IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 10, Issue.12, December 2022 E-ISSN: 2347-2693

Distributed Operating System Security and Reliability

Attah Stella[1*], Taylor O.E.[2]

[1]Department of Computer and Robotic Education, Federal College of Education Technical Omoku, Rivers State, Nigeria
[2]Department of Computer Science Rivers State University Port Harcourt, Rivers State, Nigeria

Corresponding Author: wilzex@gmail.com

DOI: https://doi.org/10.26438/ijcse/v10i12.3440 | Available online at: www.ijcseonline.org

Received: 25/Oct/2022, Accepted: 26/Nov/2022, Published: 31/Dec/2022

***Abstract*—** Major security issues in distributed operating systems are categorized into information leakage via hacking, server redundancy, vulnerability and risk assessment inefficiency. This study presents a systematic survey of security and reliability issues in a distributed operating system. A distributed operating system is a unique system program which adopts numerous central processors for real-time execution of allocated tasks. A distributed operating system connects many computer systems using a single communication channel. The frequent application of distributed operating systems to data sharing and management among cooperate entities has necessitated the need for distributed resources and computing strategies. The security and reliability features of a distributed operating system are critical and highly indispensable. Data security models for reliability of a distributed operating system were analysed, compared and discussed in the study. The essence of the discussed models was to enhance the performance of distributed operating systems. The study looked at models such as data-at-rest security model, access control model, steganography model, body area model, data classification model and cryptography model. The models were adequately compared and analysed especially in terms of performance mode, pros and cons. The study could be beneficial to developers of distributed operating systems and researchers with keen interest in the study area.

***Keywords*—** Data Models, Distributed Operating System, Reliability, Security

I. INTRODUCTION

The study presented a systematic survey of security and reliability issues in a distributed operating system. A distributed operating system is a unique system program which adopts numerous central processors for real-time execution of allocated tasks. A distributed operating system connects many computer systems using a single communication channel.

The frequent application of distributed operating systems to data sharing and management among cooperate entities has necessitated the need for distributed resources and computing strategies. The security and reliability features of a distributed operating system are critical and highly indispensable. This is because; it entails the interaction between different independent entities using a common source of communication. Since the processing features of a distributed operating system are not domiciled in a single machine, its security and reliability remains critical in order for it to function properly [7].

The aim of the study is to survey security models for distributed operating systems. The study intends to analyse current security models for distributed operating systems, compare current security models for distributed operating systems in both classical and contemporary research works and recommend the prospect of data security methods for cloud computing environments.

II. EMPIRICAL REVIEW OF THE STUDY

This section discussed reviewed empirical studies that hold some levels of significance to the study being conducted.

1. Study: Reliability Issues in Distributed Operating Systems
Author(s)/Year: [1]
Aim of the Study: to look at the various kinds and discuss some of the reliability issues involved.
Methodology: Systematic Review Method
Summary of Findings: The study concentrated on the causes of unreliability, illustrating these with some general solutions and examples. Among the issues treated are inter-process communication, machine crashes, server redundancy, and data integrity.
Identified Gap: The authors did a good job. However, the authors failed to the surveyed reliability issues with a machine learning model which would have provided more clarification and understanding.
Proposed Solution: A secured model for distributed operating system reliability

2. Study: Security Issues in Distributed Systems
Author (s)/Year: [7]
Aim of the Study: To emphasize the aspect that provides a literature review between security and reliability
Methodology: Systematic Review Method
Summary of Findings: The study defined what a secure system is, observes security policies from security

mechanisms including authentication and authorization as major processes. Considers encryption as a cryptographic technique that is useful for data confidentiality and privacy than similarly, access control as an important feature that enables authority is also assessed monitoring some proposal models.

Identified Gap: The authors did a good job. However, the authors failed to implement the surveyed reliability issues with a machine learning model which would have provided more clarification and understanding.

Proposed Solution: A secured model for distributed operating system reliability

3. Study: Some Issues, Challenges and Problems of Distributed Operating Systems

Author(s)/Year: [8]

Aim of the Study: To present a systematic literature review on the issues, challenges, problems and solutions of the Distributed Operating Systems

Methodology: Agile Method

Summary of Findings: The study analyzed critical issues which influences the performance of distributed operating systems. The study also opined that the major issues affecting the performance of a distributed operating system are security and privacy issues, scalability issues, object representation and translation issues, resource management issues and heterogeneity issues.

Identified Gap: The authors did a good job but failed to proffer solutions to each of the discussed issues affecting a distributed operating system.

Proposed Solution A secured model for distributed operating system reliability parameters such as security, scalability and resource management.

4. Study: Distributed Operating System: An Overview

Author(s)/Year: [3]

Aim of the Study: To introduce the concepts of Distributed Operating Systems

Methodology: Systematic Review Method

Summary of Findings: The study opined that distributed operating systems have many aspects in common with centralized ones, but they also differ in certain ways. As distributed computing becomes more widespread, both in high-energy physics and in other applications, centralized operating systems will gradually give way to the distributed ones.

Identified Gap: The authors did a good job but failed to address critical issues which affects the performance of a distributed operating system.

Proposed Solution: A secured model for distributed operating system reliability

5. Study: Research Paper on Distributed Operating Systems

Author(s)/Year: [11].

Aim of the Study: To explain key design issues involved in the development of distributed operating systems.

Methodology: System Analysis and Design Technique (SADT)

Summary of Findings: The study opined that Distributed systems consist of independent central processing units (CPUs) that work together to make the absolute system look like a single computer. They have a number of possible selling points, including good price/performance ratios, the capability to match distributed applications well, potentially high consistency and incremental increase as the workload grows.

Identified Gap: The authors did a good job. The developed model in the study lacked flexibility in its design. The lacked flexibility could also make the system prone to latency.

Proposed Solution A secured model for distributed operating system reliability

.

III. OVERVIEW OF SECURITY ISSUES IN DISTRIBUTED OPERATING SYSTEM

Major security issues in distributed operating systems are categorized into;

i) Information leakage via hacking and server redundancy.
ii) Vulnerability and risk assessment inefficiency.

Information leakage in a distributed operating system can be described as the unauthorized release of confidential information by a malicious insider. The activity of information leakage often results to security compromise and corrosive outcome of organizational information systems. According to [12], “The activity and perpetuation of information leakage is as a result of poor human behaviour towards information systems security” The issue of unauthorized hacking activities is as a result of unemployment, greed and financial lust among most youths in Nigeria. They utilize high software products to perpetuate cyber-crimes.

Some of them act as malicious insiders and black hackers in reputable organizations. They capitalize on the weakness and vulnerability of information systems in order to perpetuate cyber-crimes. Privacy and security lapses in data networks involve software erosion due to lack of upgrade and maintenance. Most industries and companies in Nigeria are victims to privacy and security lapses. They are left at the mercies of malicious insiders who use the back door to explore their weaknesses. This situation poses a real and constant threat to profitability and may raise the price of goods and services for consumers.

The concept of risk management can be described as tasks associated with the control of risks i.e. risk assessments, risk acceptance, risk reduction, protective measures and chance assignment. Businesses depend on information technology to effectively carry out business functions. Information and communication systems are subject to threats that can have damaging effects on organizational assets and operations. The concept of vulnerability is a security defect which enables an attacker to avoid security procedures. Malicious attackers seek to determine and exploit program vulnerabilities to occasion security

breaches. Hackers have in the past been viewed as an individual with exceptional technical talent [5] in recent times.

Hackers have acquired a bad reputation and it is used to refer to an individual who accesses computers and information stored on computers without permission. [2] Concurred with this view in describing hacking as a system with no authorization and accessing a system with a level beyond their authorization. There are three types of hackers, black hats, White Hats and grey hats. White hats are hackers who use their skills in an ethical manner. This research employs (white) ethical hacking in an attempt to influence stakeholders' cyber security management practices. Black Hats use their mastery for criminal purposes.

Ethical hacking can be described as an authorized access to an information system in order to evaluate its strength and weakness. In the search for a way to address the issue of hacking, businesses discovered that one of the best methods to assess an intruder threat will be to get independent computer security experts to try attack their system. If an action" promotes the normal well-being of society, maintains or perhaps increases individual freedoms and rights, protects people from harm, treats humans as vulnerable beings as well as accords those beings respect, as well as upholds religious, social, cultural and federal laws and morals", then it could be seen as ethical [6].

Apart from utilizing publicly accessible information to get information, the next stage involves Scanning then Enumeration. After Enumeration the next stage is System Hacking, then Privilege Escalation, next is Covering Tracks and finally Backdoor Planting. Trust is a unique strategy for online business success. When trust is breeched, then the business collapses. An online business can be referred to as business carried out with the aid of the internet. Most online businesses run on web-based applications which utilize server-side program tools. Most entrepreneurs running online businesses always crave for confidentiality, integrity and availability. In order to balance the mentioned attributes, the issue of trust and user friendliness needs to be addressed in equal proportion [14]. The word integrity is the strict adherence to moral values and discipline. Integrity is needed for trust and user-friendliness in an online business.

According to [13], "Data integrity is an integral component of information security and cloud computing". The consistency and accuracy of information shared between parties in an online business is a catalyst for trust and user-friendliness. Data integrity in an online business encompasses domain consistency, entity consistency, and referential integrity and user-defined integrity.

IV. METHODOLOGY

The study adopted a systematic review methodology. A systematic review is a review of a clearly formulated question that uses systematic and reproducible methods to identify, select and critically appraise all relevant research, and to collect and analyse data from the studies that are included in the review.

V. DATA SECURITY MODEL FOR DISTRIBUTED OPERATING SYSTEMS

There are several security models which can be utilized for the reliability of distributed operating systems. Major models for distributed operating system security are:

- Data-at-Rest Security Model.
- Access Control Model.
- Steganography Model.
- Body Area Network (BAN) Model.
- Data Classification Model.
- Cryptography Model.

A. Data-at-Rest Security Model

The data-at-rest security model provides a single gateway platform for the security of data packets in cloud computing environments. The model utilizes a defense mechanism structure known as the three-level systems. Each level of the defence mechanism structure provides security for each deployed data packet over the internet.

The first level of the model utilizes the one time password (OTP) concept. The second level of the model utilizes strong encryption algorithm for securing data packets. The third level of the model ensures that data recovery by end-users of the model is provided. However, the data-at-rest model does not have support for multiple-languages to actually facilitate the use of abstractions and allow us to harness the heterogeneity of large scale software repositories. Figure 1 shows the architecture of the Data-at-Rest security model.

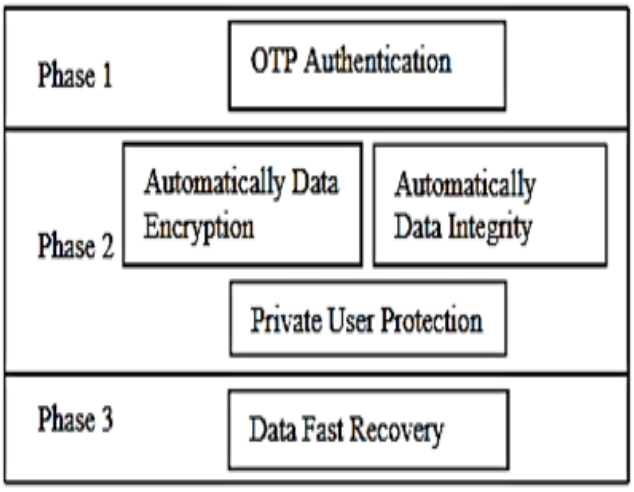

Figure 1. Architecture of Data-at-Rest Security Model (Source: [4])

B. Access Control Model

The access control model is a data security framework which limits the actions or operations that a legitimate user of a computer system can perform. The model manages and restricts the activity of an end-user. This is necessary in order to avoid data leakage in a cloud computing environment. The model is backed up by a reference monitor which appeals every potential login by a user to objects in the system. Furthermore, the reference monitor calls an authorization information storage platform in order to scrutinize activities of the end-user in a secured manner. However, performance evaluation of the access control model shows that it can be prone to attack by a malicious insider. Hence, the need for an embedded monitoring framework for the system is highly indispensable. Figure 2 shows the architecture of the access control model.

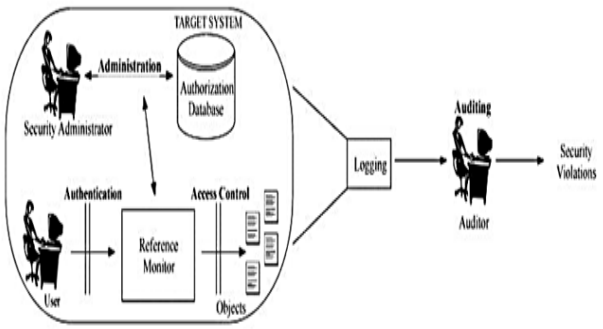

Figure 2. Architecture of an Access Control Security Model (Source: [10])

C. Steganography Model

The steganography model enables the exercise of hiding information behind an image. The concept of steganography can be likened to the technology of concealing private data within an image in order to avoid leakage. The application of steganography can be joined with pass wording as a supplementary addition for data security. Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content [13].

Steganography is performed by systems of secret codes. There are valid uses of steganography. For instance, the makers of malware products have applied the concept of steganography to the sending of malicious codes. Furthermore, several forms of steganography are utilized for tens of years, and are made up of pre-defined steps for concealing data. The current process for steganography involves the obfuscation of data via the usage of specific algorithms.

Discrete datasets can be implanted into common data files in specific ways. A major part of this is to conceal data in bits that stands for identical color pixels that are duplicated in an image file. Through the application of concealed datasets to this un-performing datasets in some less obvious way, the outcome will involve an image file that shows some resemblance to the original image [15]. Another steganographic pattern is the addition of watermark. Watermarking is the process of adding ghosted texts to a document. Watermarking as a concept of steganography is often adopted by internet publishers in order to know sources of media datasets on the internet which are lacking authorized access. There are many applications of steganography in information security. Figure 3 shows the architecture of the steganography model.

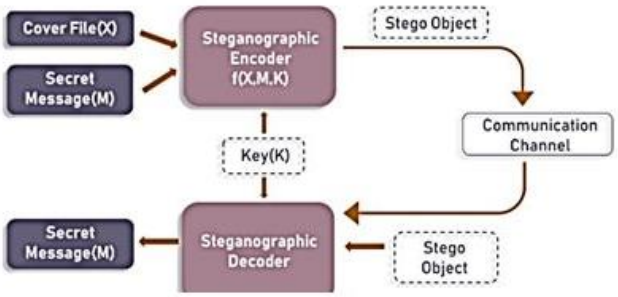

Figure 3. Architecture of the Steganography Model

D. Body Area Network Model

The body area network (BAN) model enables the joining of several embedded sensor-based objects via the internet. The BAN technology is very unique and can be applied to the enhancement of security information system. Furthermore, BAN can be applied to the medical field in which an individual can be equipped with sensor-based objects for measurement of issues that encompasses blood pressure, heart beats, and respiration and so on [14].

The concept of BAN model is quite easy to understand and has several utilizations in technology which includes:

- Network sensors that are embedded in the body.
- Network sensors that are used for physical sports.
- Network sensors that are used for programmable sounds.
- Network sensors that are used for integrating mobile devices.
- Network sensors that are used for integrating video devices.

Figure 4 shows the architecture of the body area network model.

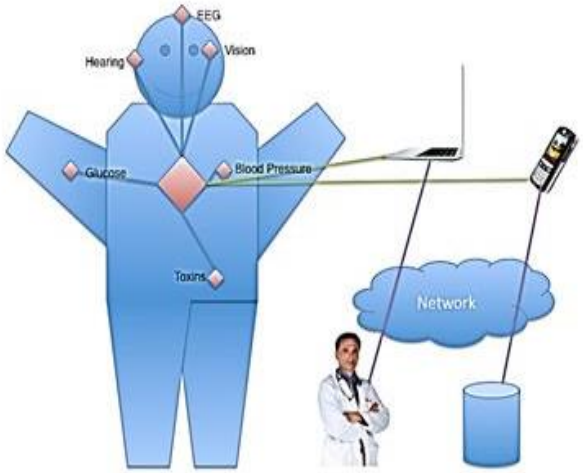

Figure 4. Architecture of a Body Area Network Model (Source: [14])

E. Data Classification Model

The data classification (DC) model enables the process of assigning different data type into a cluster that has been predefined and/or categorized [16]. It is a system whose responsibility is to carry out new documents' classification into one that its determination process is done through the use of categories that are predefined [17]. [18], stated that data classification has the aim of making a categorization of documents so that it will appear in predefined documents depending on how the appearance of their content is. Data classification concerned itself with the method through which data documents are classified into categories that are predefined [19]. Data classification is saddled with duty of assigning to predefined categories based on their content documents that appeared in a natural language. It is the division of input documents set into classes either two or more so that it will be possible for each document to be found in multiple classes [9]. The cryptography model enables the security of information and communication technique in cloud computing environments.

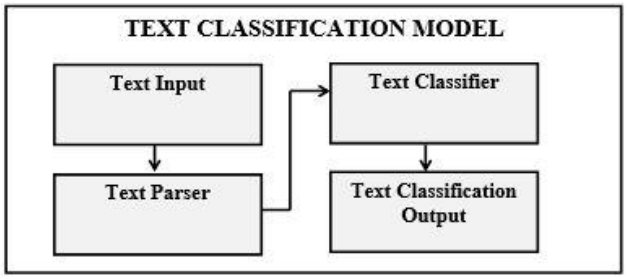

Figure 5. Architecture of a Text Classification Model (Source: [9])

F. Data Classification Model

The cryptography model enables the security of information and communication technique in cloud computing environments. Digital datasets are secured by cryptography through data transformation and prevention of unauthorized access to existing cloud computing environments. In addition, the cryptography model encompasses of a secret key, a public key and hash functions.

Comparative Analysis of Security Models for Distributed Operating Systems

Table 1 Shows the Summary and Discussion of Different Security Models

Sr. No.	***Security Model***	***Mode of Performance***	***PROS***	***CONS***
1.	Steganography	It uses systems of secret codes. Datasets are concealed in images. Discrete datasets can be implanted into common data files in specific ways. A major part of this is to conceal data in bits that stands for identical color pixels that are duplicated in an image file.	Messages are properly concealed and do not attract attention to themselves. Furthermore, Steganography supports Confidentiality and Authentication.	Image is distorted. Message easily lost if picture subject to compression such as JPEG.
2.	Body Area Network	Joining of several embedded sensor-based objects via the internet. It is associated with digital signal processing and embedded wireless personal area network (WPAN). The WPAN concept has highlighted the importance of body area network	Devices used are miniaturized and can be easily implanted.	It is characterized by low data throughput. It is prone to interference
3.	Data Classification	Carry out new documents' classification into one that its determination process is done through the use of categories that are predefined.	Establish exactly what is there, where it is stored, and how valuable and secured it is.	Many of the classifications themselves are based on subjective judgments, which may or may not be shared by everyone participating
4.	Cryptography	Data transformation and prevention of unauthorized access to existing cloud computing environments	Secures information and communication from unauthorized revelation and access of information.	The network or the computer system can be attacked and rendered non-functional by an intruder.

5.	Data-at-Rest	Utilizes a defense mechanism structure known as the three-level systems. Each level of the defense mechanism structure provides security for each deployed data packet over the internet.	Hiding Capacity: This feature deals with the size of information that can be hidden inside the cover file.	can be inefficient and time consuming
6.	Access Control	Manages and restricts the activity of an end-user. This is necessary in order to avoid data leakage in a cloud computing environment.	identifies users by verifying various login credentials, which can include usernames and passwords, PINs, biometric scans, and security tokens	Difficult to know the access right of a given subject. Difficult to revoke a user's right on all objects.

VI. DISCUSSION

Data security and reliability models are essential needs of a distributed operating system. The study scrutinized important data security models such as Steganography, Body Area Network, Data Classification, Cryptography, Data-at-Rest and Access Control. The steganography model has proven successful in data security; especially in secretly transmitting messages without the fact of the transmission being discovered. However, an identified drawback of the model is the large overhead to hide very tiny amounts of information. Hiding short messages within wide text is limited by the size of the extensive text.

The body area network has been a good monitoring tool for data sharing activities. Data packets in cloud computing environment can be secured with the body area network due to its sensors that constantly monitor specific biological functions. However, the model is still vulnerable back door interference issues. The data classification model ensures that authorized stakeholders have access to the data while preventing unauthorized access and abuse of privileges. By classifying the data stored in databases, organizations can ensure that only those who are authorized can view, modify, delete, or add sensitive information. However, many of the classifications themselves are based on subjective judgments, which may or may not be shared by everyone participating.

The cryptography model utilizes encryption technologies for data security. The model can guard information and communication from unauthorized revelation and access of information. However, the model can be difficult to access even for a legitimate user at a crucial time of decision-making. The Data-at-rest model remains a strong data security tool due to its defence mechanism structure known as the three-level systems. However, activities by the model can be inefficient which is as a result of latency. The access control provides verification and validation processes for preventing unauthorized access to an information system. The model still experiences difficulties in providing a user's right on all objects.

CONCLUSION

Data security models for reliability of a distributed operating system were analysed, compared and discussed in the study. The essence of the discussed models was to enhance the performance of distributed operating systems. The study looked at models such as data-at-rest security model, access control model, steganography model, body area model, data classification model and cryptography model. The models were adequately compared and analysed especially in terms of performance mode, pros and cons. In addition, the study presented a systematic survey of security and reliability issues in a distributed operating system. A distributed operating system is a unique system program which adopts numerous central processors for real-time execution of allocated tasks. A distributed operating system connects many computer systems using a single communication channel. The study could be beneficial to developers of distributed operating systems and researchers with keen interest in the study area.

REFERENCES

[1] Andrew, T. and Robbert, R. “Reliability Issues in Distributed Operating Systems”. International Journal of Engineering Technology (IJET), Vol.**4**, Issue.**3**, pp.**221-229, 2010.**

[2] Clarkson, M. and Logan, J. “Modified Survey of Ethical Hacking Concepts”. International Journal of Engineering Technology (IJET), Vol.**6**, Issue.**11**, pp.**34 – 39, 2005.**

[3] Deepika, C., Anjali, L. and Sandeep, Y. “Distributed Operating System: An Overview”. International Journal for Research in Applied Science and Engineering Technology (IJRASET), Vol.**2**, Issue.**4**, pp.**115 – 119, 2014.**

[4] Eman, M., Hatem, A. and Sherif, E. “Data Security Model for Cloud Computing”. Journal of Communication and Computer, 10(2013), pp.**1047 – 1062, 2013.**

[5] Falk, C. “Ethics and Hacking: The general and Specific”. Norwich University Journal of Information Assurance, **2005**.

[6] Farsole, M., Mills, H., and Peter, H. “Introduction to Computer Ethics Awareness”. International Journal of Computer Applications (IJCA), Vol.**12**, Issue.**6**, pp.**114, 2010.**

[7] Kaltrina, N. “Security Issues in Distributed Systems. A Survey”. 1st International Symposium on Computing in Informatics and Mathematics (ISCIM 2011) in collaboration between EPOKA, University and “Aleksander Moisiu” University of Durress on June 2 – 4 2011, Tirana – Durress, Albania, **2011**.

[8] Kamal, S. and Anil, K. “Some Issues, Challenges and

Problems of Distributed Software System". International Journal of Computer Science and Information Technologies. Vol.**5**, Issue.**4**, pp.**4922 – 4925, 2014.**

[9] Khan, N. Z. and Yadav, S. R. "Analysis of text classification algorithms: A Review". International Journal of Trend in Scientific Research and Development, Vol.**3**, Issue.**2**, pp.**579-581, 2019.**

[10] Kriti, K. "Database Security and Access Control Models: A Brief Overview". International Journal of Engineering, Research and Technology (IJERT), Vol.**2**, Issue.**5**, pp.**743 – 751, 2013.**

[11] Mohit, R. and Manish, L. Research Paper on Distributed Operating Systems. International Journal of Innovative Research in Technology (IJIRT). Vol.**1**, Issue.**5**, pp.**128 – 132, 2014.**

[12] Silvanus, A. "Case Study: Using Security Awareness to combat the advanced persistent threat". Paper presented at the 13th Colloquium for Information, Systems Security Education (CISSE), University of Alaska, Fairbanks, Seattle, pp.**134, 2014.**

[13] Warsaw, F., Chris, O., and Smalling, D. "Autonomous Wireless Sensors for Body Area Networks". IEEE 2017 Custom Integrated Circuits Conference, **2017**.

[14] Yang, O. "Proposed Embedded Security framework Internet of things (iot), vehicular Technology". Information Theory and Aerospace and Electric Systems Technology (wireless vitae), 2011, **2016**.

[15] Chen, R., Wong, H., and Ming, I. (2016). Document Classification and Processing Techniques for Software Computing. Available from: International Journal of Engineering Technology (IJET), Vol.**12**, Issue.**3**, pp.**223 – 227, 2022.**

[16] Rani, M. Dick, B., Sara, M., Brad, W., and Tom, L (2018). Analysis and Detection of Malicious Insiders. **2022**.

[17] Roiss, M.,and Nazlia, M. (2015). Text classification techniques: A literature review. Interdisciplinary. Available from: Journal of Information, Knowledge, and Management, Vol.**13**, pp.**117-135, 2015.**

[18] Adel, S., Fregh, M., and Palls, G. (2016). Data leak: Data Leakage Detection System. Available from: MACRO 2015 – 5th, International Conference on Recent Achievements in Mechatronics, Automation Computer Science and Robotics Vol.**6**, Issue.**4**, pp.**23 – 29, 2022.**

[19] Patel, F. N. and Soni, N. R. (2013). Increasing accuracy of k-nearest neighbour classifier for text classification, International Journal of Computer Science and Informatics, Vol.**3**, Issue.**2**, pp.**80-85, 2013.**

AUTHORS PROFILE

Attah, Stella earned her B.Sc, and Msc. in Computer science from Rivers State University, 2014, and 2019, respectively. She is currently working as a Lecturer in Department of Computer Robotic Education from Federal College of Education Omoku since 2020. She is a member of CEAN since 2022. She has published more than 10 research papers in reputed international journals including America Journa of Science and Engineering etc. and it's also available online. Her main research work focus on Load Balancing in Computational Server Environment, She has 5 years of teaching experience and 3 years of research experience.

