JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

# A Multi-Threaded Distributed Cloud IDS Model for Network Access Traffic Management and Administrative Control

[1]Pascal Adegher, [2]Paschal Uchenna Chinedu, [3]Rabiu B. Ahmad
[1]*Department of Computer Science,*
*Nigerian Defence Academy, Kaduna*
[2]*Department of Information Systems and Technology,*
*Delta State University of Science and Technology, Ozoro,*
[3]*Department of Aerospace Engineering,*
*Air force Institute of Technology, Kaduna, Nigeria*

**ABSTRACT**
*Cloud computing emerges as a way for businesses to cut expenses while simultaneously providing access to computation and resources on demand without having to setup an IT infrastructure. Through services like Amazon Web Services (AWS) or Microsoft Azure, businesses may immediately deploy and de-provision virtual machines (VMs) in accordance with their needs by only paying for the resources they really use. Cloud Service Providers (CSP) makes use of virtualization technologies in order to establish the required environment, and as such maximize the benefit of their systems. Authenticating users with passwords or digital certificates and maintaining data transmission confidentially aren't enough to provide security in a distributed system. Due to its distributed model, the cloud is susceptible to and vulnerable to highly technical distributed intrusion attempts. An innovative multi-threaded distributed cloud IDS model has been developed in this study to manage large scale network access traffic and administrative control of data and applications in the cloud. The propounded Multi-thread Cloud Intrusion Detection System (IDS) integrates knowledge and behavior analysis to identify intrusions, handles enormous flows of data packets, analyzes them, and generates reports effectively.*

**ARTICLE INFO**
*Article History*
Received: September, 2023
Received in revised form: September, 2023
Accepted: November, 2023
Published online: December, 2023

**KEYWORDS**
Cloud Computing, Infrastructure as a Service Security, Virtualization, Multi-Tenancy, Network Intrusion Detection System, Multi-threaded IDS

## INTRODUCTION

Like any new technology, cloud computing presents a rare chance to rethink security and IT governance for a better future. Risk of unwanted access to information in the cloud is a major worry for anyone involved in cloud computing, especially in a situation where security and privacy have become crucial for commercial clients.

The decision of any individual or organization to move data to the Cloud means outsourcing control of such useful data to a third party. Should they also decide to only use the Cloud for data processing rather than storage, the fact remains data removal from their private boundary- thus data is no longer under their control. Therefore, IT infrastructures have been de-perimeterized, and as such the need to tackle security from whole new perspective (Kaur & Kamboj 2023). But there is more to the issues than this.

Multi-tenancy allows the coexistence of multiple tenants in the same physical machine to enable sharing its resources (CPU, memory, network...) while also creating an isolated environment for each one simultaneously. Cloud service providers (CSP) use this architecture to allocate resources from physical machines that are not usually fully engaged to optimize their available infrastructures. Virtualization is the

*Corresponding author: Paschal Chinedu*
chinedupu@dsust.edu.ng
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

technology by which multi-tenancy is obtained. Though now drawing most attention, yet virtualization has existed for a long time in the IT world. The model allows running at the same time multiple operating systems (OS) on the same physical device. Thus, allows several users can be isolated from each other but able to execute their applications on the same physical environment.

Multi-tenancy and virtualization create an effective computing paradigm. Yet, the level of related risks plaguing it is somewhat provoking greater concerns among IT experts. Now the fact that several users (tenants) coexist on the same physical environment raises numerous questions among cloud users: who is my neighbour? How reliable is it? Is it my skill?

There is no longer trust on traditional IT infrastructure in the recent times. The lack of perimeter, no firewalls or IDS/IPS at the Internet gateway impeding the fraudsters from attacking the systems have aggravated the fear to modern computing. Furthermore, virtualization has led to the creation of a new attack surface, the virtualization layer; also, multi-tenancy and public clouds have exposed the surface to higher degree of vulnerability to hackers (Chinedu & Osuagwu, 2018; Chinedu et. al. 2020; Tank et. al. 2022).

Malicious virtual machines that are looking for ways to breach sensitive data or processes may live alongside tenants. Individual tenants or organizations concerned must be aware of this and recognize what security techniques could be implemented to curb any possible security bridge on the virtualization environment.

## STATEMENT OF PROBLEM

The need to implement virtualization technologies to enable the use of multi-tenant environments have become the bedrock for the ever-revolutionizing cloud or virtual environment. These two models (virtualization and multi-tenancy) when adopted create new set of difficulties altogether. While virtualization introduces a new layer that can be targeted, multi-tenancy promotes the process to attain the layer. The research takes interest in the need to review virtualization and multi-tenant security issues, from a new perspective not commonly assessed, in order to proffer a secure public IaaS cloud environment.

Security is a major challenge faced by cloud computing (CC) (Chinedu et al, 2013; Chinedu et al, 2015; Chinedu et al, 2018, Chinedu et al. 2020) owing to the established virtualization and multi-tenancy environment; due to its open and distributed architecture. As a result, it is weak and open to breaches that compromise the security, reliability, and integrity of cloud resources and provided services. In order to protect cloud environments from numerous threats and attacks, intrusion detection systems (IDS) have emerged as the most widely used component of computer system security and compliance standards.

### *Objectives of the Research*

This research seeks to accomplish the following objectives:

1. Unveil a model of a multi-threaded cloud IDS for Network Access Traffic Management and Administrative Control.
2. Facilitate enhanced optimization efficiency and transparency for the cloud user via monitoring of cloud service using the prescribed model,
3. Examine a few current cloud-based intrusion detection systems (IDS) in terms of the type, location, detection time, detection method, data source, and threats they are able to detect.
4. Demystify cloud computing and fear to public cloud adoption by highlighting appropriate security solution or techniques on virtualised network infrastructure for protecting a cloud against malicious tenants and outsider adversaries.

## LITERATURE REVIEW

### *Analysis of Data Efficiency and Security in Cloud Computing*

Today, one server handles all of the user's requests, regardless of the number of requests. The processing time will be long in this case since the server must handle every request

*Corresponding author: Paschal Chinedu*
✉ chinedupu@dsust.edu.ng
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

from every user at once. Data loss and packet delays and corruption could result from this. Doing this prevents the server from properly processing the user's inquiry. As a result, processing time lengthens because of the congestion and traffic. Hence, the study use the idea of cloud computing to solve these issues. The cloud computing employed in this study uses a proxy server to prevent these issues (Mahadevan & Neelamegam 2018). However, this technique improves data efficiency but not data security. When discussing data efficiency, it is important to also discuss data security because, in cloud computing, it is impossible to tell which cloud the data is coming from, making it impossible to detect data security in the current system.

The system built on the new architecture is more fault tolerant and scalable. Multiple customers can access a cluster, which consists of one server and several proxy servers. Proxy servers read or write data given by a server and store data on local drives. All files kept in various proxies are indexed by the server. When a client requests to download some data, the server first directs the request to a related proxy that has the requested data, and the proxy then sends the requested data to the client. The data request can be efficiently handled in a timely manner by combining the principles of cloud computing and grid computing (Barhaiya & Mehta 2023; Singh 2024). The main focus of the paper is security; hence the aforementioned phase only touches briefly on cloud and grid technology. The deployment of security is accomplished in two stages, namely behavioral –Knowledge.

***Behavioral Analysis***

With this technique, we must be able to distinguish between expected behavior (legal use) and a serious behavior divergence. For the network to effectively identify intrusions, proper training is required. The network learns to recognize the intrusions for a certain sample set of incursions (Galvano & Figna, 2023). But instead, we concentrate on spotting user behavioral trends and deviation from them. This approach enables us to defend against a greater variety of unidentified threats (Anashkin & Zhukova 2021; Gargi & Sandeep 2023).

**Knowledge Analysis**: We can create a rule that an expert system can use to describe malicious conduct. The ability to add new rules without changing current ones is one benefit of employing this type of intrusion detection. Computer and network security management systems include intrusion detection (ID). An ID system collects and examines data from various computer or network systems to discover potential security lapses, such as invasions (attacks from outside the business) and misuse (attacks from within the organization). Vulnerability assessment (also known as scanning) used by ID Utilizes a technology created to evaluate the security of a computer system or network (Catal, et al., 2023). The following are some intrusion detection functions:

i. Monitor and analyze the user and the system behavior.
ii. Analyze system configurations and vulnerability
iii. Assessing system and file integrity

**Related current Techniques**

***Detection of intrusions in grid and cloud computing***

An IDS is a system build to detect an intrusion on the network. In other words, once a potential cyberattack is detected, the system raises an alert (Sampson, 2022). Due to their distributed environments, cloud and grid computing is the most exposed targets for hacker attack. By carefully analyzing logs, configurations, and network traffic in such environments, Intrusion Detection System (IDS) can be utilized to strengthen security precautions. Traditional IDSs are not appropriate for cloud environments because host-based IDSs (HIDS) and network-based IDSs (NIDS) are unable to identify encrypted node communication and hidden attack trails respectively. An IDS service with an audit system at the cloud middleware layer was presented in (Kleber et al., 2010), and it is intended to cover assaults that NIDS and HIDS are unable to identify.

*Corresponding author: Paschal Chinedu*
chinedupu@dsust.edu.ng
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

The node, service, event auditor, and storage are all parts of the IDS service's architecture. Resources on the node can be accessed by means of middleware that establishes access-control rules. Through middleware, the service makes communication easier. The event auditor keeps track of and records network data while also investigating any rule or policy violations. The storage contains databases that are based on behavior (comparison of recent user activities to typical behavior) and knowledge (known trails of prior attacks). The audited data is forwarded to the IDS service core, which examines it and raises an intrusion warning. The authors used simulation to evaluate their IDS prototype, and they discovered that it performed well enough for real-time use in a cloud context. The security policies compliance check for cloud service provider and their reporting processes to cloud users, however, have not been considered. Despite this, they haven't talked about how cloud service providers' security rules are checked for compliance or how the cloud users of these standards are informed.

***Intrusion detection in the cloud***

Any business or IT organization that faces hostile intruder attacks needs to have a strong active defensive system against them. Intrusion detection systems are crucial to this. A scalable, effective, and virtualization-based methodology is needed for IDS deployment in cloud computing (Ogbomo et al., 2018; Li et al. 2022). When using the cloud, a user's data and applications are stored on the distant servers of the cloud service provider, and the user has little control over the data and resources that are stored there. In this scenario, the cloud provider is now in charge of IDS cloud administration (Momoh et al., 2021). Nevertheless, the user, not the cloud service provider, should be the administrator of the IDS for the cloud. In the paper, (Roschke et al, 2009) have proposed an integration solution for central IDS management that can combine and integrate various renowned IDS sensors output reports on a single interface. IDS sensors have been able to communicate with one another using the intrusion detection message exchange format (IDMEF) standard.

The deployment of IDS sensors on distinct cloud levels, such as application, system, and platform layers, has been recommended by the authors. The application "Event Gatherer" receives any created alerts. With the aid of the Sender, Receiver, and Handler plug-ins, the event gatherer receives alert messages, converts them into the IDMEF standard, and saves them in an event data base repository. Through the use of an IDS management system, the analysis component provides complicated attacks to the user after analysis. An efficient architecture for managing cloud IDS has been put out by the authors, which the cloud user might oversee and manage. They have made available a central IDS management system based on several sensors that communicate via the IDMEF standard and are supervised by cloud users.

***Security Issues in Cloud Computing:***

Security threats can be categorized as follow (Richard et al, 2009);

1. Cloud data confidentiality issue
2. Network and host-based attacks on remote Server
3. Cloud security auditing
4. Lack of data interoperability standards

***Cloud data confidentiality issue***

Confidentiality of data over cloud is one of the glaring security concerns. Encryption of data can be done with the traditional techniques (Chinedu et al; 2015; Chinedu & Nwankwo, 2018; Daniel et al, 2021). Data that is encrypted can be protected from malicious users, but it cannot be made private from the administrator of the data at the service provider's end. In that situation, there is still a problem with searching and indexing encrypted data. The cloud security concerns stated above are just a few, and the dynamic cloud architecture is encountering additional difficulties as a result of the quick adoption of new service paradigms.

*Corresponding author: Paschal Chinedu*
✉ chinedupu@dsust.edu.ng
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

***Network and host-based attacks on remote Server***

Host and network intrusion attacks on remote hypervisors are a major security concern, as cloud vendors use virtual machine technology (Mangrulkar, *et. al.,* 2014). DOS and DDOS attacks are launched to deny service availability to end users (Dhanya et al., 2023).

***Cloud security auditing***

Checking that the vendor is in compliance with all security regulations requires a challenging effort called cloud auditing. Sensitive user data and procedures are within the control of the cloud service provider, hence a system for automatic or outside auditing is required for forensic analysis and data integrity checks. Another issue with cloud security is the privacy of data from third-party auditors (Chinedu et. al, 2020).

***Lack of data interoperability standards***

It leads to a situation of data lock-in for cloud users. A cloud user might not be able to switch to another service provider for a variety of reasons because their data and applications might not be compatible with the platform or data storage format of the new vendor. The cloud service provider would be in charge of the security and confidentiality of the data, and the cloud user would be reliant on that one service provider (Machado et. al., 2009; Pahl et. al., 2013).

**ANALYSIS OF MULTI-THREADED CLOUD IDS MODEL: WORK PRINCIPLES**

Cloud computing provides application and storage services on remote servers. Clients do not need to be concerned about upkeep or upgrades to the hardware or software. A cloud data center's hypervisor server hosts several clients on a single physical machine as part of the cloud paradigm, which operates on the idea of virtualizing resources. The administrator would be able to keep an eye on the hypervisor and any virtual machines running on it by deploying HIDS in the hypervisor or host machine. However, there would be performance difficulties such as overloading of the VM hosting IDS and data packet dropping with the quick flow of big volume of data as in the cloud model. A host's HIDS would also be neutralized if it were hacked by an offensive attack. A network-based IDS would be more appropriate for deployment in a cloud-like architecture in such a situation. NIDS would be installed outside the VM servers on network bottlenecks like switches, routers, or gateways for network traffic monitoring in order to obtain a system-wide perspective. Such NIDS would continue to struggle with the problem of high network access rates in cloud environments. The model proposition in Sheke etal (2012) captured a multi-threaded IDS solution to handle a huge number of data packets flow in such an environment. Large amounts of data might be processed by the multi-threaded IDS, which could also lower packet loss.

The suggested IDS efficiently analyze the observed alarms before sending them to a third-party monitoring service, which then directly inform the cloud user of their system's vulnerability. Additionally, the third-party monitoring service give cloud service providers professional guidance regarding incorrect system setups and intrusion loopholes. Utilizing the cloud network, the user of the service can access data located on distant servers at the location of the service provider. The NIDS with many threads is used to track and monitor user requests and activity. With expert assistance for the cloud service provider, the alarm logs are easily transmitted to cloud users. The developed IDS model (Shelke *et al*, 2012) is depicted in Figure 1.

*Corresponding author: Paschal Chinedu*
✉ *chinedupu@dsust.edu.ng*
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 11(4), DECEMBER, 2023
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

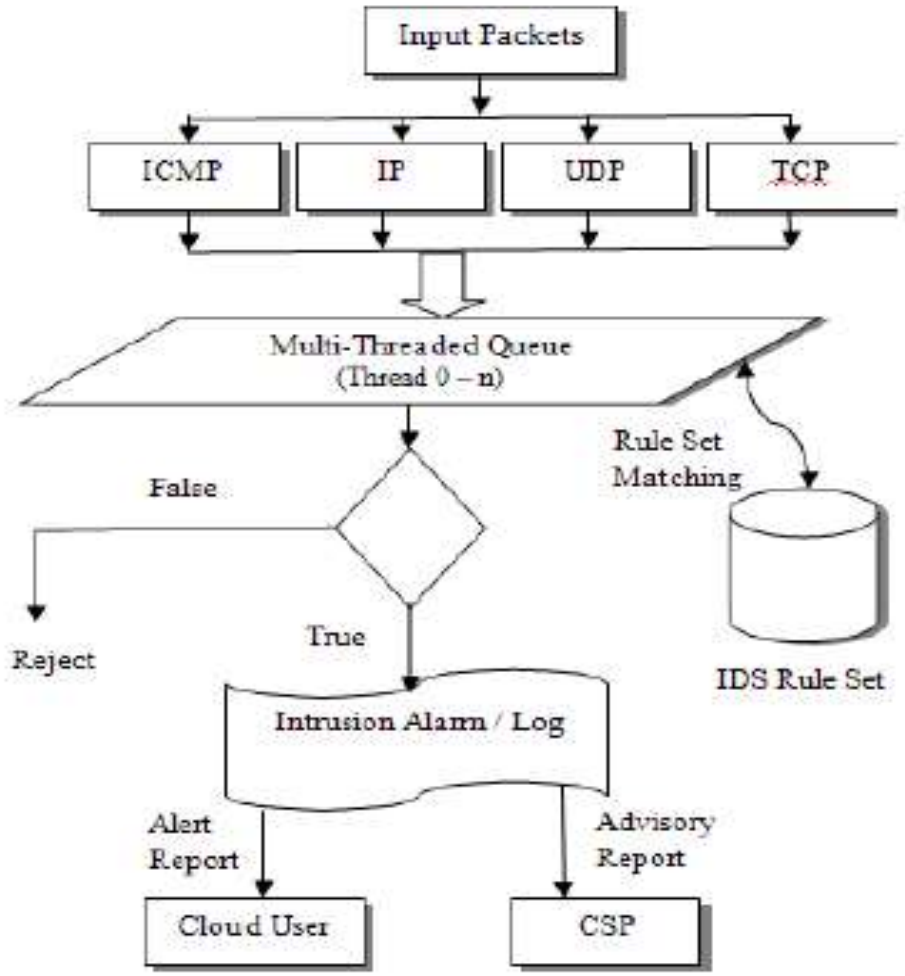


Figure 1: Flow Chart for the developed Multi-Threaded Cloud IDS Model [Source: Shelke et. al., (2012)]

Three modules makeup of the multi-threaded NIDS model for distributed cloud environment which are: capture & queuing module, analysis/ processing module and reporting module. The shared queue receives the data packets that have been recorded for analysis. The analysis and process module receive data packets from the shared queue and examines them using a pre-defined rule set and signature base. It is possible for each process in a shared queue to have numerous threads that cooperate to enhance system performance. TCP, IP, UDP, and ICMP packets are received by the main process, and various threads process and compare those packets against a set of predefined rules concurrently. The faulty packets are located by effective matching and analysis, and notifications are produced. The alert reports are created by the reporting module after reading the alerts from the shared queue. The third-party monitoring and advising service, which has the

*Corresponding author: Paschal Chinedu*
✉ *chinedupu@dsust.edu.ng*
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

necessary expertise and resources, right away produce
a report for the information of cloud users and deliver a detailed expert advisory report to cloud service providers.

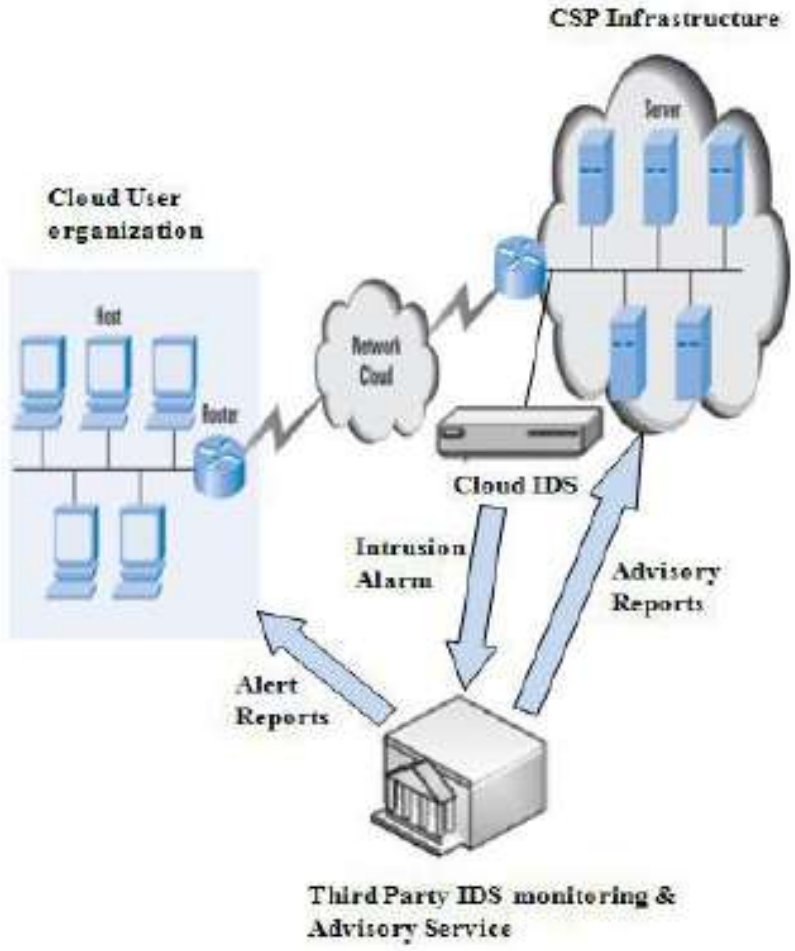


Figure 2 Cloud IDS Model. Source: Shelke et. al.,(2012)

***Advantages of Cloud IDS model***

1. A single node IDS manage a large amount of data in a cloud setting by using a multi-threaded technique.
2. The total effectiveness of cloud IDS is increased by lowering CPU, memory, and packet loss usage.
3. If a host is the target of an offended attacker and is taken over by the intruder, host-based IDS (HIDS) on that host would be compromised. In such a scenario, the attacker might wreak havoc on the data and apps and prevent HIDS from sending notifications to the administrator. Cloud infrastructure has

*Corresponding author: Paschal Chinedu*
✉ chinedupu@dsust.edu.ng
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

been suggested to use network IDS (NIDS) for improved visibility and resistance.

4. It has been recommended to utilize a third-party monitoring and advisory service that is equipped with the knowledge and tools necessary to keep an eye on intrusion data, handle it, and provide reports for cloud users as well as advisory reports for cloud service providers.
5. The Cloud IDS has been prescribed for deployment at a central location and are able to handle data analysis concurrently, which is an effective method (Shelke *et. al.,* 2012).

## DISCUSSIONS

Security is perceived as one of the main obstacles to cloud computing. Though with cloud computing business agility, scalability, and efficiency is on the increase, yet the introduction of new security risks and concerns are inevitable. Consequently, the new business computing models created is plagued with more complex challenges since they comprise not only technology issues but also substantial process changes as a result. It is therefore pertinent that securing the virtual environment of the public IaaS cloud would pave the way to eliminating consumer's fear thereby promoting increased stakeholders' adoption of cloud computing. This has been achieved by the propounded multi-threaded cloud IDS approach that is managed by a third-party monitoring service to provide improved efficiency and transparency for the cloud customer.

The research place of this new computing paradigm in evolving a rapid adoption of new technology and new business computing models for a new trend of business environment, provides the bedrock to a secure multi-threaded cloud IDS multi-tenant and virtualization resource in public Infrastructure as a Service cloud environment capable ensuring effective Network Access Traffic Management and Administrative Control.

## CONCLUSION

Given that cloud computing is a "network of networks" through the internet, the likelihood of intrusion increases with the sophistication of an intrusive attack. To stop harmful attacks in traditional networks, many IDS approaches are used. An effective, dependable, and information-transparent IDS is needed because of distributed assaults vulnerability, Cloud computing, high network access rates, and giving up control of data and applications to service providers. A multi-threaded cloud IDS approach that can be managed by a third-party monitoring service has been propounded in this research for better optimized efficiency and transparency for the cloud customer.

## REFERENCES

Anashkin Y. & Zhukova, M. (2021). Implementation of Behavioral Indicators in Threat Detection and User Behavior Analysis. AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia. Available at CEUR-WS.org

Barhaiya, H. & Mehta, D. (2023). Comparative analysis of Cloud, Grid and Distributed Computing on working perspective (February 2, 2023). Proceedings of the International Conference on Innovative Computing & Communication (ICICC) 2022, Available at SSRN: https://ssrn.com/abstract=4345699 or http://dx.doi.org/10.2139/ssrn.4345699

Catal, C., Ozcan, A., Donmez, E. et al. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Educ Inf Technol 28, 1809–1831 (2023). https://doi.org/10.1007/s10639-022-11261-8

Chinedu, P. U. (2018). Secured Cloud-Based Framework for ICT Intensive Virtual Organisation. Approved by: Owerri, Nigeria, Federal University of

*Corresponding author: Paschal Chinedu*
✉ chinedupu@dsust.edu.ng
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

Technology Owerri, Diss., 2008. Beau Bassin, Mauritius: LAP LAMBERT Academic Publishing. ISBN: 978-613-9-82456-4, Published: April 22, 2018

Chinedu, P. U., & Nwankwo, W. (2018). Security of Cloud Virtualized Resource on a SaaS Encryption Solution. *Science Journal of Energy Engineering.* Vol. 6, No. 1, 2018, pp. 8-17. doi: 10.11648/j.sjee.20180601.12

Chinedu, P. U.; Nwankwo, W; Aliu, D; Shaba, S. M.; and Momoh, M. O. (2020). Cloud Security Concerns: Assessing the Fears of Service Adoption. Archive of Science & Technology 1 (2), 164 – 174. ISSN:0189-3548 https://doi.org/10.xxx.

Chinedu, P. U., Nwankwo, W. &Eze, U. F. (2013) *Enterprise Cloud Adoption: Leveraging on the Business and Security Benefits.* West African Journal of Industrial and Academic Research, Owerri, Nigeria. Vol. 7, No. 1, June 30, 2013

Chinedu, P. U.; Nworuh, Godwin E.; Osuagwu, Oliver E.& Eze, U. F. *(2015) The security of user data: Demystifying fear to cloud model and service adoption and deployment.* International Journal of Academic Research, Azerbaijan, Russia. Vol. 7, No. 1, January 30, 2015.

Chinedu P. U., & Osuagwu, O. E. (2018). Assessing and Mitigating the Security Concerns, Threats and Associated Risks with Cloud Adoption, *Engineering Mathematics*. Vol. 2, No. 2, 2018, pp. 95-106. doi: 10.11648/j.engmath.20180202.17

Daniel, A., Shaba, S.M., Momoh, M.O., Chinedu, P.U., Nwankwo, W. (2021). A Computer Security System for Cloud Computing Based on Encryption Technique. Computer Engineering and Applications, 10 (1)

Dhanya K. A, Vajipayajula S., Srinivasan, K., Tibrewal, A., Kumar, T.S., & Kumar, T. G., (2023). "Detection of Network Attacks using Machine Learning and Deep Learning Models," Procedia Computer Science, Volume 218, 2023, Pages 57-66, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.401.

Galvano, F. & Figna, F. (2023) Security at airports around the world: Implementation of behavioral analysis application technology. Behaviour Analysis Team´s Lab. January 2023 Available at www.behaviouranalysisteam.com

Gargi S., & Sandeep K. S. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. Journal of Economic Criminology, Volume 2, 2023, 100034, ISSN 2949-7914, https://doi.org/10.1016/j.jeconc.2023.100034.

Kaur, T. & Kamboj, S. (2023). "Descriptive Analysis of the Cloud Computing Services and Deployment Models," *2023 International Conference for Advancement in Technology (ICONAT)*, Goa, India, 2023, pp. 1-6, doi: 10.1109/ICONAT57137.2023.10080749.

Li, W., Meng, W., & Kwok, L. F. (2022). Surveying Trust-based Collaorative Intrusion Detection: State-of-teArt, Challenges and Future Directions. IEEE Communications Surveys and Tutorials, 24(1), 280-305. https://doi.org/10.1109/COMST.2021.3139052

Machado, G. S., Hausheer, D. & Stiller, B. (2009). Considerations on the Interoperability of and between Cloud Computing Standards. October 2009. DOI: 10.5167/uzh-24316

Mahadevan, R. & Neelamegam, A. (2018). Cloud hosting services and resources utilizing efficient proxy server based speculative algorithm. International Journal of Engineering & Technology 7(4):2687-2691. DOI: 10.14419/ijet.v7i4.14135

*Corresponding author: Paschal Chinedu*
✉ *chinedupu@dsust.edu.ng*
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*

Mangrulkar, N., Bhagat Patil, A. R. & Pande, A. S. (2014) Network Attacks and Their Detection Mechanisms: A Review. International Journal of Computer Applications 90 (9). February 2014. DOI: 10.5120/15606-3154

Momoh, M. O., Chinedu, P. U., Nwankwo, W., Aliu, D., & Shaba, M. S. (2021). Blockchain Adoption: Applications and Challenges. *International Journal of Software Engineering and Computer Systems*, 7(2), 19-25.

Ogbomo-Odikayor. I.F., Anigbogu. S.O., Edebeatu Dom, & Anigbogu. G.N. (2018) "A hybrid model of intrusion detection system in a cloud computing environment," International Research Journal of Advanced Engineering and Science, Volume 3, Issue 3, pp. 194-200, 2018.

Pahl, C., Zhang, L., & Fowley, F. (2013). "Interoperability Standards for Cloud Architecture, Conference: 3rd International Conference on Cloud Computing and Services Science. May 2013

Richard Chow, Philippe Golle, Markus Jakobsson, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", ACM Computer and Communications Security Workshop, CCSW 09, November 13, 2009.

Roschke, Sebastian & Cheng, Feng & Meinel, Christoph. (2009). Intrusion Detection in the Cloud. IEEE International Conference on Dependable, Autonomic and Secure Computing. 729-734. 10.1109/DASC.2009.94.

Sampson, J. R. (2022). Top 10 Intrusion Detection and Prevention Systems. *CLEARNETWORK*. Available: https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/

Shelke, P. K.; Sontakke, S. & Gawande, A. D. (2012). Intrusion Detection System for Cloud Computing. *International Journal of Scientific & Technology Research* Volume 1, Issue 4, May 2012, ISSN 2277-8616 67. Retrieved 17 March 2024 from www.ijstr.org

Singh, A. (2024). Grid Computing: How Does it Work? Available online at https://www.shiksha.com/online-courses/articles/grid-computing-how-does-it-work/ Accessed: 17/06/2024

Tank, D., Aggarwal, A. & Chaubey, N. (2022) Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. International Journal of Information Technology 14, 847–862 (2022). https://doi.org/10.1007/s41870-019-00294-x

*Corresponding author: Paschal Chinedu*
✉ *chinedupu@dsust.edu.ng*
*Department of Information Systems and Technology, Delta State University of Science and Technology, Ozoro*