A Digital Forensic Framework Design for Joined Heterogeneous Cloud Computing Environment

Zayyanu Umar[1], Deborah U. Ebem [2], Francis S. Bakpo [3] and Modesta Ezema[4]

deborah.ebem@unn.edu.ng [2], Francis.bakpo@unn.edu.ng[3] modesta.ezema@unn.edu.ng[4]

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

Department of Computer Science, University of Nigeria .[2], [3], [4] Nsukka,
Enugu, Nigeria

Abstract

Cloud computing is now used by most companies, business centres and academic institutions to embrace new computer technology. Cloud Service Providers (CSPs) are limited to certain services, missing some of the assets requested by their customers, it means that different clouds need to interconnect to share resources and interoperate between them. The clouds may be interconnected in different characteristics and systems, and the network may be vulnerable to volatility or interference. While information technology and cloud computing are also advancing to accommodate the growing worldwide application, criminals use cyberspace to perform cybercrimes. Cloud services deployment is becoming highly prone to threats and intrusions. The unauthorised access or destruction of records yields significant catastrophic losses to organisations or agencies. Human intervention and Physical devices are not enough for protection and monitoring of cloud services; therefore, there is a need for more efficient design for cyber defence that is adaptable, flexible, robust and able to detect dangerous cybercrime such as a Denial of Service (DOS) and Distributed Denial of Service (DDOS) in heterogeneous cloud computing platforms and make essential real-time decisions for forensic investigation. This paper aims to develop a framework for digital forensic for the detection of cybercrime in a joined heterogeneous cloud setup. We developed a Digital Forensics model in this paper that can function in heterogeneous joint clouds. We used Unified Modeling Language (UML) specifically activity diagram in designing the proposed framework, then for deployment, we used an architectural modelling system in developing a framework. We developed an activity diagram that can accommodate the variability and complexities of the clouds when handling inter-cloud resources.

Keywords:

Framework, Cloud Computing Heterogeneity, Digital Forensics, Cloud Service Providers.

1. Introduction

Cloud computing technology makes it unnecessary for industrial organisations and academic institutions to procure hardware and software because organisations' important information is often stored in data centers around the globe of cloud service providers (CSP), no longer on local disk drives of institutions.

Manuscript received June 5, 2024
Manuscript revised June 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.6.24

Cloud computing services is a concept which allows omnipresent, secure, on-demand network access to customisable computing resources shared pool (such as databases, networks, software, processing and services) that can easily be provided and dispatched with a limited commitment of management or involvement of cloud service provider [9].

Cloud computing supports science and technological applications including computer finance, data mining and many other data-intensive operations by facilitating a paradigmatic shift from local to network-centered computing and network-centered information[25].

By the advent of cloud computing services, the data is spread from one or different data centres to different regions and in various file format systems, flowing from one site to other different sites. A cloud computing service consumer can be from any perspective of the world and yet another big challenge is the volatility aspect of the data in use.

The National Institute of Standards and Technology (NIST) describes Cloud Computing service as: "A framework for allowing universal, easy, on-demand network access to a shared pool of customisable 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" [28].

Cloud computing has five main features: ubiquitous network connectivity, self-service Asset pooling, pay peruse, quick elasticity on demand. The software-based cloud service providers can be grouped into three major categories, is termed to as 'cloud service models' such as Infrastructure as service, Platform as service, and Software as service,[7].

Cloud resource management assists in deciding what and volume resources are in need and level of accessible to a user-request so that items such as availability, protection, performance and use of CPUs can be verified [12].

When Cloud computing deployment increasing, consumers and other providers need to use new models to leverage

further their full capacity, including the introduction of cloud federations. Despite the aforementioned benefits, cloud service has also contributed to numerous problems emerging. Until cloud deployment multiple considerations need to be addressed. Many of these challenges are ascribed to remote available resources, cloud computing location in another country, no cloud service monitoring etc. Most of the above problems give the cyber-attacker the solid basis to evaluate the loopholes and manipulate the cloud infrastructure[35].

The Usage of a Virtual Machine (VM) and Hypervisor Software is also a security issue as Hypervisor and VM technologies are vulnerable to attacks at the VM level. Such problems include quite a few on-site computing companies and may include a large number of hardware and software systems. Attackers may exploit vulnerabilities in the VM infrastructure to violating the espionage act or to execute attacks such as DDoS. (Distributed Denial of Services)[17].

Multi-cloud can be described as combining different individual clouds to communicate with each other to serve customers whatever they want, how they want, and for protection. This heterogeneity is a severe problem of shared cloud computing environments as it generates obstacles in the way of the omnipresent cloud realisation. Another obstacle is the lock-in of vendors, customers submitting a request for cloud service have to tailor their requests to suit the cloud provider's pattern and interfaces, resulting in costly and difficult future relocations[38].

Since cloud computing offers many benefits to consumers and poses many security threats for a digital forensics investigation, many clouds are also facing the same. Trustable-security remains a peculiar problem, if we are transferring business data to a hybrid, public and private cloud platform. Likewise, a decision by an company to stay in-house with company data will not improve security threats. A company retains some strategic flexibility by remaining in-house compared to cloud environment. This is because business customers are forced to work with unfamiliar cloud network administrator handling such a highly scalable data house[32].

In particular, there are six main stages of an electronic forensic procedure: identification, storage, compilation, assessment, examination, and presentation. The Cloud Forensics as a term was first used in 2010, and is defined as a hybrid of two notions; digital forensics and cloud computing [5], the researcher applied traditional digital forensics methods to monitor threats or locate prosecutable exhibits. NIST: "Cloud Computing Forensic Science Challenges" [31] described digital forensic for cloud service platform as using expert concepts, professional practice and validated methods to construct past, live and tempted cloud computing incidents by detecting, gathering, storing, analysing, interpreting and reporting digital evidence. Green [19], found that in the cloud environment, there are three different forms of digital forensics: live or post-incident before the event.

Before incident: To track the network to try to turn any possible unusual behaviour into a standard forensic network system when an attack occurs.

Live incident: Live forensic investigator tries to arrest forensic information before turning off the power from a live and operating device. Generally speaking, the live forensic acquisition is usually carried out to collect unreliable details that will be missing if a conventional forensic data gathering is introduced.

Post-incident: as the name implies, the police receive a physical and logical record of every module for necessary investigation after an incident happens. There are many types of research in cloud computing systems that share forensic investigations. Most works are either on the client or server sides and are more limited to the individual Cloud computing center.

Numerous cloud systems like Amazon Web Service, Open Stack, Rackspace, Microsoft Azure, Google Compute Engine and so on offer pay-as-you-go access to cloud customers that is users charge for the cloud resources used[37]. Most cloud service providers are now focused on interoperable platforms. The aim is to integrate varied cloud service providers into a single cloud service platform [41]. Other scholars suggested an interest in developing a network where various cloud service platforms can seamlessly access resources that we and others call the multicloud[36].

The main problem with joining many or similar existing cloud service providers is that most cloud systems are not consistent and cannot share resources among themselves, as everyone communicates with a different dialect[18]. There are no specific service requirements for combining two or more clouds, and these principles are based on browser pages. Many cloud providers utilise SOAP(Simple Object Access Protocols), while others use REST (Representational State Transfer) as protocols for interaction. Each product has its distinct features, like security and authentication specifications[16]. Cloud environments have also not considered cloud interoperability into account, and each Cloud has its platform and software interfaces[38].

Incoherence in data and login formats of individual clouds to other cloud computing environments yields problems for contemporary researchers. They need to attain the context of the different data fields in every access to conduct a comprehensive analysis[24]. Inability to accept one operating system logging format into the other operating systems logging formats generates incompatibility and inconsistency with cloud network devices and operating systems logging functions. It leads to logging hierarchical a challenging task[33]. Through implementing this new technology to join several clouds to interoperate and enjoy other interconnection advantages,

intruders lunch malicious act to grab a specific resource on cloud service platforms to hack resources or access crucial information. Network service intruders use available cloud computing modules as their tools to launch an attack[6]. Mega cloud companies have to introduce a new mechanism to convert logs of various content and specifications from varied cloud environments into a common standard mechanism with standardised representations of data fields to help detect malicious users and analyse giant cloud logs, allowing service customers to be interoperable and privatised.

Numerous researchers have conducted researches in the area of cybercrimes in a cloud computing environment, digital forensics investigation and heterogeneity among current cloud service platforms. The absence of standards for control and settings of heterogeneous infrastructures and lack of a digital forensic framework for detection cybercrime denies companies who need to utilise heterogeneous infrastructures in the transaction model of advantage from infrastructure heterogeneity such as resource management, geographical advantages, pricing model, hypervisor type benefits, recovery, and security.
Despite all researches conducted in the area of cloud cybercrimes detection and subjecting it to digital forensics processing, still, numerous researchers indicate the need for a framework that deals with cybercrimes detection pertaining heterogeneous cloud computing environment and to facilitate digital forensic investigation[3, 11, 40].

Framing a standard model for a digital forensic model that penetrate shared transactions between different cloud systems and identify the intruder and the intrusion scene will simplify a digital forensic investigator's tasks. In this article, we present a proposed framework for digital forensic that can be used in interconnected different configured clouds setup to detect cybercrime that can be useful to a cloud computing environment forensic investigator. Various authors have published articles on cloud heterogeneity, cloud computing services and digital forensics on cloud service systems. Despite all researches done in the field of cloud forensics, numerous studies have also highlighted the need for a comprehensive study involving a collaboration of different cloud service platform models, supporting different cloud platform types, liberates security threat logs and promotes virtual forensic investigation[1, 20, 21, 34]. The contemporary academicians are looking for work that addresses the security threat of joined cloud service platform interoperability with specific log formats and standards[4, 13, 26, 38, 39].

In this work, we propose a framework for digital forensic that can be used in joined heterogeneous configured clouds platform for detection of cybercrime and onward forwarding for prosecution. The paper is divided into introduction, research questions, and review of related works, methodology, proposed framework, discussions on proposed framework and conclusion.

2. HETEROGENEOUS CLOUD ENVIRONMENT

This can be described as a combination of several vendors at different stages (coordination of different vendors by single hypervisor at different stages) or the same level (coordination of vendors by multiple different hypervisors), service scheduling algorithm, service broking, security mechanisms deployed, host operating system and other infrastructures' capacity[10]. Table 1.0 shows the structure.

Table 1: Heterogeneous Cloud Service Providers(CSP)

Provider	Operating System	Hypervisor	S
CSP1	Linux	?	
CSP2	Window	?	
CSP3	Unix	?	H

3. RELATED WORKS

In a study report with the title "A Novel Digital Forensic Framework for Cloud Computing Environment"[14], developed an approach that can be applied for forensic investigation in the virtual cloud computing environment instead of conventional approaches to apprehending digital criminals, seizing physical computer system gadgets such as a server, external memory, hard drive and other noticeable components and then launching offline forensic investigation instruments. He identified problems and criteria for forensic analysis in digital computing. He addressed the issues surrounding the live and dead forensic investigation in his research.
Alharbi[2], The study report with the title "Proactive System for Digital Forensic Investigation," developed a mechanism requiring active digital forensic investigation in the cloud service platform. It solved the issues facing Reactive Electronic forensics (RDF), using the seized devices for investigation.

In another study by Martini and Choo[27], they designed a system that segregates the storage and collection and of information between the process of digital forensics in cloud computing and the conventional method of digital forensics. In the scope of the system they created, they addressed challenges and issues of electronic forensic cloud computing. The study report with a title: "New challenges in digital forensics: online storage and anonymous communication," The investigator built a system to overcome the challenges posed by digital forensics on cloud computing storage platform and discussed anonymous

communication challenges. It used Dropbox to launch an attack to test the framework's workability[30].

In a study with the title "Digital Forensic Investigations in the Cloud: A Proposed Approach for Irish Law Enforcement." An approach was designed to overcome the shortcomings of conventional forensic investigation system and the issues presented to digital forensic professionals working in law enforcement in Ireland by cloud computing. The author studied the traditional methods of forensic investigation and the reasons they are deficient to be deployed into a cloud service platform[23].

In another study with the title "Digital Forensics for Infrastructure-as-Service Cloud Computing" Alexander"[1], established unique forensic problems in a cloud service environment. He examined the specificities with current forensic investigation remote tools. The author built a platform that enables trusted software as a Service template forensics using the cloud computing service platform of OpenStack.

In another study by Kebande[22], the author suggested a design and called it "Cloud Forensic Readiness as a service model (CFRaaS)." He created a prototype of CFRaaS software application. The CFRaaS model uses a malicious botnet's functionality, but its functionality is modified to establish possible cloud proof. The template retains such evidence electronically and stores it for DFR purposes in an electronic forensic database.

Zawoad Hasan established that forensic cloud infrastructure facilitated in identification and preservation of the necessary evidence while preserving the confidentiality and dignity of proof. The model is the popular opensource on Openstack. The first defined properties in clouds to aid trusted forensics[42].
Alqahtany Clarke [5] designed a model of acquisition and evaluation, which extracts the non-Cloud Service Provider(CSP) client facts. The template provides proof that is prosecutable and rich.

In a thesis with a title: "Forensicloud: An Architecture for Digital Forensic Analysis in the Cloud," the authors designed a system to reduces the duration needed for basic research through balancing the high performance computing power and integrating available tools to function within that context. Besides, authors with such a template have access to specific licensed resources that are not free to subscribe[29].

Sherman and Dykstra designed a forensic tool for cloud computing environment called FROST: FROST has been designed. The software helps law enforcement, cloud clients and forensic investigators to collect reliable forensic information irrespective of cloud system platforms. The mechanism was designed mainly for private cloud platform: Openstack only[15].

In another work, developed by Arthur, "Cloud Forensic Evidence Management System (FEMS)" to tackle the problems of storing digital evidence and ensure digital evidence-related accuracy and credibility. It used the Biba Integrity Model to preserve the integrity of digital evidence in FEMS, but they also used Casey's Certainty Scale in the assessment of reliability[8].

In another work titled: "Cybercrime forensic system in cloud computing." Using Encase and FTK, the author developed a system for tracking and analysing cloud crime[40].

Zawoad, Hasan and Skjellum [43] developed an Open Cloud Forensics concept and revealed shortcomings of digital forensic systems by analysing cloud computing environments and various entities involved in the Cloud while implementing existing cloud infrastructures. The system (OCF) in a realistic scenario could help useful electronic forensics.

4. METHODOLOGY

The paper considered the heterogeneity that exists between the individual cloud computing environment, such as virtual machine platform, scheduling algorithm, Security mechanisms, cloud service broking, service pricing and infrastructure capacity, etc. Middleware has to be employed for conversion and de-conversions, translations and Re-translations of individual differences of cloud environments. The design used Service Level Agreement (SLA) and standards binding all interconnecting individual cloud computing platforms. We used Unified Modeling Language (UML) specifically activity diagram in designing the proposed framework, then for the deployment diagram, we used an architectural modelling system in developing a framework.

5. PROPOSED FRAMEWORK

Cloud computing service providers' diversity gives rise to design requirements that can resolve discrepancies and test the policy enforcement and other Service Level Agreement. Therefore, resolving cloud discrepancies enables the creation of a practical integrated forensic platform to simplify court procedures. The interconnection of heterogeneous cloud environments will also determine the issue of leaving the subscriber locked-in, looking for a resource that his primary subscribed Cloud does not have. Figure 1 below depicts the interconnections of

heterogeneous Cloud to share resources. The above figure depicts the

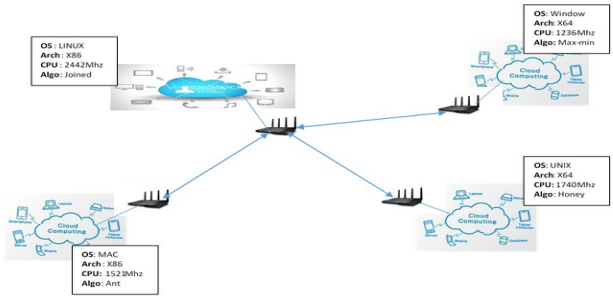

Figure 1: Joined Heterogeneous Clouds Diagram

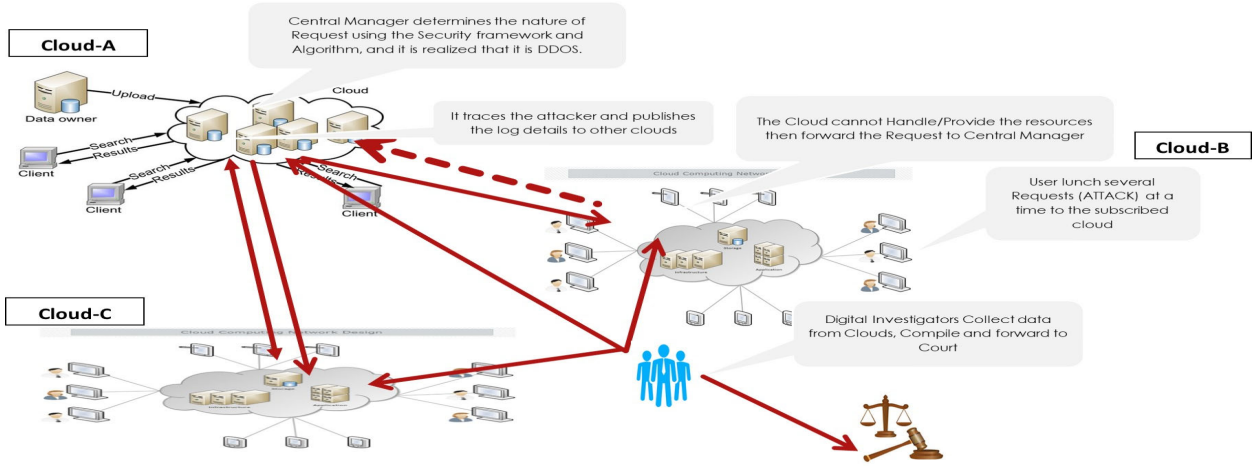

Figure 2: Architectural Design for Forensic framework in Joined clouds

diagram) states how the inter-connected clouds interoperate to enable subscribers to share resources amongst the joined heterogeneous Cloud. Compliance with standards,

interconnection of different cloud configurations to share resources. If one Cloud does have resources requested by its subscribers, then the cloud channel the packets requests to the central Cloud for services. The following figure 2 below depicts a scenario of intrusion detection in joined heterogeneous clouds. The next figure 3(activity

Figure 3: Service Provision amongst Joined Heterogeneous Clouds

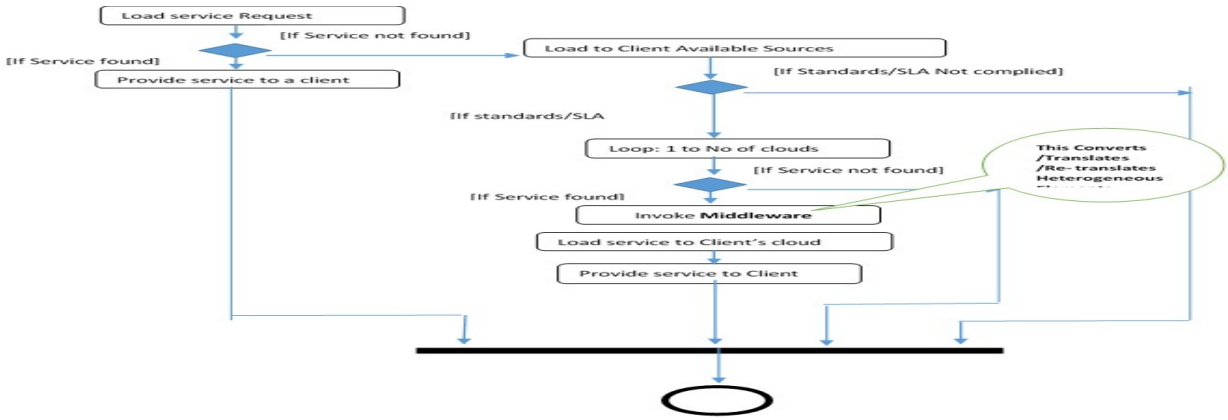

Figure 3: Service Provision amongst Joined Heterogeneous Clouds

Service Level Agreement (SLA) and service cost and use of Middleware has to be provided in the interconnection of different cloud setup. The following figure 4 depicts how the central Cloud detects the cybercrime and publish the attackers log details to all connected clouds for future references by a digital investigator.

6. PROPOSED FRAMEWORK DISCUSSION

In this paper, the diagrams depict that the clouds are joined to a central cloud that is responsible for managing the affairs of interoperation and enable different clouds to share resources. Each Cloud is distinct with different scheduling algorithms, operating systems, set of

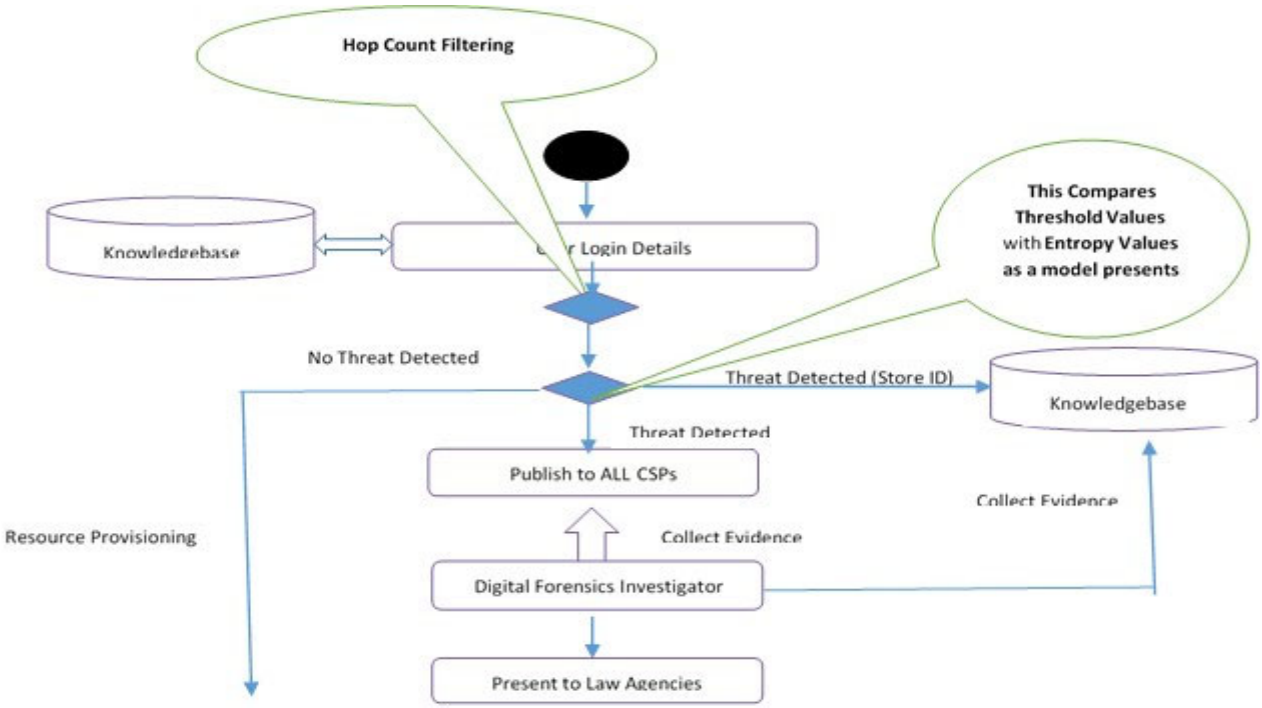

Figure 4: Activity Diagram for Forensics Service in Joined Clouds

subscribers, system architectures and other features entirely different. In this diversity, it also introduces the proposed digital forensics framework. A client from individual Cloud submits a resource-request to his subscribed CSP; then if the CSP does not have such a resource, the CSP forwards the resource-request to the CENTRAL CLOUD, the Central Manager must verify the essence of the request (Anomaly Analysis) when the request comes to Central Manager, If there is a threat, the details of intrusion will be copied to the central Cloud's Permanent Memory and distributed to ALL subscribed Cloud Service Providers. Then, Digital Forensics Investigator gathers information from linked CSPs Memory and Central Manager Persistent Memory of intrusion/attacker log data, compiles and Present to Court when necessary.

7. CONCLUSION AND FUTURE WORK

Variability in designed joint cloud service providers gives rise to the inability to interact with cloud service providers and restrict cloud service active users to be trapped in their resource demands. Harmonising the heterogeneity among interconnected clouds by developing a prototype and system that can accommodate the complexities and differences, then, there will be the satisfaction to subscribers and smooth interoperability service providers. With the design of a concrete forensic system to manage both diversity obstacles and for the detection infringed unauthorised access to joined cloud services, the problem can be solved. Because of its robustness, high complexity and heterogeneity, future research is needed to build a basic forensic framework for the Internet of Things (IoT).

References

[1] Josiah Alexander. *Digital Forensics for Infrastructure-as-a-Service Cloud Computing*. PhD thesis, University of Maryland, Baltimore., 2013.

[2] Soltan Abed Alharbi. *Proactive System for Digital Forensic Investigation*. PhD thesis, University of Victoria, 2014.

[3] Syed Ahmed Ali, "Challenges in Cloud Forensics," in *International Conference on Cloud and Big Data Computing*, pp. 6–10, Barcelona, 2018.

[4] Sameera Almulla, Youssef Iraqi, and Andrew Jones, "a State-of-the-Art Review of Cloud Forensics," *JDFSL*, vol. 9, no. 4, p. 22, 2014.

[5] Saad Alqahtany and Nathan Clarke, "A forensicallyenabled IAAS cloud computing architecture," in *12th Australian Digital Forensics Conference.*, p. 10, Perth, Western Australia, 2014. Australian Digital Forensics Conference.

[6] Saad Alqahtany, Nathan Clarke, Steven Furnell, and Christoph 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.

[7] Michael Armbrust, Ion Stoica, Matei Zaharia, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, and Ariel Rabkin, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, p. 50, 2010.

[8] Kweku Kwakye Arthur. *Considerations Towards the Development of a Forensic Evidence Management System*. PhD thesis, University of Pretoria, 2010.

[9] Noam H. Arzt, "Case Study for Cloud Computing Solutions in Public Health," in *CSTE Annual Conference Raleigh, NC June 5, 2019 Noam*, p. 20, 2019.

[10] Blog BMC. "Homogeneous vs. Heterogeneous Clouds: Pros, Cons, and Differences – BMC Blogs,".

[11] Aqil Burney, Muhammad Asif, and Zain Abbas, "Forensics Issues in Cloud Computing," no. August, pp. 63–69, 2016.

[12] Pooja Chopra, R P S Bedi, and Rule Base, "Applications Of Fuzzy Logic in Cloud Computing : A Review," vol. 6, no. 11, pp. 1083–1086, 2017.

[13] Yuri Demchenko, Fatih Turkmen, Cees De Laat, and Mathias Slawik, "Defining Intercloud Security Framework and Architecture Components for MultiCloud Data Intensive Applications," pp. 945–952, 2017.

[14] Povar Digambar. *A Novel Digital Forensic Framework for Cloud Computing Environment*. PhD thesis, BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI, 2015.

[15] Josiah Dykstra and Alan T Sherman, "Design and implementation of FROST : Digital forensic tools for the OpenStack cloud computing platform," *Digital Investigation*, vol. 10, no. 13, pp. S87–S95, 2013.

[16] Majda Elhozmari and Ahmed Ettalbi, "Towards a Cloud Service Standardization to ensure interoperability in heterogeneous Cloud based environment," vol. 16, no. 7, pp. 60–70, 2016.

[17] Jannatul Ferdous, Fuad Newaz Khan, Karim Mohammed Rezaul, Maruf Ahmed Tamal, Abdul Aziz, and Pabel Miah, "A Hybrid Framework for Security in

Cloud Computing Based on Different Algorithms," vol. 2020, pp. 1–7, 2020.

[18] Clint p. Garrison, *Digital forensics for network, internet and cloud computing*. Elsevier Inc, 2010.

[19] TLP Green. "Exploring Cloud Incidents,". Tech. Rep. June, 2016.

[20] George Grispos and William Bradley Glisson, "Calm Before the Storm : The Challenges of Cloud Computing in Digital Forensics," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 4, no. 2 , pp. 28–48, 2012.

[21] Priyesh Kanungo, "Design Issues in Federated Cloud Architectures," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 5, pp. 937–939, 2016.

[22] Victor Rigworo Kebande. *A Novel Cloud Forensic Readiness Service Model by*. PhD thesis, UNIVERSITY OF PRETORIA Department, 2017.

[23] Tahar Kechadi and Le-Khac Nhien-An, "Digital Forensic Investigations in the Cloud A Proposed Approach for Irish Law Enforcement," no. January 2016, 2015.

[24] Karen Kent and Souppaya. "GUIDE TO COMPUTER SECURITY LOG MANAGEMENT,". tech. rep., 2006.

[25] Chong Mao Lihua Liu, Zhengjun Cao, "A Note on One Outsourcing Scheme for Big Data Access Control in Cloud," *I.J. of Electronics and Information Engineering*, vol. 9, no. 1, pp. 36–45, 2018.

[26] David Lillis, Brett A Becker, Tadhg O Sullivan, Mark Scanlon, Tadhg O'Sullivan, and Mark Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in *11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, no. May, 2016.

[27] Ben Martini and Kim-Kwang Raymond Kwang Raymond Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digital Investigation*, vol. 9, no. 2, pp. 71–80, 2012.

[28] Peter Mell and Timothy Grance. "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology,". tech. rep., 2011.

[29] Cody Miller, Dae Glendowne, David Dampier, and Kendall Blaylock, "Forensicloud: An Architecture for Digital Forensic Analysis in the Cloud," *Journal of Cyber Security and Mobility*, vol. 3, no. 3, pp. 231 – 262, 2014.

[30] Martin Mulazzani. *New challenges in digital forensics : online storage and anonymous communication by*. PhD thesis, 2014.

[31] NIST. "Cloud Computing Forensic Science Challenges,". tech. rep., National Institute of Standards and Technology, USA, 2014.

[32] Eric Opoku Osei and James Benjamin HayfronAcquah, "Cloud Computing Login Authentication Redesign," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 1–8, 2014.

[33] P K Sahoo and R K Chottray, "Research Issues on Windows Event Log," vol. 41, no. 19, pp. 23–29, 2012.

[34] Sonal Saokar, Sulabha Patil, and Rajiv Dharaskar, "DESIGN FRAMEWORK OF DIGITAL FORENSIC FOR CLOUD COMPUTING : A REVIEW," vol. 3, no. 12, pp. 91–93, 2015.

[35] Jitendra Singh, "Cyber-Attacks in Cloud Computing: A Case Study," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 78–87, 2014.

[36] Michael Smit, Bradley Simmons, and Marin Litoiu, "Distributed , Application-level Monitoring for Heterogeneous Clouds using Stream Processing," 2013.

[37] Stelios Sotiriadis and Nik Bessis, "An Inter-Cloud Bridge System for Heterogeneous Cloud Platforms," *Future Generation Computer Systems*, 2015.

[38] Adel Nadjaran Toosi, Rodrigo N Calheiros, and Rajkumar Buyya, "Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey," *ACM Computing Surveys*, vol. 47, no. 7, p. 57, 2014.

[39] Jingxin K Wang, Jianrui Ding, and Tian Niu, "Interoperability and Standardization of Intercloud Cloud Computing," 2012.

[40] Cheng Yan, "Cybercrime forensic system in cloud computing," in *International Conference on Image Analysis and Signal Processing, IASP 2011*, no. Dc, pp. 612–613, 2011.

[41] Feng Yu, Casey Stella, and Kriss 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, no. 2, 2014.

[42] Shams Zawoad, Ragib Hasan, and Cloud Cover, "Trustworthy Digital Forensics in the Cloud," *Computer*, vol. 49, no. 3, pp. 78–81, 2016.

[43] Shams Zawoad, Ragib Hasan, and Anthony Skjellum, "OCF: An Open Cloud Forensics Model for Reliable

Digital Forensics," *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*, no. July, pp. 437–444, 2015.

Biography

Zayyanu Umar is a native of Birnin kebbi, kebbi state, Nigeria. He is currently a PhD student at Department of Computer Science, University of Nigeria, Nsukka, Nigeria(UNN), with a special area of interest in Cloud computing, Network security, Digital forensic science and software development. He holds M. Sc in Computer science, B. Sc Computer science. He is Associate Chief Lecturer with Waziri Umaru Federal polytechnic, Birnin Kebbi, Kebbi State. He is happily married with children.

Dr.Ir.Engr.(Mrs) Deborah Uzoamaka Ebem is a senior lecturer in the department of Computer Science, University of Nigeria, Nsukka. She received a B.Engr. degree from Anambra State University of Technology (ASUTECH) and a postgraduate diploma in management from University of Nigeria, Nsukka. She also received master's degrees in Computer Science and Engineering and Computer Engineering from Enugu State University of Science (ESUT) and the Technical University Delft, The Netherlands, respectively. She further holds a PhD in Computer Science from Ebonyi State University, Abakaliki, Nigeria. She was a Research Fellow and Scholar at Massachusetts Institute of Technology, Cambridge USA. Dr.(Mrs.) Ebem has published journal articles in both international and local journals. Her research interests are artificial intelligence, ICT development, deployment and application, Perceptual Measurement of Speech Quality and Speech Intelligibility, development of Igbo Hearing in Noise Test (IHINT), Parallel Computing and Parallel Algorithm, Mobil Outdoor games, data communication networks, cybercrime, and Enterprise Resource Planning (ERP).

Prof Francis S. Bakpo is a Professor in the Department of Computer Science University of Nigeria Nsukka. He received his Master's degree in Computer Science and Engineering from Kazakh National Technical University, Almaty (formerly, USSR) in 1994 and Doctorate degree in Computer Engineering in 2008 from Enugu State University of Science and Technology, Agbani. He joined the Department of Computer Science, University of Nigeria Nsukka as a Corp member in 1995 and was later retained by the Department in 1996 as lecturer II and further progressed from the rank of lecturer II to Professor in 2010.

Dr. (Mrs.) Modesta .E. Ezema attended Queen of the Rosary Secondary School Nsukka. She obtained a BSc (Hons) in Computer Science ,(UNN) M.Sc in Computer Science (ESUT) and a PhD in Computer Science from the Ebonyi State University Abakalikki respectively. She joined the services of UNN in 2005 and is currently a Lecturer I in the Department of Computer Science, University of Nigeria, Nsukka.