Joined Diverse Cloud Computing Systems; A Digital Forensic Framework

Zayyanu Umar[1*], Francis S. Bakpo[2], Deborah U. Ebem[2], and Modesta E. Ezema[2]

[1]Department of Computer Science, College of Science and Technology, Federal Polytechnic, Birnin kebbi, Kebbi, Nigeria

[2]Department of Computer Science, Faculty of Physical Science, University of Nigeria Nsukka, Enugu, Nigeria

Email: zayyanuumar1@yahoo.com

Abstract- Most commercial complexes and academic institutions now use cloud computing to adopt new communications system. Cloud services vendors might be restricted to specific resources, lacking some services to their customers' requests; this leads to the need for multiple cloud data centers to collaborate to share resources. With distinctions in various features and architectures, the cloud computing systems may be interconnected, and such networks may be exposed to instability or intrusion. Although cloud computing platforms and computer technology are also making strides to meet the increasing application worldwide, attackers use Internet services to commit cyber-attacks. Deployment of cloud infrastructure is becoming increasingly vulnerable to attacks and intrusions. Unauthorized access to or destruction of records gives organizations or agencies significant devastating losses. Human influence and available tools are not adequate to protect and control cloud service vendors. Therefore, there is a need for efficient, resilient, versatile, reliable architecture and a model capable of detecting hazardous cybercrimes on joined diverse cloud service providers, and it can facilitate real-time digital forensic investigations. We specifically used an activity diagram of Unified Modeling Language (UML) to design the proposed architecture. We adopted an architectural modeling approach to develop an architecture for deployment. This study presents a framework for digital forensics to detect cybercrime in a heterogeneous networks setup that is joined together. We built a model using a UML activity diagram capable of managing cloud instability and complexities while managing inter-domain services.

Keywords: *Architecture, Cloud Computing, Cloud Centers Diversity, Digital Forensics.*

INTRODUCTION

Cloud technology turns it not necessary for commercial industry and research institutions to acquire hardware and software. Nowadays, cloud service provider (CSP) data centers house essential information from organizations, no longer on institutions local disk drives.

Cloud-based services are terms that enable omnipresent, safe access to an on-demand network to flexible shared computing resources (such as networks, data repositories, applications and processing (Yu et al., 2014).

With the introduction of cloud storage infrastructure, cloud service provider disseminates an organization's data within data centres to various continents and with distinct file format schemes, streaming from one server to multiple regions. A customer of cloud computing services can subscribe to the world's chosen location, but the major problem is the uncertainty nature of the facts that are in use.

The National Institute of Standards and Technology (NIST) states what cloud computing is: "*A framework for allowing universal, easy, on-demand network access to a shared pool of customizable computing resources (e.g., networks, databases, space, software, and services) that can be easily distributed and released with minimal management effort or interference* *between service providers. This cloud model consists of five key features, three service models and four deployment models"* (Digambar et al., 2015).

The five essential cloud-computing elements are as follows: universal network access, Asset self-service balancing, cost-peruse, and on-demand rapid elasticity. Categories of cloud service providers based on software are into three main groups, called 'online business models' such as service network, service platform, and service software (Green and Audience, 2016).

When the adoption of cloud computing grows, organizations and other customers continue to use innovative approaches to leverage their full potential through cloud organisations' implementation completely. With the inherent advantages of cloud service vendors, cloud service environments have led to the emergence of various problems. Prospective cloud services subscribers need to consider multiple elements before subscribing to a particular or interconnected cloud environment(s). Many of these problems are due to limited available resources, cloud services location in another world with different settings, no monitoring of cloud services etc. Most of these issues offer a person with a malicious ego a solid foundation for evaluating the vulnerabilities and exploiting the cloud infrastructure(Miller et al., 2014).

Inter-cloud is defined as merging various clouds to exchange information and serve customers as much as possible whenever they wish to make a request and safety and security. This diversity is a significant challenge in collaborative cloud computing settings as it raises obstacles concerning the cloud's omnipresent realization. A further challenge is vendor lock-in; consumers making service requests have to adapt their demands to conform to the cloud provider's trends and interfaces, resulting in expensive and challenging possible relocations (Zawoad et al., 2015).

There are six primary levels of digital forensic processes: identification, collection, evaluation, examination, storing and reporting. Forensics in Cloud settings as a concept has been used and described since 2010 as a combination of two ideologies; cloud computing and digital forensics (Alqahtany and Clarke, 2014); the authors used conventional digital forensics to track breaches or identify indictable evidence.

"NIST: Cloud Computing Forensic Science Challenges" defined cloud service platform digital forensics as using expert principles, professional experience and validated methods to create past, live and tempted incidents in cloud computing by identifying, capturing, processing, evaluating, interpreting and publishing digital evidence"(NIST, 2014).

Green (2016) found three distinct categories of digital forensics in the cloud system: post-incident, live incident and before the incident.

Before the incident: Monitor the activities on a network and turn any potentially suspicious activity into a typical network framework when a network attack takes place.

Live incident: Forensics expert attempts to arrest forensic attack activities before shutting off the live operating system. Besides, live forensic acquisition is frequently conducted to gather malicious activities information that may be lacking when using a traditional forensic data collection.

Post-incident: as the term suggests, after an incident, the investigator gives police a logical and physical record of each unit for the required investigative process.

In cloud computing systems, multiple conducted kinds of research related to digital forensic investigations. Some studies are both on a customer and server-side, and some are focused on the operating system of a cloud environment. Various cloud services providers provide pay per use cloud services to cloud users (Sotiriadis and Bessis, 2015).

The primary need is to combine multiple cloud service providers as one cloud service platform (Yu et al., 2014). Some researchers have indicated a need to build a network whereby joined varied cloud service providers can gain access to agreed provided services despite the disparity in the individual cloud environment to a joined cloud services(Dykstra and Sherman, 2013).

The biggest problem with choosing to join several cloud resources providers is that most individual cloud systems can not work collaboratively, as each communicates with a unique dialect (Yan, 2011). There have been no clear service standards for two or perhaps more clouds to be incorporated, but operating systems are based on those definitions. Many data centres use either Representational State Transfer (REST) or Simple Object Access Protocols (SOAP) as an interaction scheme. Each scheme has its distinctive features, for example, login authentication (Ali, 2018). Existing cloud architectures also have not taken into cognizant cloud compatibility, and each cloud environment has its structural platform and user interfaces (Zawoad et al., 2015).

Inconsistency in different cloud data and ways of logging into another cloud computing systems creates issues for contemporary researchers and performs a thorough review; the researchers must attain the meaning of the various data fields in each connection (Demchenko et al., 2017). Incapability to recognize one system-logging scheme into other logging protocol creates inconsistency and incompatibility with Cloud-connected devices and logging processes of operating systems. It gives rise to a challenging task being logged hierarchically (Zawoad et al., 2016). By introducing this new technology for accessing multiple clouds to communicate and collaborate and reap other interoperability benefits, malicious user lunches act to target specific cloud unit resources to spoof services or access sensitive data. Attackers of service providers use the existing cloud environment components as their tools to mount an offensive activity (Alqahtany and Clarke, 2014).

Numerous scholars researched cyber-attacks, computer forensics studies and heterogeneity between existing cloud platforms in cloud data centres. The lack of standards for monitoring and setting up a heterogeneous network and the need for a digital forensic system for cybercrime detection deny corporations that will need to exploit heterogeneous technology advantages from infrastructural differences such as resource management, environmental benefits, recovery, hypervisor-type advantages, pricing model and protection in the transaction model.

With the existing studies on digital forensics analysis and cloud cybercrime detection, there is still a need for a system that addresses cybercrime detection relevant to joined varied cloud computing systems and enables digital forensic examination (Yan, 2011;Samy et al., 2018;Burney et al., 2016).

Throughout this study, we proposed a new digital forensic Model, which can be used for cybercrime detection and forwarding for prosecution throughout joined heterogeneous configured clouds network. We divide this article into the following, Introduction, Review of Related Works, Methodology, Proposed Frameworks, Framework Discussion and Conclusion and Future Work.

DIVERSITY IN CLOUD SERVICE ENVIRONMENTS

Combining various cloud service providers at different stages (a collaboration of multiple vendors at different stages by the individual hypervisor) or the same level (a collaboration of service providers by numerous heterogeneous hypervisors deployed security mechanisms) service broking, service scheduling algorithm, power infrastructures and host operating system is referred to as Joined cloud environments (BMC, 2012). The table below shows a heterogeneous structure in cloud environments.

Table 1: Diverse Cloud Service Provider (CSP)

CSP	Hypervisors	OS	Schedul. Algo.	Resource Price	Securi. Mechanisms
CSP1	Hyper-V	Window	Max-Min	?	?
CSP2	KVM	Unix	Honey-Been	?	?
CSP3	VMware	Linux	Ant-colony	?	?

REVIEW OF RELATED WORKS

Digambar (2015) developed a framework mainly for forensic examination in a cloud computing system despite traditional forensic approaches; it was designed to apprehend digital criminals, seize networking gadgets and other physical computer sets such as storing device hard disks, server, etc. The digital investigator defines concerns and criteria around digital software forensic research. Through this report, The investigator discusses the problems surrounding the forensic investigation, both live and dead.

Alharbi (2014), with research entitled "Proactive Framework for Digital Forensic Investigation", established a system in the cloud service platform, which requires active digital forensic investigation. It addressed the problems faced by Reactive Electronic Forensics (RDF), when computers, networks gadgets confiscated are used for a study.

Martini and Choo (2012) established a framework that separates information processing and storage between conventional forensics and digital forensics in the cloud-computing environment. They addressed problems and challenges related to electronic forensic cloud computing within the framework of the program they were designing.

In the study entitled: "New challenges in digital forensics: online storage and anonymous communication", The researcher developed a model to tackle the bottlenecks raised by digital forensics processes on a cloud computing platform and analyzed arising issues in anonymous communication. The author tested the framework's workability using Dropbox by launching an attack (Mulazzani, 2014).

In research entitled "Digital Forensic Investigations in the Cloud: A Proposed Approach for Irish Law Enforcement," an approach was conceived to address the weaknesses of the traditional digital forensics scheme and the issues presented to Ireland's law enforcement digital forensic practitioners in the cloud computing scene. The scholar has researched the conventional forensic analysis approaches and the causes of why they are insufficient for delivery to a cloud platform (Kechadi and Nhien-An, 2015).

Alexander (2013) created specific forensic problems inside a cloud environment in a study entitled "Digital Forensics for Infrastructure-as-Service Cloud Computing." He studied the specificities of the forensic investigation currently accessible with remote methods. The author built a system using OpenStack's cloud storage application model to allow trusted software as a forensic prototype of the cloud.

Zawoad et al. (2016) found that the forensic cloud infrastructure permits identifying and preserving the necessary evidence with confidentiality and integrity. The open-source model on Openstack is popular. First features found to assist trustworthy forensics in cloud environments.

Kebande (2017), entitled "Internet Forensic Readiness as a Service Model (CFRaaS)". The authors built a software application named a CFRaaS system. The application uses malicious botnet features but modifies its capabilities to create potential cloud proof. CFRaaS preserves such information electronically for Digital Forensic Research purposes in an electronic forensic database.

Alqahtany and Clarke (2014) developed a digital forensic evidence extraction scheme and evaluation that reveals the non-Cloud Service Provider (NCSP) customer details. The template gives ample and prosecutable facts.

In a thesis entitled: "Forensicloud: An Architecture for Digital Forensic Assessment in the Cloud," the author proposed a technology that would prevent the length of time required for scientific research by combining computing resources with high-performance incorporating existing tools to work in that context. Additionally, writers with such a system gain access to unique, locked resources that can not be freely subscribed (Miller et al., 2014).

FROST was developed as a cloud computing environment digital forensic tool, entitled Sherman and Dykstra: FROST. The app enables forensic experts and law enforcement; get reliable and prosecutable forensic information on cloud networks independently of platforms. The proposed framework was specially developed for a particular cloud platform known as OpenStack (Dykstra and Sherman, 2013).

"Cloud Forensic Evidence Management System (FEMS)" addresses digital evidence storage problems in another study created by Arthur, and it ensures accuracy and credibility related to digital evidence. The authors used the Biba Integrity Model to store the integrity of digital evidence in FEMS securely, and they used Casey's Certainty Scale in reliability tests (Arthur, 2010).

In the study entitled: "Cybercrime forensic system in cloud computing." The authors presented a cloud crime tracking and analysis system using Encase and FTK (Yan, 2011).

Zawoad et al. (2015) designed an Open Cloud Forensics framework. They found challenges in the existing digital forensic structure by analyzing cloud computing environments and different cloud-participating entities while incorporating existing cloud infrastructure and services. In a realistic scenario, the system (OCF) could support contemporary digital forensics processes.

METHODOLOGY

The study examined the diversity between specific cloud computing systems, including virtual machines, scheduling algorithms, protection mechanisms, broking of cloud services, pricing of services and capability of infrastructure, etc. The deployment of middleware is paramount to convert and de-convert, translate and re-translate individual cloud computing systems variations. We also considered Service level agreement (SLA) and other vital specifications for interconnecting specific cloud computing systems in the proposed architecture. We primarily used an activity diagram to develop the proposed structure; then, we used an architectural modelling method to create a deployment diagram framework.

PROPOSED FRAMEWORK

Diversities in cloud service providers give rise to proposed criteria to address conflicts and test compliance policies and level service agreements. Consequently, solving cloud inconsistencies allows the development of a realistic advanced forensic platform to improve legal processes.

The compatibility of heterogeneous cloud systems will also decide to lock the customer searching for a resource that his principal subscribed cloud service vendor does not support. Figure 1 below shows the heterogeneous resources sharing Cloud interconnections.

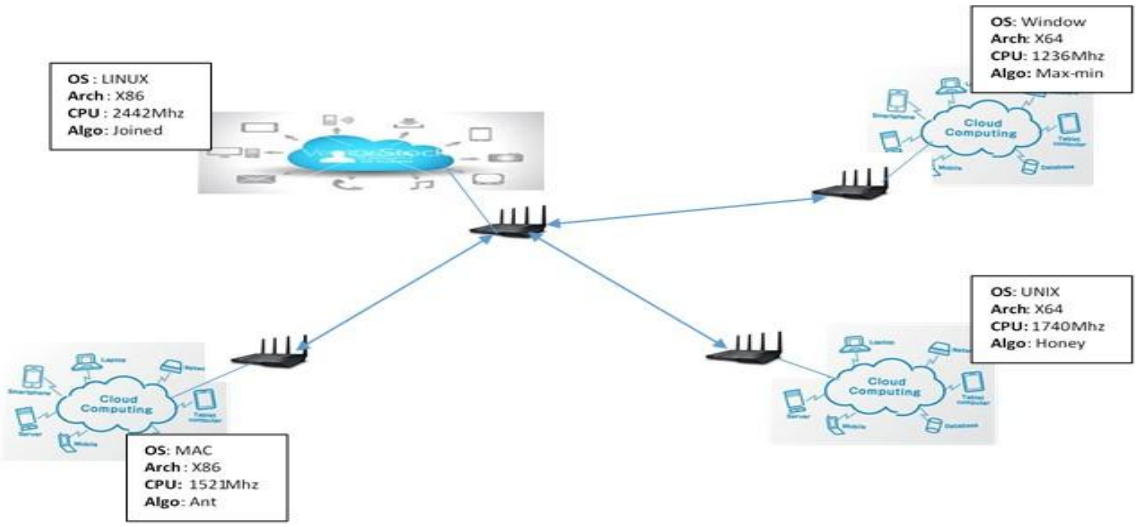

Figure 1: Joined Heterogeneous Clouds Diagram

The diagram portrays the interconnection to share resources of various cloud configurations. If one cloud needs support from its users, then the cloud data centre channels request the central cloud services. Following figure 2 below illustrates an intrusion detection scenario in heterogeneous clouds that are joined together.

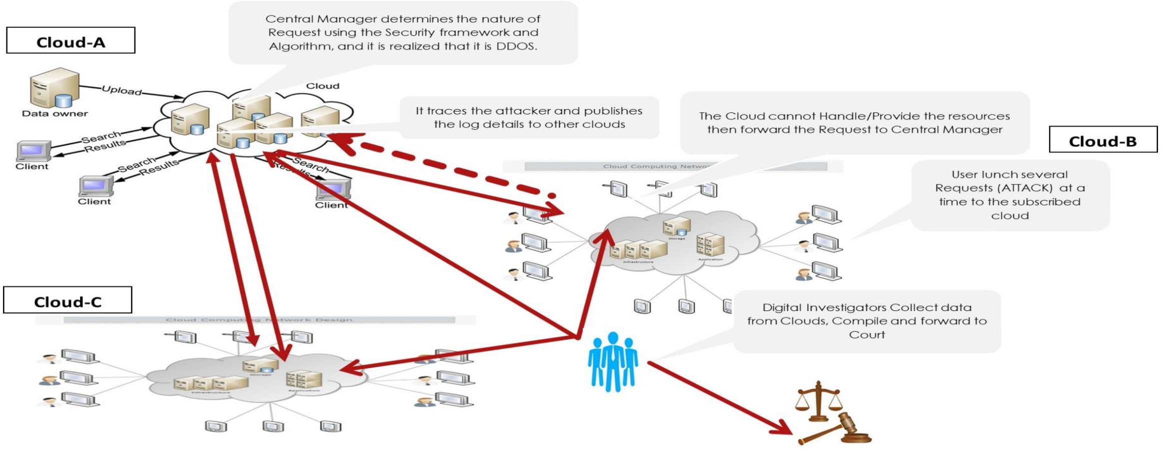
Cloud-A
Central Manager determines the nature of Request using the Security framework and Algorithm, and it is realized that it is DDOS.
Upload
Data owner
Cloud
Search
Results
Client
Search
Results
Client
Search
Results
Client
It traces the attacker and publishes the log details to other clouds
The Cloud cannot Handle/Provide the resources then forward the Request to Central Manager
Cloud-B
User lunch several Requests (ATTACK) at a time to the subscribed cloud
Cloud-C
Digital Investigators Collect data from Clouds, Compile and forward to Court

Figure 2: A Deployment Plan for Digital Forensic Process in Joined Heterogeneous clouds

Once the request comes to Central Cloud, there will be request status checks as presented in figure 3; if the service request is legitimate, then the central cloud will loop to find where the service in need is found, and standards complied, then forward to the local cloud in a request, then to the client as portrayed in figure 4

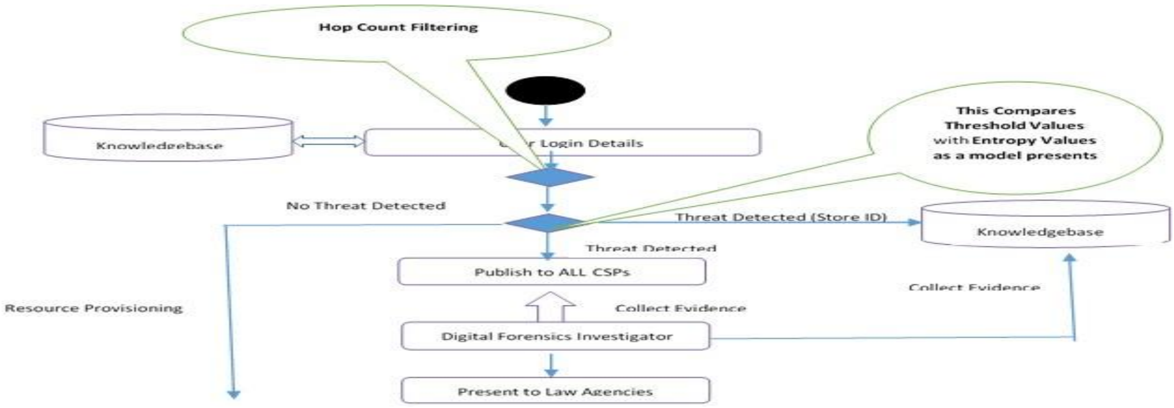

Figure 3: Digital Forensics Activity in Joined Heterogeneous Clouds Environment

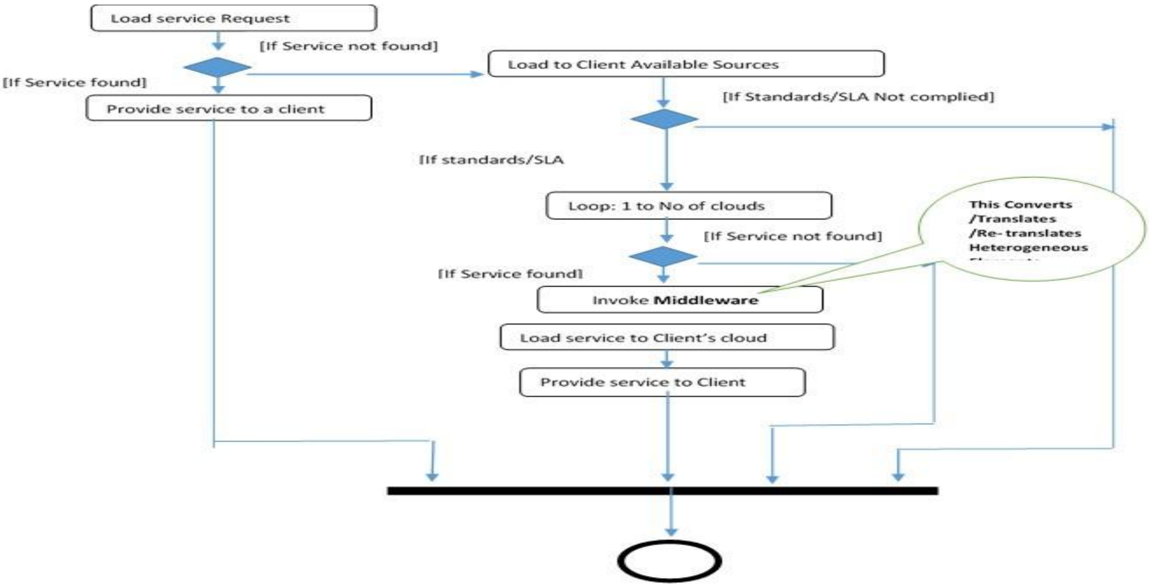
Load service Request
[If Service not found]
[If Service found]
Load to Client Available Sources
Provide service to a client
[If Standards/SLA Not complied]
[If standards/SLA
Loop: 1 to No of clouds
[If Service not found]
This Converts /Translates /Re-translates Heterogeneous
[If Service found]
Invoke Middleware
Load service to Client's cloud
Provide service to Client

Figure 4: Service Provisioning in Joined Heterogeneous Cloud Environments

THE FRAMEWORK DISCUSSION

In this article, the diagrams show clouds linked to a dedicated central cloud computing system responsible for handling interoperation issues and enabling resource sharing between different clouds. Each cloud environment has an entirely different scheduling algorithms, operating systems, user collection, device architectures and other features. It also validates the variety in the general approach to digital forensics. A CLOUD customer order for a service to its registered CSP; if the Cloud Service Provider has no such assets, the subscribed CSP shall forward the order to the central cloud, the Central Manager shall, upon receipt of the request, check the authenticity and authorization of the logs (Anomaly Analytics). Instead, Digital Forensics Investigator collects, compiles, and Present to Court information from the Central Manager Persistent Memory and CSPs Memories the Intrusion log data.

CONCLUSION AND FUTURE WORK

The ability to connect with cloud service providers and restrict active cloud service users from being trapped in their resource requirements results in heterogeneity in developed joint cloud vendors. It will be happy to harmonize interconnected clouds' heterogeneity by building a prototype and platform that can cope with complexities and variations, subscribers and smooth interoperability services providers. The problem is solved by proposing a concrete forensic infrastructure to handle both diversity barriers and by infringing unauthorized access to joined cloud resources for identification. Future research is needed to develop a simple forensic system for the Internet of Things (IoT) due to its robustness, high complexity and heterogeneity.

References

Alexander, J. (2013). *Digital Forensics for Infrastructure-as-a-Service Cloud Computing*. University of Maryland, Baltimore.

Alharbi, S. A. (2014). *Proactive System for Digital Forensic Investigation*. University of Victoria.

Ali, S. A. (2018). Challenges in Cloud Forensics. *International Conference on Cloud and Big Data Computing*, 6–10.

Alqahtany, S., & Clarke, N. (2014). A forensically-enabled IAAS cloud computing architecture. *12th Australian Digital Forensics Conference.*, 10. https://doi.org/10.4225/75/57b3e3a5fb87e

Arthur, K. K. (2010). *Considerations Towards the Development of a Forensic Evidence Management System*. University of Pretoria.

BMC, B. (2012). *Homogeneous vs. Heterogeneous Clouds: Pros, Cons, and Differences – BMC Blogs*. Web Pages. https://www.bmc.com/blogs/what-price-homogeneity

Burney, A., Asif, M., & Abbas, Z. (2016). *Forensics Issues in Cloud Computing*. *August*, 63–69.

Demchenko, Y., Turkmen, F., Laat, C. De, & Slawik, M. (2017). *Defining Intercloud Security Framework and Architecture Components for Multi-Cloud Data Intensive Applications*. 945–952. https://doi.org/10.1109/CCGRID.2017.144

Digambar, P. (2015). *A Novel Digital Forensic Framework for Cloud Computing Environment* (Issue 2011). BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI.

Digambar, P., Philosophy, D. O. F., & Digambar, P. (2015). *A Novel Digital Forensic Framework for Cloud Computing Environment* (Issue 2011). BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI.

Dykstra, J., & Sherman, A. T. (2013). Design and implementation of FROST : Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, *10*(13), S87–S95. https://doi.org/10.1016/j.diin.2013.06.010

Green, T. (2016). *Exploring Cloud Incidents* (Issue June).

Green, T., & Audience, T. (2016). *Exploring Cloud Incidents* (Issue June).

Kebande, V. R. (2017). *A Novel Cloud Forensic Readiness Service Model by*. UNIVERSITY OF PRETORIA Department.

Kechadi, T., & Nhien-An, L.-K. (2015). *Digital Forensic Investigations in the Cloud A*

Proposed Approach for Irish Law Enforcement. *January 2016*.

Martini, B., & Choo, K.-K. R. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, *9*(2), 71–80. https://doi.org/10.1016/j.diin.2012.07.001

Miller, C., Glendowne, D., Dampier, D., & Blaylock, K. (2014). Forensicloud: An Architecture for Digital Forensic Analysis in the Cloud. *Journal of Cyber Security and Mobility*, *3*(3), 231–262. https://doi.org/10.13052/jcsm2245-1439.331

Mulazzani, M. (2014). *New challenges in digital forensics : online storage and anonymous communication by* (Vol. 2014).

NIST. (2014). *Cloud Computing Forensic Science Challenges*.

Samy, G. N., Maarop, N., Abdullah, M. S., Perumal, S., Albakri, S. H., Shanmugam, B., Jeremiah, P., & Hasan, S. (2018). Digital Forensic Investigation Challenges based on Cloud Computing Characteristics. *International Journal of Engineering & Technology*, *7*(4), 7–11. https://doi.org/10.14419/ijet.v7i4.15.21361

Sotiriadis, S., & Bessis, N. (2015). An Inter-Cloud Bridge System for Heterogeneous Cloud Platforms. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2015.02.005

Yan, C. (2011). Cybercrime forensic system in cloud computing. *International Conference on Image Analysis and Signal Processing, IASP 2011*, *Dc*, 612–613. https://doi.org/10.1109/IASP.2011.6109117

Yu, F., Stella, C., & Schueller, K. A. (2014). A Design of Heterogeneous Cloud Infrastructure for Big Data and Cloud Computing Services. *OPEN JOURNAL OF MOBILE COMPUTING AND CLOUD COMPUTING*, *1*(2).

Zawoad, S., Hasan, R., & Cover, C. (2016). Trustworthy Digital Forensics in the Cloud. *Computer*, *49*(3), 78–81. https://doi.org/10.1109/MC.2016.89

Zawoad, S., Hasan, R., & Skjellum, A. (2015). OCF: An Open Cloud Forensics Model for Reliable Digital Forensics. *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*, *July*, 437–444. https://doi.org/10.1109/CLOUD.2015.65