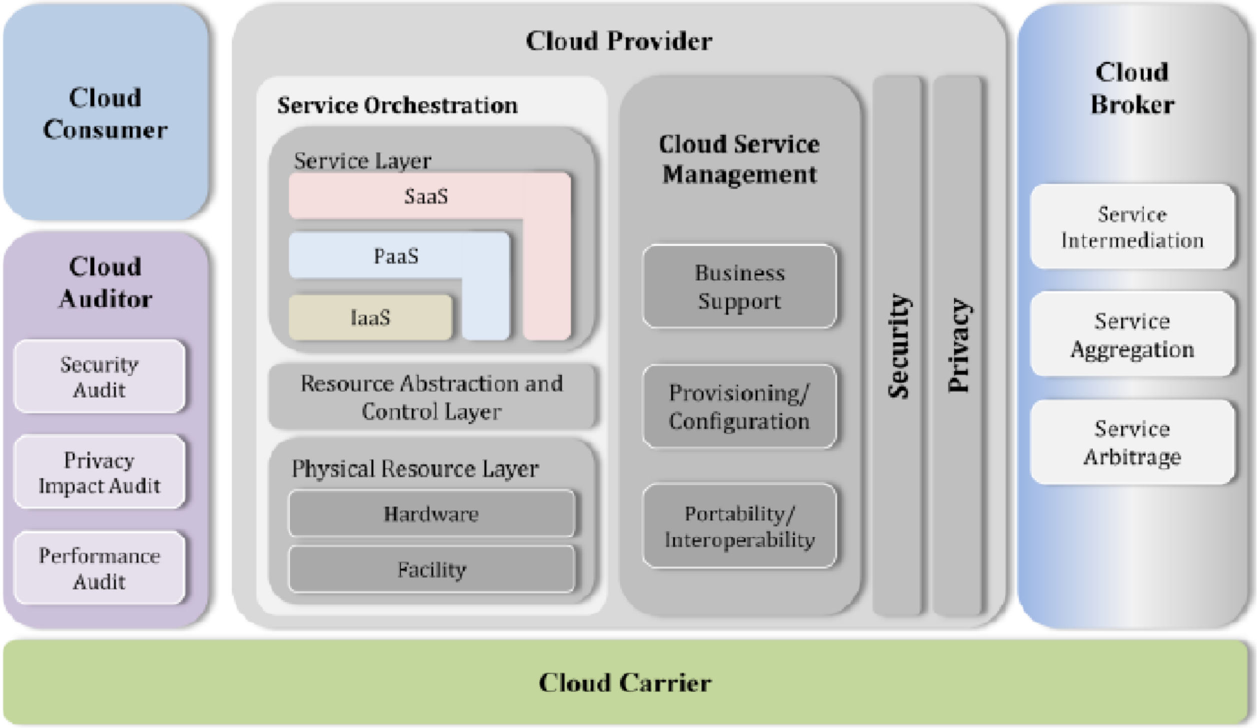


Figure 1: NIST Conceptual Reference Model for Cloud Computing

#	Actor	Description
1	Consumer	A cloud user may be an individual or organization who enters into a formal contract with cloud service provider.
2	Service Provider	An individual or organization that provides cloud services or solutions to meet users' needs.
3	Auditor	An entity that can carry out an un-biased evaluation of services provided through a cloud platform, its systems, performance and general safety and security of how the cloud set up is implemented.
4	Broker	A party responsible for managing usage, performance and provisioning of cloud services and manages the engagement between the cloud users and cloud service providers.
5	Carrier	An entity that is responsible for ensuring there is connectivity and transport of provisioned services from a *Cloud Service Provider* to *a Cloud User or Client*

Table 1: NIST Cloud Computing Reference Model, Actors

2.4 CLOUD COMPUTING SERVICE DEPLOYMENT

According to (Liu et al., 2011) the operation of a cloud infrastructure may comprise of one of four deployment models; private, public, community or hybrid cloud. The authors affirm that that the differences between the service deployment models mentioned is determined by the limitation in provisioning of computing resources to consumers. The table below explains further, the Cloud Computing Service Deployment Models as advanced by the NIST.

Deployment Model	Description
Public Cloud	An arrangement where the cloud platform and associated solutions are provisioned to consumers over a public network. Owners of Public clouds provide services for purchase and serve various pools of consumers.
Private Cloud	Provides clients with restricted or private access and usage of cloud resources. A private cloud may be owned and managed by the client's organization or a private entity.
Community Cloud	A Cloud platform that serves various consumers from many organizations which share specific commonalities. Cross-organizational access to resources among users is allowed in such an arrangement.
Hybrid Cloud	A combination of two or more clouds, which remain completely separate but are linked by proprietary or standard technologies to facilitate application or data portability.

Table 2: NIST Cloud Computing Service Deployment Models

2.5 CLOUD COMPUTING SERVICE ORCHESTRATION

According to (Bousselmi et al., 2014), Cloud computing is service-oriented and can be structured into three layers to form the widely known delivery models namely; Infrastructure as a Service (IaaS) which consists of material resources, Platform as a Service (PaaS) which consists of development and deployment resources and the Software as a Service layer (SaaS).

Service Orchestration as explained by (Liu et al., 2011) is essentially a assortment of system apparatus that support the activities and services of cloud providers based on their model of service provisioning as they avail services to their clients. Figure 2 below presents a stack diagram that depicts how cloud services are provisioned.

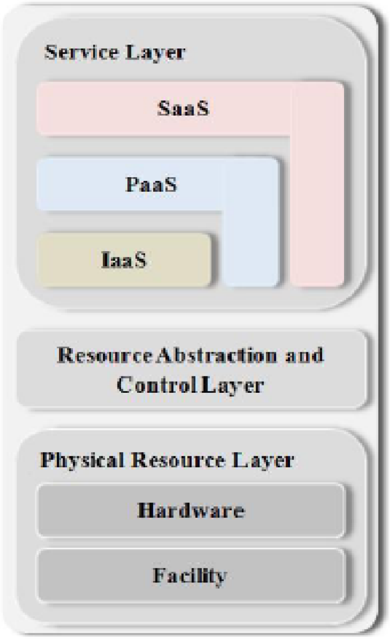


Figure 2: NIST Cloud Computing Service Deployment Models

2.6 REVIEW OF EXISTING CLOUD FORENSICS MODELS

2.6.1 SECURE LOGGING-AS-A-SERVICE MODEL

Logs in cloud infrastructures are essential in conducting investigations necessary to reveal illegal or fraudulent activities by adversaries to aid in prosecution, (Zawoad et al., 2016). While advancing their model on Secure Logging as a Service, the authors explained that, while cloud platforms were beneficial computing models, the computational power and storage resources occasioned by computer clouds can also motivate malicious users to carry out attacks through the said platforms.

In their proposition of the Secure Logging as a Service Scheme (SecLaaS) as a reliable solution for carrying out cloud forensics, the authors cite challenges such as; reduced level of controls where consumers of cloud services extensively rely on service providers to acquire logs from computer clouds. They argued that over dependence of Cloud Service Providers brings about the trust issues of their employees who are often not licensed investigators. They caution that, Cloud Service Providers could be compromised to tamper with the logs while leveraging on the controls they have over the generated logs and may not be obliged to provide all required logs in situations where such requests conflict with their internal policies on data protection. Essentially, the lack of logging standards, volatility of logs, and the multi-tenancy nature of cloud platforms, where virtualized resources can be provisioned from shared hardware where logs of various other may be co-located are among the challenges that the proposed framework sought to address.

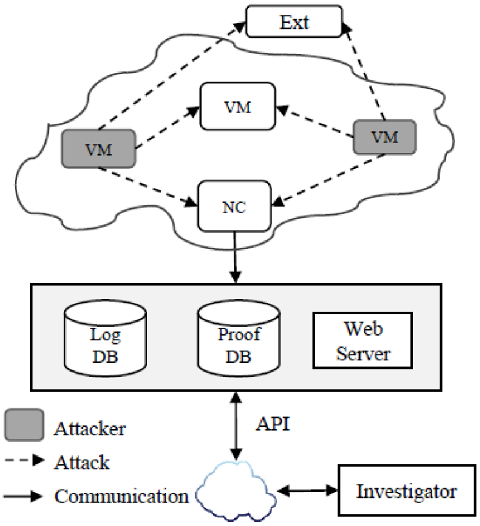


Figure 3: Conceptual Framework for SecLaaS

As illustrated in the conceptual framework in figure: 3 above, virtual machines in the cloud can be attacked by a malicious user or the user could carry out an attack on the Node Controller which is responsible for hosting the virtual machine instances and managing the virtual network endpoints in order to initiate some side channel attacks. Figure 3 depicts a scenario where logs can securely be stored and availed to forensic investigators in the event of such attacks.

2.6.2 A MULTI-TENANCY CLOUD TRUST MODEL WITH QOS MONITORING

The model proposed by (Mutulu, 2015) focuses on the Infrastructure as a Service (IaaS) platform. It explains the importance of ensuring that clients of cloud solutions have a means of ascertaining the cloud services providers' trust and quality of services offered before committing to sign up. The author further emphasized on the need to employ continuous quality of service monitoring in real-time through the proposed model. This he argues, aids in evaluating cloud providers and builds more trust with clients and ensures that clients sign up for cloud services that meet specific standards and metrics.

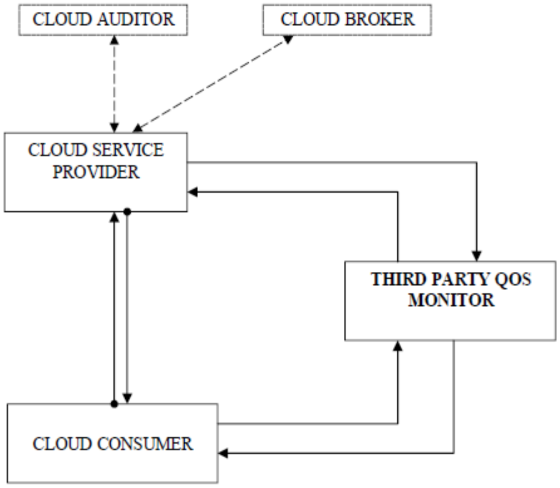


Figure 4: Illustration of proposed Multi Tenancy Model

2.6.3 The Persistent Storage Device for the Client's Data

This solution advocates for the implementation of a persistent storage resource for volatile customer data on cloud platforms (Damshenas et al 2012). The authors opined that, while the solution could be costly, its attendant benefits which range from; easy access to evidentiary data on cloud platforms, improved access to data and security among others, outweigh the cost implication. The authors add that for the success of such an arrangement depends significantly on a universal policy in the form of a service level agreement between service providers and clients.

2.6.4 Managing Volatile Data on Cloud Platforms

According to (Simou et al., 2016) live investigations and data acquisition could be used as an alternative approach to the traditional methods of acquiring digital forensics data from the cloud. Similarly, (Grispos et al.,) while emphasizing on the proposed method for live acquisition explained that, the live investigations and acquisition approach enables the acquiring of data that would otherwise be lost if virtual machines or computers were powered off however, they further affirmed that while the approach would increase the amount of information acquired, encryption mechanisms implemented by cloud service providers could prevent the effectiveness of such approaches.

2.6.5 FORENSICS ENABLED CLOUD ARCHITECTURE

The model proposed by (Zawoad et al., 2015) emphasized on the importance of preserving generated logs, provenance information, and proof of data possession along with timestamp data in a secure manner in order to support a trustworthy digital forensics process on cloud platforms. The authors opined that, cloud users, investigators and the court authority should all have access to acquired evidence.

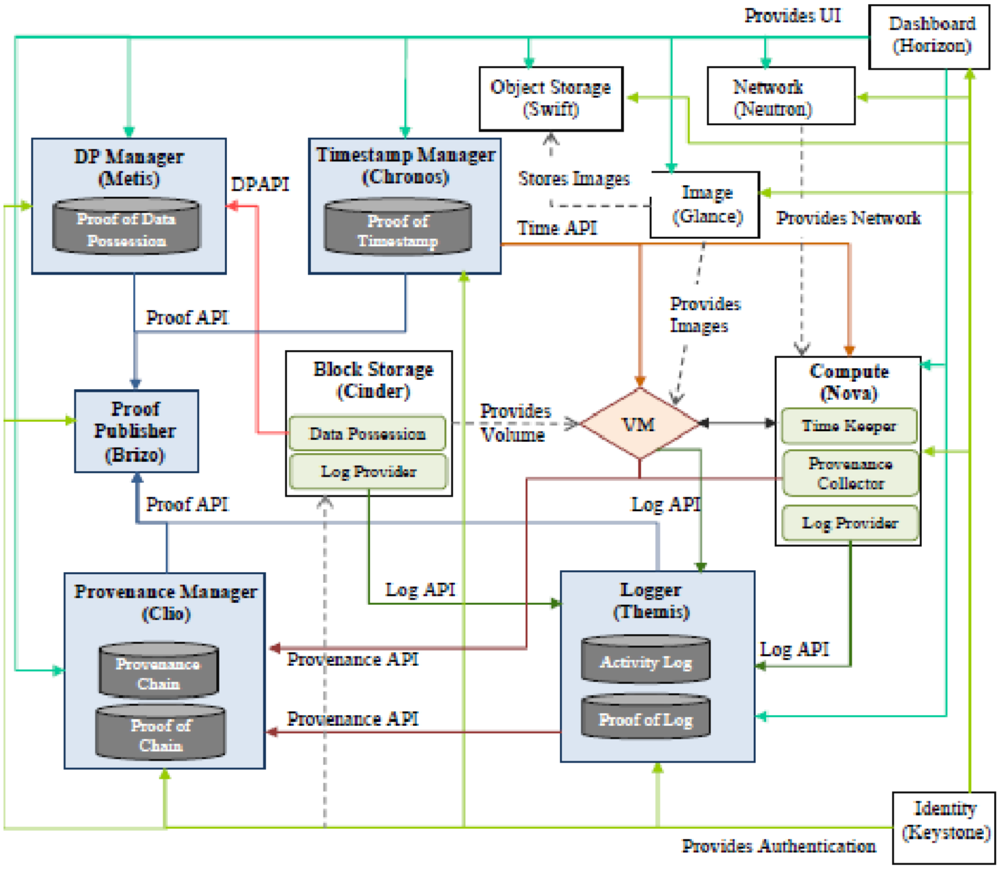


Figure 5: Conceptual Framework for the Forensics Enabled Cloud Architecture

2.6.6 OPEN CLOUD FORENSICS

In their proposal for the Open Cloud Forensics Model (Zawoad and Hasan, 2015) emphasized on the importance of the role of CSPs in carrying out forensics investigation on the cloud. Their model considered a role for CSPs as supporters of a reliable forensics investigative process. The authors affirmed that, a dependable digital forensics process should have CSPs as a central entity in executing a continuous process flow which provides and translates the Electronically Stored Information (ESI) to verifiable ESI so as to preserve its privacy and integrity. They essentially referred to this process as a continuous forensics process on a forensics-aware cloud computing system.

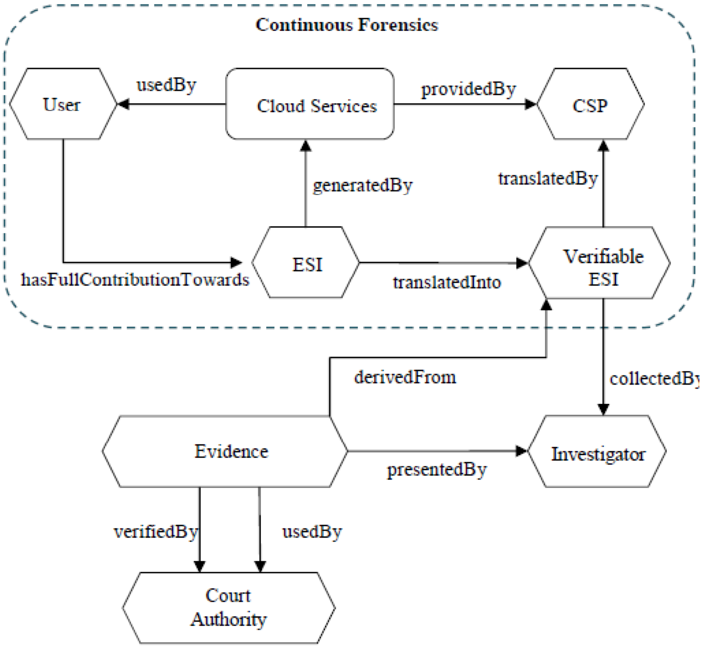


Figure 6: Figure 6: Open Cloud Forensics Model (OCF)

2.6.7 RESEARCH GAP

The Literature review provided a description of the Cloud Architecture, the Cloud Service Deployment Models as well as the Cloud Service Orchestration. The Cloud Computing Reference Model according to US National Institute of Standards was also discussed, conceptual frameworks on cloud forensics advanced by various researchers along with the attendant challenges of carrying out cloud forensics. The previous works recognize the critical importance of logs in digital forensics and have addressed some challenges of cloud forensics while proposing various remedies however, they do not provide a complete framework for; persistently acquiring of admissible evidence from cloud resources, preserving the evidence in an exclusive and secured repository through enabling legislation and availing it to both investigative agencies and judicial authorities in a verifiable manner. Further, the prevailing challenges of; data privacy, malicious cloud users and involvement of CSPs who may collude with investigators are not addressed in the previous models discussed.

2.7 CONCEPTUAL FRAMEWORK

2.6.1 THE PROPOSED MODEL

Public sector Institutions are bound to adopt cloud solutions, to take advantage of the ever increasing computational power, storage among other services provided by cloud platforms consequently, a solution to the prevailing challenges of carrying out digital forensics on the cloud platforms due to their black box nature and the increased attack surface provided by the various actors involved remains vital. The purpose of this framework is to demonstrate and communicate the processes and components required for acquiring admissible digital forensics evidence from cloud platforms through a persistent forensics process, storage of the acquired evidence in a secure repository and provision of the same in a verifiable manner to investigative agencies and Judicial authorities.

2.6.2 SCOPE

The framework focuses the Infrastructure as a Service cloud platform and associated solutions as the cloud service orchestration model of choice that could largely be adopted by public sector institutions.

2.6.3 THE CONCEPTUAL FRAMEWORK

The subject Public Sector Institution will subscribe to the cloud service and will be provided with cloud resources that may be virtual servers or VMs to support their enterprise systems while providing services as per the Institution's mandate. A logging utility will be configured for remote logging of specific application, event, service and system logs. Generated logs will be persistently stored in an exclusive repository hosted by a mandated Government Institution through enabling legislation.

Investigative agencies will have read-only access to the stored evidence during presentation of the evidence to judicial authorities, who will also have read only access of the stored logs to verify their validity. The read-only access of the repository ensures that data integrity of stored evidence is guaranteed and addresses issues of possible collusion between investigators, malicious users and CSPs in an attempt to corrupt the evidence and sabotage an ongoing investigation.

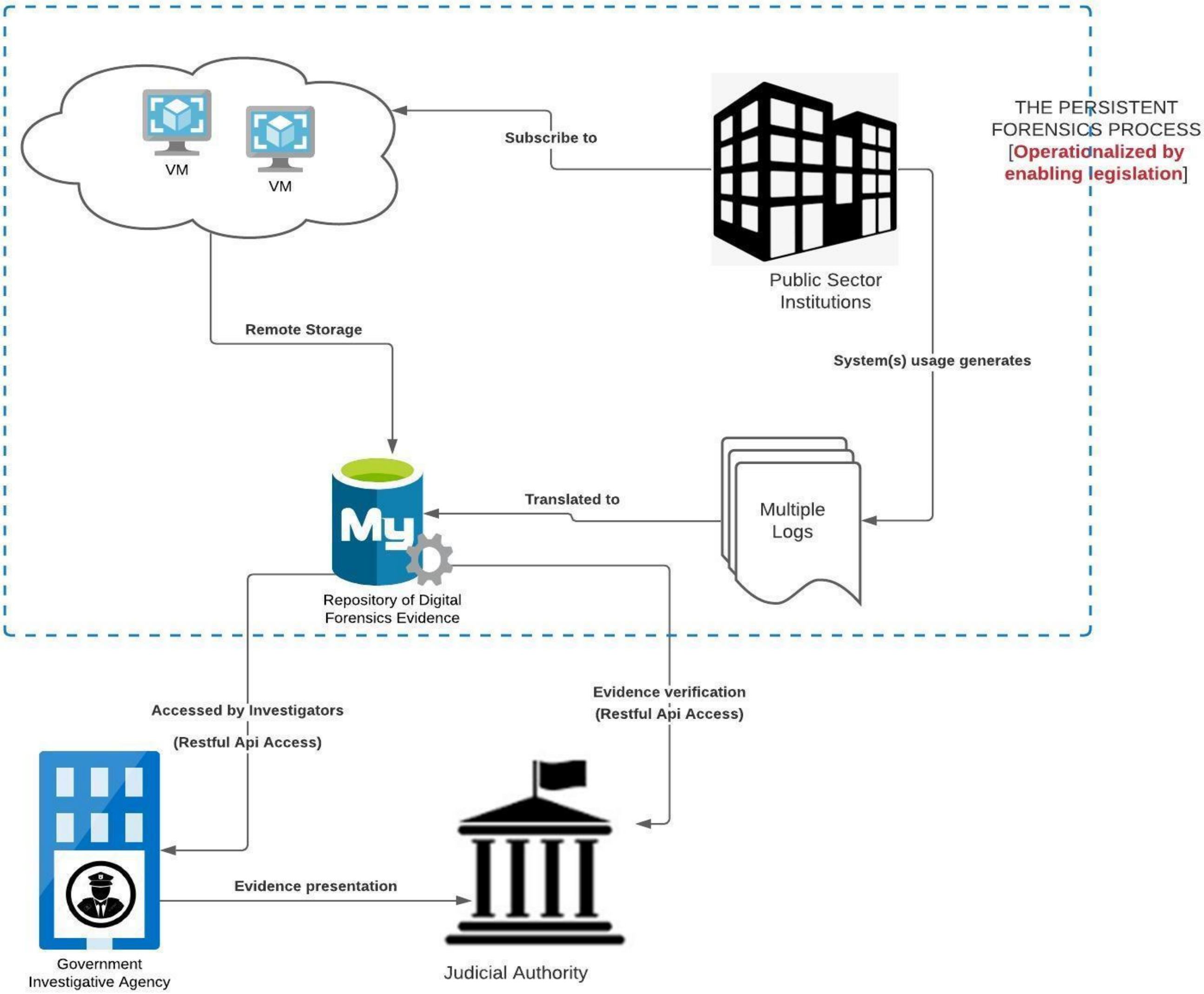

VM
VM
Subscribe to
Public Sector Institutions
THE PERSISTENT FORENSICS PROCESS [Operationalized by enabling legislation]
Remote Storage
System(s) usage generates
Translated to
Multiple Logs
Repository of Digital Forensics Evidence
Accessed by Investigators
(Restful Api Access)
Evidence verification
(Restful Api Access)
Evidence presentation
Government Investigative Agency
Judicial Authority

Figure 7: A persistent cloud forensics model

3.1 CHAPTER THREE: METHODOLOGY

3.2 RESEARCH DESIGN

The research was based on an exploratory research design. Existing literature on cloud forensics frameworks was reviewed to determine whether models similar to the proposed work have been implemented. The aim was also to determine the existence of cloud forensics models, which provide persistent storage of digital forensic evidence from cloud platforms and ensure evidence acquired is admissible and verifiable. The exploratory model suits this research because, while existing models have been advanced and logging solutions exist, there are various unknown requirements for the successful implementation of the proposed solution along with necessary legislative support.

3.3 DATA COLLECTION

The data collection approach used in this research was qualitative. The qualitative data collection involved focus group discussions where participants comprised of digital forensics analysts, investigators and a legal practitioner. The discussions focused on getting an insight from the participants on; the digital forensics processes in the context of multi-tenant cloud platforms and the traditional on-premise environments, how existing legislation supports digital forensics investigations, the admissibility and reliability of digital forensics evidence in legal suits.

3.4 SAMPLING

The focus group comprised of 2 investigators, 2 digital forensics analysts and a legal practitioner from the Ethics and Anti-Corruption Commission. Logged records generated from configured virtual machines on the Amazon cloud computing platform were also used.

3.5 SYSTEM DEVELOPMENT

The Rapid Application Development concept (RAD) was used to develop the prototype using the Laravel, an open source Php framework and Vue.js, a front-end JavaScript framework. The RAD model was chosen because it is iterative and different stages of the prototype application development can be reviewed when needed. Development of applications with RAD is also reasonably fast compared to the traditional Software Development Life Cycle due to the wide availability development tools and techniques. It is not essential to know all the requirements of the project beforehand in Rapid Application Development, new requirements can be added and changed as development is ongoing, until an acceptable outcome is achieved from which the final product or system will be developed.

3.6 DATA ANALYSIS

Qualitative data collected from the focus group discussion hence qualitative content analysis was used for analysis. As opined by (Margrit, 2013), qualitative content analysis is essential in interpreting material that requires some degree of interpretation. The method was therefore used to identify common themes and patterns from the responses of practitioners, on the digital forensics processes in the context of cloud platforms and the required support by existing legislation in conducting digital forensics on cloud environments. A summary of the common themes identified on the analysis conducted is provided in the table below.

Code	Description
Digital forensics processes in use by investigative agencies.	Traditional seizure of hardware and evidence extraction techniques for on-premise installations. There are no known solutions for carrying out cloud forensics
Reliability of evidence extracted through traditional digital forensics techniques in litigation.	Case dependent. Prosecutors guide the process of determining the significance and usage of expert evidence provided. Evidence Authenticity and Reliability issues always abound.
Concern on the relevance of existing legislation and usage of digital forensics evidence in litigation.	More legislative support from the Computer Misuse and Cyber crimes act 2018 The Law recognizes Critical Information Infrastructure, and the need to protect such systems countrywide. Amendments will be required to accommodate the framework advanced by this study
The need for relevant cloud forensics laws to aid in acquiring of evidence and support legal suits.	A well thought out legislation is required to address the unique requirements of carrying out cloud forensics. Such laws will bind or hold all stakeholders to account.

Table 3:Content analysis from focused group data

3.7 CONCEPTUAL DESIGN

The conceptual framework as illustrated on section 2.6.3 depicts a system where, public institutions will subscribe to cloud services provisioned through the Infrastructure as a Service (IaaS) clouds which are multi-tenant. The resources provided through the cloud platform(s) will be virtual computing resources that can be configured to log both system events and user transactions.

Through enabling legislation, the logged data will be reposed on a secured database and will be utilized as digital forensics evidence by investigative agencies, which will have read-only access to the stored data. The conceptual design below illustrates the processes and interactions between entities involved in the envisioned model.

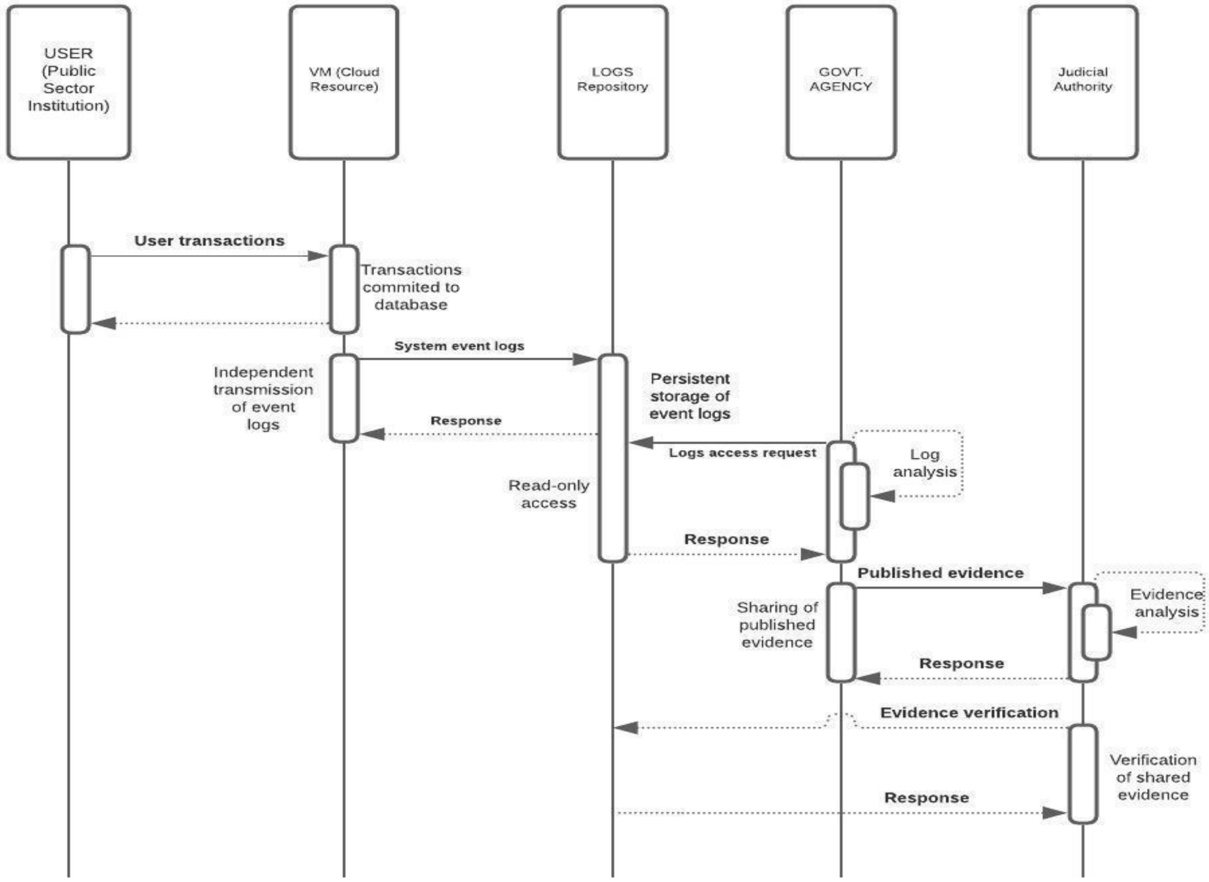


Figure 8: The Conceptual framework

3.8 SOFTWARE DEVELOPMENT APPROACH

The aim of this study is to provide a framework for aiding in the carrying out of cloud forensics by investigative agencies in Kenya, to solve cyber crime cases involving public sector institutions that have subscribed to cloud services on IaaS (Infrastructure as a Service) Clouds. The framework will provide for the independent acquiring of evidence in the form of logs from cloud resources without the intervention of cloud service providers. The deliverables include;

- A centralized logging repository for system events and evidentiary logs that can serve as admissible evidence in legal suits.
- A prototype that is designed to provide for read only access of the stored logs by investigative agencies and the judicial authority
- Sharing of verifiable evidence between Investigative agencies and the judicial authority, whose integrity is not questionable.

3.9 SYSTEM ANALYSIS

3.9.1 FUNCTIONAL REQUIREMENTS

The functional requirements of the proposed system and its application in the envisaged problem domain are highlighted in this section. The requirements enumerated and discussed below are as captured in the conceptual design.

Role Based Authentication

Access to the system and logged data by investigative agencies and the judicial authority is role based. Investigation administrators will have access to all logged data, can associated evidence with a public sector institution under investigation and publish the same to be viewed by a judicial authority. The judicial authority will only view what has been published by the investigative agency. The judicial authority and investigative agency administrators can both create users with varying roles.

System Access

Access to the system by the data and process owners (Investigative agency users and the Judicial Authority users) will be decentralized. All authenticated users will have segregated controls to allow for access of relevant data stored in the evidence repository. However, investigative agency users will have full authenticated access to stored records due to the nature of their work as initiators of investigations and originators of cases that need to be escalated for prosecution.

Security and Data Integrity

The integrity of data stored in the centralized database is guaranteed. The conceptual design envisages an environment where, the cloud resources in use by public sector institutions autonomously transmit system events and user transaction logs persistently, upon being appropriately configured. Access to the stored data is read-only and therefore prevents the likelihood of collusion between services providers, investigators, cloud users and adversaries to interfere with investigations of incidents aided by the stored evidentiary data.

Authenticated access by process and data owners also guarantees that all records can only accessed for viewing purposes and only expert opinions or explanatory notes can be authored about the records while the authenticity of the records themselves is maintained.

Verifiability

Transmission and storage of logs from cloud resources to the centralized repository occurs autonomously through configured logging utilities. The stored data is therefore; recorded in its original form, it is time-stamped and can be traced back to the originating systems hosted on the cloud platform acquired by the target public sector institution.

Scalability

The system is readily scalable and has the capacity of processing required transactions for all institutions whose data is reposed in the centralized database.

3.9.2 SYSTEM PROCEDURES

Module: User Management

The system should provide for:

1. Creation of Investigative Agency user profiles and credentials
2. Creation of Judicial Authority user profiles and credentials
3. Role-based authenticated access by both Agency and Judicial Authority users
4. Allow users to update their profile details

Module: Database Access

The system should provide for:

1. Role-based access to the system and logs from centralized repository
2. Viewing of all logs by authorized Agency users
3. Viewing of published logs by authorized Judicial authority users

Module: Case Management

The system should provide for:

1. Creation of a new case by an authorized Investigative Agency user
2. Update of case details by an authorized Agency user
3. Allocation of a new case to an Investigator
4. Publishing of logs relevant to a specific legal suit
5. Viewing of published cases and verifiable evidence by authorized Judicial authority users
6. Assignment of a published case to a particular judicial officer

Module: User Access Management

The system should provide for:

1. Creation of new user roles
2. A matrix for management of user roles or workflows
3. Assignment of a specific or multiple roles to users

3.9 SYSTEM DESIGN

3.9.1 SYSTEM ARCHITECTURE

The System illustrated on figure8 represents5 key processes as itemized below;

a) Access to cloud resources

This will be done by users of public sector institutions with various roles and functions on the enterprise systems reposed in the cloud platforms.

b) Persistent Transaction logging

Logging utilities (Auditd, and Mariadb Audit,) will facilitate the continuous capture of users' and system events to be consumed via Rsyslog for onward transmission to a centralized remote repository.

c) Centralized storage

A remote database shall receive logs transmitted from the cloud resources and enterprise systems used by public sector institutions.

d) Access to evidentiary logs

Investigative agencies and the Judicial authority users will have read only access to stored logs for the sole purpose of prosecuting legal suits. Access by the Judicial authority users on evidence stored, will be possible upon publishing of the records of interest associated with a particular suit by Investigators.

e) Case management

The Investigative agency users will create a case against a specific public sector institution, assign an investigator to a case and associate evidence with the target case. Upon publishing of evidence, the case details will be accessible to the judicial authority. The authority will in turn assign an officer to that particular legal suit and eventually publish a judgment upon conclusion of the suit.

A Detailed System Architecture

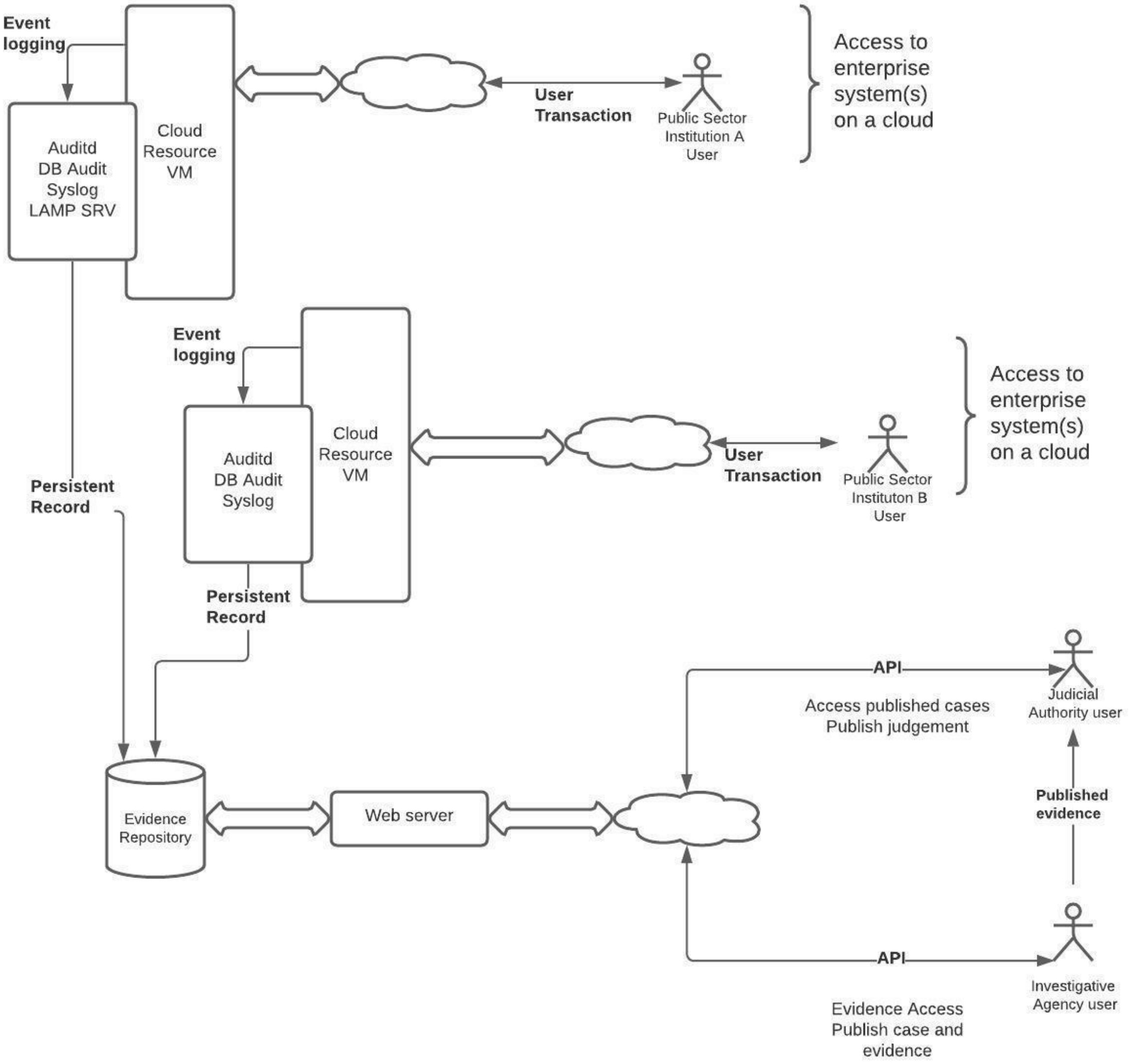


Figure 9: The System Architecture

3.9.2 System Entities and Users

Public Sector Institution User

Refers to a user of a public sector institution, who is authorized to access or interact with an enterprise system hosted in the cloud platform (cloud resource).

Investigative Agency User

Refers to a user of an Investigative Agency, who is authorized to access the evidence repository and view evidentiary logs from the public sector institutions.

Judicial Authority User

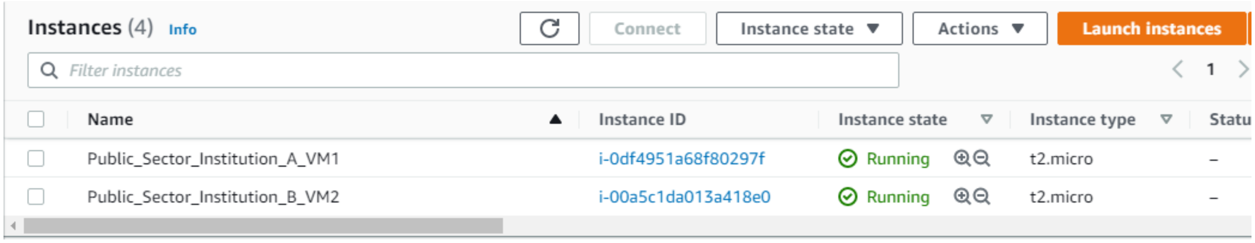
Refers to a user of the Judicial Service Authority, who has access to shared evidence published by investigators and is authorized to access legal suits.

Persistent record(s)

Refers to a record stored through the process of generation of a log or logs from both enterprise systems hosted on the cloud and user events, resulting from the interactions users will have on the enterprise systems. The record(s) are transmitted from the cloud resource(s) and stored in the remote evidence repository.

Cloud Resource

Refers to the cloud infrastructure acquired by a public sector institution.



□	Name ▲	Instance ID	Instance state ▽	Instance type ▽	Statu
□	Public_Sector_Institution_A_VM1	i-0df4951a68f80297f	✓ Running	t2.micro	–
□	Public_Sector_Institution_B_VM2	i-00a5c1da013a418e0	✓ Running	t2.micro	–

Figure 10: Simulation with AWS Ec2 cloud resources (Ubuntu 18.04.5 LTS)

User Transactions

Refers to users' activities on the public sector institution's cloud infrastructure and enterprise systems hosted on the cloud platform.

LAMP Server

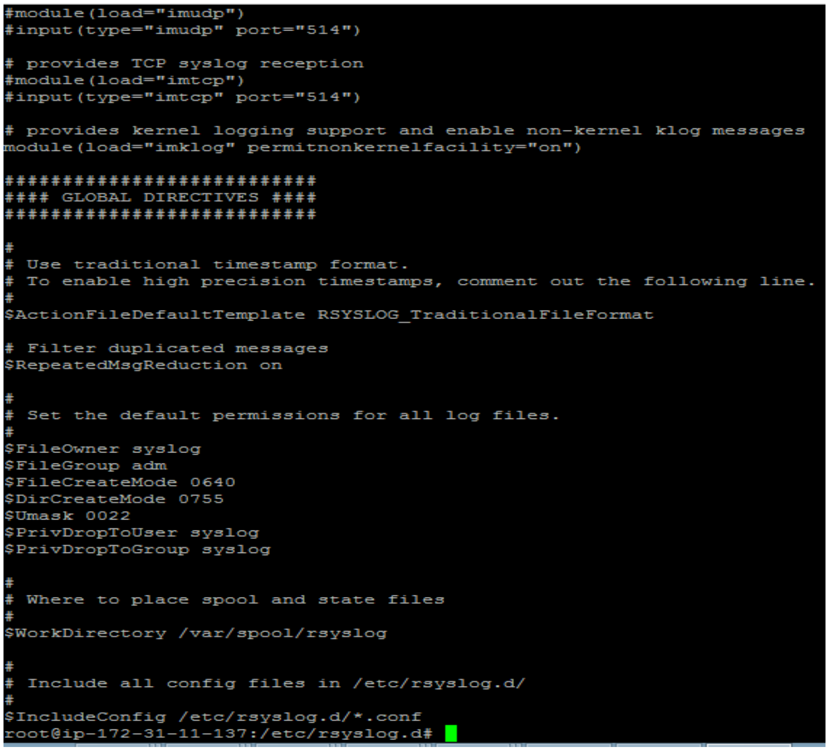
Refers to a Linux Apache Mysql and Php set up on the cloud resource (virtual machine) used by a public sector institution.

Web server

The web service engine configured to process requests from both Judicial Service Authority and the Investigative Agency users.

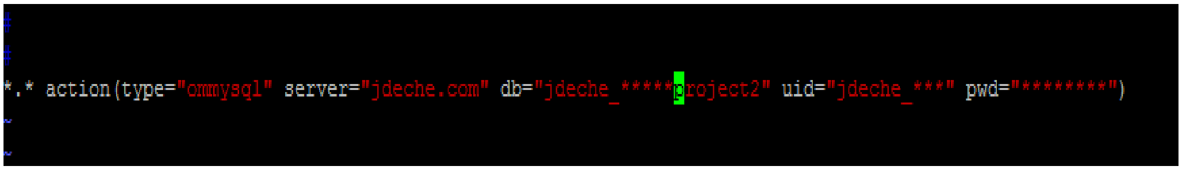
Rsyslog

Refers to the log processing utility that is configured to send logs to the remote database.



```
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
root@ip-172-31-11-137:/etc/rsyslog.d#
```

Figure 11: Sample Rsyslog configurations

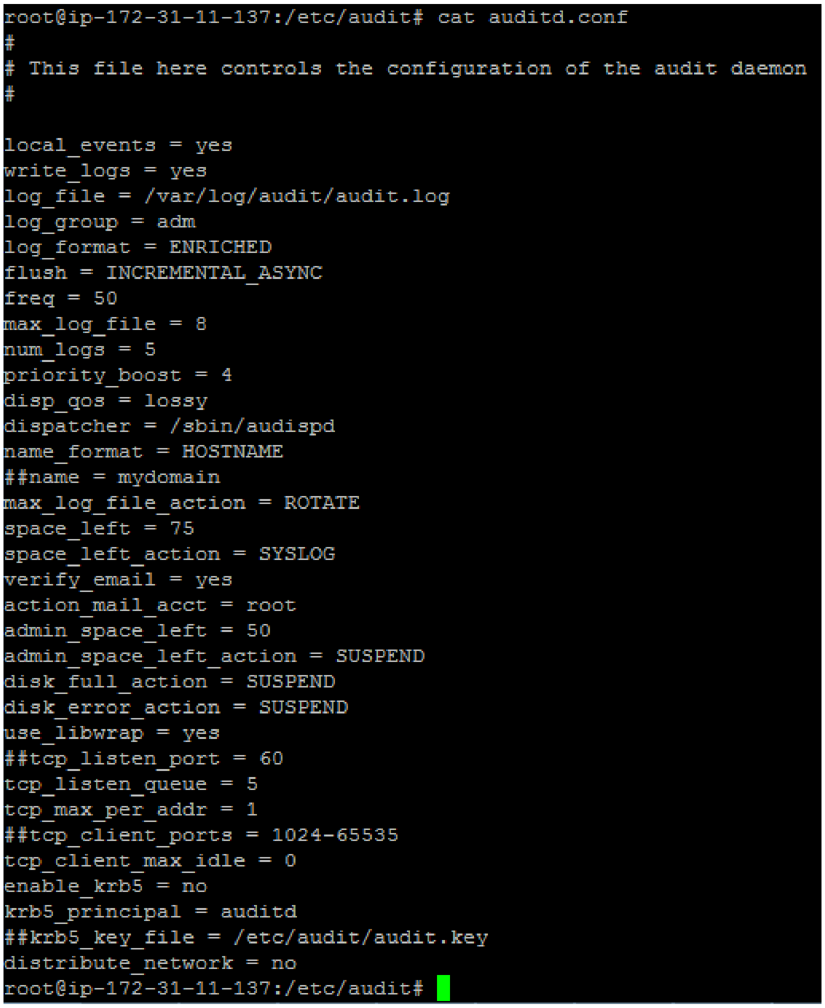


```
#
#
*.* action(type="ommysql" server="jdeche.com" db="jdeche_*****project2" uid="jdeche_***" pwd="********")
~
~
```

Figure 12: Connection string for logging to the remote database

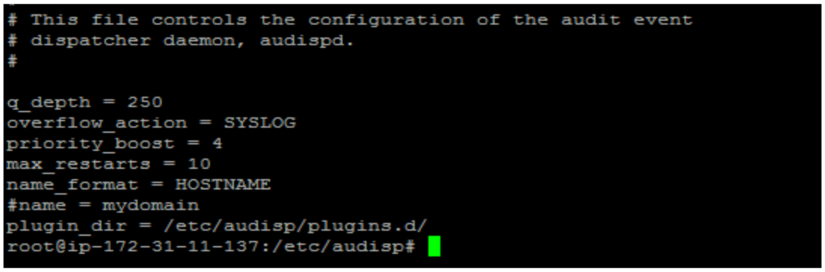
Auditd

A native feature of the Linux operating system's kernel that gathers information on system activities that can aid in investigating incidents.



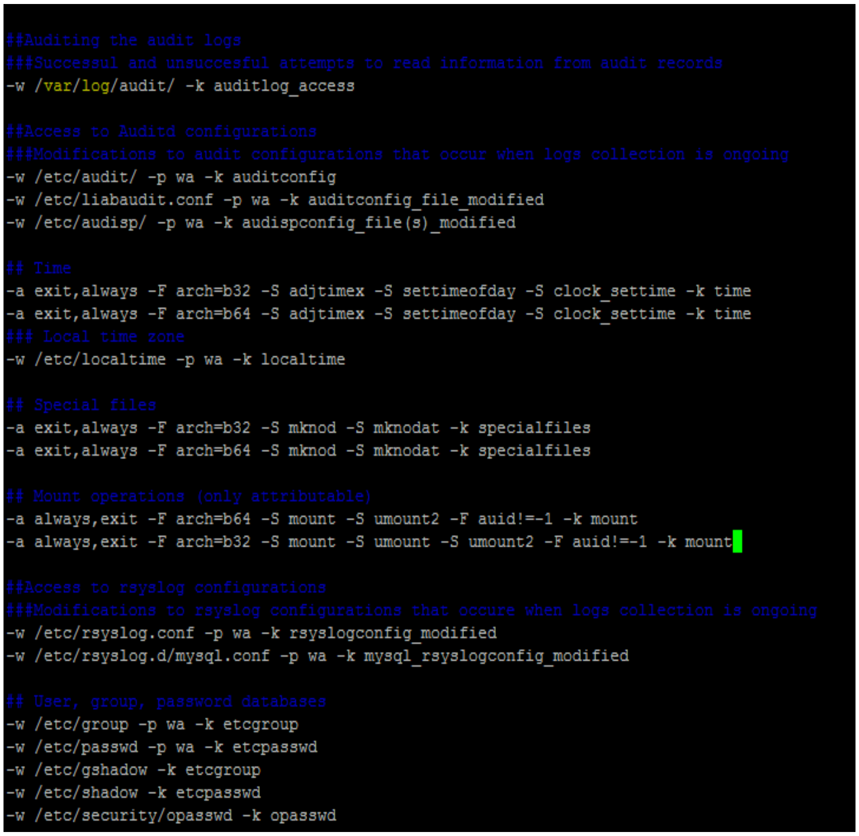
```
root@ip-172-31-11-137:/etc/audit# cat auditd.conf
#
# This file here controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = HOSTNAME
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
root@ip-172-31-11-137:/etc/audit#
```

Figure 13: Sample Auditd configurations



```
# This file controls the configuration of the audit event
# dispatcher daemon, audispd.
#

q_depth = 250
overflow_action = SYSLOG
priority_boost = 4
max_restarts = 10
name_format = HOSTNAME
#name = mydomain
plugin_dir = /etc/audisp/plugins.d/
root@ip-172-31-11-137:/etc/audisp#
```

Figure 14: Configuring Auditd to log through Rsyslog

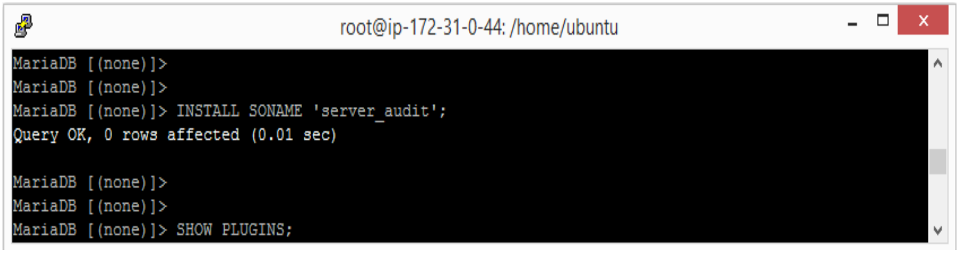


```
##Auditing the audit logs
###Successul and unsuccesful attempts to read information from audit records
-w /var/log/audit/ -k auditlog_access

##Access to Auditd configurations
###Modifications to audit configurations that occur when logs collection is ongoing
-w /etc/audit/ -p wa -k auditconfig
-w /etc/liabaudit.conf -p wa -k auditconfig_file_modified
-w /etc/audisp/ -p wa -k audispconfig_file(s)_modified

## Time
-a exit,always -F arch=b32 -S adjtimex -S settimeofday -S clock_settime -k time
-a exit,always -F arch=b64 -S adjtimex -S settimeofday -S clock_settime -k time
### Local time zone
-w /etc/localtime -p wa -k localtime

## Special files
-a exit,always -F arch=b32 -S mknod -S mknodat -k specialfiles
-a exit,always -F arch=b64 -S mknod -S mknodat -k specialfiles

## Mount operations (only attributable)
-a always,exit -F arch=b64 -S mount -S umount2 -F auid!=-1 -k mount
-a always,exit -F arch=b32 -S mount -S umount -S umount2 -F auid!=-1 -k mount

##Access to rsyslog configurations
###Modifications to rsyslog configurations that occure when logs collection is ongoing
-w /etc/rsyslog.conf -p wa -k rsyslogconfig_modified
-w /etc/rsyslog.d/mysql.conf -p wa -k mysql_rsyslogconfig_modified

## User, group, password databases
-w /etc/group -p wa -k etcgroup
-w /etc/passwd -p wa -k etcpasswd
-w /etc/gshadow -k etcgroup
-w /etc/shadow -k etcpasswd
-w /etc/security/opasswd -k opasswd
```

Figure 15: Sample Auditd rules

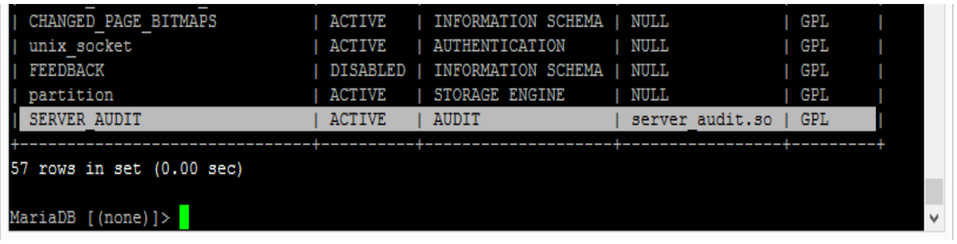
MariaDBAudit

Refers to MariaDB's audit plugin which is configured to log users' activities while interacting with the database.



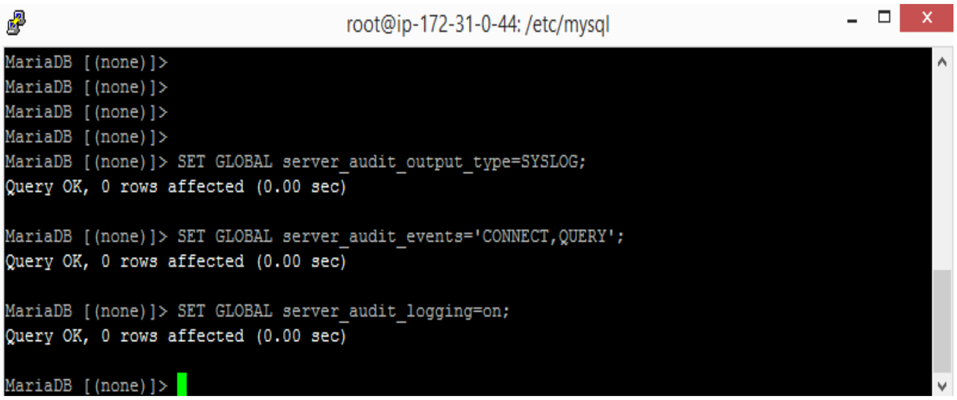
```
MariaDB [(none)]>
MariaDB [(none)]>
MariaDB [(none)]> INSTALL SONAME 'server_audit';
Query OK, 0 rows affected (0.01 sec)

MariaDB [(none)]>
MariaDB [(none)]>
MariaDB [(none)]> SHOW PLUGINS;
```

Figure 16: Sample MariaDB server audit plugin configurations



```
| CHANGED_PAGE_BITMAPS          | ACTIVE   | INFORMATION_SCHEMA | NULL            | GPL     |
| unix_socket                   | ACTIVE   | AUTHENTICATION     | NULL            | GPL     |
| FEEDBACK                      | DISABLED | INFORMATION_SCHEMA | NULL            | GPL     |
| partition                     | ACTIVE   | STORAGE ENGINE     | NULL            | GPL     |
| SERVER_AUDIT                  | ACTIVE   | AUDIT              | server_audit.so | GPL     |
+-------------------------------+----------+--------------------+-----------------+---------+
57 rows in set (0.00 sec)

MariaDB [(none)]>
```

Figure 17: Active MariaDB plugin status



```
MariaDB [(none)]>
MariaDB [(none)]>
MariaDB [(none)]>
MariaDB [(none)]>
MariaDB [(none)]> SET GLOBAL server_audit_output_type=SYSLOG;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> SET GLOBAL server_audit_events='CONNECT,QUERY';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> SET GLOBAL server_audit_logging=on;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]>
```

Figure 18: Sample MariaDB configurations to capture CONNECT and QUERY logs

System Processes

User Authentication

A process of identifying authorized users, their specific roles and access rights to various system resources.

Add User

A process of enrolling both the Investigative agency and Judicial authority users into the system.

Add Role

A process of creating user roles for both Investigative agency and Judicial Authority users

Create Case

A process of creating a new case for a public sector institution under investigation.

Publish evidence

A process of associating specific evidence from the repository with a case under investigation and allowing access to authorized Judicial authority users.

Append expert opinion

A process of attaching a more descriptive explanation against evidentiary logs associated with a particular case.

Assign Investigator

A process of assigning a case to a specific investigator.

Assign Judicial Officer

A process of assigning a case to a specific Judicial service officer.

Evidence Verification

The process of verifying the authenticity of evidence shared by an investigative agency

Data Storage

Online MySQL database

The central repository for evidentiary logs generated by users of public sector institutions while interacting with enterprise systems hosted on cloud platforms.

Users Database

The database of the Investigative Agency and Judicial Authority users authorized to access the system.

User Roles

Super User

The overall administrator of the web portal whose roles include among others; setting up all user roles, creating administrators for both the Judicial authority and Investigative Agencies and creating new user roles.

Agency Admin

A user whose roles include adding new users (Investigators), assigning user rights, creating new cases, accessing and publishing evidence against cases created and analyzing stored evidentiary logs.

Agency Investigator

A user whose roles include, analyzing evidence of a case and publishing relevant evidence for onward access and viewing by judicial authority users.

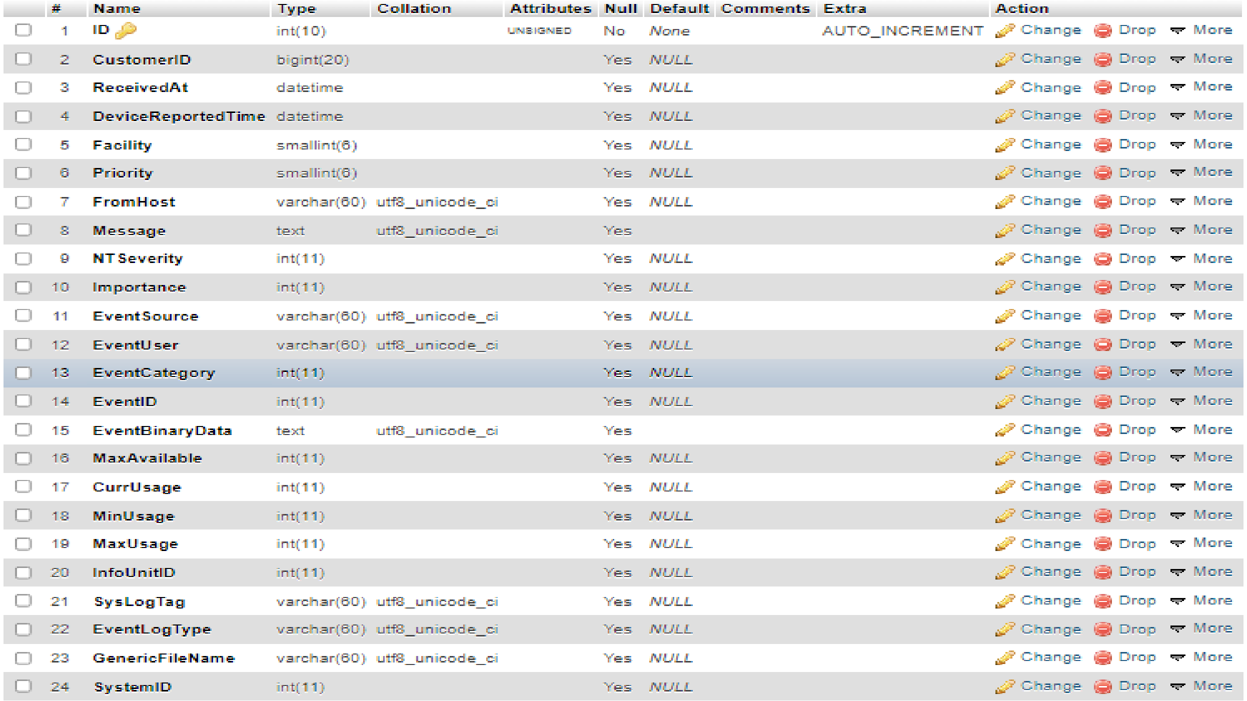
Judicial Authority Admin

A user whose roles include case management, user management and updating status of legal suits.

Judicial Authority Officer

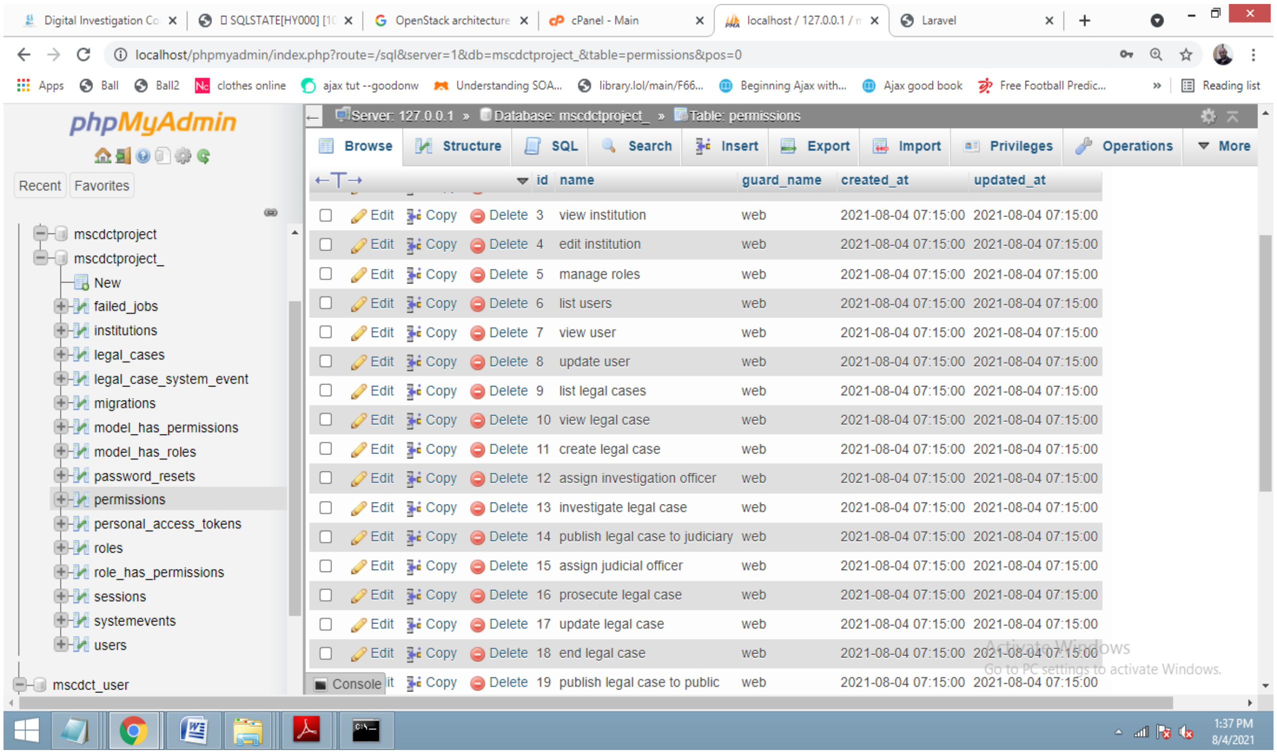
A user whose roles include verifying the authenticity of published evidence and updating the status of a case.

Database



	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
□	1	ID	int(10)		UNSIGNED	No	*None*		AUTO_INCREMENT	Change Drop More
□	2	CustomerID	bigint(20)			Yes	*NULL*			Change Drop More
□	3	ReceivedAt	datetime			Yes	*NULL*			Change Drop More
□	4	DeviceReportedTime	datetime			Yes	*NULL*			Change Drop More
□	5	Facility	smallint(6)			Yes	*NULL*			Change Drop More
□	6	Priority	smallint(6)			Yes	*NULL*			Change Drop More
□	7	FromHost	varchar(60)	utf8_unicode_ci		Yes	*NULL*			Change Drop More
□	8	Message	text	utf8_unicode_ci		Yes				Change Drop More
□	9	NTSeverity	int(11)			Yes	*NULL*			Change Drop More
□	10	Importance	int(11)			Yes	*NULL*			Change Drop More
□	11	EventSource	varchar(60)	utf8_unicode_ci		Yes	*NULL*			Change Drop More
□	12	EventUser	varchar(60)	utf8_unicode_ci		Yes	*NULL*			Change Drop More
□	13	EventCategory	int(11)			Yes	*NULL*			Change Drop More
□	14	EventID	int(11)			Yes	*NULL*			Change Drop More
□	15	EventBinaryData	text	utf8_unicode_ci		Yes				Change Drop More
□	16	MaxAvailable	int(11)			Yes	*NULL*			Change Drop More
□	17	CurrUsage	int(11)			Yes	*NULL*			Change Drop More
□	18	MinUsage	int(11)			Yes	*NULL*			Change Drop More
□	19	MaxUsage	int(11)			Yes	*NULL*			Change Drop More
□	20	InfoUnitID	int(11)			Yes	*NULL*			Change Drop More
□	21	SysLogTag	varchar(60)	utf8_unicode_ci		Yes	*NULL*			Change Drop More
□	22	EventLogType	varchar(60)	utf8_unicode_ci		Yes	*NULL*			Change Drop More
□	23	GenericFileName	varchar(60)	utf8_unicode_ci		Yes	*NULL*			Change Drop More
□	24	SystemID	int(11)			Yes	*NULL*			Change Drop More

Table 4: The Rsyslog database schema



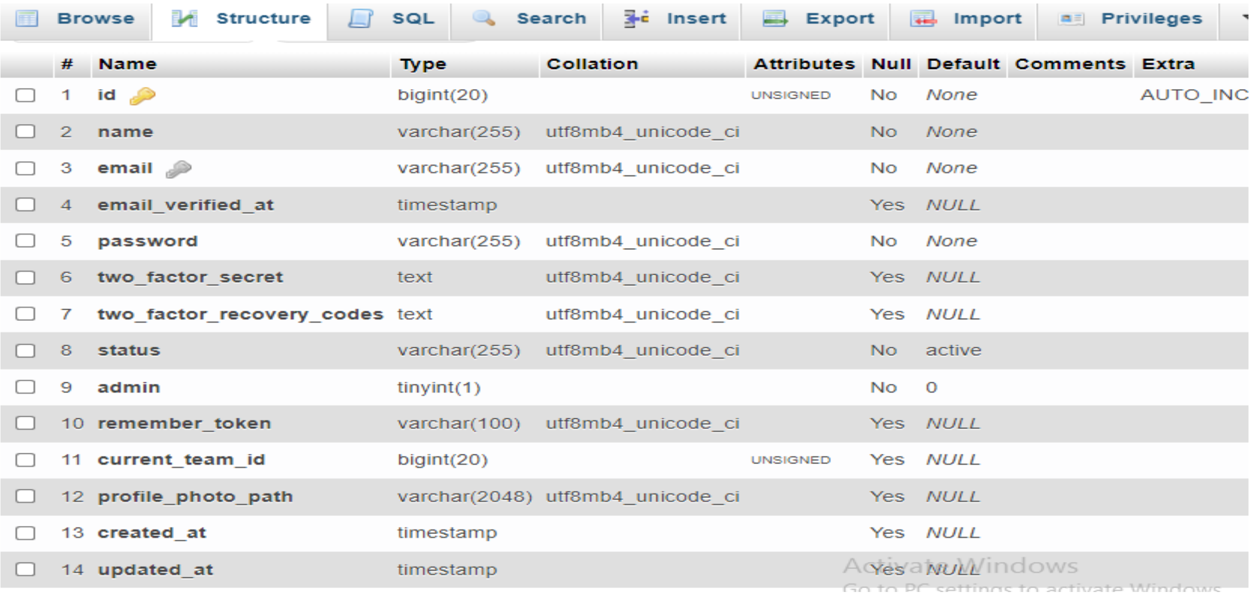
localhost/phpmyadmin/index.php?route=/sql&server=1&db=mscdctproject_&table=permissions&pos=0

Server: 127.0.0.1 » Database: mscdctproject_ » Table: permissions

- mscdctproject
- mscdctproject_
  - New
  - failed_jobs
  - institutions
  - legal_cases
  - legal_case_system_event
  - migrations
  - model_has_permissions
  - model_has_roles
  - password_resets
  - permissions
  - personal_access_tokens
  - roles
  - role_has_permissions
  - sessions
  - systemevents
  - users
- mscdct_user

				id	name	guard_name	created_at	updated_at
□	Edit	Copy	Delete	3	view institution	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	4	edit institution	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	5	manage roles	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	6	list users	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	7	view user	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	8	update user	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	9	list legal cases	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	10	view legal case	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	11	create legal case	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	12	assign investigation officer	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	13	investigate legal case	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	14	publish legal case to judiciary	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	15	assign judicial officer	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	16	prosecute legal case	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	17	update legal case	web	2021-08-04 07:15:00	2021-08-04 07:15:00
□	Edit	Copy	Delete	18	end legal case	web	2021-08-04 07:15:00	2021-08-04 07:15:00
	it	Copy	Delete	19	publish legal case to public	web	2021-08-04 07:15:00	2021-08-04 07:15:00

Table 5*: List of user permissions or roles on the system*

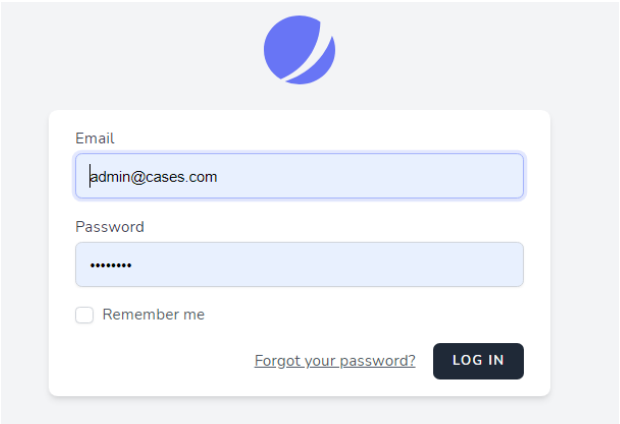


	#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra
□	1	**id**	bigint(20)		UNSIGNED	No	*None*		AUTO_INC
□	2	**name**	varchar(255)	utf8mb4_unicode_ci		No	*None*		
□	3	**email**	varchar(255)	utf8mb4_unicode_ci		No	*None*		
□	4	**email_verified_at**	timestamp			Yes	*NULL*		
□	5	**password**	varchar(255)	utf8mb4_unicode_ci		No	*None*		
□	6	**two_factor_secret**	text	utf8mb4_unicode_ci		Yes	*NULL*		
□	7	**two_factor_recovery_codes**	text	utf8mb4_unicode_ci		Yes	*NULL*		
□	8	**status**	varchar(255)	utf8mb4_unicode_ci		No	active		
□	9	**admin**	tinyint(1)			No	0		
□	10	**remember_token**	varchar(100)	utf8mb4_unicode_ci		Yes	*NULL*		
□	11	**current_team_id**	bigint(20)		UNSIGNED	Yes	*NULL*		
□	12	**profile_photo_path**	varchar(2048)	utf8mb4_unicode_ci		Yes	*NULL*		
□	13	**created_at**	timestamp			Yes	*NULL*		
□	14	**updated_at**	timestamp			Yes	*NULL*		

Table 6: Users table

System Input Design

The login page for authorized system users.



Email

admin@cases.com

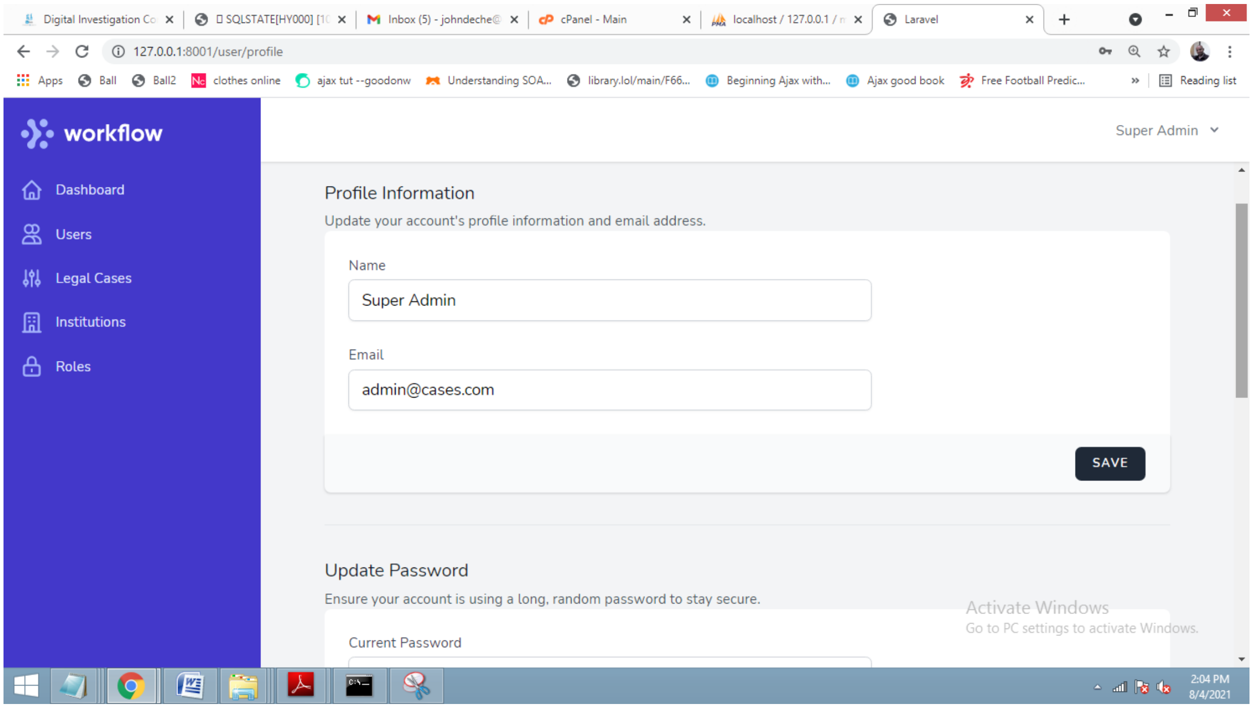
Password

••••••••

□ Remember me

Figure 19: System Login window

A provision for updating a system user's profile details.



Profile Information

Update your account's profile information and email address.

Name: Super Admin

Email: admin@cases.com

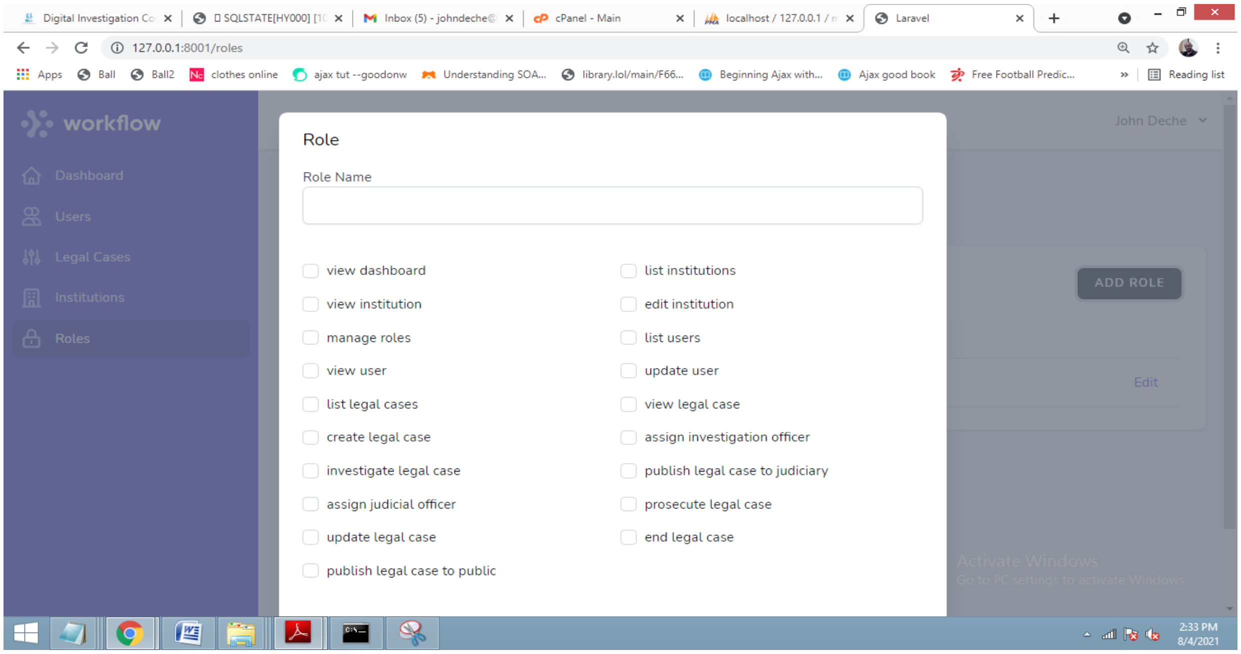
Update Password

Ensure your account is using a long, random password to stay secure.

Current Password

Figure 20: User profile update window

A provision for creating various user roles to provide for role-based access to the system's modules and database.



Role

Role Name

- □ view dashboard
- □ view institution
- □ manage roles
- □ view user
- □ list legal cases
- □ create legal case
- □ investigate legal case
- □ assign judicial officer
- □ update legal case
- □ publish legal case to public
- □ list institutions
- □ edit institution
- □ list users
- □ update user
- □ view legal case
- □ assign investigation officer
- □ publish legal case to judiciary
- □ prosecute legal case
- □ end legal case

Figure 21: User role management matrix

4.1 CHAPTER FOUR: PROTOTYPE TESTING AND RESULTS

This section reports on the tests carried out for the developed prototype along with the various methods used. The testing criteria used are provided in clause 4.2 and a summary of sampled results obtained against selected test cases, which are aligned to the objective of this research highlighted in section 4.3.

4.2 PROTOTYPE TESTING CRITERIA

The prototype developed was assessed against the following objectives and capabilities;

i) Role based access to the prototype by both Investigative Agencies and Judicial Service Authority users and a controlled view of stored logs

ii) Configuring logging utilities (Auditd, Rsyslog, Mariadb audit plugin) on the cloud resources to autonomously transmit and store evidentiary logs resulting from users' activities on a centralized repository

iii) Access to logs stored on the centralized repository through the prototype

iv) Access of published logs by judicial authority users for the purpose of prosecuting legal suits.

4.3 TEST CASES AND RESULTS

The test cases illustrated in the table below were used to validate the system and the outcome is provided alongside each test case.

Test Cases and Results

#	Test Case Description	Provided input	Expected Results	Actual results	Remarks
1	User enrolment, assignment of rights for system access by Super Admin user	● New user's full names: o John Deche ● Role type: o Agency Admin ● Username: o jdeche ● Password: pass***d	● Agency Admin enrolled successfully	● Agency User enrolled successfully	Pass
2	User enrolment, assignment of rights for system access by Judicial Admin user	● New user's full names: o Ken Deche ● Role type: o Judiciary Admin ● Username: o Kdeche ● Password: pass***d	● Judicial Authority Admin enrolled successfully	● Judicial Authority User enrolled successfully	Pass
3	Successful Role-based access by Investigative Agency user	● Login credentials; (username and password)dk@cases.com and p*****rd	● User redirected to landing page as per the role assigned	● Judicial Authority or Agency user re-directed to specific profiles	Pass
4	Unsuccessful Role-based access by Agency and Judicial Authority users.	● Non-existent Login credentials; (username and password)	● Invalid login by user. User redirected to login page	● Invalid login by user. User redirected to login page	Pass

5	Auditd capture of unsuccessful root login from a Secure Shell Protocol terminal	login as: root	Unsuccessful root user login through Secure Shell Protocol by root user	node=ip-172-31-11-137 type=USER_LOGIN msg=audit (1627288424.185:474): pid=3377 uid=0 auid=4294967295 ses=4294967295 msg='op=login acct=28756E6B6E6F776E2075736 57229 exe="/usr/sbin/sshd" hostname=? addr=205.185.125.109 terminal=sshd res=failed' UID="root" AUID="unset"	Pass
6	Auditd deleted directory watch rule	root@ip-172-31-11-137:rmdir/home/jdeche /workspace	Successful delete of workspace directory in user jdeche's workspace folder	node=ip-172-31-11-137 type=SYSCALL msg=audit(1627441264.623:474): arch=c000003e syscall=84 success=yes exit=0 a0=7ffcaf23f865 a1=2 a2=7f5f8aed0000 a3=5579760c1010 items=2 ppid=2818 pid=2835 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=8 comm="rmdir" exe="/bin/rmdir" key="workspace_dir_accessed"	

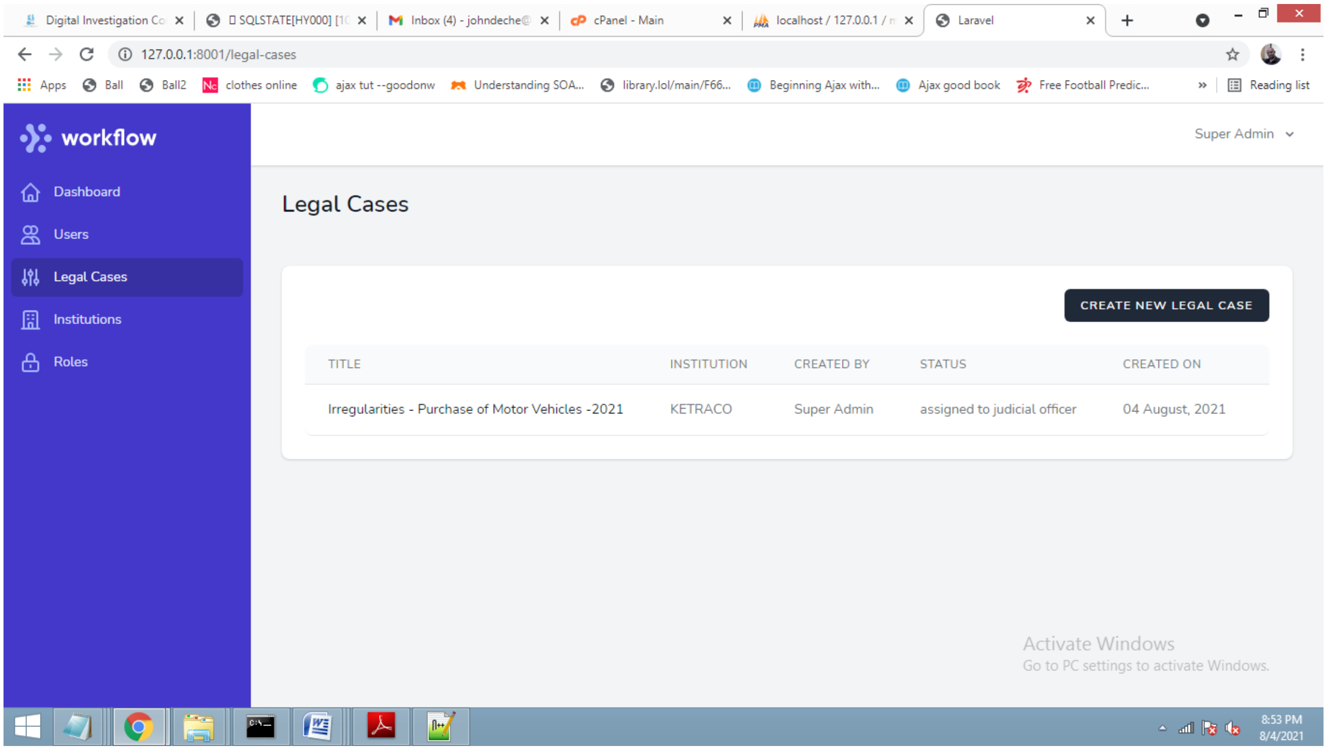
				ARCH=x86_64 SYSCALL=rmdir AUID="ubuntu" UID="root" GID="root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"	
7	Auditd configuration file access and modification watch rule	root@ip-172-31-11-137:cat /etc/rsyslog.d/mysql.conf	Logged access to Rsyslog configuration file by root user	node=ip-172-31-11-137 type=PATH msg=audit(1627334523.264:618): item=0 name="/etc/rsyslog.d/mysql.conf" inode=1669 dev=ca:01 mode=0100600 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0 OUID="root" OGID="root"	Pass
8	Auditd configuration file access and modification watch rule	root@ip-172-31-11-137:cat /etc/audit/rules.d/audit.rules	Logged access and modification to auditd configuration file by root user	node=ip-172-31-11-137 type=PATH msg=audit(1627335371.965:683): item=1 name="/etc/audit/rules.d/audit.rules " inode=542448 dev=ca:01 mode=0100640 ouid=0 ogid=0 rdev=00:00 nametype=CREATE cap_fp=0 cap_fi=0 cap_fe=0	Pass

				cap_fver=0 cap_frootid=0 OUID="root" OGID="root"	
9	MariaDB select query audit rule - Logging a login attempt into the simulated Births Registration System	- User name: jdeche - Password: pa*****d	- Logged select query on the users table of the Births Registration System’s database	ip-172-31-0-44,root,localhost, 122,501,QUERY,registration,'SELECT * FROM `users` WHERE username=\'jdeche\'\nand password=\'1cbceae2c22e235b6bd5bf28d4c462db\'',0	Pass
	MariaDB insert query audit rule - Logging an insert query by a user into the simulated Births Registration System	- Inserted Records into table newborndata; childfname: Aziz childlname: Ahmed motherfname: Shamsia motherlname: Rama fatherfname: Hamisi fatherlname: Abdul placeofbirth: Mombasa Hospital dob: 2019-10-10 residence: Kisauni certno: 55441 verificationstatus:NA firstapprovalstatus:NA secondapprovalstatus:NA verifyingofficer:NA	- Logged insert query on newborndata table by user	ip-172-31-0-44,root,localhost, 129,511,QUERY,registration,'INSERT INTO newborndata(`childfname`, `childlname`, `motherfname`, `motherlname`, `fatherfname`, `fatherlname`, `placeofbirth`, `dob`, `residence`, `certno`,`verificationstatus`, `firstapprovalstatus`,`secondapprovalstatus`, `verifyingofficer`,`approver1`, `approver2`)\nVALUES(\'Aziz\',\'Ahmed\',\'Shamsia\',\'Rama\',\'Hamisi\',\'Abdul\',\'Mombasa Hospital\',\'2019-10-10\',\'Kisauni\',\'55441\',\'NA\',\'NA\',\'NA\',\'NA\',\'NA\',\'NA\')',0	Pass

10	Access to stored evidentiary logs by Investigative Agency users through the web-based system	● Stored evidentiary logs on remote repository	● Access to logs from Amazon EC2 Virtual machines transmitted to remote database successfully	● Access to logs from Amazon EC2 Virtual machines transmitted to remote database successfully	Pass
11	Access to published evidentiary logs by Judicial authority user through the web-based system	● Published logs by agency Investigator associated with a legal suit	● Successful access to published logs by Judicial by Judicial Authority user	● Successful access to published and verifiable logs and by Judicial Authority user	Pass

Table 7: Test cases and results

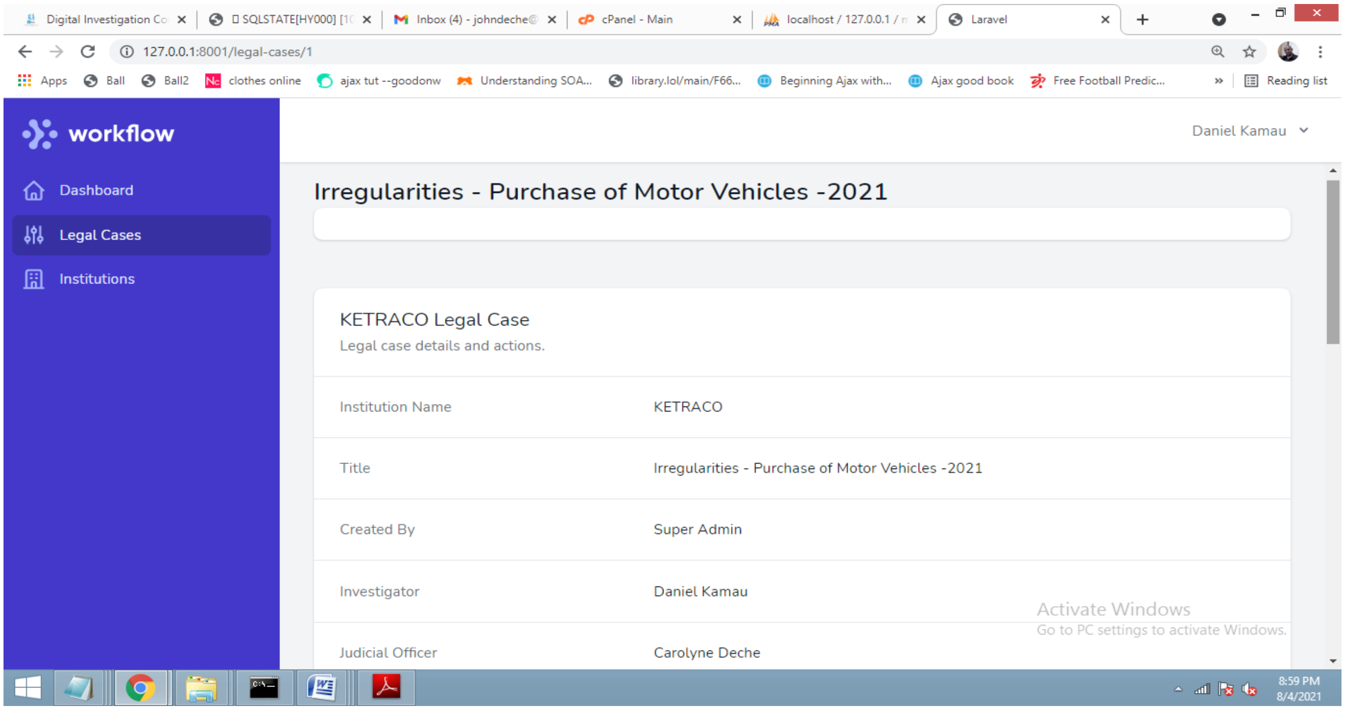
4.4 STATUS OF THE SYSTEM



Legal Cases

TITLE	INSTITUTION	CREATED BY	STATUS	CREATED ON
Irregularities - Purchase of Motor Vehicles -2021	KETRACO	Super Admin	assigned to judicial officer	04 August, 2021

Figure 22: Case creation page



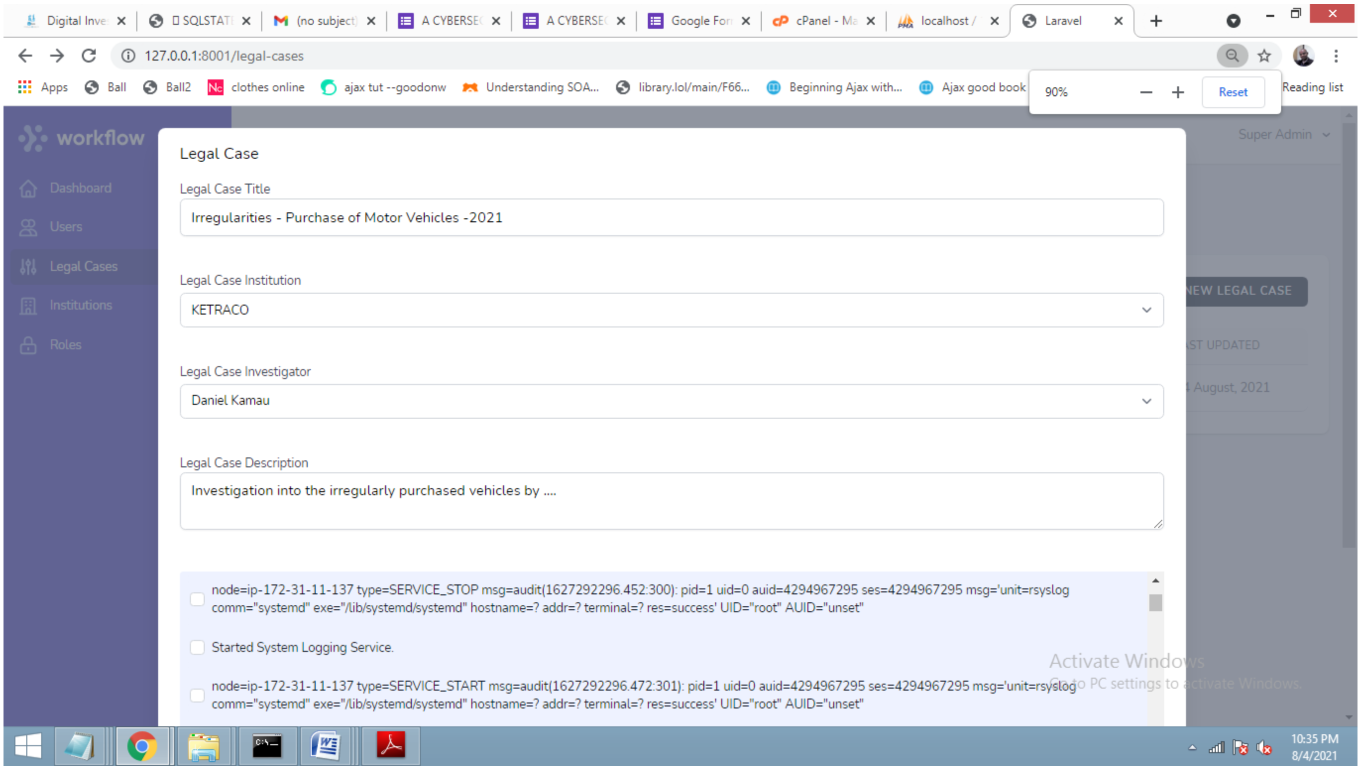
Irregularities - Purchase of Motor Vehicles -2021

KETRACO Legal Case

Legal case details and actions.

Institution Name	KETRACO
Title	Irregularities - Purchase of Motor Vehicles -2021
Created By	Super Admin
Investigator	Daniel Kamau
Judicial Officer	Carolyne Deche

Figure 23: Created case and details



Legal Case

Legal Case Title

Irregularities - Purchase of Motor Vehicles -2021

Legal Case Institution

KETRACO

Legal Case Investigator

Daniel Kamau

Legal Case Description

Investigation into the irregularly purchased vehicles by ....

```
□ node=ip-172-31-11-137 type=SERVICE_STOP msg=audit(1627292296.452:300): pid=1 uid=0 auid=4294967295 ses=4294967295 msg='unit=rsyslog
  comm="systemd" exe="/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
□ Started System Logging Service.
□ node=ip-172-31-11-137 type=SERVICE_START msg=audit(1627292296.472:301): pid=1 uid=0 auid=4294967295 ses=4294967295 msg='unit=rsyslog
  comm="systemd" exe="/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
```

Figure 24: Created case and associated logs

5.0 RESULTS AND DISCUSSION

This chapter provides illustrations of expert users' responses on user experience. The system's reliability and implementation on a real-world environment is also provided along with an analysis of the sample results in section 4.3.A discussion on the main system modules, procedures used and results obtained is also provided.

A brief survey by various practitioners on the general usability and user experience generated the responses provided in the section below;

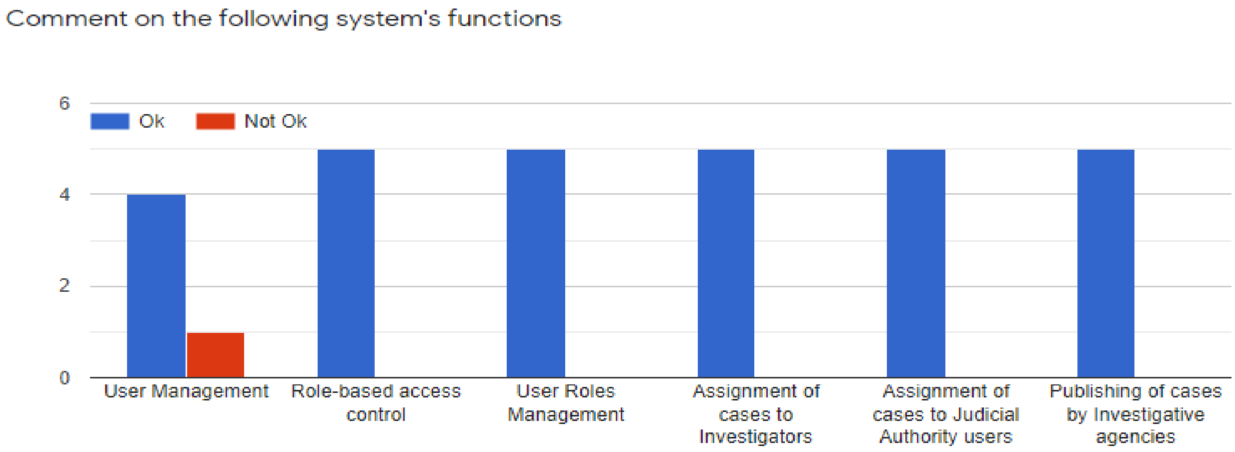


Figure 25: Survey response on various system functions

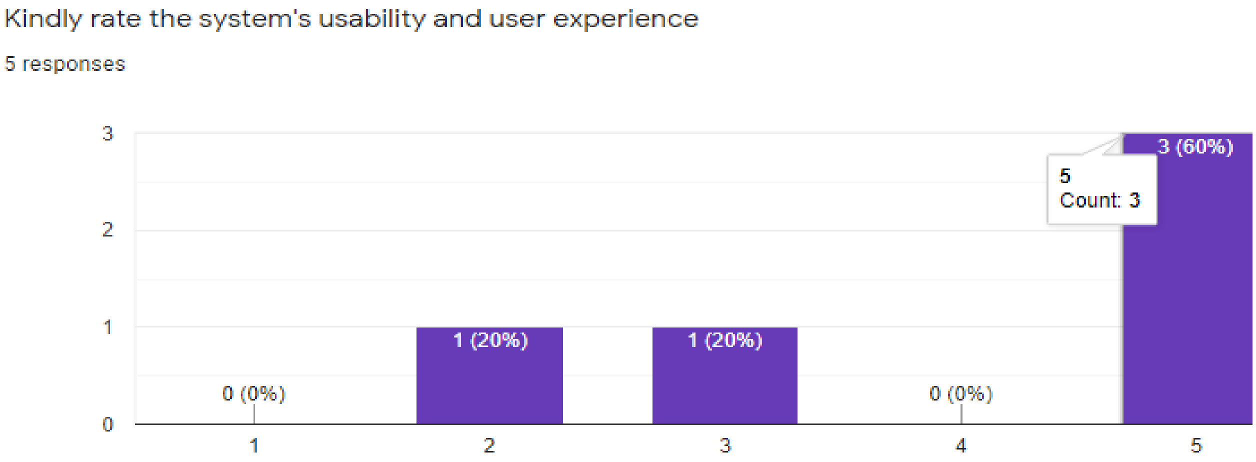


Figure 26: Survey response on the system's usability and user experience

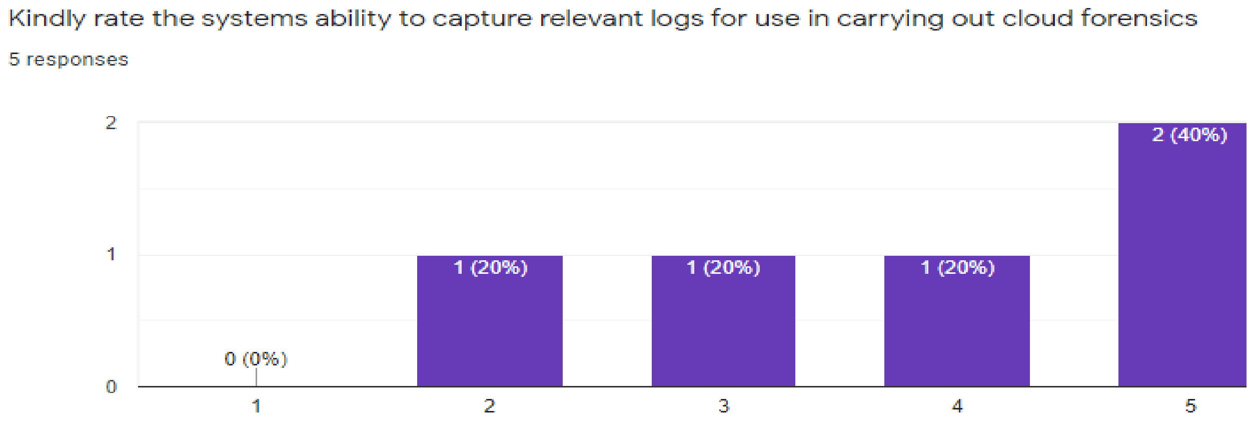


Figure 27*: Survey response on usability and user experience*

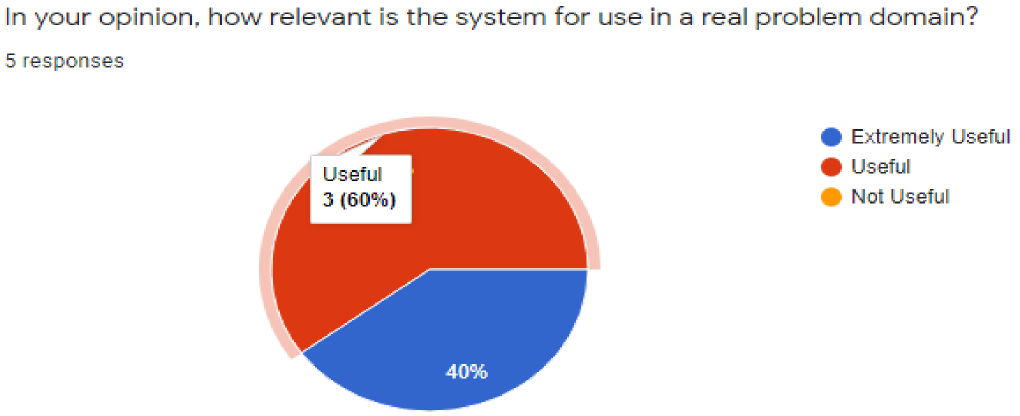
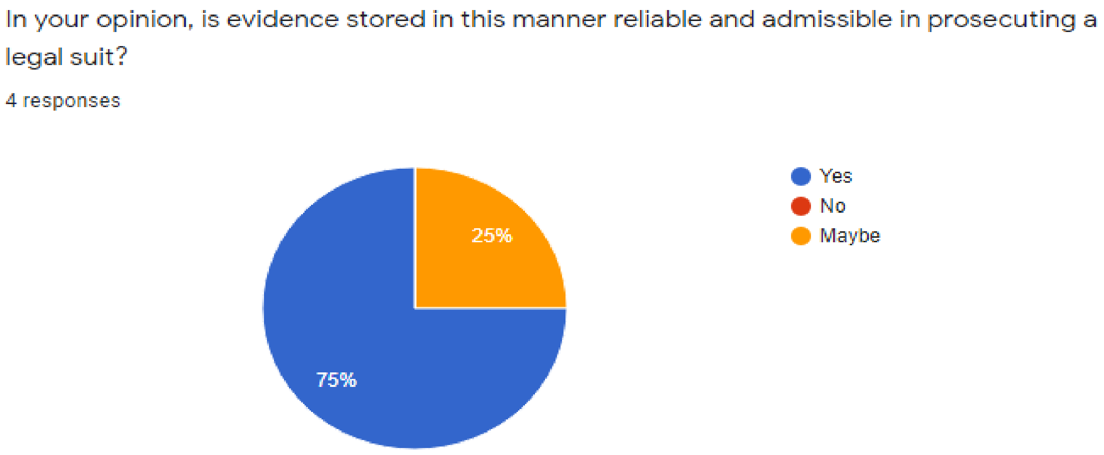


Figure 28: Survey response on relevance of system in a real problem domain



In your opinion, is evidence stored in this manner reliable and admissible in prosecuting a legal suit?

4 responses

Figure 29: Survey response on reliability of evidentiary logs captured

5.1 SYSTEM COMPONENTS, MODULES AND FUNCTIONS

This research and development project successfully analyzed and designed a prototype for; a persistent cloud forensics model that can aid investigative agencies in carrying out reliable digital forensics on cloud platforms.

The system comprises of cloud resources which are virtual machines configured to run enterprises applications used by institutions (a simulation of a web-based births registration system has been used to achieve this). A remote database is also used and serves as a centralized repository for generated and transmitted logs. The logs repository is accessed through a secured web system by the mandated Investigative agencies and the Judicial service authority.

Autonomous Log Aggregation and Storage

It is functionally possible to autonomously log and store records of user activities from cloud resources without the intervention of the cloud service providers or the utilization of third-party logging services. This is achieved through the configuration of the following native Linux utilities and the remote MySQL database;

Rsyslog: An open source log processing utility that implements the Syslog protocol. It can be configured to forward log messages via the IP network. Rsyslog has been configured and used in the prototype to transmit logs generated by user activities on virtual machines which are simulated public sector cloud environments. The logs are transmitted and stored in a remote MySQL database hosted on a web domain.

The utility’s mysql.conf reposed in /etc/rsyslog.d/mysql.conf contains the ommysql module that offers the native support for logging to MySQL databases. This has been configured to log on the remote database as illustrated in **figures 11** and **12**.

Auditd: A service or user space component on the Linux operating system that writes audit records to disk. Auditd is a native feature to the Linux kernel that is capable of collecting certain types of system activities to facilitate incident investigation. The daemon has been configured to generate records of specific user activities that are consumed by the Rsyslog utility. Illustrations of sample configurations of auditd rules applied to capture specific user activities are provided on **figure 15**.

Mariadb Audit: A plugin used to log the Mariadb relational databases management system's activities. The plugin is capable of logging executed queries, connection sessions and database tables accessed. The logging of user connection activities, queries executed and tables accessed have successfully been configured on the prototype as illustrated on figures; 15, 16 and 17. Output from the plugin is consumed by Rsyslog for onward forwarding to the remote database storage.

Remote MySQL: A MySQL database hosted on a web domain. The Rsyslog database schema illustrated in **table3** is used to create the database for storage of remotely transmitted logs.

The Web System: A web-based system developed using Laravel and Vue for accessing logs on the remote database. The system allows for role-based authentication where, Investigators and users from the Judicial service authority can successfully log in and access system resources as dictated by their roles which include; Agency Admin, Agency Investigator, Judicial Admin and Judicial Officer. Investigative Agencies have access to a case management module where, new cases can be created and associated with the evidence of interest from a particular public sector institution, while Judicial Service authority users can view cases and evidence published by investigators for verification and subsequent judicial processes. A module has also been developed for appending expert opinion against evidence in use, for ease of analysis. An illustration is provided on figures:19-21 and 22-24.

Cloud Resources: Virtual Machines are used to serve as a simulated environment for cloud resources acquired by public sector institutions. An illustration is provided on figure 9, of Amazon EC2 virtual servers. A model births registration system and database are hosted in a LAMP server of Virtual Machine A and records of user activities on the system can successfully be captured through the Mariadb audit plugin and relayed to the remote database plugin. Virtual Machine B has been used to provide auditd's generated logs of user's interaction with the resource. Both scenarios have been successfully demonstrated under the test cases and results section on table 4.

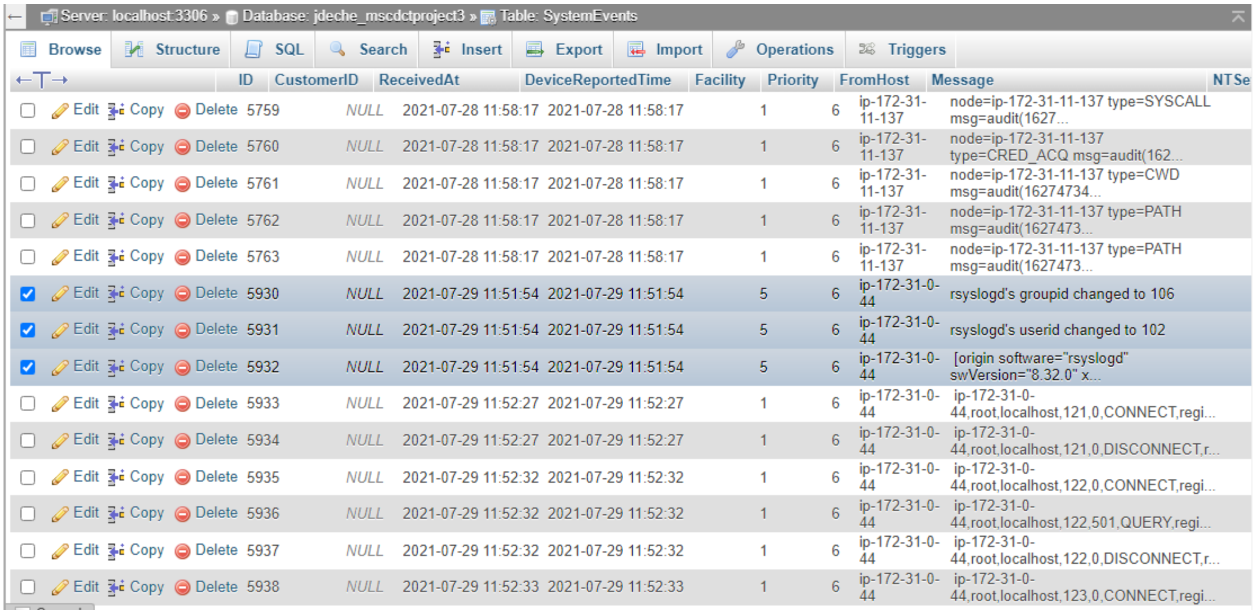
5.2 RESULTS ANALYSIS

In this section, sampled results were further discussed with respect to the intended objectives of the prototype developed.

Connect and Insert Query Audit rules

The main accomplishment of this study was to demonstrate the ability to autonomously acquire useful digital evidence from the Infrastructure as a Service Cloud platform, to aid in carrying out forensics investigations on the cloud by investigative agencies. The screen short of records stored on the remote database on table 5 and accessed evidence through the web system on figure 24demonstrate that the native Linux utilities can successfully be configured to record specific user activities that may be reliably used to investigate incidents on enterprise systems hosted on the cloud.

Evidentiary Logs


←
Server: localhost:3306 » Database: jdeche_mscdctproject3 » Table: SystemEvents
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Triggers

←T→	ID	CustomerID	ReceivedAt	DeviceReportedTime	Facility	Priority	FromHost	Message	NTSe
☐ Edit Copy Delete	5759	*NULL*	2021-07-28 11:58:17	2021-07-28 11:58:17	1	6	ip-172-31-11-137	node=ip-172-31-11-137 type=SYSCALL msg=audit(1627...	
☐ Edit Copy Delete	5760	*NULL*	2021-07-28 11:58:17	2021-07-28 11:58:17	1	6	ip-172-31-11-137	node=ip-172-31-11-137 type=CRED_ACQ msg=audit(162...	
☐ Edit Copy Delete	5761	*NULL*	2021-07-28 11:58:17	2021-07-28 11:58:17	1	6	ip-172-31-11-137	node=ip-172-31-11-137 type=CWD msg=audit(16274734...	
☐ Edit Copy Delete	5762	*NULL*	2021-07-28 11:58:17	2021-07-28 11:58:17	1	6	ip-172-31-11-137	node=ip-172-31-11-137 type=PATH msg=audit(1627473...	
☐ Edit Copy Delete	5763	*NULL*	2021-07-28 11:58:17	2021-07-28 11:58:17	1	6	ip-172-31-11-137	node=ip-172-31-11-137 type=PATH msg=audit(1627473...	
☑ Edit Copy Delete	5930	*NULL*	2021-07-29 11:51:54	2021-07-29 11:51:54	5	6	ip-172-31-0-44	rsyslogd's groupid changed to 106	
☑ Edit Copy Delete	5931	*NULL*	2021-07-29 11:51:54	2021-07-29 11:51:54	5	6	ip-172-31-0-44	rsyslogd's userid changed to 102	
☑ Edit Copy Delete	5932	*NULL*	2021-07-29 11:51:54	2021-07-29 11:51:54	5	6	ip-172-31-0-44	[origin software="rsyslogd" swVersion="8.32.0" x...	
☐ Edit Copy Delete	5933	*NULL*	2021-07-29 11:52:27	2021-07-29 11:52:27	1	6	ip-172-31-0-44	ip-172-31-0-44,root,localhost,121,0,CONNECT,regi...	
☐ Edit Copy Delete	5934	*NULL*	2021-07-29 11:52:27	2021-07-29 11:52:27	1	6	ip-172-31-0-44	ip-172-31-0-44,root,localhost,121,0,DISCONNECT,r...	
☐ Edit Copy Delete	5935	*NULL*	2021-07-29 11:52:32	2021-07-29 11:52:32	1	6	ip-172-31-0-44	ip-172-31-0-44,root,localhost,122,0,CONNECT,regi...	
☐ Edit Copy Delete	5936	*NULL*	2021-07-29 11:52:32	2021-07-29 11:52:32	1	6	ip-172-31-0-44	ip-172-31-0-44,root,localhost,122,501,QUERY,regi...	
☐ Edit Copy Delete	5937	*NULL*	2021-07-29 11:52:32	2021-07-29 11:52:32	1	6	ip-172-31-0-44	ip-172-31-0-44,root,localhost,122,0,DISCONNECT,r...	
☐ Edit Copy Delete	5938	*NULL*	2021-07-29 11:52:33	2021-07-29 11:52:33	1	6	ip-172-31-0-44	ip-172-31-0-44,root,localhost,123,0,CONNECT,regi...	

Table 8: remote database storage of transmitted logs

Auditd deleted directory, Configuration file access and modification watch rules

The rules stated above and demonstrated in items 6, 7, 8 of the test case and results section on table 4 reveal that it is possible to explain user's activities based on the status of system calls triggered by those activities as they interact with systems. Deleted files and / or directories therefore, and modification of configuration files can be a pointer to an elaborate fraudulent activity or incident perpetrated by users that could be traceable using logs captured and securely stored remotely.

6.0 SUMMARY AND RECOMMENDATIONS

The need for ever increasing demands for computing resources, the abundance of computing power on cloud platforms and the inevitability of access to the said solutions by public sector institutions, require the development and operationalization of a reliable framework that can facilitate the execution of digital forensics investigations on cloud platforms.

Digital forensics evidence like any form of evidence that can be relied upon in a legal suit must apply two fundamental tests; authenticity (where the evidence originated) and Reliability (how the evidence was handled). The literature review conducted established that, existing models emphasize on the involvement of cloud service providers hence lack in the aspects autonomous log aggregation and persistent storage of evidentiary logs. This consequently puts at risk the evidence acquired and its ability to meet the reliability and authenticity tests. The framework advanced by this study provides a solution for provisioning of reliable digital forensics evidence that meets the tests aforementioned.

Further, logs captured as evidenced in the tests carried out provide a better chance of answering the investigative questions in the context of cyber crime investigations which are; the What, Where, When, Why, Who and How.

This section summarizes the research findings based on the research questions as well as the framework, and recommendations for future work.

6.1 SUMMARY OF FINDINGS

Existing technologies are either provisioned as; cloud based log aggregation solutions (logging as a service) where cloud service providers are centrally involved in the transmission and storage of evidentiary logs, on-premise software solutions with limited or no guarantee on prevention of sabotage and collusion by malicious users with intent to commit cyber crime or fraud as they interact with enterprise systems.

Research Question 1: What solutions can be used to acquire evidence for digital forensics from terminated virtual machines on cloud computing platforms?

Results obtained from the configuration of the native Linux utilities and application of audit rules against user activities on the simulated cloud environments demonstrate that, the framework and native applications on enterprise systems hosted on the cloud can be relied upon in acquiring and retaining digital forensics data from perpetrators of fraudulent activities even after computing resources are terminated.

Research Question 2: What mechanisms can be used to acquire digital evidence from virtual computing resources on cloud computing platforms through a persistent digital forensics process?

The framework advanced by this study and the results obtained from the prototype developed and tested have demonstrated that, cloud resources can persistently relay evidentiary logs that can aid in carrying out digital forensics. This can be achieved through appropriate configurations of native applications on the computing resources of IaaS clouds as illustrated in this research.

Research Question 3: What solutions can be implemented to ensure verifiable digital evidence from cloud computing platforms is acquired without direct intervention by Cloud Service Providers (CSPs)?

The web-based prototype that implements the framework advanced by this research comprises of logging utilities as well as a centralized log repository that is utilized to store evidentiary logs from cloud resources. The prototype demonstrates that intervention of Cloud Service providers in cloud forensics can be avoided. However, appropriate legislations and immutable configurations of logging utilities are essential considerations. The enabling laws will ultimately serve to compel all stakeholders including CSPs to enable such an un-attended and autonomous process.

7.0 CONCLUSION AND RECOMMENDATION

7.1 CONCLUSION

The overall objective of this study was to provide a framework for acquiring admissible digital forensics evidence from cloud computing platforms, focusing on the IaaS model, to aid investigative agencies in carrying out forensic investigations. Specifically, this study sought to demonstrate the possibility of retaining evidence from terminated cloud resources and acquiring of forensic evidence from the cloud regardless of the challenges associated with the multi-tenancy nature presented by the platform of interest (IaaS cloud).

Autonomous log aggregation, transmission from cloud computing resources and storage as demonstrated by the prototype and illustrated by the framework advanced by this study, can certainly provide a usable platform for achieving the objectives aforementioned. As emphasized in this research however, enabling laws will be essential in binding all stake holders to allow for successful operationalization of the proposed framework. The independence of the persistent cloud forensics process where cloud service providers' involvement is avoided as evidentiary digital forensics data is acquired, has also been demonstrated as an achievable endeavor.

7.2 RECOMMENDATIONS FOR FURTHER WORK

The practical application of the framework in a real problem domain will require the amendments and enforcement of relevant laws tonsure compliance by public sector institutions and all stakeholders involved. Existing legislation, such as the Computer misuse and Cyber crimes act of 2018contains relevant clauses on the management of critical enterprise software however, appropriate amendments will be required to ensure the creation of a remote evidence repository and the web-based access system as advanced by this study, is supported by law and that public sector institutions are obligated to allow for the storage of logs resulting from user activities as they interact with enterprise systems hosted on cloud platforms.

Additionally, a more secure implementation of the model using instances of the Rsyslog client and server will be worth exploring. These can provide for a more secure transmission of logs which could easily be a target for hackers. Ensuring total immutability of configuration files of utilities used on cloud resources will also require further research.

7.3 LIMITATIONS

This system comprises of multi-faceted environments namely; cloud resources hosting enterprise software for public sector institutions, a web-portal for access and management of logs generated from the systems hosted on the cloud. Further, a centralized log repository is also a critical component and is essentially a relational database management system that could be hosted on an internet domain or a data center.

As rapid transmission of logs occur from various systems of target institutions, both the database and the web application should be reposed on highly resourceful transmission links and capable servers. The entire framework will also work more securely if the logging utility Rsyslog is implemented in a client server mode. This will allow for secure transmission of logs and could also be configured further to avoid transmission losses.

REFERENCES

Balduzzi, M., Zaddach, J., Balzarotti, D., Kirda, E. & Loureiro, S.2012 A security analysis of amazon's elastic compute cloud service. In Proceedings of the 27th Annual ACM Symposium on Applied Computing, pp.1727-1434. Trento, Italy: ACM Press

Birk, D.& Wegener, C., 2011. Technical Issues of Forensic Investigations in Cloud Computing Environments. Workshop on Cryptography and Security in Clouds. 10.1109/SADFE.2011.17.

Bhatia, A. & Saggi, M., 2015. A Review on Mobile Cloud Computing: Issues, Challenges and Solutions. International Journal of Advanced Research in Computer and Communication Engineering, 4(6), pp.29–34.

Bousselmi, K., Brahmi, Z. and Gammoudi M. M., 2014. Cloud Services Orchestration: A Comparative Study of Existing Approaches. 10.1109/WAINA.2014.72.

Damshenas, M., Dehghantanha, A., Mahmoud, R., bin Shamsuddin, S. 2012. Forensics investigation challenges in cloud computing environments. In Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, Malaysia, 26–28 June 2012; pp. 190–194.

Grispos G, Storer T, &Glisson W., 2012. Calm before the storm: the challenges of cloud computing in digital forensics. International Journal of Digital Crime and Forensics (IJDCF), IGI Global: Hershey 2012; 4(2):28–48.

Foster, I., Zhao,Y., Raicu, I., &Lu. S. 2008. Cloud Computing and Grid Computing 360-Degree Compared, Grid Computing Environments Workshop, Austin, TX, USA, 2008, pp. 1-10, doi: 10.1109/GCE.2008.4738445.

Ramachandra, G., Iftikhar, M., & Khan., F.A. (2017) A Comprehensive Survey on Security in Cloud Computing, Procedia Computer Science, Volume 110, 465-472, http://dx.doi.org/10.1016/j.procs.2017.06.124

Tong, J., Mao, J., Bohn, R., Liu, F. & Messina, J. "NIST Cloud Computing Reference Architecture", *NIST Special Publication 500-292*, US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, July 2011.

Marty, R. 2011. Cloud application logging for forensics. In Proceedings of the 2011 ACM Symposium on Applied Computing, Taichung, Taiwan, 21–24 March 2011; pp.178–184.

Mell, P., & Grance, T., 2011. The NIST definition of cloud computing. National Institute of Standards and Technology, 53, 50.

Wall, D. S. 2017. Towards a Conceptualization of Cloud (Cyber) Crime. 529-538. 10.1007/978-3-319-58460-7_37.

Zwattendorfer, B., & Tauber, A., 2013. The public cloud for e-government. International Journal of Distributed Systems and Technologies (IJDST), 4(4), 1-14.

Zawoad, S., Dutta, A.K. & Hasan, R., 2016. Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service. *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp.148–162.

Zawoad, S., Hasan, R.& Skjellum, A. 2015. OCF: An Open Cloud Forensics Model for Reliable Digital Forensics. 10.1109/CLOUD.2015.65.

Zawoad, S., Dutta, A.K. and Hasan, R., 2016. Towards Building Forensics Enabled Cloud Through Secure Logging-as-a-Service. *IEEE Transactions on Dependable and Secure Computing*, 13(2), pp.148–162.

Zawoad,S., & Hasan, R.2016. Trustworthy Digital Forensics in the Cloud. Computer, 49(3), pp.78–81.

Marinescu, D. 2013. Cloud Computing: Theory and Practice. Cloud Computing: Theory and Practice. 1-396.

Market Research Media, “Global cloud computing market,” http://goo.gl/AR3FBD, [Accessed March 22, 2021] https://marketresearchmedia.com/global-cloud-computing-market/

Mell, P. & Grance, T. 2011. The NIST definition of cloud computing (draft). NIST Special Publication, 800, 7.

Schreier M. 2013. Qualitative content analysis in practice. London: Sage.

Mutulu P. 2020. A Multi-Tenancy Cloud Trust Model Using Quality of Service Monitoring: A Case of Infrastructure as a Service (IaaS)

Microsoft, 2017. Using Cloud Services to Advance Digital Transformation in Government. Available at http://www.govtech.com/library/papers/Using-Cloud-Services-to-Advance-Digital-Transformation-in-Government-81067.html?promo_code=GOVTECH_web_library_list. Accessed: 6/07/2021

Simou, S., Kalloniatis, C., Kavakli, E.,& Gritzalis, S. 2014. Cloud Forensics: Identifying the Major Issues and Challenges. 271-284. 10.1007/978-3-319-07881-6_19.

Simou, S., Kalloniatis, C., Gritzalis, S. and Mouratidis, H. 2016. A survey on cloud forensics challenges and solutions. Security and Communication Networks, 9(18), pp.6285–6314.