Journal of Future Internet
2019 Vol. 3, No. 1, pp. 1-11
ISSN(e): 2409-790X
ISSN(p): 2413-8401
DOI: 10.18488/journal.102.2019.31.1.11
© 2019 Conscientia Beam. All Rights Reserved.

A FRAMEWORK FOR DIGITAL FORENSIC IN JOINT HETEROGENEOUS CLOUD COMPUTING ENVIRONMENT

Zayyanu Umar[1+]
Etuh Emmanuel[2]

[1]*Department of Computer Science, Waziri Umaru Federal Polytechnic, Birnin-Kebbi, Kebbi State, Nigeria.*
Email: zayyanuumar1@yahoo.com
[2]*Department of Mathematics and Computer Science, Arthur Jarvis University, Akpabuyo,Cross River, State, Nigeria.*
Email: emma.etuh@arthurjarvisuniversity.edu.ng

(+ Corresponding author)

Article History
Received: 14 February 2019
Revised: 18 March 2019
Accepted: 23 April 2019
Published: 28 June 2019

Keywords
Digital forensics
Framework
Cloud resources
Cloud computing heterogeneity
Cloud service providers.

ABSTRACT

The cloud computing is nowadays an embracing computing technology by many organizations, academic institutions and business centers. Resources availability, resources capacity, security are among the factors that subscriber consider while rating Cloud Service Providers when subscribing. Cloud Service Providers (CSPs) are limited in some resources, lacking some resources requested by their customers, this gave rise to the need 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. The architectural modeling system was used in developing framework. In this paper, a Digital Forensic Framework that can detect intrusion within heterogeneous joint clouds was developed with the architectural model and algorithm that can handle the joint clouds heterogeneity and complexity during inter-clouds resources management. This study originates a new framework and an algorithm that enable detecting crime and locating a scene of a crime for digital investigation (digital forensic) in a joined different configured cloud service providers (CSPs) platforms.

Contribution/Originality: This study originates a new framework and an algorithm that enable detecting crime and locating a scene of a crime for digital investigation (digital forensic) in a joined different Configured cloud service providers (CSPs) platforms.

1. INTRODUCTION

Cloud computing technology renders the acquisition of hardware and software by the industrial institutions and academic institutions useless, as sensitive data and/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), Microsoft Azure and others, provide services to cloud-end users on a pay-as-you-go service, the users only pay cloud resources utilized [1]. Today, various Cloud Service Providers (CSPs) are aiming to interoperable clouds. The effort is to aggregate or join different forms of cloud service providers, to one cloud platform [2]. Some scholars also have indicated broad interest in creating a cloud-of-clouds where multiple cloud service providers can gain access to resources of each other seamlessly; this can be referred to as a multi-cloud [3]. The main issues with joining multiple and differently configured cloud service providers are enormous, most of the cloud systems are not compatible with one another and cannot share services with one another since everyone speaks a different language [4]. There are no specified service standards that are specific to the effort of joining two or more clouds and these standards are deployed on web browser interfaces. Some cloud providers use SOAP, other ones use REST as communication protocols. Each service has its specific characteristics such as authentication and security requirements [5]. Cloud service providers have not taken into consideration Cloud interoperability issues and each Cloud comes with its own service and interfaces for services [6]. Inconsistency in log formats and data representations with individual cloud to other clouds present challenges to digital investigator, who needs to capture the meaning of the various fields of data in each log to perform a thorough analysis [7].

"The failure of one operating system logging format to be accepted to the other logging format of another operating system creates incompatibility and heterogeneity with the logging functions within clouds operating systems or network devices. This makes centralizing logging a really challenging task" [8]. 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 utilizing existing cloud services as their infrastructure to target their victims [9]. To assist in detecting malicious users and in analyzing the giant clouds logs, mega cloud organizations 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 give confidences to customers who use the service. Developing a universal digital forensic system model that can penetrate into different cloud platforms' transactions to 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 foreign cloud service platforms. Despite the extensive research conducted in the field of cloud forensics, 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 [10-13].

The contemporary researchers are seeking research that handles the security issues for interoperability of joint cloud service platforms with different log formats and standards [6, 14-17].

2. BACKGROUND

Cloud computing is a new system of computation that uses the internet instead of a stand-alone computer to carryout users' computing activities like 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 [18].

The National Institute of Standards and Technology (NIST) defined 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" [19].

There are five main features of cloud computing: ubiquitous network access, on demand self-service, resource pooling, pay- per use 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" these categories are: (a) Platform-as-a-Service (PaaS), (b) Software-as-a-Service (SaaS) and (c) Infrastructure-as-a- Service (IaaS) [18].

Platform-as-a-Service (PaaS) model is used by developers to develop new applications on 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 [20].

Software-as-a-service (SaaS) provides software to the 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 [21].

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

2.1. Cloud Resource Management

Resource management helps in determining which and how much resources are needed and available for the current request, so that Quality of Service (QOS) components such as availability, security, reliability and CPU utilization can be checked [22]. Various cloud-based resource management mechanisms in the existing literature are briefly explained below

2.2. Clouds Resource Management Mechanisms

Various cloud based resource Management mechanisms are as follows:

Queuing Model-Based: A dynamic resource provisioning mechanism is proposed while removing deadlocks among the processes requesting for resources [23].

Reliability-Based: This policy takes care of resource provisioning in cloud based environment while improving reliability of the virtual machines providing these resources [24].

Various brokering strategies have been proposed while modifying the backfilling scheduling algorithm to give a fault free environment for private cloud for provisioning resources [25].

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 public cloud for resources [26, 27].

Service Level Agreement (SLA) based: Resource provisioning policy for heterogeneous clouds is proposed by considering their SLA. The policy results in maximum utilization of resources also by decreasing risk of underutilization of resources [28].

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 [29].

Deadline Based: The researcher proposed deadline driven resource provisioning algorithm for cloud application platform ANEKA while reducing application execution time [30].

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 [31].

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

By the emergence of cloud computing, data is distributed on platforms in different regions from one to various data centers in different file systems and different formats, spilling from one platform server to another. A user can be in any location of the world and the volatile nature of data in use is another big challenge.

In this regards, there is 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 in 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.

A recent development in cloud technologies indicates the need for migration onto emerging Multi-cloud models and frameworks. They provide a common and interoperable environment capability.

Multi-cloud can be defined as an integration of heterogeneous individual clouds to interoperate together to serve the customers' needs; what they want, the way they want it, and for a security purpose.

This heterogeneity in a joint cloud computing environments is a severe challenge as it intensifies barriers in the path of the ubiquitous cloud realization. The main obstruction is vendor lock-in, which is un- avoidable 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 [6]. As Cloud Computing provides several benefits to customers and poses several security challenges to digital forensics and criminal investigation, so also joint multiple clouds in an increasing capacity faces 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 [32] 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, drawn and proven methods to build past, live and attempted cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence.

Audience [33] 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 behavior into a traditional network forensics process when an incidence happen.

Live incident: Live forensic investigator aims at arresting forensic data from a live and running system before switching off the power. In general, live forensic acquisition is commonly conducted to get volatile data that will be lost when 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 big challenge to the investigator, as the evidence has to be tenable, reliable, original and court ready.

3. LITERATURE REVIEW

There are alot of researches partaining the forensic investigations in cloud computing services. Majority of the researches 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 [34] 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 components then deploying offline forensics tools for investigations. He was able to identify the challenges and requirements for virtual computing forensic investigation. In his study, he was able to address the issues realted to the dead/live forensic investigation.

Alharbi [35] in his thesis report titled *"Proactive System for Digital Forensic Investigation"*designed a system that takes live digital forensics investigation in cloud computing environment. It mitigates the challenges faced by Reactive Digital forensics(RDF) that takes the investigation on seized devices.

Martini and Choo [36] developed a framework that differentiates the way data are collected and preserved between cloud computing digital forensics process and traditional digital forensics processess. They discussed challenges and issues of cloud computing digital forensic in context of framework they developed.

In the thesis report titled: "*New challenges in digital forensics: online storage and anonymous communication*" the reesearcher developed a framework that mitigates recents 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 lunched on dropbox to test the workability of the framework [37]. 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 delopyed in cloud computing [38].

In his thesis report titled "*Digital Forensics for Infrastructure-as-Service*

Cloud Computing", Alexander [10] identified specific challenges of forensics in cloud computing and analysed the depecicies with existing forensic remote tools. He developed a tool that can enable trustworthy forensics of Software as a service(SAAS) model using openstack cloud environment. Kebande [39] in his thesis report proposed model and named it Cloud Forensic Readiness as a Service (CFRaaS) model and developed CFRaaS software application prototype. The CFRaaS model use 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 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 and Hasan [40].

Alqahtany and Clarke [32] developed acquisition and analysis model that extracts evidence from client not from Cloud Service Provider(CSP). The model gives admissible and richer evidence.

In another research titled: Forensicloud: An Architecture for Digital Forensic Analysis in the Cloud, the researchers developed a framework that reduce the time taken when taking digital investigation by leveraging on the power of a high performance computing platform and by deploying existing tools to operate within this environment. Furthermore, the researchers with thier model gave access to some liceinced tools that are not opensources tools to use [41].

Dykstra and Sherman developed a cloud forensic tool called FROST.The tool 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 [42].

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 integrity of digital evidence in FEMS while Casey's Certainty Scale is employed in integrity classification scheme [43].

In another research titled: *Cybercrime forensic system in cloud computing*. The researcher developed framework to monitor and analyse the cybercrimes in cloud computing using Encase and FTK Yan [44].

Zawoad, et al. [45] 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.

There are several digital forensic tools built to serve a proprietary platform. The following table indicates different digital forensic tools built on a different platform to serve on individual platform and does not work for others platforms.

Table-1. Digital Forensic Tools with Different 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

Source: Rani and Geethakumari [46].

4. FRAMEWORK OF PROPOSED SYSTEM

The heterogeneity among the cloud computing service providers gives rise to the need 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 concrete unified forensic system in simplifying court processes.

4.1. The Proposed Framework is as Follows

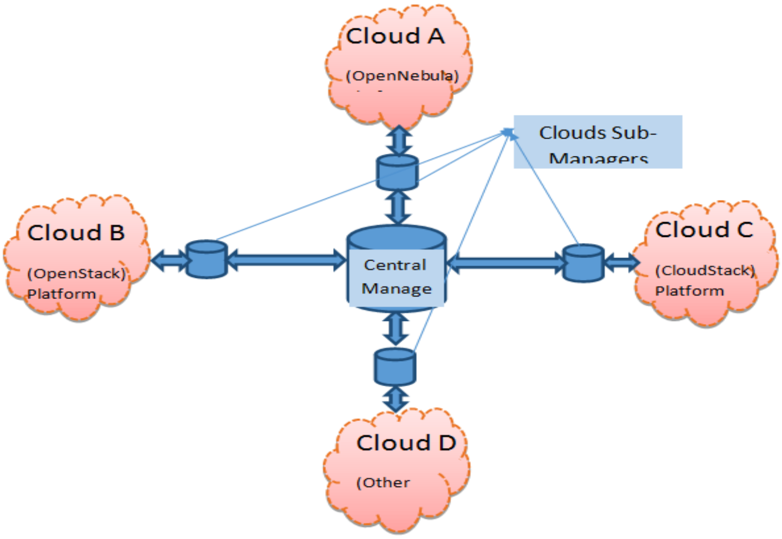

Figure-1. Heterogeneous Joint Clouds Framework.

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

4.2. 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*/
        THEN 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.

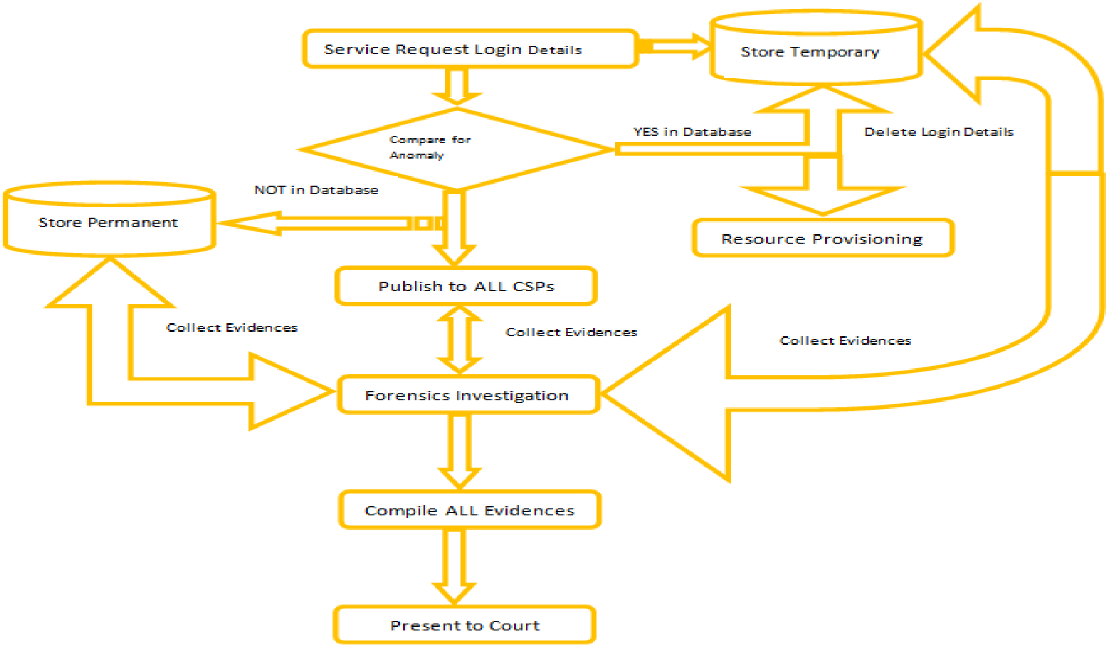

Figure-2. Activity Diagram of Digital Forensic System.

5. DISCUSSION ON THE PROPOSED SYSTEM

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

But by provision of Sub-Manager and Central Manager, the two, ensure compatibility and standard compliance, so as to have interoperability among the registered joint clouds.

Table-2. Central Manager Responsibilities (as in Figure 1).

Control and Management	Operations
• Synchronization	• Service Broker
• Security Monitoring	• Service Registration
• Service Life cycle 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-3. Sub-Manager Responsibilities (as in Figure 1).

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	

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, if 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 exist, then the request will be processed and the Login detail and Request attributes will be deleted from the Temporal 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 evidences of intrusion from Temporal Memory, CSPs Memory and Central Manager Persistent Memory, compile and Present to Court when need arises.

6. CONCLUSION AND FUTURE WORK

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

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Contributors/Acknowledgement: Both authors contributed equally to the conception and design of the study.

REFERENCES

[1] S. Sotiriadis and N. Bessis, "An inter-cloud bridge system for heterogeneous cloud platforms," *Future Generation Computer Systems*, vol. 54, pp. 180-194, 2015. Available at: https://doi.org/10.1016/j.future.2015.02.005.

[2] F. Yu, C. Stella, and K. A. Schueller, "A design of heterogeneous cloud infrastructure for big data and cloud computing services," *Open Journal of Mobile Computing and Cloud Computing*, vol. 1, pp. 1-16, 2014.

[3] M. Smit, B. Simmons, and M. Litoiu, "Distributed, application-level monitoring for heterogeneous clouds using stream processing," *Future Generation Computer Systems*, vol. 29, pp. 2103-2114, 2013. Available at: ttps://doi.org/10.1016/j.future.2013.01.009.

[4] C. P. Garrison, *Digital forensics for network, internet and cloud computing*. USA: Elsevier Inc, 2010.

[5] M. Elhozmari and A. Ettalbi, "Towards a cloud service standardization to ensure interoperability in heterogeneous cloud based environment," *nternational Journal of Computer Science and Network Security*, vol. 16, pp. 60–70, 2016.

[6] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected cloud computing environments: Challenges, taxonomy, and survey," *ACM Computing Surveys (CSUR)*, vol. 47, pp. 1-47, 2014. Available at: https://doi.org/10.1145/2593512.

[7] K. Kent and Souppaya, *Guide to computer security log management*. USA: NIST Special Publication 800-92, 2006.

[8] P. K. Sahoo and R. K. Chottray, "Research issues on windows event log," *International Journal of Computer Applications*, vol. 41, pp. 23–29, 2012. Available at: https://doi.org/10.5120/5650-8030.

[9] S. Alqahtany, N. Clarke, S. Furnell, and C. Reich, "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*, 2016.

[10] J. Alexander, *Digital forensics for infrastructure-as-a-service cloud computing*. Baltimore County: University of Maryland, 2013.

[11] G. Grispos and W. B. Glisson, "Calm before the storm: The challenges of cloud computing in digital forensics," *International Journal of Digital Crime and Forensics*, vol. 4, pp. 28–48, 2012. Available at: https://doi.org/10.4018/jdcf.2012040103.

[12] P. Kanungo, "Design issues in federated cloud architectures," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, pp. 937–939, 2016.

[13] S. Saokar, S. Patil, and R. Dharaskar, "Design framework of digital forensic for cloud computing: A review," *International Journal of Advanced Computational Engineering and Networking*, vol. 3, pp. 91–93, 2015.

[14] S. Almulla, Y. Iraqi, and A. Jones, "A state-of-the-art review of cloud," *The Journal of Digital Forensics, Security and Law*, vol. 9, p. 22, 2014. Available at: https://doi.org/10.15394/jdfsl.2014.1190.

[15] Y. Demchenko, F. Turkmen, M. Slawik, and D. C. Laat, "Defining intercloud security framework and architecture components for multi-cloud data intensive applications," presented at the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). IEEE, 2017.

[16] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current challenges and future research areas for digital forensic investigation," presented at the 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), 2016.

[17] J. K. Wang, J. Ding, and T. Niu, "Interoperability and standardization of intercloud cloud computing." Available: https://arxiv.org/pdf/1212.5956.pdf, 2012.

[18] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, and A. Rabkin, "A view of cloud computing," *Communications of the ACM*, vol. 53, p. 50, 2010. Available at: https://doi.org/10.1145/1721654.1721672.

[19] P. Mell and T. Grance, "The NIST definition of cloud computing recommendations of the national institute of standards and technology," *Nist Special Publication*, vol. 145, p. 7, 2011.

[20] R. Buyya, R. Buyya, C. S. Yeo, C. S. Yeo, S. Venugopal, S. Venugopal, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, pp. 599-616, 2009. Available at: https://doi.org/10.1016/j.future.2008.12.001.

[21] S. Khan, A. Gani, A. W. A. Wahab, S. Iqbal, A. Abdelaziz, O. A. Mahdi, A. I. Abdallaahmed, M. Shiraz, Y. R. B. Al-Mayouf, and Z. Khan, "Towards an applicability of current network forensics for cloud networks: A SWOT analysis," *IEEE Access*, vol. 4, pp. 9800-9820, 2016. Available at: https://doi.org/10.1109/access.2016.2631543.

[22] P. Chopra and R. Bed, "Study of cloud computing techniques: Resource," *International Journal of Computer Engineering and Applications*, vol. 11, pp. 213–222, 2017.

[23] S. K. Sood, "Dynamic resource provisioning in cloud based on queuing model," *International Journal of Cloud Computing and Services Science*, vol. 2, pp. 314-320, 2013.

[24] G. Tian and D. Meng, "Failure rules based node resource provision policy for cloud computing," in *Proceedings of the International Symposium on Parallel and Distributed Processing with Applications. IEEE Computer Society*, 2010, pp. 397-404.

[25] B. Javadi, J. Abawajy, and R. Buyya, "Failure-aware resource provisioning for hybrid Cloud infrastructure," *Journal of Parallel and Distributed Computing*, vol. 72, pp. 1318–1331, 2012. Available at: https://doi.org/10.1016/j.jpdc.2012.06.012.

[26] K. Choudhury, "Resource management in a hybrid cloud infrastructure," *International Journal of Computer Applications*, vol. 79, pp. 41–45, 2013. Available at: https://doi.org/10.5120/13796-1925.

[27] R. K. Grewal and P. K. Pateriya, "A rule-based approach for effective resource provisioning in hybrid cloud environment," *International Journal of Comp Uter Science and Informatics*, vol. 1, pp. 101–106, 2012. Available at: https://doi.org/10.1007/978-3-642-35461-8_5.

[28] S. Kumar, A. Nadjaran, and S. K. Gopalaiyengar, "SLA-based virtual machine management for heterogeneous workloads in a cloud datacenter," *Journal of Network and Computer Applications*, vol. 45, pp. 108–120, 2014. Available at: https://doi.org/10.1016/j.jnca.2014.07.030.

[29] V. Nelson, "Semantic based resource provisioning and scheduling in inter-cloud environment," presented at the 2012 International Conference on Recent Trends in Information Technology, Chennai, Tamil Nadu, India, 2012.

[30] C. Vecchiola, R. N. Calheiros, D. Karunamoorthy, and R. Buyya, "Deadline-driven provisioning of resources for scientific applications in hybrid clouds with Aneka," *Future Generation Computer Systems*, vol. 28, pp. 58-65, 2012. Available at: https://doi.org/10.1016/j.future.2011.05.008.

[31] T. Subramanian and N. Savarimuthu, "Application based brokering algorithm for optimal resource provisioning in multiple heterogeneous clouds," *Vietnam Journal of Computer Science*, vol. 3, pp. 57-70, 2016. Available at: https://doi.org/10.1007/s40595-015-0055-8.

[32] S. Alqahtany and N. Clarke, "A forensically-enabled IAAS cloud computing architecture," in *12th Australian Digital Forensics Conference. Perth, Western Australia: Australian Digital Forensics Conference*, 2014, p. 10.

[33] T. Audience, "Exploring cloud incidents," *The European Union Agency for Network and Information Security (ENISA)*, pp. 1–14, 2016.

[34] P. Digambar, *A novel digital forensic framework for cloud computing environment.* Pilani: Birla Institute of Technology and Science, 2015.

[35] S. A. Alharbi, *Proactive system for digital forensic investigation*: University of Victoria, 2014.

[36] B. Martini and K. K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, vol. 9, pp. 71–80, 2012. Available at: https://doi.org/10.1016/j.diin.2012.07.001.

[37] M. Mulazzani, *New challenges in digital forensics: Online storage and anonymous communication.* Faculty of Informatics, Vienna University of Technology, Vienna, 2014.

[38] T. Kechadi, *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.* Ireland: University College Dublin, 2015.

[39] V. R. Kebande, *A novel cloud forensic readiness service model: Department of computer science.* South Africa: University of Pretoria, 2017.

[40] S. Zawoad and R. Hasan, "Trustworthy digital forensics in the cloud," *Computer*, vol. 49, pp. 78-81, 2016. Available at: https://doi.org/10.1109/mc.2016.89.

[41] C. Miller, D. Glendowne, D. Dampier, and K. Blaylock, "Forensicloud: An architecture for digital forensic analysis in the cloud," *Journal of Cyber Security and Mobility*, vol. 3, pp. 231-262, 2014. Available at: https://doi.org/10.13052/jcsm2245-1439.331.

[42] J. Dykstra and A. T. Sherman, "Design and implementation of FROST: Digital forensic tools for the openstack cloud computing platform," *Digital Investigation*, vol. 10, pp. S87-S95, 2013. Available at: https://doi.org/10.1016/j.diin.2013.06.010.

[43] K. K. Arthur, *Considerations towards the development of a forensic evidence management system*: University of Pretoria, 2010.

[44] C. Yan, "Cybercrime forensic system in cloud computing," in *Proceedings of 2011 International Conference on Image Analysis and Signal Processing, IASP 2011, (Dc)*, 2011, pp. 612–613.

[45] S. Zawoad, R. Hasan, and A. Skjellum, "OCF: An open cloud forensics model for reliable digital forensics," in *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015, (July)*, 2015, pp. 437–444.

[46] D. R. Rani and G. Geethakumari, "An efficient approach to forensic investigation in cloud using VM snapshots," in *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, 2015.

Views and opinions expressed in this article are the views and opinions of the author(s), Journal of Future Internet shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.