GSJ: Volume 12, Issue 3, March 2024, Online: ISSN 2320-9186

www.globalscientificjournal.com

A MODEL APPROACH TO ADDRESSING CLOUD FORENSICS CHALLENGES

Richard Omollo and Shem Aketch
Department of Computer Science and Software Engineering
Jaramogi Oginga Odinga University of Science and Technology, KENYA.

ABSTRACT

Cloud computing environment has become prospective battle field for cyber attackers with the rapid growth of cloud adoption in both private and public sectors; the major challenge being data protection from various attacks. This paper attempts to provide a possible solution for such threats by exposing various issues related to data security in cloud and the various challenges faced by forensic experts in cloud. The main objective of the paper was to identify challenges and solutions for cloud forensic and log management. This paper is descriptive in nature. Cloud forensics is more complex because of its features such as location independence, elastic resource provision and loss of control. Regulations are required for secured access of cloud services. New mechanisms are also needed for safe custody of logs until produced in the court of law. This study is essential to the Information Technology field, particularly network administrators and security staff of networked organizations to have this course in practice making sure that they have the challenges pertaining to this on their finger tips for decision making.

KEYWORDS: Cloud, Digital Forensics, Model, Challenges

1.0 INTRODUCTION

Cloud computing environment (use of Web-based application for every task rather than installing software or storing data on a computer) has a large impact on digital forensics. In recent times, cybercrime has increased dramatically in the media and with the ever-increasing rate of cybercrimes, from phishing to hacking and stealing of personal information not only confined to a particular country but the globally at large, there is a need for forensic experts to be available in public and private organizations (B. Greer, 2017). Spam email or phishing is a fraudulent scheme used by attackers to solicit personal or financial information to commit victimization or identity theft (Broadhurst and Alazab, 2017). However, there are certain stigmas attached to these crimes that make it harder for the attacked to cope with their situation. Most often because of the portrayals of crimes that idealize (Joseph C. S., 2007) cybercrimes and do not necessarily show all of the effects of these crimes on the attacked or their environment.

Both digital forensics and cloud computing environment are much more complex than how they are portrayed. They produce copious amounts of side effects that bring a lot of challenges to the Information Technology (IT) professionals through readjustments; some of which are not publicized as others are due to professional and employee negligence. Information Technology professionals and employees may decide to crimple an organization, changing how other employees perceive one another, how they act and even how they communicate. However, through different types of crimes and criminals, communication in situations like these is essential to understanding one another. According to Keyun et.al. (2011), cloud computing is appealing to the organizations and the individuals to shift their business due to its significant features including processing speed, storage, infinite elasticity and most prominently the mobility which allow the user to access it from anywhere and any-time. All these features compel the user to adopt this emerging technology.

Cloud computing is far and wide adapted by many people around the globe with continuously growing and emerging technology and this has generated a security concern for the stored data in cloud environment. When security attacks or policy violations occur, it is indispensable to conduct a digital forensic investigation. Internet users make use of cloud services such as Amazon Cloud Drive, Office 365, Google Drive and Dropbox and from a digital forensics point of view, these services present a number of unique challenges, as has been reported in the 2014 National Institute of Standards and Technology's draft report (NIST, 2014). Due to the distributed nature of cloud services, data can potentially reside in multiple legal jurisdictions, leading to investigators relying on local laws and regulations regarding the collection of evidence (Syed, A.A. et al., 2017).

This study is essential to the Information Technology field, particularly network administrators and security staff of networked organizations to have this course in practice making sure that they have the challenges pertaining to this on their finger tips for decision making in the world where 60% of Companies to face talent shortage of Cyber Security professionals in 2019 (Kenya Cyber Security report 2018). The study explores digital forensic (technical, legal and administrative) challenges in a cloud computing environment, help assess the challenges that come with digital forensics and find out what happens to the cloud computing when subjected to the challenges.

2.0 LITERATURE REVIEW

Digital Forensics and Cloud computing are reviewed separately here due to the tremendous differences in the two. In this study, we compared against one another to cross analyze the similarities and the differences in digital forensic challenges in cloud computing environment.

2.1 DIGITAL FORENSICS

Suleman K. et al., (2014) defined digital forensics as a method of discovering digital evidence from the digital devices without any compromise on its integrity. Digital devices may be a computer, laptop, smart phone, smart watches and wearable, digital camera and storage medium. The digital devices are vital for creation of digital evidence because they are booty (they contain remnants that can help in an examination), contains data that is a proof of a crime and lastly, they may have been utilized to encourage a crime. According to Pichan, A. et al., (2015), digital evidence can be determined as the valued information for the investigation perspectives which is received, kept on, and transmitted by the digital devices. Saurav N. & Raymond A. (2017) classified digital forensic as Computer forensics, Mobile forensic, Memory forensics, and Network forensics. For forensics activity, the overall computer forensics process is sometimes viewed as comprising four stages: Acquisition (Identification and Preservation), Analysis (Technical Analysis), Evaluation (What the Lawyers Do) and Presentation (Presenting digital evidence in a manner that is legally acceptable in any legal proceedings).

2.2 CLOUD COMPUTING

Cloud computing is endlessly mounting and up-and-coming technology. Hardware and software resources that provide diverse services over the network or the internet to address the user requirements are called "Cloud" (Saurav, N. & Raymond, A., 2017). Here, resources refer to computing applications, network resources, platforms, software services, virtual servers and computing infrastructure. The cloud computing can be conceived as pay-go-use model wherein the clients pay for the requested resources. Cloud computing eliminates the costs and complexity of buying, configuring and managing the hardware and software. Cloud computing refers to sharing or distributing computing resources among the various clients. NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Peter, M. & Timothy, G., 2011).

From the definition, National Institute of Science and Technology (NIST) defines five characteristics of the cloud including on-demand self- service, ubiquitous network access, resource pooling, rapid elasticity, and metered service. Service models are categorized by the type of computing resources provided to the end users. Syed, A.A. et al., (2017) gives three cloud computing services model consisting of infrastructure, platform and software as a service. Infrastructure as a service (IaaS) entails clients provided with the hardware structure like processing, storage and network capacity on rental basis. The server(s), storage and hardware are delivered as a service e.g., Amazon Simple Storage Service (S3). Platform as a Service (PaaS) allows the client to deploy applications of customer in the cloud. the development platform is provided as a service e.g. Microsoft Azure. In Software as a Service (SaaS), clients are allowed to use cloud service provider's application in a network. Applications are delivered as a service over the Internet e.g., Google Mail. There are four well-known deployment models used in cloud computing namely; Public, Private, Hybrid, and Community clouds (Sheik, K. et al., 2016). In Public cloud, resources are shared among multiple tenants. The infrastructure is placed on the premises of the Cloud Service Provider (CSP). Users do not have control over the location of the infrastructure. In Private Cloud, resources (including hardware, storage, and networks) are delicately provisioned to a single client or a company. Private cloud offer better security. Public and private cloud jointly forms the Hybrid cloud that allows data and application.

2.3 CLOUD FORENSICS

2.3.1 OVERVIEW

Cloud forensics is a cross discipline of cloud computing and digital forensics. Cloud computing environment is becoming a new theatre of war of cybercrime where new challenges are being posed to defend the cyber attacks. Cyber criminals can be described as a person(s) who legitimately involves in destruction of privacy or security of data and utilizing unauthorized resources causing loss to the digital users. To meet the challenges of digital data threat, digital forensics methods are applied over the remote servers of cloud giving way to a new term called "Cloud Forensics". The cloud can be used as subject, object and the tool (Suchana, D., 2016). The cloud behaves as an object when the Cloud Service Providers are directly influenced by the distributed denial of service (DDoS) attacks. A cloud plays a role of subject, if criminal activities have been done within the cloud e.g Identity theft of the cloud users. If the crime is committed by using cloud, the cloud is considered as a tool.

Highly distributed cloud architecture poses forensic as a difficult job (Saurav, N. & Raymond, A., 2017). According to the NIST "cloud computing forensic is done through identification, collection, preservation, examination, and interpretation and reporting of digital evidence. The application of digital forensic science in cloud environments is a subset of network forensics. Four different aspects of the cloud forensics have been coined as Technical, Administrative (Management/Organizational) and Legal. The technical dimension involves developing tools and methods to carry out the forensic process in cloud environment. Tools are needed for evidence acquisition, data recovery, evidence examination, evidence analysis and evidence segregation. In administrative dimension, the hierarchy of administration staff, their association and role in cloud forensics are defined. Apart from internal structure of a cloud, its association with other clouds is also explored. The organizational dimension encompasses interaction between the cloud actors (CSP, customer, and legal advisor) in order to accomplish the forensic investigation. The legal dimension encompasses the development of rules, regulations and agreements to assure that the forensic activity is done according to the law.

In cloud forensic, both machine and the process are beyond the access of the investigator. Saurav, N. & Raymond, A. (2017) identified three challenges of cloud forensic namely Distributed architecture, deficiency of handling big data and lack of forensic tools and services. The investigator has to depend upon CSP in order to do his forensic activity. Reilly, D., 2011 gave Features of Cloud computing that are not favorable for forensic investigations and include evidence search and seizure procedures are impractical, Maintenance of chain of custody is also very difficult to track, There is a general loss of control for investigation due to remote data centers and Lack of cloud forensic tool to support in cloud investigations.

There are various usages of cloud forensics. We summarize them as follows: Investigation, Troubleshooting, Log Monitoring, Data and System Recovery and Due Diligence/Regulatory Compliance.

Cloud forensic challenges can be grouped into three namely; technical, administrative (organizational) and legal challenges.

i) **Technical Challenges:** The cloud forensic investigations prove to be difficult mostly because of the inherent features of cloud architecture. The evidence data can be at rest (Stored in storage device), in transit (sent across a network) or in process (executed in a processor). This means that each of them requires different type of tool to capture the data. Further based on the cloud layer the evidence may be present in the RAM, storage of server, in the Virtual Machine (VM) or a part of the client application. Further the data can be volatile or non-volatile. Registry entries, processes, temporary internet files are examples of volatile data. Then there is the issue of capturing the data before the server or VM that is hosting it is shut down or rebooted. It is observed that the evidence can be collected relatively easily at IaaS layer that is of lower abstraction than that of SaaS which is of higher abstraction. Ruan K., et al., (2011) say that the SaaS users are not aware of the location of forensic data, log files and metadata to monitor their sessions. There is a universal claim that the Cloud Service Providers (CSPs) intentionally hide the details from the users. The distribution of data centers across the globe makes the data collection more difficult. The investigators have to get a warrant for cloud data access from sites with different jurisdictions and laws. Getting a warrant is usually time consuming and costly and lead to loss of data (Simou, S., 2014). Further, the investigators have to rely on CSP for investigation. The CSPs may not be willing to extend the support due to the fear that it may be used against them. Further there may be availing services of other CSPs. Then all the parties are to be involved. They also state the problems in preserving the data without compromise from the CSP. Proper security mechanisms are needed to protect the evidence. Further timelines are needed to maintain the chain of event across different time zones. It is also important to note that co-users of a session under investigation should not be affected in any way by the investigation procedures.

ii) **Administrative Challenges:** In order to establish a forensic capability, each cloud organization, including the providers and customers of cloud services, is required to define a structure of internal staffing, provider-customer collaboration, and external assistance (Investigators, IT Professionals, Incident Handlers, Legal Advisors and External Assistance) in the Cloud Forensics Investigations. The cloud providers have no specific employees to handle cloud forensics. Cloud is vulnerable to risks, attacks and scandals. Apart from managing globally distributed data centers, Cloud should have dedicated personnel to handle each of these problems for better operation. Internal security professionals are needed to protect cloud from various types of attacks. Incident handlers are needed to handle complaints on mismanagement of cloud like data leakage, data loss, storing objectionable content, internal staff threats etc. It is also essential for the CSP to build goodwill with the internal staff and users to avoid these problems.

iii) **Legal Challenges:** Eecke (2015) listed a number of legal issues to be addressed due to the multi-jurisdiction and multi-tenancy nature of cloud. The cloud providers are held responsible for hosting the illegal data and therefore a distinction is needed to find who is responsible. Easy registration service systems allow users to create multiple, proxy accounts that may be used for malicious purpose. At present, issues are raised on storing of objectionable content. However, there is no notice on execution of harmful processes. On the other side, CSPs maintain the overall control and include clauses to terminate services without further clarification.

The terms and conditions of a cloud service are bound by Service Level Agreement (SLA), signed by the cloud user and provider. Usually, SLA contains the details of the service and delivery conditions. Researchers have identified the limitations of clauses in terms of security and cloud forensics. The SLA clauses must protect the CSP from legal action due to malicious activity of a cloud user. The clauses should also grant CSP rights to remove/block the objectionable content. (Ruan K., et al., 2011) say that there are no terms and conditions in SLA regarding the segregation of duties between CSP and user. Terms of use to enable general forensic readiness in the cloud is missing. Providers do not provide interfaces to gather forensic data as they have no control over the location of data.

2.3.2 CLOUD CRIME

The cloud picks up has potential implications for changes in the organization of cyber-crime and the organization of (cyber) criminals. The organization of cybercrime and cybercriminals is very different to the organization of crime offline. Whilst there has been a tendency by media to sensationalize cybercrime by linking it with mafia groups, the literature covering this issue suggest that the nature of cybercrime and conceptualizations of traditional organized crime groups are highly mismatched (Wall, 2015). Indeed, the literature points to new forms of organization online that follow the distributed (networked), globalized and informational patterns of cyber-crime. So, using the transformation terminology once again, we can talk about cyber-assisted forms of organization, where crime groups use technologies to assist their existing operations, including some traditional organized crime groups taking their existing areas of crime business online. There are also examples of cyber-enabled organization, where new groups of criminals use the internet networks to organize themselves to commit financial crimes. They obtain personal information online (say, though Phishing), then give it to offline money mules to monetarize the information. Take away the internet and they would commit the same crimes more locally and in much smaller volumes. Finally, there are cyber-dependent organized crime groups, who commune online and commit crimes online. They are likely never to have met and are often unlikely to know each other's identity other than by pseudonym.

The definition of computer crime by Casey (2000) can be extended to cloud crime. Cloud crime is any crime that involves cloud computing. The Cloud can be the object, subject or tool of crimes. The Cloud is the object of the crime when the CSP is the target of the crime and is directly affected by the criminal act, e.g. DDOS (Distributed Denial of Service) attacks targeting part(s) of the Cloud or even the entire cloud. The Cloud is the subject of the crime when it is the environment where the crime is committed, e.g., unauthorized modification or deletion of data residing in the Cloud, identity theft of users of the Cloud. The Cloud can also be the tool used to conduct or plan a crime, e.g., evidence related to the crime can be stored and shared in the Cloud and a Cloud that is used to attack other Clouds is called a dark Cloud.

The same way cybercrime may be understood as a new way of committing traditional crimes such as fraud and theft, cloud computing presents criminals with new tools with which to commit these offences (Alhadeff, J., 2009). Despite this, little work has been carried out in relation to the implications of cloud computing for LEAs and criminal investigation (Sherman, A. & Dykstra, J., 2012). However, it has been suggested that many current law enforcement procedures have not been adapted to investigate attacks on cloud services (Choo, K.R., 2010).

Analogous to cybercrime generally, cloud systems may be both the object and the subject of criminal activity (Choo, K.R. et al., 2007). Rogue elements may target cloud systems with the intention of capturing or corrupting data (Sherman, A. & Dykstra, J., 2012). This can be achieved through the use of malware. Criminals may also use cloud computing systems to store illicit or illegal data (e.g. child exploitation material) or, due to the quantity of processing power often available in a cloud computing environment, use the cloud as the base for a "brute force attacks" to crack passwords and encryption (Choo, K.R., 2010). The scam operated by using phishing emails which infected the victim's computers with a Trojan capable of mimicking the website of the victim's bank.

A report of Cloud Security Alliance (CSA) in 2016 publishes following treacherous threats (Irfan et al., 2016): Data Breaches, Weak Identity, Credential and access management, Insecure interface and APIs, system and application vulnerability, account hijacking, malicious insider, advanced persistent threats, data loss, insufficient due diligence, Abuse and nefarious use of cloud service, Denial of Service (DOS) and Shared technology issues

2.3.3 CLOUD FORENSIC PROCESS

The Digital Forensic Investigation Framework (DFIF) (Rahayu, S.S. et al., 2008) groups and merges the same activities or processes that provide the same output into an appropriate phase. The proposed map simplifies the existing complex framework and it can be used as a general DFIF for investigating all incident cases without tampering the evidence and protect the chain of custody. The framework consists of five phases which are preparation, collection and preservation, examination and analysis, presentation and reporting and disseminating the case.

In 2010, Digital Forensic Evidence Processes (Cohen, F.B., 2010) defined nine stages, identification, collection, preservation, transportation, storage, analysis - interpretation and attribution, reconstruction, presentation and destruction. All of these should be done in a manner that meets the legal standards of the jurisdiction and the case.

Aleksandar, V. & Venter, H.S., (2012) introduced Harmonized digital forensic investigation process model in 2012 and proposed several actions to be performed constantly and in parallel with the phases of the model, in order to achieve efficiency of investigation and ensure the admissibility of digital evidence. The phases defined in terms of scope, functions and order. These are: incident detection, first response, planning, preparation, incident scene documentation, identification, collection, transportation, storage, analysis, presentation and conclusion.

The Forensic Investigations Process (Hong, G. et al., (2012) in cloud environments was based on the Forensic Process with the four stages. Due to the evolution of cloud computing the stages were changed to apply basic forensic principles and processes. The four distinct steps are: (a) determine the purpose of the forensics requirement, (b) identify the types of cloud services (SaaS, IaaS, Paas), (c) determine the type of background technology used and (d) examine the various physical and logical locations, which are client side, server side and developer side.

In 2012, Cloud Forensics Process (Chen, G. et al., 2012) focused on the competence and admissibility of the evidence along with the human factor. The process consists of four stages which includes (a) ascertain the purpose of the cloud forensic, (b) ascertain the type of the cloud service, (c) ascertain the type of the technology behind the cloud and (d) carry out specific investigation on the base of stage c such as ascertain the role of the user, negotiate with the CSP, and collect potential evidence. In 2012, the Integrated Conceptual Digital Forensic Framework for Cloud Computing (Ben, M. & Choo, K., 2012) proposed, based on McKemmish and NIST. It emphasizes on the differences in the preservation of forensic data and the collection of cloud computing data for forensic purposes. It consists of four stages, identification and preservation, collection, examination and analysis, reporting and presentation.

S. Simou et al., (2014) proposed a model similar to DFWR model with three additions: collection phase in the preservation stage, analysis stage in the examination stage and finally the decision stage is excluded, due to the fact that it cannot be considered "forensic". This model is convenient for analyzing and associating challenges in cloud forensics and was derived based on the suggestions and drawbacks located from the investigation of similar approaches presented before. The model consists of four steps:

(i) *Identification* which is the first stage and deals with identifying all possible sources of evidence in a cloud environment in order to prove that the incident took place.

(ii) *Preservation – Collection* which deals with the collection of the evidence, from the locations they reside in clouds, the different types of media and the tools used to do so.

(iii) *Examination – Analysis* which involves the extraction of data from the previous stage and the inspection of the huge amount of data identified in order to locate the proper evidence for the incident occurred.

(iv) *Presentation* stage which is the final stage and deals with the presentation of the evidence in a court of law.

Pichan et al. (2015) present digital forensic model for cloud computing that consists of:

(i) Identification
(ii) Preservation
(iii) Collection or acquisition
(iv) Examination and analysis
(v) Reporting and presentation.

Pichan et al. describes the sub process activities, the challenges and recommended solution in each phase of the process. Manoj, S.K.A. & Bhaskari, D.L. (2016) proposed a model for investigating cyberattacks in cloud environment.

The main actors and their roles in the proposed model are:

(i.) *Cloud Customer* (CC) which is the end user who benefits the cloud services and should have a unique identity,

(ii.) *Trusted Third Party* (TTP) is involved to help ensure identification and sort out the security breaches with occasional help from cyber forensics team,

(iii.) *Cloud Service Provider* (CSP) which is the owner of the servers and databases which he lends on rent basis, the CSP should register itself to TTP in-order to offer services to CC's.

(iv.) *Cloud Forensics Investigation Team* (CFIT): The CFIT team will come into action when it receives a request from TTP to deal with suspicious activities in cloud. The CFIT is also have the privilege of using the latest tools as TTP will always have the latest updated versions of forensics software.

Arafat, Y. et al., (2017) proposed a framework based on technical challenges to perform forensic investigation process in cloud computing environment using digital evidence which included seven phases including: Identification, Collection, Preservation, Understanding, Examination, Reporting and Close. The model identified common technical challenges and proposed possible solutions to the challenges but failed to address the administrative (Organizational) and legal challenges.

Cloud forensic is the search to reliable evidence within the electronic information; this may result to infringing on personal privacy and challenging fundamental legal principles to protect forensic data. The investigations undergo legal and policy development to interconnectivity. Cybersecurity protects systems and networks against unauthorized access, data manipulation, and defense against any hacker or intruder (Olayemi, 2014). Hence IT managers and business outfit and government agencies should ensure overall system integrity and sustainability of their network infrastructure. Also, organizations should increase its defense –in- depth approach to network and computer security with the adoption of appropriate cybersecurity wares. More so, given that collecting evidence the digital media is properly examined and checked to identify, preserve recover and analyze facts and opinions about the information gathered. The evidence is usually difficult to collect as the right tools are not available to collect them or they are of low quality or as revealing the identity of the criminal is difficult.

3.0 RESEARCH METHODOLOGY

This study used the qualitative exploratory case study research method. A qualitative approach helped in establishing exploratory actions in understanding the meaning behind actions and behaviors in employing strategies by IT managers in a cyber forensic investigation, hence ensuring reliability in data collection. The research method was also used for conducting interviews was to obtain unique and comprehensive information from the participants undergoing the interview (Tuominen, Tuominen & Jussila, 2013). The justification for selecting qualitative rather than quantitative or mixed methods was by the preference to collect multiple sources of data. From the description of Malina, Hanne, and Selto (2011), mixed method researchers employ emphases on both qualitative and quantitative approaches to create a research outcome stronger than either method individually. The preferred method of the study was the qualitative method not quantitative or mixed method because researchers use the qualitative method as a means to involve directly with the participants (Toloie-Eshlaghy et al., 2011). The qualitative method was used to seek an in-depth understanding of IT managers based on an insider's experience and perception of the phenomenon.

This paper uses the case study research design for the study. A case study design is an increasingly popular approach among qualitative researchers (Hyett, Kenny, & Dickson, 2014). Using a case study design has a level of flexibility that researchers may not have with other research methods such as phenomenology, narrative, and ethnography design (Hyett et al., 2014). The qualitative research method was used to establish exploratory actions by researchers to understand the meaning behind actions and behaviors and to see the phenomenon from the perspective of the participants (Sinkovics & Alfoldi, 2012). The method allows the use of an in-depth exploration of the phenomenon by actively engaging with participants who have experiences with the phenomenon and expresses their perceptions in their understanding (Cohen, 2010). This paper uses the qualitative method to explore actions to understand the meaning behind actions and behaviors and to see the phenomenon from the perspective of the IT managers which both quantitative and mixed method which cannot of providing (Sinkovics & Alfoldi, 2012). Quantitative research method, on the contrary, is used by researchers to represent the generalization of a population with the use of numerical data to prove or disapprove a hypothesis (Hoare & Hoe, 2013).

3.1 PROPOSED CLOUD FORENSICS MODEL

While a number of studies have investigated digital forensics challenges, there remains little in the way of research concerning digital forensics challenges in cloud environments. As such, the aim of this research is to propose a model to investigate the factors that influence organizations to undertake cloud forensics. The proposed model to aid the investigation of the technical, legal and organizational factors that influence the challenges of forensics of cloud computing consumers are discussed below. This section is divided into two namely: model development and cloud forensic model.

3.1.1 MODEL DEVELOPMENT STAGES

According to private institutions in charge of computer forensics, said it must preserve, obtain and submit data that have been properly processed and electronically documented. The phases of computer forensics are as follows (Román, R.F.M., 2016): *Identification, Preservation, Analysis* and *Presentation.* The Model development process, as shown in Figure 1, is divided into four phases and challenges per stage. Alex, M.E. & Kishore, R. (2017) gave the challenges and sub challenges in cloud forensic are described in Table 1. Crime scene reconstruction, Chain of custody, cross border law and Law presentation are some other major challenges.

Based on the Roman (2016) proposed model, the following are some of the cloud forensic challenges as per stage:

i) Identification Stage

Decentralized data: Allows data to be created, stored, processed and distributed over several data centers and physical machines. Stored data is replicated, distributed and fragmented. A Log frame work is recommended to curb the challenge

Deleted data: Deleted data can be collected from the media using data carving methods and difficult to achieve and manage of snap shot images. Frequent snapshots

Dependence on CSP: Good SLA guarantees benefit accessibility and consistence. SLA specifying the specific forensic Services is preferred.

Inaccessibility: Snapshot or forensic image is a process of taking a clone of virtual image including running system's memory, and saving the clone to a persistent storage. By data imaging tools such as EnCase, FTK Imager, X-Ways, F- Response, Paladin etc., over a secure network link. Snapshot analysis and Remote data acquisition are the best solution.

Multi-tenancy and resource sharing: Adds to the complexity of forensics data collection and easy to seize the hardware. Popular method of isolating the instance and supported by the vendors. Isolation of cloud instance and Sandboxing.

Unknown or not accessible physical location: Adversely affects CSPs ability to ensure flexibility, service availability and manageability. Most of the SLA guidelines are mainly focused on security requirements and less on forensic requirements. Resource tagging, Robust SLA with CSPs and SLA in support of cloud forensics are possible solutions

ii) Preservation Stage

Chain of custody: this can be used to verify the chain of custody and data integrity. RSA Signature

Data integrity: Live forensic techniques and cloud provider's expertise use their own crucial environment. Investigators should be exposed to Live forensic training.

Data volatility: Having a persistent storage and keeping the storage synchronized frequently between the VM instances and persistent storage have been suggested by researchers to counter the data volatility issues. Persistent storage

iii) Analysis Stage

Cryptography: there should be a better way to check the suspect's phones or tablets for unencrypted files or data or passwords. Brute-force and Mobile forensics.

Encrypted data: Possible more future implementation. Cloud key management infrastructure

Evidence time lining: End-to-end log helps to create a time line of events. To curb the challenge, the CSPs should provide the ownership and history of data Objects. Logs should be secured with proper time stamps. Secure Provenance

Lack of Log Frame work: Creates challenges in time lining of events and logs really help an investigator to connect the dots. Comprehensive Log Management system

Partial evidence: An examination with partial evidence is real risk because partial or incomplete evidence may be inadmissible in court.

Recovery of deleted data: More complex task in cloud computing environments and recovering of deleted data from backups, repositories, previous snapshots or other handsets or computer can solve. Backups and Repositories and Snapshots and Mobile forensics and computer forensic

Return to early stages of investigation

iv) Reporting Stage

Jurisdiction: there is a challenge in Legal Agreements and a challenge in presenting the case. Cross border law, international relations should be put in place to help reduce jurisdiction challenges.

Crime scene reconstruction: Lack of applicable tools and supporting process and guidelines and reconstruction of cloud storage and evidence. Framework, process and guidelines, supported by tools and technology are the proposed solution.
Complexity of cloud: Difficult to explain the complexity of cloud to Jury. Time lining of events Evidence returns and secure deletion: Returning of the evidence is not always needed. Legal training and Legal advice

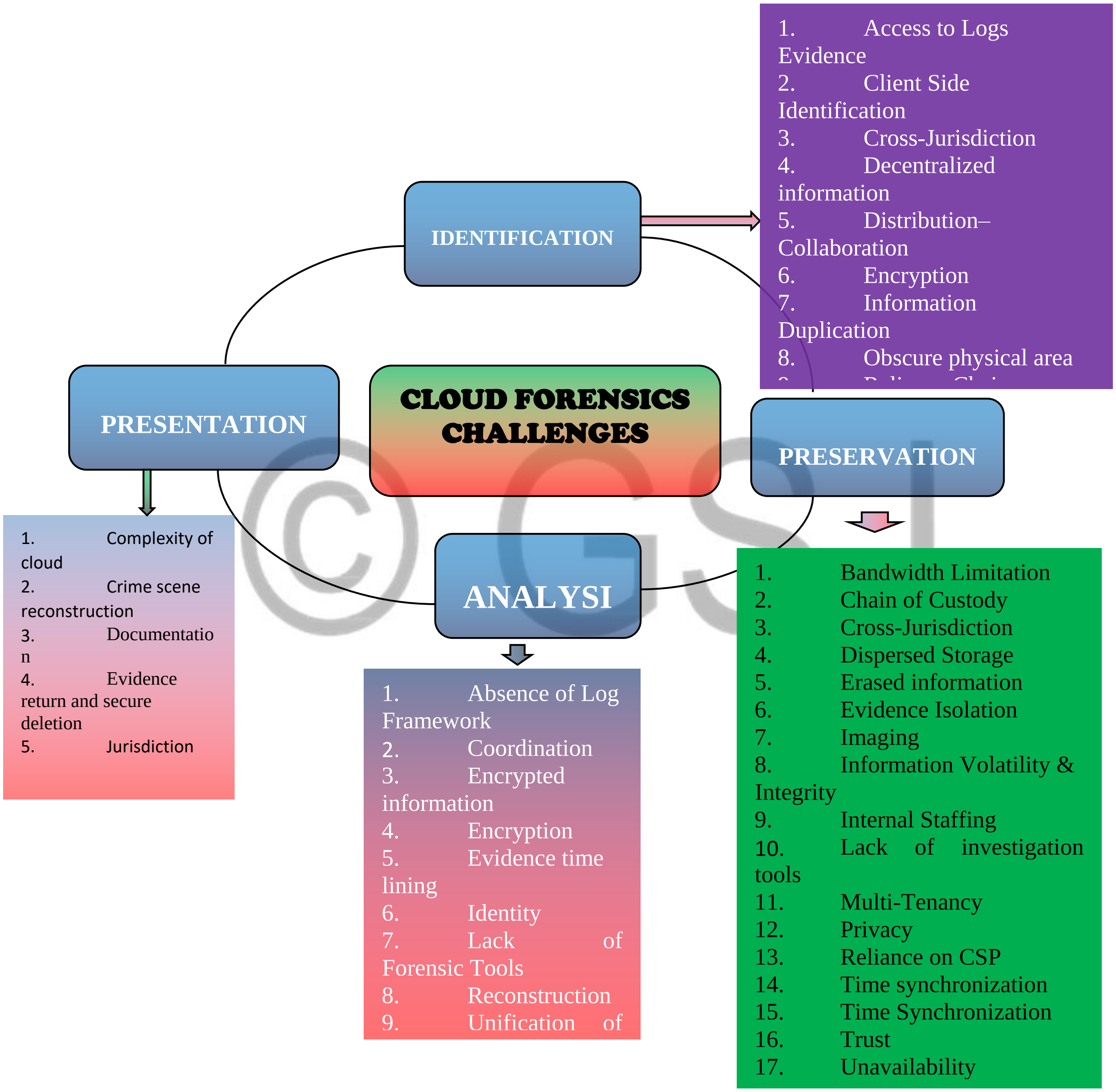

Figure 1: Computer Forensics Challenges Model

2.3.4.2 PROPOSED CLOUD FORENSIC MODEL

The proposed Cloud Forensic Challenges model, as illustrated in Figure 2, includes three categories, namely, technical, legal and organizational factors. These factors act as a cloud forensic readiness and are discussed below:

i) *Technical Factors:* These are the technological aspects that influence forensic readiness in cloud environments. They include: *Cloud infrastructure (*preparing the underlying infrastructure to support digital forensics investigations. Infrastructure preparation includes networking, system and laboratory), *Cloud architecture (*the system architecture must be designed in a specific way so as to increase its forensics capabilities, which results in the obtaining of admissible digital evidence), *Cloud Forensic technologies (*these include specialized forensic software or tools which are vital when it comes to collecting evidence in any digital investigation. It can be difficult to conduct a digital investigation without proper technology, and as a result these technologies should be reliable and accurate in order to provide admissible evidence) and *Cloud security (*security programs are utilized in the digital forensics field as a trigger alarm. Thus, in order to conduct a digital investigation, incidents must first be detected by a monitor system in a timely manner. This can be achieved by using various technologies such as Intrusion Detection Systems (IDS), as well as Anti-virus and Anti-Spyware technology).

ii) *Legal Factors:* These include the aspects that are related to agreements between consumers and providers, multi-jurisdictions and regulatory authorities. They include: *Service Level Agreement (SLA) (* a contract between a Cloud Service Providers (CSPs) and customers that documents what services the provider will offer, including forensics investigations. The SLA should clearly specify CSP and customers' responsibilities associated with forensic investigations), *Regulatory (*adherence to laws and regulations, such as admissibility of digital evidence in court and the chain of custody) and *Jurisdiction (*judicial region. Since CSPs may provide cloud services from another region or area, it is necessary for organizations to determine the judicial regions, if any, and consider all multi-jurisdictions).

iii) *Organizational Factors:* they illustrate the characteristics of an organization and its employees that can facilitate cloud forensic readiness. They include: *Management support (refers* to the top management level of an organization's support structure – the structure which helps the organization to become forensically ready. This includes authorization, decision making and funding), *Readiness strategy (*an organization's plan to achieve forensics readiness. Generally speaking, the strategy pertains to how the readiness would work. This includes identifying hypothetical scenarios, possible evidence sources, and budget planning), *Governance* (concerns about the implementation of cloud forensics readiness in an organization. This includes managing procedures and responsibilities in order to collect evidence and attain a successful forensic investigation), *Culture* (the pattern of beliefs, values, assumptions and practices that have a direct impact on the implementation of digital forensics. Understanding culture before implementing digital forensics is very important, as it leads to successful potential forensics investigations), *Training (*the provision of training programs to technical staff and awareness programs to nontechnical staff on forensics best practices) and *Procedures (*a number of guidelines, procedures and instructions designed to guide the digital forensics investigations. These include proactive and reactive forensic procedures).

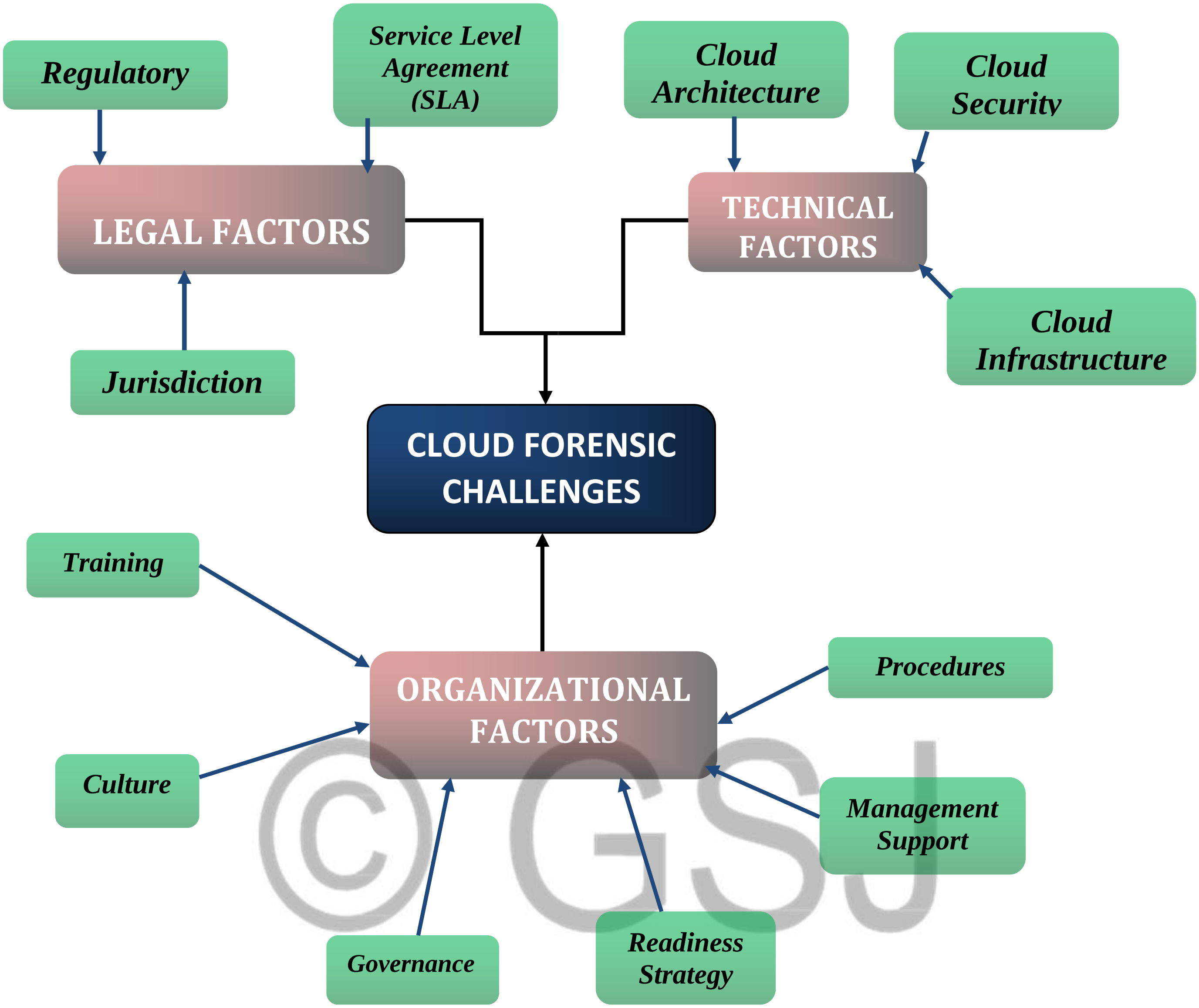

Figure 2: Proposed Model on Technical, Legal and Organizational Challenges

4.0 CONCLUSION

Challenges and available solutions for cloud forensic investigations and log management are explored in this paper. It is clear that cloud forensics is more complex because of its features such as location independence, elastic resource provision and loss of control. Further studies should propose a solution for new forensic tools to be developed for effective cloud forensic investigations. Focus is also required in devising improved international law standards, amending SLA to incorporate forensic clauses. Regulations are required for secured access to cloud services. New mechanisms are needed for safe custody of logs until produced in the court of law.

REFERENCES

Aleksandar, V. & Venter, H.S. (2012) Harmonized Digital Forensic Investigation Process Model. *Information Security for South Africa (ISSA).* IEEE.

Alex, M.E. & Kishore, R. (2017). Forensics framework for cloud computing. *Comput. Electr. Eng.* 60, (2017), 193–205. DOI:https://doi.org/10.1016/j.compeleceng.2017.02.006

Ameer, P., Mihai, L. & Sie, T. (2015). *Cloud Forensics: Technical Challenges, Solutions and Comparative Analysis.* Digit. Investig. 13, (2015), 38–57. DOI:https://doi.org/10.1016/j.diin.2015.03.002.

Ben, M. & Choo, K. (2012). An Integrated Conceptual Digital Forensic Framework for Cloud Computing. *Digital Investigation* 9(2). pp 71–80

Birk, D. & C. Wegener (2011*)*. Technical Issues Of Forensic Investigations In Cloud Computing Environments in Systematic Approaches to Digital Forensic Engineering (SADFE). *2011 IEEE Sixth International Workshop on IEEE*.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology*. 8(1). 1–20.

Casey, E. (2000). *Digital Evidence and Computer Crime*. Academic Press.

Chen, G., Du, Y., Qin, P. & Du, J. (2012). Suggestions to Digital Forensics in Cloud Computing ERA. In: *2012 3rd IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC).* IEEE

Cohen, F.B. (2010) Fundamentals of digital forensic evidence. *Handbook of Information and Communication Security*. pp. 789–808. Springer, Heidelberg.

Eecke, P. V. (2015). *Cloud Computing Legal issues*. Retrieved from http://www.isaca.org/Groups/ProfessionalEnglish/cloudcomputing/GroupDocuments/DLA_Cloud%20computing%20legal%20 issues.pdf.

Hong, G., Jin, B. & Shang, T. (2012). Forensic Investigations in Cloud Environments. *2012 International Conference on Computer Science and Information Processing (CSIP).* IEEE.

Hyett, N., Kenny, A., & Dickson, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-Being*, 9, n/a. doi:10.3402/qhw.v9.23606

Irfan, M., Abbas, H., Sun, Y., Sajid, A. & Pasha, M. (2016). *A Framework for Cloud Forensics Evidence Collection and Analysis Using Security Information and Event Management*. (2016). DOI:https://doi.org/10.1002/sec

Joseph C. Sremack (2007). The Gap between Theory and Practice in Digital Forensics. *Annual ADFSL Conference on Digital Forensics, Security and Law Proceedings.* LECG, Washington, DC USA

Keyun Ruan, Joe Carthy, Tahar Kechadi, & Mark Crosbie. 2011. *Cloud Forensics*. 35–46.

Khan, S., Ahmad, E., Shiraz, M., Gani, A., Wahab, A.W.A. & Bagiwa, M.A. (2014). Forensic Challenges in Mobile Cloud Computing. *2014 Int. Conf. Comput. Commun. Control Technol.* I4 oct (2014), 343–347. DOI: https://doi.org/10.1109/I4CT.2014.6914202

Malina, M., Hanne, N., & Selto, F. (2011). Lessons learned: Advantages and disadvantages of mixed method research. *Qualitative Research in Accounting and Management.* 8(1), 59-71. doi:10.1108/11766091111124702

Manoj, S. K. A. & Bhaskari, D.L. (2016) Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. *International Conference on Computational Modeling and Security (CMS 2016).* 149 – 154

National Institute of Standards and Technology Interagency or Internal Report 8006 (2014, June). *Cloud Computing Forensic Science Challenges*.

Olayemi, J. O. (2014). A Socio-Technological Analysis of Cybercrime And Cyber Security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3), 116-125. doi:10.5897/IJSA2013.0510

Peter, M. & Timothy, G. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *Natl. Inst. Stand. Technol. Inf. Technol*. Lab. 145, (2011), 7. DOI:https://doi.org/10.1136/emj.2010.096966

Pichan, A., M. Lazarescu, and S.T. Soh, (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*. **13**: p. 38-57.

Rahayu, S.S., Yusof, R. & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security.* 8(10), 163–169.

Reilly, D., Wren, C., & Berry, T. (2011). Cloud Computing: Pros and Cons for Computer forensic Investigations. *International Journal of Multimedia and Image Processing, Infonomics Society*, 1(1), 26-34.

Román, R.F.M., Mora, N.M.L., Vicuña, J.P.N & Orozco, J.I.P. (2016). Digital Forensics Tools. *International Journal of Applied Engineering Research* ISSN 0973-4562. Volume 11, Number 19 (2016) pp. 9754-9762.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). *Cloud forensics: An Overview*. Advances in Digital forensics, 7, 35-49.

Saurav, N. & Raymond, A. (2017). *Forensics As A Service: Three-Tier Architecture For Cloud Based Forensic Analysis.* Proc. - 15th Int. Symp. Parallel Distrib. Comput. ISPDC 2016. 178–183. DOI:https://doi.org/10.1109/ISPDC.2016.31

Serianu (2018). *Africa Cyber Security Report* – Kenya. Cyber Security Skills Gap

Sheik, K., Ahmad, M. & D. Lalitha Bhaskari (2016). Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment. *International Conference on Computational Modeling and Security (CMS 2016)*

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud Forensics: Identifying the major issues and challenges. *In Proceedings of 26th International Conference, CAiSE, Thessaloniki, Greece, June, 2014*. 16-20.

Suchana, D. (2016). *Review on Cloud Forensics: An Open Discussion on Challenges and Capabilities*. 145, 1 (2016), 1–8.

Syed, A.A., Shahzad, M. & Farhan, S. (2017). Challenges and Solutions in Cloud Forensics. ICCBDC'18, August 3–5, 2018, Barcelona, Spain © 2018. *Association for Computing Machinery (ACM)* ISBN 978-1-4503-6474-4/18/08…$15.00. https://doi.org/10.1145/3264560.3264565.

Toloie-Eshlaghy, A., Chitsaz, S., Karimian, L., & Charkhchi, R. (2011). A Classification of Qualitative Research Methods. *Research Journal of International Studies.* 20. 106-123. Retrieved from http://www. eurojournals.com.

Tuominen, T., Tuominen, P., & Jussila, I. (2013). A Tool to Be Used Deliberately: Investigating the Role of Profit In Consumer Co-Operatives. *International Business Research*. 6, 122-133. doi:10.5539/ibr.v6n11p1

Wall, D.S. (2015) ‘Dis-organized Crime: Towards a Distributed Model of the Organization of Cybercrime. *The European Review of Organized Crime* 2(2): 71-90.