THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Development of Digital Forensic Framework for Joint Heterogeneous Cloud Computing Platforms

Zayyanu Umar
Senior Lecturer, Department of Computer Science,
Waziri Umaru Federal Polytechnic, Birnin Kebbi, Kebbi, Nigeria
Francis, S. Bakpo
Professor, Department of Computer Science
University of Nigeria, Nsukka, Enugu, Nigeria
Musa Alkali AbubakarTanko
Lecturer, Department of Computer Science
Waziri Umaru Federal Polytechnic, Birnin Kebbi, Kebbi, Nigeria

Abstract
The cloud computing is nowadays an embarrassing computing technology by many organisations, academic institutions and business centres. Cloud Service Providers (CSP)s are limited to some resources, lacking some resources requested by its customers, this gives rise to the needs for interconnecting multiple clouds to interoperate and share resources. The interconnected clouds can be in different features and schemes, and the system can be prone to insecurity or intrusion. In this paper, we developed a Digital Forensics framework that can detect an intrusion within heterogeneous joint clouds. We also developed architecture and algorithm that can handle the joint clouds heterogeneity and complexity during inter-clouds resources management.

Keywords: *Digital forensics, framework, cloud computing heterogeneity, cloud service providers*

1. Introduction

Cloud computing technology renders the acquisition of hardware and software by the industrial institutions and academic institutions useless, as sensitive data or information are often stored in cloud service provider's data centers around the globe not on institutions local disk drives anymore.

Different cloud platforms such as OpenStack, Amazon Web Service (AWS), Rackspace, Google Compute Engine (GCE) and Microsoft Azure and others, provide services to cloud-end users on a pay-as-you-go service, the users only pay cloud resources utilised(Sotiriadis & Bessis, 2015).

Today, various Cloud Service Providers (CSP) aimed to interoperable clouds. The effort is to join different forms of cloud service providers, aggregated to one cloud platform(Yu, Stella, & Schueller, 2014).

Some scholars also indicated broad interest in creating a cloud-of-clouds where multiple cloud service providers can gain access of resources of each other seamlessly, which we and others call the multi-cloud(Smit, Simmons, & Litoiu, 2013). The main issues with joining multiple and different configured cloud service providers are most of the cloud systems are not compatible with one another and cannot share services with other, since everyone speaks a different language(Garrison, 2010). There are no service standards that are specific to that effort of joining two or more clouds, and these standards are deployed on web browser interfaces. Some of the cloud providers use SOAP; other ones use REST as communication protocols. Each service has its specific characteristics such as authentication and security requirements(Elhozmari& Ettalbi, 2016). Cloud service providers have not taken into consideration Cloud interoperability issues and each Cloud comes with its service and interfaces for services (Toosi, Calheiros, & Buyya, 2014). Inconsistency in log formats and data representations with an individual cloud to other clouds, present challenges to a digital investigator, who needs to capture the meaning of the various fields of data in each log to perform a thorough analysis(Kent & Souppaya, 2006).

"The failure of one operating system logging format to be accepted to the other logging format of operating system creates incompatibility and heterogeneity with the logging functions within clouds operating systems or network devices. This makes centralizing logging is a challenging task"(Sahoo& Chottray, 2012).

With the development of this new technology of joining multiple clouds to interoperate and derive other benefits of interconnections, the intruders get unauthorized access to some resources on cloud computing servers with a malicious ego to steal services or gain access to some vital information. For example, cybercriminals are utilising existing cloud services as their infrastructure to target their victims(Alqahtany, Clarke, Furnell, & Reich, 2016).

To assist in detecting malicious users and in analysing the giant clouds logs, mega clouds organisations need to deploy automated methods of converting logs with different content and formats from different individual clouds into a

single standard format with consistent data field representations, this facilitates interoperability and gives confidences to customers of the service.

Developing a universal digital forensic system model that can penetrate joint different cloud platforms transactions and detect the intruder and the scene of intrusion can simplify the tasks of a digital forensic investigator.
Numerous researchers have conducted research on digital forensics on cloud computing services and heterogeneity among the existing different cloud service platforms.

Despite all researches conducted in the area of cloud forensics, also numerous researchers pointed out the need for a broad study that comes up with joint multiple cloud service platform system that supports varying formats of individual cloud platforms, unifies security threats logs and facilitates digital forensic investigation(Alexander, 2013; Grispos & Glisson, 2012; Kanungo, 2016; Saokar, Patil, & Dharaskar, 2015).

The contemporary researchers are seeking for researches that handle the security issues for interoperability of joint cloud service platforms with different log formats and standards(Almulla, Iraqi, & Jones, 2014; Demchenko, Turkmen, Laat, & Slawik, 2017; Lillis, Becker, O'Sullivan, & Scanlon, 2016; Toosi et al., 2014; Wang, Ding, & Niu, 2012).

1.1. Background

Cloud computing is a new system of using the internet instead of stand-alone in taking computing activities; such as desktop publishing, software development, storing data on a local drive, using processors and other activities.
Cloud computing was defined as both hardware, system software services and application software services that cloud service provider (CSP) deliver to customers as services over the Internet (Armbrust et al., 2010).
The National Institute of Standards and Technology (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. This cloud model is composed of five essential characteristics, three service models, and four deployment models"(Mell& Grance, 2011).
There are five main features of cloud computing are ubiquitous network access, on-demand self-service, resource pooling, pay- peruse business, rapid elasticity.

The Cloud Service Providers based on the services each renders can be classified into three main categories, which are also named as "cloud service models" such as (a) Platform-as-a-service (PaaS), (b) Software-as-a-service (SaaS) and (b) Infrastructure-as-a-service (IaaS) (Armbrust et al., 2010).

Platform-as-a-service (PaaS) model is used by developers to develop new applications on the infrastructure provided by the CSPs. In PaaS, CSP assists programmers/developers by providing open/proprietary languages, the initial basic configuration for communication, monitoring, distributing the application, scalability of an application, and so on(Buyya et al., 2009).

Software-as-a-service (SaaS) provides software to users. The application is accessed via a web browser. Users gain access to any application provided by CSP without concern about its configuration and installation. The examples of SaaS include Gmail, Google apps, Microsoft 365, Cisco WebEx and Salesforce(Khan et al., 2016).

Infrastructure as a Service (IaaS), where a customer makes use of the CSP's computing, storage or networking infrastructure (Chen, 2016). Examples include Amazon Web Service (AWS), Google Compute Engine (GCE), Rackspace, and Microsoft Azure.

1.2. Cloud Resource Management

Resource management helps in determining that which and how much and which resources are needed and available for the current request, so that Quality of Service(QoS) components such as availability, security, reliability and CPU utilisation can be checked(Chopra & Bed, 2017).
Various cloud-based resource management mechanisms are in the existing literature and explained briefly:

1.3. Clouds Resource Management Mechanisms

Different cloud-based resource Management mechanisms are as follows:

1.3.1. Queuing Model-Based

A dynamic resource provisioning mechanism is proposed while removing deadlocks among the processes requesting resources(Sood, 2013).

1.3.2. Reliability-Based

This policy takes care of resource provisioning in a cloud-based environment while improving the reliability of the virtual machines providing these resources(Tian& Meng, 2010).
Various brokering strategies have been proposed while modifying the backfilling scheduling algorithm to give a fault-free environment for private cloud for provisioning resources(Javadi, Abawajy, & Buyya, 2012).

1.3.3. Hybrid Cloud-Based

Resources have been allocated to the processes on the basis of priority of the process. High Priority processes go to the private cloud for resources whereas medium and low priority processes go to the public cloud for resources(Choudhury, 2013; Grewal & Pateriya, 2012).

1.3.4. Service Level Agreement (SLA) based

Resource provisioning policy for heterogeneous clouds is proposed by considering their SLA. The policy results in maximum utilisation of resources also by decreasing the risk of underutilization of resources (Kumar, Nadjaran, & Gopalaiyengar, 2014).

1.3.5. Ontology-Based

An InterCloud Resource Provisioning Scheme is proposed and the researcher addressed the problem of interoperability between the clouds with the help of ontology(Nelson, 2012).

1.3.6. Deadline Based

The researcher proposed deadline driven resource provisioning algorithm for cloud application platform ANEKA while reducing application execution time (Vecchiola, Calheiros, Karunamoorthy, & Buyya, 2012).

1.3.7. Application Based

Cloud-based brokering strategy is proposed where the resources are provisioned from the best-suited service provider and results in decreasing cost and promotes scalability and robustness(Subramanian & Savarimuthu, 2016).

1.3.8. Cost-Based

A cost-effective resource provisioning policy is proposed adjusting in multiple private and public clouds

By the emergence of cloud computing, the data is distributed to different regions from one or various data centres in different file systems and different forms, spilling from one platform server to another. A user can be from any angle of the world and volatility nature of data in use is another big challenge.

In this regard, there is a need to design a proactive measure that alleviates and provides support to digital investigator especially, when it comes to heterogeneity in cloud service platforms.

As deployment of Cloud Computing increases, the needs of using new models are arising from clients and other service providers to exploit further its full capacity, one of which is the deployment of Cloud federations.

Recent development in cloud technologies indicates a need for movement onto emerging Multi-cloud models and frameworks. They provide a standard and interoperable environment's ability.

Multi-cloud can be defined as integrating heterogeneous individual clouds to interoperate together to serve the customers what they want and as they want and for a security purpose.

This heterogeneity in a joint cloud computing environment is a severe problem as it intensifies barriers in the path of the ubiquitous cloud realisation. The central obstruction is vendor lock-in, which is unavoidable at this level, customers applying cloud solutions want to tailor their applications to fit the pattern and interfaces of the cloud provider, which cause future relocation costly and difficult(Toosi et al., 2014).

As Cloud computing provides several benefits to customers and faces several security challenges to digital forensics and criminal investigation, so also multiple joint clouds face the same.

In general, a digital forensic procedure includes six main stages: identification, preservation, collection, examination, analysis and presentation.

The term of Cloud Forensics was first introduced in 2010, and is described as the join of two concepts; cloud computing and digital forensics (Alqahtany & Clarke, 2014), the investigator uses the conventional digital forensics processes to track the threats or identify admissible evidence to the court.

NIST: Cloud Computing Forensic Science Challenges (2014) defined Cloud computing forensic as the use of expert principles, technological custom and drawn and proven methods to build past, live and tempted cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence.

Audience (2016) opined that there are three potential types of digital forensics in the cloud environment: before the incident, live, and post-incident. Before incident: to supervise the network and attempt to turn each suspicious abnormal behaviour into a traditional network forensics process when an incident happens. Live incident: Live forensic investigator aims at arresting forensic data from a live and running system before switching off the power. In general, a live forensic acquisition is commonly conducted to get volatile data that will be lost when a traditional forensic acquisition is deployed. Post-incident: After an incident, the investigators get a logical and physical copy of each artifact for further investigation process. Heterogeneity in Cloud Forensic is also a significant challenge to the investigator, as the evidence has been tenable, reliable, and original and court ready.

2. Lliterature Review

There are a lot of researches pertaining the forensic investigations in cloud computing services. Majority of the studies are either of client side or server side and are more restricted to one single cloud service provider(CSP).

In the thesis report titled ”A Novel Digital Forensic Framework for Cloud Computing Environment”, Digambar(2015), devised a framework that can be used for virtual cloud computing environment forensic investigation instead of conventional approach of arresting a digital crime by seizing physical computer system components as an exhibit, such as hard-drive, external memory, server, and other visible parts then deploying offline forensics tools for investigations. He was able to identify challenges and requirements for virtual computing forensic investigation. In his study, he was able to address the issues related to the dead/live forensic examination.

Alharbi(2014) in his thesis report titled "Proactive System for Digital Forensic Investigation" designed a system that takes live digital forensics investigation in a cloud computing environment. It mitigates the challenges faced by Reactive Digital forensics(RDF) that takes the investigation on seized devices.

Martini & Choo(2012) developed a framework that differentiates the way data are collected and preserved between in cloud computing digital forensics process and traditional digital forensics processes. They reviewed two traditional existing digital forensics frameworks McKemmish (1999) and NIST (Kent et al., 2006). They discussed the challenges and issues of cloud computing digital forensic in the context of the framework they developed. In the thesis report titled: "New challenges in digital forensics: online storage and anonymous communication" the researcher developed a framework that mitigatesrecent challenges for digital forensics in some cloud storage platform and studied the issues related to anonymous communication. The Dropbox cloud storage platform was used, in which an attack was launched on dropbox to test the workability of the framework(Mulazzani, 2014).

In another research titled "Digital Forensic Investigations in the Cloud A Proposed Approach for Irish Law Enforcement". The framework was developed to mitigate the limitations of traditional digital forensics and the challenges Cloud computing presents for digital forensic practitioners working in Irish law enforcement. The researcher analysed the traditional digital forensics methods and why they are inadequate to be deployed in cloud computing(Kechadi, 2015).
In his thesis report titled "Digital Forensics for Infrastructure-as-ServiceCloud Computing", Alexander(2013) identified specifics challenges of forensics in cloud computing and analysed the deficiencies with existing forensic remote tools. He developed a tool that can enable trustworthy forensics of Software as a service(SAAS) model using the OpenStack cloud environment.

Kebande (2017)in his thesis report, the proposed model and named it Cloud Forensic Readiness as a Service (CFRaaS) model and developed CFRaaS software application prototype. The CFRaaS model uses the functionality of a malicious botnet, but its functionalities are modified to form potential evidence from the cloud. The model digitally preserves such evidence and stores it in a digital forensic database for DFR purposes.

Zawoad & Hasan developed Forensic enabled cloud architecture to provide the required evidence identification and preservation while protecting the privacy and integrity of the evidence. The design is on OpenStack, the popular open source. They first identified properties to support trustworthy forensics in clouds(Zawoad & Hasan, 2016)

Alqahtany & Clarke (2014) developed an acquisition and analysis model that extracts evidence from the client, not from the Cloud Service Provider(CSP). The model gives admissible and more abundant evidence.

In another research titled: Forensicloud: An Architecture for Digital Forensic Analysis in the Cloud, the researchers developed a framework that reduces a time taking when taking a digital investigation by leveraging the power of a high-performance computing platform and by deploying existing tools to operate within this environment. Furthermore, the researchers with their model give access to some licensed tools that are not opensource tools to use(Miller, Glendowne, Dampier, & Blaylock, 2014).

Dykstra and Sherman developed a cloud forensic tool called FROST.The device enables cloud user, law enforcement, and forensic investigators to extract trustworthy forensic data independent of the cloud provider. The tool was developed only for OpenStack private cloud platform(Dykstra & Sherman, 2013).

Arthur, in his thesis, developed Cloud Forensic Evidence Management System (FEMS) to address challenges faced in preserving digital evidence in maintaining reliability and integrity associated with digital evidence. The Biba Integrity Model is used in maintaining the integrity of digital evidence in FEMS while Casey's Certainty Scale is employed in integrity classification scheme(Arthur, 2010).

In another research titled: Cybercrime forensic system in cloud computing. The researcher developed a framework to monitor and analyse the cybercrimes in cloud computing using Encase and FTK(Yan, 2011).

Zawoad, Hasan, & Skjellum (2015) proposed the Open Cloud Forensics framework and listed limitations of digital forensics when deploying current cloud infrastructures by examining cloud architectures and various entities involved in a cloud. The framework (OCF) can support reliable digital forensics in a realistic scenario.

The following table indicates different digital forensic tools built on a different platform to serve on an individual platform and does not work for other platforms.

Tools	Used for	Platform
SANS SIFT	Analysis	Linux
CAINE	Reporting	Linux
DEFT	Analysis, Reporting	Linux
Xplico	Acquisition	Linux
PlainSight	Acquisition, examination	Linux
Sleuth	Analysis	Linux, Window
Blackthorn	Identification, Acquisition, Analysis, Reporting	Windows
ProDiscover	Preservation, Reporting	Windows
Volatility	Acquisition	Windows
FTK Imager	Examination	Windows

Table 1
Source: (Rani & Geethakumari, 2015)

3. Proposed Framework

The heterogeneity among the cloud computing service providers gives rise to the needs of interface that can settle the differences and checkmate the standard compliance and other Service Level Agreement (SLA). Also, cementing the differences among clouds facilitates in developing a concrete unified forensic system in simplifying court processes.
The proposed framework is as follows:

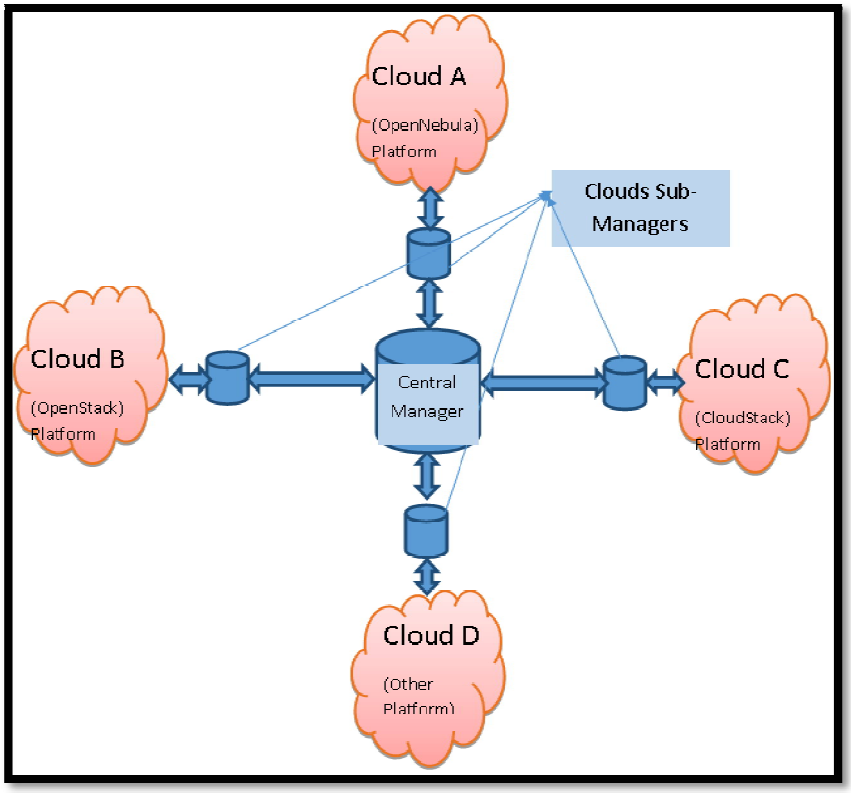

Figure1: Heterogeneous Joint Clouds Framework

The above model indicates four heterogeneous Cloud Service Providers (CSPs) each with a different service manager.

3.1. The Proposed Multiple Joint Clouds Algorithm

The proposed algorithm is of two modules; one is Sub-Manger Device(SMD) and second is for Central-Manager Device(CMD).

Sub-Manger Device(SMD) Algorithm
/*Service Request from Client or User*/
DO /*Loop for number of service requests*/
LOAD Service_Request /*User demand for the service*/
LOAD Service_request Type /*Load decriptions to service Request*/
LOAD Service_Request Capacity
/*Requested Service found on CSP DataBase*/
IF Service_Request FOUND on CSP_DB
/*Independent CSP has to provide the service to its clients*/
LCSP Provide_Service
ELSE
/*Sub-manager provides Sources of requested services on Requesting client Interface*/
LOAD_to_Client; Available Sources
/*Sub-manager make neccessary conversions and configurations*/
CONFIGURE Service_Request Settings
/*Sub-manager loads service request to Central-Manager*/
LOAD_to_CMD Service_Request
ENDIF
WHILE Service_Request <> 0 /*Repeats loop until request =0*/

The Central Manager:Algorithm
/*Service Request from Sub-Manager Device*/
DO /*Loop for Number of Service Requests*/
LOAD Service_Request /*Load Request from SMD*/

LOAD Service_Request type
LOAD Service_Request Capacity
/*Heterogeneity amongs CSPs has to be Cleared*/
IF Standards_Compliance: Ok;
Services_Registration: Ok;
THEN
IF Service_Registered <>Service_Request /*Demanded service NOT Registered*/
THEN
MSG_Requesting_SMD: Service NOT Registered
ELSE
For i = 1 to n /*n - number of CSPs*/
IF Service_Request <> FOUND
THEN
MSG_Requesting_SMD: Service NOT Available
ELSEIF Service_Request FOUND on m /*m - number of CSPs*/
THEN
COMPARE Price_Match /*Resources Billing System*/
IF Price_Match:Ok;
LOAD Service_Request to Nearest FOUND SMD
SMD LOAD Service_Request to CSP
CSP LOAD service to SMD
SMD LOAD Service to CMD
CMD confirm Payment
CMD LOAD Service to Requesting_SMD
WHILE Service_Request <> 0

The following is the proposed digital forensic system domicile in Central Manager of the above heterogeneous Cloud Service Providers.

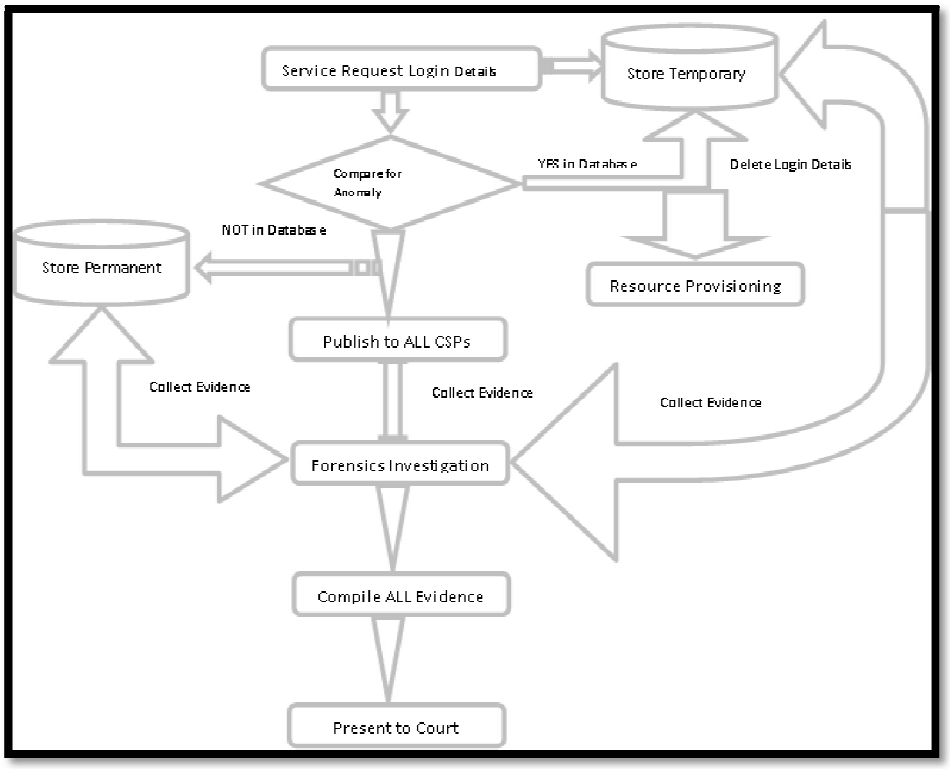

Figure 2: Activity Diagram of Digital Forensic System

4. Discussion on the Proposed Framework

In figure 1, the clouds are joined together and each is assumed to be with the distinct service manager (OpenNabula, Cloudstack, OpenStack, etc.). Each of the Service managers services its customers differently and each has a distinct feature entirely different from others which may lead to the inability of different clouds to inter-operate and share resources.

But by a provision of Sub-Manager and Central Manager, the two, ensure compatibility and standards compliances, to have interoperability among the registered joint clouds.

Control and Management	Operations
• Synchronisation	• Service Broker
• Security Monitoring	• Service Registration
• Service Lifecycle Management	• CSP and Client Registration
• Standards Compliance Monitoring	• SLA Management and Negotiation
• Topology Management	
• Configuration and Protocol Management	
• Metadata Management	
• Admission, Decommissioning and Re-admission	

Table 2: Central Manager Responsibilities

To Central Manager	To CSP
• Present Service Request	• Present Services
• Dynamic Protocols Configuration	• Collect service request
• Present All CSP available Resources	• Present service denial
• Standards Compliance	
• Request for Admission, Re-admission or withdrawal	

Table 3: Sub-Manager Responsibilities

Figure 2 states proposed digital forensics system within that heterogeneity. The User/Subscriber from one cloud make a request of service to his CSP with his LOGIN DETAILS, then the CSP has no such service, then the CSP tenders the request to SUB-MANAGER for onward processing with CENTRAL MANAGER. When request comes to Central Manager, Login detail and Request attributes will be copied to Temporary Memory, then the Central Manager will take LOG AUTHENTICATION (Anomaly Database Analysis), if it exists, then the request will be processed and the Login detail and Request attributes will be deleted the Temporary Memory, else, the REQUEST IS INTRUSION, it will be copied to Persistent Memory and also publish to ALL registered CSPs. The Digital Forensics Investigator collect evidence of intrusion from Temporary Memory, CSPs Memory and Central Manager Persistent Memory, compile and Present to Court when a need arises.

5. Conclusion and Future Work

Heterogeneity in intended joint clouds leads to an inability to interoperate among the Cloud Service Providers and gives way to cloud service intruder to access unauthorised resources. But by harmonizing the differences with devising a framework that can handle the complexity and differences, there will be smooth interoperability. The problem is solved with the development of a concrete framework to handle both heterogeneity issues and to detect Intrusion to unauthorised cloud resources. There is a need in future researches to develop a digital forensic system for the Internet of Things due to its robustness, high complexity and heterogeneity.

6. References

i. Alexander, J. (2013). Digital Forensics for Infrastructure-as-a-Service Cloud Computing. University of Maryland, Baltimore County in.
ii. Alharbi, S. A. (2014). Proactive System for Digital Forensic Investigation. The University of Victoria.
iii. Almulla, S., Iraqi, Y., & Jones, A. (2014). A State-of-the-Art Review of Cloud. JDFSL, 9(4), 22.
iv. Alqahtany, S., & Clarke, N. (2014). A forensically-enabled IAAS cloud computing architecture. In 12th Australian Digital Forensics Conference. (p. 10). Perth, Western Australia: Australian Digital Forensics Conference. https://doi.org/10.4225/75/57b3e3a5fb87e
v. Alqahtany, S., Clarke, N., Furnell, S., & Reich, C. (2016). A forensic acquisition and analysis system for IaaS: Architectural model and experiment. In Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016. https://doi.org/10.1109/ARES.2016.58
vi. Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., ...Rabkin, A. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50. https://doi.org/10.1145/1721654.1721672
vii. Arthur, K. K. (2010). Considerations Towards the Development of a Forensic Evidence Management System. The University of Pretoria.
viii. Audience, T. (2016). Exploring Cloud Incidents, (June), 1–14.
ix. Buyya, R., Buyya, R., Yeo, C. S., Yeo, C. S., Venugopal, S., Venugopal, S., ...Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(June 2009), 17. https://doi.org/10.1016/j.future.2008.12.001
x. Chopra, P., & Bed, R. (2017). STUDY OF CLOUD COMPUTING TECHNIQUES : RESOURCE. International Journal of Computer Engineering and Applications, XI(Xi), 213–222.
xi. Choudhury, K. (2013). Resource Management in a Hybrid Cloud Infrastructure. International Journal of Computer Applications, 79(12), 41–45.

xii. 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

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

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

xv. Elhozmari, M., &Ettalbi, A. (2016). Towards a Cloud Service Standardization to ensure interoperability in heterogeneous Cloud based environment, 16(7), 60–70.

xvi. Garrison, C. p. (2010). Digital forensics for network, internet and cloud computing.

xvii. Grewal, R. K., &Pateriya, P. K. (2012). A Rule-based Approach for Effective Resource Provisioning in Hybrid Cloud Environment. International Journal of Computer Science and Informatics, 101–106.

xviii. Grispos, G., &Glisson, W. B. (2012). Calm Before the Storm : The Challenges of Cloud Computing in Digital Forensics, 4(2), 28–48.

xix. Javadi, B., Abawajy, J., &Buyya, R. (2012). Failure-aware resource provisioning for hybrid Cloud infrastructure. J. Parallel Distrib. Comput., 72(10), 1318–1331. https://doi.org/10.1016/j.jpdc.2012.06.012

xx. Kanungo, P. (2016). Design Issues in Federated Cloud Architectures, 5(5), 937–939. https://doi.org/10.17148/IJARCCE.2016.55229

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

xxii. Kechadi, T. (2015). Digital Forensic Investigations in the Cloud A Proposed Approach for Irish Law Enforcement Digital Forensic Investigations in the Cloud A Proposed Approach for Irish Law Enforcement James Plunkett, Nhien-An Le-Khac, and M-TaharKechadi University College Dublin, Ireland, (January 2016).

xxiii. Kent, K., &Souppaya. (2006). GUIDE TO COMPUTER SECURITY LOG MANAGEMENT.

xxiv. Khan, S., Gani, A., Abdul Wahab, A. W., Iqbal, S., Abdelaziz, A., Mahdi, O. A., … Chang, V. (2016). Towards an Applicability of Current Network Forensics for Cloud Networks: A SWOT Analysis. IEEE Access, 4, 9800–9820. https://doi.org/10.1109/ACCESS.2016.2631543

xxv. Kumar, S., Nadjaran, A., &Gopalaiyengar, S. K. (2014). SLA-based virtual machine management for heterogeneous workloads in a cloud datacenter. Journal of Network and Computer Applications, 45, 108–120. https://doi.org/10.1016/j.jnca.2014.07.030

xxvi. Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current Challenges and Future Research Areas for Digital Forensic Investigation. https://doi.org/10.13140/RG.2.2.34898.76489

xxvii. Martini, B., &Choo, K. 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

xxviii. Mell, P., &Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. Nist Special Publication, 145, 7. https://doi.org/10.1136/emj.2010.096966

xxix. 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

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

xxxi. Nelson, V. (2012). Semantic-based Resource Provisioning and Scheduling in Inter-cloud Environment, 250–254.

xxxii. Rani, D. R., &Geethakumari, G. (2015). An efficient approach to a forensic investigation in the cloud using VM snapshots. In 2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015. https://doi.org/10.1109/PERVASIVE.2015.7087206

xxxiii. Sahoo, P. K., &Chottray, R. K. (2012). Research Issues on Windows Event Log, 41(19), 23–29.

xxxiv. Saokar, S., Patil, S., &Dharaskar, R. (2015). DESIGN FRAMEWORK OF DIGITAL FORENSIC FOR CLOUD COMPUTING : A REVIEW, (12), 91–93.

xxxv. Smit, M., Simmons, B., &Litoiu, M. (2013). Distributed, Application-level Monitoring for Heterogeneous Clouds using Stream Processing.

xxxvi. Sood, S. K. (2013). Dynamic Resource Provisioning in Cloud based on Queuing Model. International Journal of Cloud Computing and Services Science (IJ-CLOSER), 2(4).

xxxvii. 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

xxxviii. Subramanian, T., &Savarimuthu, N. (2016). Application-based brokering algorithm for optimal resource provisioning in multiple heterogeneous clouds. Vietnam Journal of Computer Science, 3(1), 57–70. https://doi.org/10.1007/s40595-015-0055-8

xxxix. Tian, G., &Meng, D. (2010). Failure rules based node resource provision policy for Cloud computing. International Symposium on Parallel and Distributed Processing with Applications. https://doi.org/10.1109/ISPA.2010.69

xl. Toosi, A. N., Calheiros, R. N., &Buyya, R. (2014). Interconnected Cloud Computing Environments : Challenges, Taxonomy, and Survey, 47(1).

xli. Vecchiola, C., Calheiros, R. N., Karunamoorthy, D., &Buyya, R. (2012). Deadline-driven provisioning of resources for scientific applications in hybrid clouds with Aneka. Future Generation Computer Systems, 28(1), 58–65. https://doi.org/10.1016/j.future.2011.05.008

xlii. Wang, J. K., Ding, J., &Niu, T. (2012). Interoperability and Standardization of Intercloud Cloud Computing.

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

xliv. 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).

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

xlvi. 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