ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse134952020.pdf
https://doi.org/10.30534/ijatcse/2020/134952020

Statistical Model for Cybercrime Detection in Joined Heterogeneous Cloud Computing Environments

Zayyanu Umar[1], Francis S. Bakpo[2], Musa Alkali Abubakar Tanko[3], Musa Ibrahim Kamba[4] and Modesta. E. Ezema[5]
[1, 3, 4]Department of Computer Science,
College of Science and Technology,
Federal Polytechnic, BirninKebbi.
Corresponding Author: zayyanuumar1@yahoo.com[1]
musaibnabubakar@gmail.com[3],
musaikamba@gmail.com[4]
[2,5]Department of Computer Science,
Faculty of Physical Science
University of Nigeria, Nsukka, Enugu.
francis.bakpo@unn.edu.ng[2]

ABSTRACT

Many commercial facilities and academic institutions now use cloud computing in an attempt of adopting new digital innovations. Cloud Computing Providers might be constrained to some services, lacking several resources their customers requested, meaning that distinct cloud services need to come together in collaboration to interoperate and exchange resources among themselves. In different characteristics and structures, clouds may be interlinked, and the interconnected systems may be prone to instability or intrusion. Although digital transformation and cloud services are also making progress in meeting the influencing policies internationally, terrorists use virtual space to commit cyberattacks. Adoption of cloud services has become highly sensitive to attacks and intrusions. Security breach or corruption of data gives organizations or agencies significant catastrophic losses. Divine influence and physical devices really aren't sufficient to protect services provided by clouds; thus, there is a need for an effective cyber protection model that is implementable, versatile, reliable and capable of detecting hazardous cyber-attacks on joined heterogeneous cloud providers, making it essential to decrease in real-time. This paper focuses on developing a Statistical Model for cybercrime detection in a heterogeneous cloud systems that are joined. When defining the implementation of the proposed model, we used an architecture and design modelling system. We used statistical notations and diagrams to contain the complexities and variability of the joining cloud data centres when adopting shared resources and possible cybercrime detection. The proposed model was experimented using WEKA tool to test Anomaly and Normal Accuracy performance of three (3) Classification existing algorithms: C4.5 and Random Decision tree and NaïveBayes. The dataset used was CICDDOS2019, the dataset was generated observing abstract behaviour of 25 users based on heterogeneous HTTP, HTTPS, FTP, SSH, and email protocols, Operating Systems and initiating different DDOS attacks. After a comparison of Classification model results, yielding in the highest accuracy and detection rates as well as the lowest false rates. The results specify that the classification capability of the C4.5 is inherently superior to the classification of Random Tree and the NaïveBayes.

Key words: Statistical Model, Cloud Computing Heterogeneity, Cybercrime, Cloud Service Providers

1. INTRODUCTION

Provisions of modern technology; cloud infrastructure services render it pointless to manufacturing organisations or educational establishments to buy devices and software, as the essential information of organisations is now housed in cloud data centres across the globe, no more on organisations' storage drives.

Cloud-based services are a term that enables omnipresent, safe, access to an on-demand network to flexible shared computing resources (such as networks, Data repositories, applications and processing and it can swiftly distribute and transported with a small amount of commitment to managing or involving service providers [1].

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

The National Institute of Standards and Technology (NIST) describes Cloud Computing offers 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" [2].

Cloud computing has five essential parts: omnipresent network access, Asset self-service balancing, cost-peruse, on-demand fast elasticity. Cloud service providers based on software can be categorised into three main groups, called 'online business models' such as service network, service platform, and service software[3].

In order to check things such as the availability, security, performance and usage of CPUs, cloud resource management helps to assess what and how much resources are needed and how to open a user request[4].

When the adoption of cloud computing grows, organisations and other customers continue to use innovative approaches to completely leverage its full potential through the implementation of cloud organisations.

Inter-cloud is defined as merging various clouds to exchange information and serve customers as much as want, whenever they wish to make a request and for safety and security. This diversity is a significant challenge in collaborative cloud computing settings as it raises obstacles concerning the cloud's omnipresent realisation.

A further challenge is vendor lock-in, consumers making service requests have to adapt their demands to conform with the trends and interfaces of the cloud provider, resulting in expensive and challenging possible relocations[5].

Because cloud storage provides customers with many advantages and presents many potential problems to a digital forensics process, many providers often face the same.

There are six primary levels of digital forensic processes: identification, collection, evaluation, examination, storing and reporting.

Forensics in Cloud settings as a concept has been used and described since 2010, as a combination of two ideologies; cloud computing and digital forensics[6], the authors used conventional methods of digital forensics to track breaches or identify indictable evidence.

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

Green[7], found three distinct categories of digital forensics that occur in the cloud system: post-incident, live incident and before the incident.

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

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

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

In cloud computing systems, there are many types of research which communicate forensic investigations. Some activities are both on a customer and server-side and are focused on the operating system of a cloud environment.

Various cloud services such as Open Stack, Microsoft Azure and so on provide pay as use cloud services to cloud users[8].

Many cloud service providers now rely on systems that can be interoperable. The primary goal is to combine multiple cloud service providers as one cloud service platform[9].

Some researchers have indicated a need in building a network whereby joined varied cloud service providers can gain access to agreed provided services despite the disparity that exist in the individual cloud environment to a joined cloud services[10].

The biggest problem with choosing to join several cloud resources providers is that most of the individual cloud systems can not work collaboratively with each other, as each communicates with a unique dialect[11]. There have been no clear service standards for two or perhaps more clouds to be incorporated, but operating systems are based on those definitions. Many data centres use Representational State Transfer (REST) or Simple Object Access Protocols (SOAP) as an interaction scheme[12]. Each scheme has its distinctive features; for example, login authentication[13]. Cloud architectures also have not taken into cognisant cloud compatibility, and each cloud environment has its structural platform and user interfaces[5]. Inconsistency in different cloud data and ways of logging into another cloud computing systems creates issues for contemporary researchers and to perform a thorough review; the researchers must attain the meaning of the various data fields in each connection[14].

Incapability to recognise one system logging scheme into other logging protocol creates inconsistency and incompatibility with Cloud-connected devices and logging processes of operating systems. It gives rise to a challenging task being logged hierarchically[15]. By introducing this new technology for accessing multiple clouds to communicate and collaborate and reap other interoperability benefits, malicious user lunches act to target a specific cloud unit resources to spoof services or gain access to sensitive data. Attackers of service providers use the existing cloud environment components as their tools to mount an offensive activity[16].

Mega cloud providers need to implement a new framework to translate log data of different pieces of information and requirements from multiple cloud services into a uniform model framework with the uniform format of data fields to enable identifying illicit activity and analyse cloud logs, allowing for compatibility and privatisation of provider

services.

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

Considering all studies on digital forensics analysis and cloud cybercrime detection, there is still a need for a system that addresses cybercrime detection relevant to joined varied cloud computing systems and enables digital forensic examination[17][18][19].

The model would simplify a digital forensic investigator's tasks by implementing a quality structure for a computer forensics framework that penetrates shared interactions between various cloud environments and recognises both the intruder and the scene of intrusion.

In this paper, we show a proposed model for digital forensics which could be used to trace cyber threats that may be beneficial to a cloud services digital forensic investigator in interconnected different configured clouds setups.

Numerous scholars have written articles on cloud computing environments diversity, digital forensics concerning cloud infrastructure systems and cloud computing services. Given all cloud forensics work, various studies also demonstrated the need for a detailed survey comprising different cloud service system models collaborating, supporting multiple types of cloud systems, posting security threat reports, and encouraging online forensic analysis[20][21][22][23].

Contemporary researchers are searching for a practice that tackles the security challenge of compatibility with different log formats and specifications joined to the cloud service network[24][25][26][5],[27].

Throughout this study, we proposed a statistical digital forensic Model, which can be used for cybercrime detection and forwarding for prosecution throughout joined heterogeneous configured clouds network.

1.1CLOUD ENVIRONMENT HETEROGENEITY

Joined cloud environments was explained as combining various cloud service providers at different stages (a collaboration of multiple vendors at different stages by the individual hypervisor) or the same level (a collaboration of service providers by numerous heterogeneous hypervisors deployed security mechanisms,) service broking, service scheduling algorithm, power infrastructures and host operating system[28]. The heterogeneous structure in cloud environments is shown in Table 1.

Table 1: Cloud Service Providers(CSPs) Heterogeneity

Service Provider	OS	Scheduling Algorithm	Security Mechanism
CSP 1	LINUX	Ant-Colony	?
CSP2	UNIX	Max Min	?
CSP3	WINDOW	Honey-been foraging	?

2. RELATED WORK

In a research paper entitled "A Novel Digital Forensic Framework for Cloud Computing Environment" [29], a framework has been developed to use for forensic examination in a cloud computing system despite the existence of traditional forensic approaches; it was developed to apprehend digital criminals, seize networking gadgets and other physical computer sets such as storing device, hard disks, server, etc. The digital investigator defines concerns and criteria around digital software forensic research. Through this report, The investigator discusses the problems surrounding the forensic investigation, both live and dead.

Alharbi[30], With a research entitled "Proactive Framework for Digital Forensic Investigation" established a system in the cloud service platform, which requires active digital forensic investigation. It addressed the problems faced by Reactive Electronic Forensics (RDF), when computers, networks gadgets confiscated are used for a study.

From another research [31] made by Martini and Choo, they established a framework that separates the processing and storage of information between the conventional forensics and the digital forensics in cloud computing environment. They addressed problems and challenges related to electronic forensic cloud computing within the framework of the program they were designing.

In an article entitled "Use of Information Technology in Crime Investigation"[32], In crime detection, the scholars have a comprehensive study of various forms, approaches and challenges in applying IT. A comprehensive review was carried out of the opportunities of revision, which culminated, in particular, in a number of important IT crime investigations. A Bayesian framework is developed in order to determine the system profile of the perpetrator, and as a method of executing the procedure-a multi-agency method, common in non-linear and complex situations.

The study entitled: "New challenges in digital forensics: online storage and anonymous communication," The researcher developed a model to tackle the bottlenecks raised by digital forensics processes on a cloud computing platform and analysed arising issues in anonymous communication. The author tested the framework 's workability using Dropbox by launching an attack[33].

In research named "Digital Forensic Investigations in the Cloud: A Proposed Approach for Irish Law Enforcement," an approach was conceived to address the weaknesses of the traditional digital forensics scheme and the issues presented to Ireland's law enforcement digital forensic practitioners in cloud computing scene. The scholar has researched the conventional forensic analysis approaches and the causes of why they are insufficient for delivery to a cloud platform[34].
Alexander[20], created specific forensic problems inside a cloud environment in a study entitled "Digital Forensics for Infrastructure-as-Service Cloud Computing." He studied the specificities of the forensic investigation currently accessible with remote methods. The author built a system using the cloud storage application model of OpenStack to allow trusted software as a forensic prototype of the cloud.
A study conducted by Zawoad and Hasan[35] found that the forensic cloud infrastructure permits the identification and preservation of the necessary evidence with confidentiality and integrity. The open-source model on Openstack is popular. First features found to assist trustworthy forensics in cloud environments.
A study conducted by Kantale V. and Sanghavi J., Various correlations of the algorithms in various conditions were suggested by the authors. They checked all the algorithms in various tasks and under various patterns of the virtual machine (VM) in the study. According to the report, machine learning-based algorithms work better than others in terms of general load balancing performance[36].

A study report by Kebande[37], entitled “Internet Forensic Readiness as a Service Model (CFRaaS)”. The authors built a software application named a CFRaaS system. The application uses malicious botnet features but modifies its capabilities to create potential cloud proof. CFRaaS preserves such information electronically for Digital Forensic Research purposes in an electronic forensic database.
Alqahtany& Clarke[6] developed a scheme for digital forensic evidence extraction and evaluation that reveals the non-Cloud Service Provider(NCSP) customer details. The template gives ample and prosecutable facts.
In a thesis entitled: "Forensicloud: An Architecture for Digital Forensic Assessment in the Cloud," the author proposed a technology that would prevent the length of time required for scientific research by combining computing resources with high-performance and incorporating existing tools to work in that context. Additionally, writers with such a system gain access to unique, locked resources that can not be freely subscribed[38].
FROST was developed cloud computing environment digital forensic tool, entitled Sherman and Dykstra: FROST. The app enables forensic experts and law enforcement, get reliable and prosecutable forensic information on cloud networks independently of platforms. The proposed framework was specially developed for a particular cloud platform known as OpenStack[39].
"Cloud Forensic Evidence Management System (FEMS)" addresses digital evidence storage problems in another study created by Arthur, and it ensures accuracy and credibility related to digital evidence. The authors used the Biba Integrity Model to store the integrity of digital evidence in FEMS securely and they used Casey's Certainty Scale in reliability tests[40].
In the study entitled: "Cybercrime forensic system in cloud computing." The authors presented a cloud crime tracking and analysis system using Encase and FTK[19] .
Zawoad, Hasan, &Skjellum[41], designed an Open Cloud Forensics framework and found challenges in the existing digital forensic structure by analysing cloud computing environments and different cloud-participating entities while incorporating existing cloud infrastructure and services. On a realistic scenario, the system (OCF) could support contemporary digital forensics processes.

3.0 METHODOLOGY

The study examined the complexity of cloud computing systems, such as the architecture of virtual machines, security mechanisms, scheduling algorithm, cloud service brokerage, service price and efficiency of the network, etc. Middleware will be used to convert, de-convert, translate and retranslate variations in a private cloud environment. The architecture used the Service Level Agreement (SLA) and specifications that connects various cloud computing systems. We used a basic activity diagram of Unified Modeling Language (UML) in developing the model, and we used an architectural modelling approach to propose an order for the deployment diagram.
The proposed model was experimented using WEKA tool to test Anomaly and Normal Accuracy performance of three (3) Classification existing algorithms: C4.5 and Random Decision tree and Naïve Decision Tree. The data used was CICDDOS2019, The dataset was generated observing abstract behaviour of 25 users based on heterogeneous HTTP, HTTPS, FTP, SSH, and email protocols, Operating Systems and initiating different DDOS attacks.

4.0 PROPOSED STATISTICAL MODEL IN JOINED CLOUD ENVIRONMENTS

Diversities in a cloud service providers gives rise to proposed criteria to address conflicts and test compliance policies and level service agreements. Consequently, solving cloud inconsistencies allows the development of a realistic advanced forensic platform to improve legal processes.
The compatibility of heterogeneous cloud systems will also decide the question of locking the customer in search of a resource which is not supported by his principal subscribed cloud. Figure 1 below shows the heterogeneous Resource Sharing Cloud interconnections.

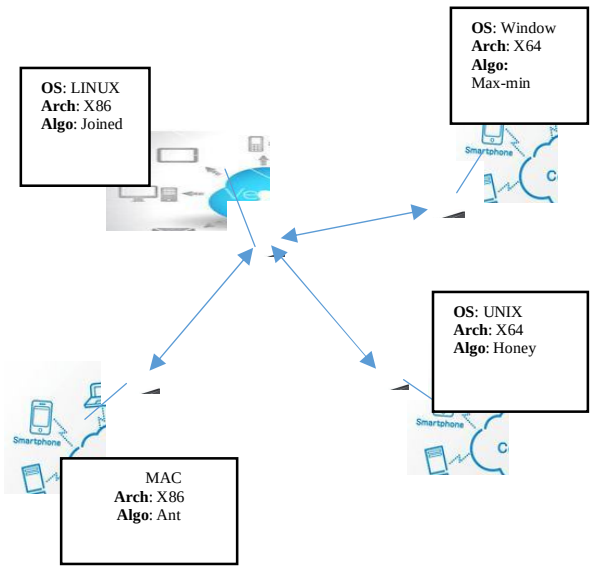

Figure 1: Joined Heterogeneous Clouds Diagram

The figure above shows how various cloud configurations interconnect to share resources.
Attacks detection using a statistical approach is superior to other methods of packet labelling, as it doesn't require updating on routing code. The following proposed statistical model is used in joining three different cloud setup for cybercrime detection.

$$V = ((X\alpha \ U \ Y\beta \ U \ Z\theta) - (X\alpha \ U \ Y\beta) - (Y\beta \ U \ Z\theta) - (X\alpha \ U \ Z\theta))E\frac{Uj}{Si}$$

Xα U Yβ U Zθ stands for Service Level Agreement(SLA) for a joined set of Cloud service platforms, each with distinctions to others and $E\frac{Uj}{Si}$ stands for the possible crime that may happen during clouds communications while subscribers are seeking services.

$$V = ((X\alpha \ U \ Y\beta \ U \ Z\theta) - (X\alpha \ U \ Y\beta) - (Y\beta \ U \ Z\theta) - (X\alpha \ U \ Z\theta))E\frac{Uj}{Si}$$

Si Stands for a set of services that each Cloud service provider provides
Si = {S1, S2, S3, S4,……..….SM}---eq1
Uj Stands for a set of registered Users for each Cloud service provider
Uj = {U1, U2, U3, U4,……..….UM}
E Stands for Evidence generated based Detection model while Cloud service providers(CSPs) inter-relate with each other. The following figure 2 below illustrates the statistical model for detection of intrusion in heterogeneous cloud computing environments that have joined.

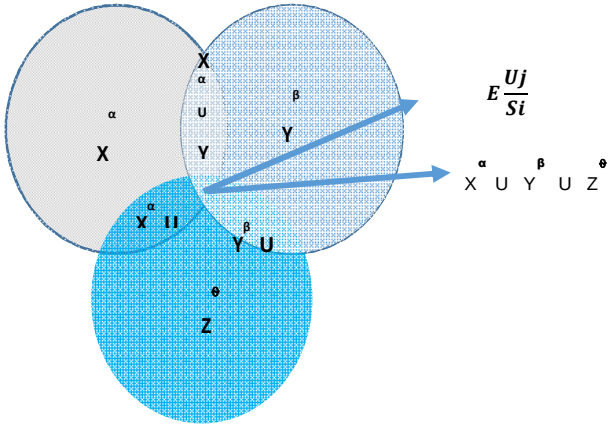

Figure 2: Statistical Model for Forensic in Joined cloud environments

Figure 3 (activity diagram) shows how the interconnected clouds communicate to allow clients to benefits from each other resources within the heterogeneous cloud environment that has been joined

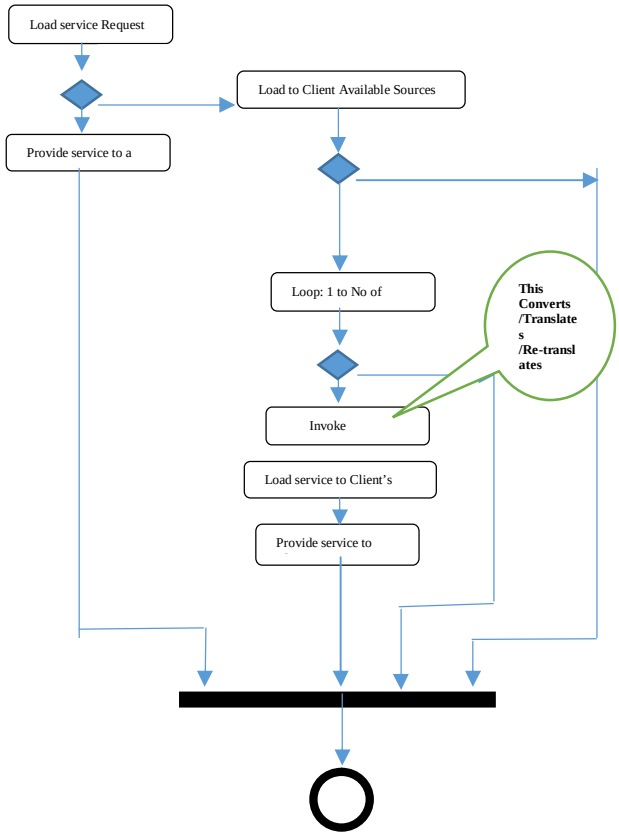

Figure 3: Provision of service between Joined Heterogeneous Cloud Environments.

Conformity with requirements, Middleware's service, Service Level Agreement (SLA), service pricing and usage must be given in the connectivity of different cloud setups.
The diagrams depict clouds linked to a dedicated central cloud computing system which is responsible for handling interoperation issues and enabling resource sharing between different clouds. With entirely different scheduling algorithms, operating systems, user collection, device

architectures and other features, each cloud is distinct. It also validates the variety in the general approach to digital forensics. A CLOUD customer order for a resource to its subscribed CSP; if the Cloud Service Provider does not have such assets, the subscribed CSP shall forward the order to the CENTRAL CLOUD, the Central Manager shall, upon receipt the request check the essence of the application (Anomaly Analytics). Instead, Digital Forensics Investigator collects, compiles, and Present to Court information from the Central Manager Persistent Memory and CSPs Memories the Intrusion log data.

5.0 RESULT AND DISCUSSION

CICDDoS2019 contains benign and the most up-to-date frequent DDoS attacks, which resembles the actual real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter-V3 with labelled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack features.

The dataset was generated observing abstract behaviour of 25 users based on heterogeneous HTTP, HTTPS, FTP, SSH, and email protocols, Operating Systems and initiating different DDOS attacks.

Weka has been widely accepted in academia and business circles for implementation of data mining algorithms and data mining analysis.

The performance of the proposed algorithm on CICDDOS2019 dataset is evaluated using the Performance parameters, namely Accuracy (A), Precision(P), Detection Rate (DR) and False Positive Rate (FPR).

The intrusion detection system (IDS) needs high precision and accuracy for a decent level of performance and, conversely, the false alarm rate should below. The following table 2 and formulae specify these terms:

Accuracy = $\frac{TP+TN}{TP+FP+TN+FN}$

Precision = $\frac{TP}{TP+FP}$

True Positive Rate (TPR) = $\frac{TP}{TP+FN}$

False positive rate (FPR) = $\frac{FP}{TN+FP}$

True Negative Rate (TNR) = $\frac{TN}{TN+FP}$

False Negative Rate (FNR) = $\frac{FN}{TP+FN}$

Table 2: Confusion Matrix Template

Predicted Value (predicted by the test)		Actual Value (as confirmed by experiment) positives	Actual Value (as confirmed by experiment) negatives
	positives	**TP** True Positive	**FP** False Positive
	negatives	**FN** False Negative	**TN** True Negative

The following Table3, Table 4 and Table 5 display the Details Accuracy Performances of three selected algorithms and it follows the confusion matrix result of each.

Table 3: Detailed Accuracy Performance Result using the C4.5 algorithm

TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
0.999	0.000	1.000	0.999	1.000	0.999	1.000	1.000	Normal
1.000	0.001	0.999	1.000	0.999	0.999	1.000	1.000	Anomaly
1.000	0.000	1.000	1.000	1.000	0.999	1.000	1.000	W. Avg.

=== Confusion Matrix Result Using C4.5Algorithm ===

```
a       b   <-- classified as
 4709     3 |   a = NORMAL
    0  2290 |   b = ANORMALY
```

Table 4: Detailed Accuracy Performance Result Using Random Tree Algorithm

TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
0.992	0.000	1.000	0.992	0.996	0.987	0.999	1.000	Normal
1.000	0.008	0.983	1.000	0.991	0.987	0.999	0.998	Anomaly
0.994	0.003	0.994	0.994	0.994	0.987	0.999	0.999	W. Avg.

=== Confusion Matrix Result Using Random TreeAlgorithm

```
a       b   <-- classified as
 4673    39 |   a = NORMAL
    1  2289 |   b = ANORMALY
```

Table 5: Detailed Accuracy Performance Result Using NaiveBayes Algorithm

TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
0.811	0.011	0.993	0.811	0.893	0.754	0.991	0.986	Normal
0.989	0.189	0.718	0.989	0.832	0.754	0.991	0.993	Anomaly
0.869	0.069	0.903	0.869	0.873	0.754	0.991	0.988	W. Avg.

=== Confusion Matrix Result Using NaiveBayes Algorithm

```
a       b   <-- classified as
 3821   891 |   a = Normal
   25  2265 |   b = Anomaly
```

Comparison between C4.5, Random Tree and NaiveBayes classification algorithms

The following figure 4 shows the Classification prediction result of C4.5,RandomTree and NaïveBayes Algorithms.

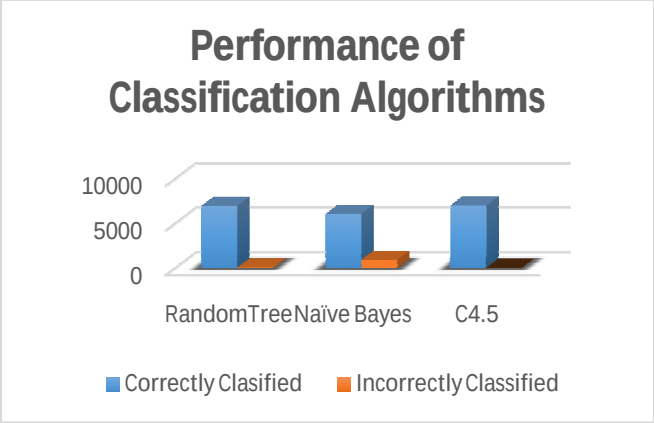

Figure 4: Classification rates of three algorithms

Accuracy comparisons of C4.5, Random Tree and NaiveBayes classification algorithms

The following table 6 and figure 5 depict the Accuracy performance Result of C4.5,RandomTree and NaïveBayes Algorithms.

Table 6: Accuracy Performance Result (True Positive and False Positive Rates)

Algorithm	True Positive	False Positive	Precision	Recall	F-Measure
RandomTree	99.40%	3.00%	99.40%	99.40%	99.40%
Naïve Bayes	86.90%	6.90%	90.30%	86.90%	87.30%
C4.5	100.00%	0.00%	100.00%	100.00%	100.00%

The following chart depicts the accuracy performance of the three algorithms:

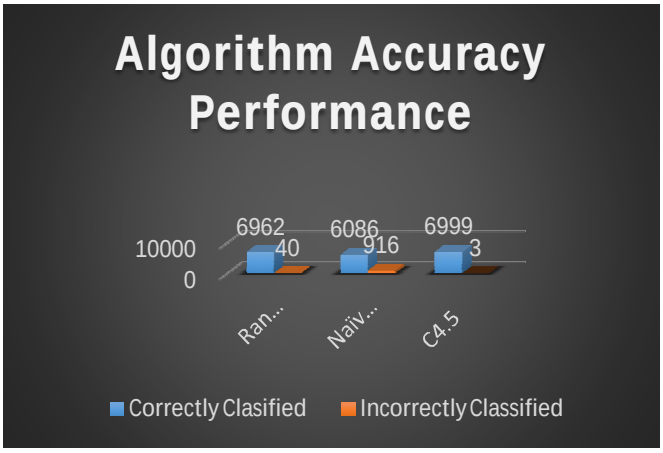

Figure 5: Anomaly Detection Rate of the three Algorithms

6.0 CONCLUSION AND FUTURE WORK

Diversity in planned collaborative vendors of cloud services leads to a refusal to communicate with cloud service vendors and prevents customers in their resource requirements from isolating active cloud service. Harmonising heterogeneity among joined cloud environments is by designing a model capable of managing inconsistencies, contradictions, and disparities will result in satisfying the clients of joined cloud environments and an efficient interoperability service provision. An intruder infringes unauthorised access to joined cloud services. Still, by introducing a functional forensic system to deal with both barriers to diversity in joined cloud environments, the intrusion activities can be detected. The result presents the highest accuracy and detection rates as well as the lowest false rates after a comparison of Classification models. The results indicate that the C4.5 classification capability is inherently superior to the Random Tree classification and the NaïveBayes Decision Tree classification. The future study is required in a digital forensic investigation concerning the Internet of Things (IoT) due to its robustness, high complexity and heterogeneity.

REFERENCES

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

[2] P. Mell and T. Grance, "The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology," 2011. doi: 10.1136/emj.2010.096966.

[3] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, p. 50, 2010, doi: 10.1145/1721654.1721672.

[4] P. Chopra and R. Bed, "STUDY OF CLOUD COMPUTING TECHNIQUES : RESOURCE," *Int. J. Comput. Eng. Appl.*, vol. XI, no. Xi, pp. 213–222, 2017.

[5] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected Cloud Computing Environments: Challenges, Taxonomy, and Survey," *ACM Comput. Surv.*, vol. 47, no. 7, p. 57, 2014.

[6] S. Alqahtany and N. Clarke, "A forensically-enabled IAAS cloud computing architecture," in *12th Australian Digital Forensics Conference.*, 2014, p. 10, doi: 10.4225/75/57b3e3a5fb87e.

[7] T. Green and T. Audience, "Exploring Cloud Incidents," 2016.

[8] S. Sotiriadis and N. Bessis, "An Inter-Cloud Bridge System for Heterogeneous Cloud Platforms," *Futur. Gener. Comput. Syst.*, 2015, doi: 10.1016/j.future.2015.02.005.

[9] F. Yu, C. Stella, and K. A. Schueller, "A Design of Heterogeneous Cloud Infrastructure for Big Data and Cloud Computing Services," *OPEN J. Mob. Comput. CLOUD Comput.*, vol. 1, no. 2, 2014.

[10] M. Smit, B. Simmons, and M. Litoiu, "Distributed , Application-level Monitoring for Heterogeneous Clouds using Stream Processing," 2013.

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

[12] F. Alshraiedeh and N. Katuk, "SOAP and RESTful web service anti-patterns: A scoping review," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 5, pp. 1831–1840, 2019, doi: 10.30534/ijatcse/2019/05852019.

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

[14] K. Kent and Souppaya, "GUIDE TO COMPUTER SECURITY LOG MANAGEMENT," 2006.

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

[16] 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, doi: 10.1109/ARES.2016.58.

[17] S. A. Ali, "Challenges in Cloud Forensics," in

International Conference on Cloud and Big Data Computing, 2018, pp. 6–10.

[18] A. Burney, M. Asif, and Z. Abbas, "Forensics Issues in Cloud Computing," no. August, pp. 63–69, 2016.

[19] C. Yan, "Cybercrime forensic system in cloud computing," in *International Conference on Image Analysis and Signal Processing, IASP 2011*, 2011, no. Dc, pp. 612–613, doi: 10.1109/IASP.2011.6109117.

[20] J. Alexander, "Digital Forensics for Infrastructure-as-a-Service Cloud Computing," University of Maryland, Baltimore., 2013.

[21] P. Kanungo, "Design Issues in Federated Cloud Architectures," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 5, pp. 937–939, 2016, doi: 10.17148/IJARCCE.2016.55229.

[22] N. H. Ab Rahman, W. B. Glisson, Y. Yang, and K.-K. R. Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," *IEEE Cloud Comput.*, vol. 3, no. 1, pp. 50–59, 2016, doi: 10.1109/MCC.2016.5.

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

[24] S. Almulla, Y. Iraqi, and A. Jones, "a State-of-the-Art Review of Cloud Forensics," *JDFSL*, vol. 9, no. 4, p. 22, 2014.

[25] Y. Demchenko, F. Turkmen, C. De Laat, and M. Slawik, "Defining Intercloud Security Framework and Architecture Components for Multi-Cloud Data Intensive Applications," pp. 945–952, 2017, doi: 10.1109/CCGRID.2017.144.

[26] D. Lillis, B. A. Becker, T. O. Sullivan, M. Scanlon, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," in *11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*, 2016, no. May, doi: 10.13140/RG.2.2.34898.76489.

[27] J. K. Wang, J. Ding, and T. Niu, "Interoperability and Standardization of Intercloud Cloud Computing," 2012.

[28] B. BMC, "Homogeneous vs. Heterogeneous Clouds: Pros, Cons, and Differences – BMC Blogs," *web pages*, 2012. https://www.bmc.com/blogs/what-price-homogeneity (accessed Oct. 11, 2019).

[29] P. Digambar, D. O. F. Philosophy, and P. Digambar, "A Novel Digital Forensic Framework for Cloud Computing Environment," BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI, 2015.

[30] S. A. Alharbi, "Proactive System for Digital Forensic Investigation," University of Victoria, 2014.

[31] B. Martini and K.-K. R. K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," *Digit. Investig.*, vol. 9, no. 2, pp. 71–80, 2012, doi: 10.1016/j.diin.2012.07.001.

[32] N. Huybinh, "Use of Information Technology in Crime Investigation," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 2, pp. 2–5, 2020.

[33] M. Mulazzani, "New challenges in digital forensics : online storage and anonymous communication by," 2014.

[34] T. Kechadi and L.-K. Nhien-An, "Digital Forensic Investigations in the Cloud A Proposed Approach for Irish Law Enforcement," no. January 2016, 2015.

[35] S. Zawoad, R. Hasan, and C. Cover, "Trustworthy Digital Forensics in the Cloud," *Computer (Long. Beach. Calif).*, vol. 49, no. 3, pp. 78–81, 2016, doi: 10.1109/MC.2016.89.

[36] V. Kantale and J. Sanghavi, "Statistical Evaluation of Task Scheduling Algorithms in Cloud Environments," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 2, pp. 15–21, 2020.

[37] V. R. Kebande, "A Novel Cloud Forensic Readiness Service Model by," UNIVERSITY OF PRETORIA Department, 2017.

[38] C. Miller, D. Glendowne, D. Dampier, and K. Blaylock, "Forensicloud: An Architecture for Digital Forensic Analysis in the Cloud," *J. Cyber Secur. Mobil.*, vol. 3, no. 3, pp. 231–262, 2014, doi: 10.13052/jcsm2245-1439.331.

[39] J. Dykstra and A. T. Sherman, "Design and implementation of FROST : Digital forensic tools for the OpenStack cloud computing platform," *Digit. Investig.*, vol. 10, no. 13, pp. S87–S95, 2013, doi: 10.1016/j.diin.2013.06.010.

[40] K. K. Arthur, "Considerations Towards the Development of a Forensic Evidence Management System," University of Pretoria, 2010.

[41] S. Zawoad, R. Hasan, and A. Skjellum, "OCF: An Open Cloud Forensics Model for Reliable Digital Forensics," *Proc. - 2015 IEEE 8th Int. Conf. Cloud Comput. CLOUD 2015*, no. July, pp. 437–444, 2015, doi: 10.1109/CLOUD.2015.65.