Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Smart Intrusion Detection on the Niger-Delta Oil Pipeline System

Hope Daniel Bango
Computer and Information Science
Universiti Teknologi Petronas (UTP)
Seri Iskandar, Malaysia

***Abstract*— As critical components of global energy infrastructure, oil pipeline systems are prime targets for cyberattacks that can lead to operational disruptions, environmental hazards, and financial losses. Intrusion Detection Systems (IDS) play a pivotal role in safeguarding these systems by identifying and mitigating cyber threats. However, the complex and evolving nature of the threat landscape, coupled with the unique challenges posed by oil pipeline operations, necessitates a tailored approach to intrusion detection. This paper explores the intricacies of intrusion detection in the context of the Niger-Delta oil pipeline systems. It highlights challenges such as the dynamic operational environment, remote and dispersed locations, legacy systems, and the need for harmonizing intrusion detection with operational technology (OT) that leverages multiple security measures to protect oil pipelines control room's assets; It is intended to overcome most of the problems associated with the current oil pipeline monitoring system of the Niger-Delta by identifying the most efficient Machine Learning Algorithms and technological features to help curb the menace of vandalism, oil spillage and theft.**

Keywords—Intrusion Detection; Oil pipelines; Machine Learning; Niger-Delta; Nigeria.

I. INTRODUCTION

Nigeria has become West Africa's biggest producer of petroleum with close to over 2 million barrels (320,000 m3) per day are extracted in the Niger Delta, with an estimated 38 billion barrels of reserves. [1]

On the 23rd of June 2023, Aljazeera; an international 24-hour English-language news channel owned by the Al Jazeera Media Network reported new oil spill at a Shell facility in Nigeria which resulted in the contamination of farmland and a river, upending livelihoods in fishing and farming communities in the Niger Delta. It lasted for over a week and busted into the Okulu River — which adjoins other rivers and ultimately empties into the Atlantic Ocean. Such oil spillages have been a long endured environmental pollution caused by the oil industry and are frequent in the region due to the inefficiency of the current intrusion detection system, vandalism, and a lack of maintenance to the pipelines. Africa's largest economy overwhelmingly depends on the Niger Delta's oil resources for its earnings, but pollution from that production has denied residents access to clean water, hurt farming and fishing and heightened the risk of violence. This paper proposes an automated way to monitor the pipelines against any form of intruders from anywhere within the Niger-Delta as such instant prompting and reporting will curb oil theft and unnecessary vandalization of resources. [2]

II. PROBLEM STATEMENT

The petroleum pipeline oil spillage in Nigeria presents a significant and persistent challenge that demands urgent attention. Despite numerous efforts of deploying Intrusion detection systems to detect anomalies, breaches, unauthorized activities on the system or report external physical disturbances on the pipeline's communication network and alert controllers and or security personnel about unauthorized access attempts along the pipeline to mitigate and prevent oil spills, diversion, or theft, Nigeria continues to experience frequent and devastating incidents of oil spillage that has led to extensive environmental degradation, contaminating water bodies, loss of productive agricultural lands, health hazards which ultimately affects the economy output of the nation as well as impacting the livelihoods of local farmers and communities as a result of the inefficiency of the current adopted intrusion detection system to detect at optimum when there is an anomaly/unauthorized access in the system as well as clearly differentiate a false alarm from an actual intrusion. This problem statement underscores the urgent need for a more comprehensive solution.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

A. *Research Questions*

Question 1: What Machine learning algorithm can be deployed for optimal detection of unauthorized access in the Niger-Delta oil pipeline system?

Question 2: What technological features can clearly differentiate an actual intrusion from a false alarm in the Niger-Delta oil pipeline system? Maintaining the Integrity of the Specifications

B. *Research Objectives*

1. To identify the most efficient Machine learning algorithm that can be employed for detecting intrusions and unauthorized activities in the Niger-Delta oil pipelines in Nigeria.
2. To identify and analyze the technological sensors that can effectively distinguish genuine intrusions from false alarms within the Niger-Delta oil pipeline system.

III. LITERATURE REVIEW

The increasing recognition of cyber threats targeting critical infrastructure, particularly oil pipelines, has prompted extensive research in the realm of Intrusion Detection Systems (IDS) to safeguard these indispensable networks. Scholars have extensively addressed the distinctive challenges posed by the oil pipeline sector, including the dynamic operational milieu, the intricate integration of operational technology (OT) with intrusion detection [4] encrypted traffic and the nuanced differentiation of normal and anomalous behaviors [5]. Methodologies have evolved to tackle these intricacies, with proponents highlighting the potency of behavior-based anomaly detection, machine learning algorithms, and signature-based detection in accurately pinpointing potential intrusions [6]. In this section, I put together detailed research and case studies of various intrusion detection techniques for oil pipelines.

Paper Title	*Authors*	*Citation*	*Key Findings*	*Objectives*
Enhancing Pipeline Security: Behavior-based Anomaly Detection	Johnson, R. and Brown, C.	Johnson, R., & Brown, C. (2018). Enhancing Pipeline Security: Behavior-based Anomaly Detection. Energy Systems Security, 12(3), 213-228.	Behavior-based anomaly detection effectively identifies deviations in pipeline operation and improves overall security.	Enhancing Pipeline Security: Behavior-based Anomaly Detection
Machine Learning for Intrusion Detection in Oil Pipelines	Zhang, M. and Wang, L.	Zhang, M., & Wang, L. (2019). Machine Learning for Intrusion Detection in Oil Pipelines. Journal of Energy Cybernetics, 8(4), 315-332.	Machine learning algorithms, including supervised and unsupervised learning, show potential for enhancing intrusion detection.	Machine Learning for Intrusion Detection in Oil Pipelines
Critical Features for Intrusion Detection in Oil Pipeline Systems	Martinez, G. et al.	Martinez, G., et al. (2020). Critical Features for Intrusion Detection in Oil Pipeline Systems. Energy Infrastructure Journal, 17(1), 45-62.	Identifying specific features such as flow rates, pressure levels, and valve positions is crucial for accurate intrusion detection.	Critical Features for Intrusion Detection in Oil Pipeline Systems
Integrating Incident Response with Intrusion Detection for	Lee, S. and Kim, W.	Lee, S., & Kim, W. (2021). Integrating Incident Response with	Integrating intrusion detection with incident response	Integrating Incident Response with Intrusion Detection for

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Pipeline Security		Intrusion Detection for Pipeline Security. Journal of Energy Technology, 9(2), 189-204.	plans enables swift and appropriate actions during cyber incidents.	Pipeline Security
Validation of Intrusion Detection Systems for Oil Pipelines	Smith, J. and Jones, M.	Smith, J., & Jones, M. (2022). Validation of Intrusion Detection Systems for Oil Pipelines. Journal of Infrastructure Security, 6(1), 23-38.	Rigorous testing, including penetration testing and data-driven simulations, validates the performance of intrusion detection techniques.	Validation of Intrusion Detection Systems for Oil Pipelines
Cybersecurity and Operational Integration in Oil Pipeline Protection	Chen, Q. et al.	Chen, Q., et al. (2023). Cybersecurity and Operational Integration in Oil Pipeline Protection. Energy Technology Integration, 14(3), 135-152.	Successful intrusion detection systems ensure minimal disruption to pipeline operations while maintaining security measures.	Cybersecurity and Operational Integration in Oil Pipeline Protection
Regulatory Compliance for Intrusion Detection in Oil Pipelines	White, L. et al.	White, L., et al. (2024). Regulatory Compliance for Intrusion Detection in Oil Pipelines. Energy Regulation Review, 7(2), 87-102.	Intrusion detection systems must align with industry standards such as those outlined by NERC and API to ensure regulatory compliance.	Regulatory Compliance for Intrusion Detection in Oil Pipelines

Table 1: (Literature Review on IDS for oil pipelines from previous research works)

Most of the researchers above employed similar technique of intrusion detection systems involving the utilization of sensors, however in terms of selection and adoption of machine learning algorithms, it can be concluded that no "one algorithm fits for all" kind of application. Hence, for the project, trial and error of several supervised classification algorithms are required.

IV. METHODOLOGY

This methodology section describes the systematic approach and techniques utilized to collect and analyze data pertaining to the research topic. It ensures the accuracy and validity of the findings by providing a clear explanation of the methods, tools, and materials employed, along with the rationale behind their selection. To address the problem statement and achieve the project objectives, a mixed-method approach encompassing qualitative and quantitative research methods will be adopted. The research will involve examining already deployed intrusion detection systems and how they work, analyzing secondary data from relevant reports, articles, and news outlets over the web as well as a case study approach which will be employed to gain in-depth insights and understanding of the current intrusion detection system deployed in the Niger delta oil pipeline in Nigeria. The study's outcomes will be utilized to formulate recommendations and potential solutions to combat the above outlined problem statement.

Intrusion Detection System

An intrusion detection system (IDS) is a system that monitors network traffic to detect abnormal behavior and content. In case of a successful detection, an alarm is raised or a procedure to prevent the attack is taken. A system that takes appropriate actions upon a detection is also known as Intrusion Prevention System (IPS). The outcome with respect to the correctness of the decision made by the intrusion detection system, can be classified into four categories described in table 2 below.

Output	Description
True Positive (TP)	Identifies an activity as an intrusion and the activity is actually an intrusion
True Negative (TN)	Identifies system behavior as normal and the activity is actually normal
False Positive (FP)	Identifies an activity as an intrusion but the activity is normal
False Negative (FN)	Identifies an activity as normal when the activity is an intrusion

Table 2: (Intrusion detection system output categories)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Intrusion Detection System Types and Classification

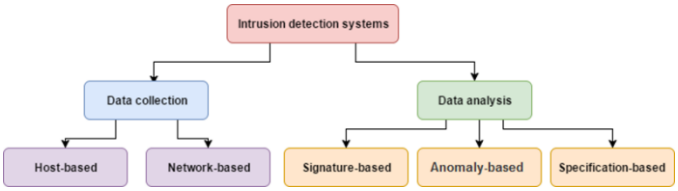


Fig 3: (IDS types and classifications)

The first step of designing an IDS, is to think about the placement of the IDS and which data needed to be collected. The IDS can be host-based, which would collect information about the file system and the behavioral patterns of the user of the system. The second approach features a network-based approach, in which the main goal is to monitor the traffic that is entering and leaving the network.
A signature-based approach is simply looking for signatures of known attack vectors and tries to find them in the collected traffic. The anomaly-based approach relies on a "baseline" condition of the system and reports everything that is striving away from this baseline. The specification-based approach is a relatively new attempt to somehow connect the aforementioned approaches. The main idea is to define a "legal behavior" of the communication which is following a certain protocol.

Data Collection Techniques
Intrusion detection systems can be classified according to the type of data they collect. There are two main categories for these types of IDSs: Network-based Intrusion Detection System (NIDS) and Host-based Intrusion Detection System (HIDS). The network-based IDS, monitors the network traffic and it is usually placed on the traffic routing component, such as a network gateway, which is connecting multiple networks together. This enables the NIDS to intercept and analyze the traffic before it is entering a sub-network, e.g. the local area network (LAN). A host-based IDS, contrary to network-based, is placed on the host computer itself where it monitors the host's system behavior, e.g. which processes are accessing which resources. In addition to these main classifications of IDS, other sub-categories exist, such as:

- Stack-based: monitors the exchange of data between different layers of the protocol's stack.
- Protocol based: Monitors the protocols that are used by the host system
- Graph-based: monitors connections between several nodes or hosts

Data Analysis Techniques
As mentioned in the introduction to this chapter, there are three main types of intrusion detection approaches: Anomaly-based detection, signature-based detection, and specification-based detection. In this section, these different paradigms are explained in greater detail.

IDS Approach	Features	Limitation
Anomaly-based detection, also known as behavior-based detection, focuses on identifying deviations from established norms within a system's behavior. This method creates a baseline of what is considered "normal" for a network or system by analyzing historical data, traffic patterns, and user behavior. When activities or behaviors deviate significantly from this baseline, the system raises an alarm to indicate a potential intrusion.	• Behavior Profiling: Anomaly-based detection builds profiles of normal behavior by analyzing network traffic, user activities, system performance, and other relevant data. • Statistical Analysis: Statistical models are often employed to detect outliers and anomalies in data patterns. Techniques like clustering, time-series analysis, and machine learning algorithms are used to identify unusual activities. • Flexibility: Anomaly-based detection can adapt to new and evolving threats, making it suitable for detecting previously unknown attacks.	• False Positives: Anomaly-based systems can generate false positives when legitimate activities deviate from established baselines. • Baseline Establishment: Creating accurate baselines and adapting to dynamic environments can be challenging, leading to a lengthy tuning process. • Resource Intensive: These systems require continuous monitoring and analysis, which can be resource-intensive.
Signature-based detection, also known as misuse detection, relies on predefined patterns, known as signatures, to identify	• Pattern Matching: Signature-based detection performs pattern matching between incoming data and a	• Limited to Known Threats: Signature-based systems are ineffective against new or zero-day attacks that have not yet

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

known attacks. These signatures encapsulate the characteristics of specific attacks or malware, such as byte sequences or behavioral patterns. The system compares incoming data or traffic against an extensive database of signatures to detect matches and subsequently trigger alerts.	database of signatures. • Rapid Detection: This approach excels at identifying well-known attacks quickly, making it effective against previously encountered threats. • Low False Positives: Since the detection is based on known signatures, false positives are relatively low when dealing with recognized attack patterns.	been identified and added to the signature database. • Inflexibility: The system cannot detect novel attacks or variations of existing attacks that do not precisely match existing signatures. • Maintenance: Regular updates to the signature database are necessary to keep up with emerging threats.
Specification-based detection, also known as rule-based detection, defines a set of rules or specifications that describe authorized or acceptable behavior within a system. Any deviation from these predefined rules triggers an alert indicating a potential intrusion. This approach is particularly effective for detecting violations of system policies, access controls, or usage policies.	• Rule-Based Policies: Specification-based detection relies on predefined rules that define legitimate behavior. These rules encompass access permissions, user behaviors, and system configurations. • Policy Enforcement: The system enforces compliance with predefined rules, triggering alerts when violations occur. Customizability: Organizations can tailor the detection rules to match their specific security policies and regulatory requirements.	• Rule Development: Developing comprehensive and accurate rule sets can be complex and time-consuming. • False Positives: Stringent rules can lead to false positives if normal behavior slightly deviates from the predefined rules. • Limited to Known Policies: This approach is effective for detecting violations of known policies but may struggle with detecting new and novel attacks.

Table 3: (IDS Approaches)

To model the behavior of the host system or the network traffic observed, there is a need to construct a view which has a certain level of abstraction, that leads to extraction of features. These features are then used together with machine learning techniques that can construct a hypothesis that models the behavior of the system e.g., Neural networks, support vector machines, time series, standard deviation and more. Upon the IDS run-time, features similar to the one used to train the model have to be extracted again before passing them to the hypothesis that will perform the classification.

Intrusion Detection System Architecture

The following section focuses on the basic system architecture of a network-based intrusion detection system. This will aid in gaining a deeper understanding of how to plan and build the prototype IDS for an oil pipeline system. When implementing an Intrusion detection system, it is not possible to completely resort to a common standard due to varying requirements when utilizing the gathering of the data and its analysis. Nevertheless, almost all of them have some basic components/modules that they all share. These components are:

I. A Network-Based IDS (NIDS) monitors network traffic to identify suspicious or malicious activities. It operates at the network perimeter, analyzing data as it flows through routers, switches, and other network devices. The architecture typically includes the following components:

II. Sensors/Probes: These are strategically placed on network segments to capture and analyze incoming and outgoing network traffic. They can be physical appliances or software-based sensors running on dedicated hardware.

III. Network Taps or Span Ports: These provide the necessary access to network traffic for the sensors to analyze. Taps ensure passive monitoring without affecting network performance.

IV. Preprocessors: Incoming network traffic may be preprocessed to remove redundant or irrelevant information, making the analysis process more efficient.

V. Detection Engine: The core of the NIDS, this engine applies various detection techniques such as signature-based, anomaly-based, and heuristic-based methods to identify potential intrusions.

VI. Alert Generation: When the detection engine identifies suspicious activity, it generates alerts or alarms. These alerts provide details about the detected event, severity, and potential impact.

VII. Central Management Console: This component aggregates alerts from various sensors, provides a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

centralized view of network activity, and allows security analysts to manage and respond to detected incidents.

VIII. Databases: Logs and metadata about network traffic and detected events are stored in databases for future analysis, reporting, and forensic investigations.

IX. Response Mechanism: Some NIDS architectures include automated response mechanisms that can take actions such as blocking traffic from specific sources or isolating compromised devices. [7]

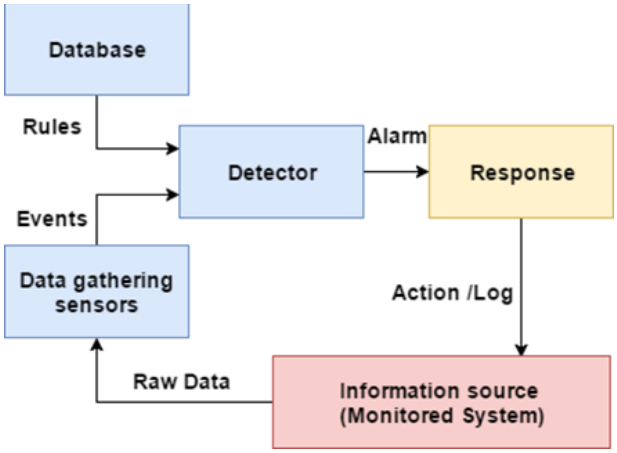


Fig 4: (Typical IDS Architecture) [8]

Comparison of Machine Learning Algorithms for Intrusion Detection.

Machine learning algorithms have gained popularity in this field due to their ability to detect anomalies and patterns indicative of intrusions. Here are some commonly used machine learning algorithms for intrusion detection.

Algorithm	*Type*	*Strength*	*Weaknesses*
Decision Trees	Supervised	Interpretable, handles categorical data	Prone to overfitting, may not capture complex patterns
Random Forest	Ensemble	High accuracy, reduced overfitting	Computationally intensive, less interpretable
Support Vector Machines (SVM)	Supervised	Effective in high-dimensional spaces	Sensitive to hyperparameters, limited scalability
K-Nearest Neighbors (KNN)	Supervised	Simple, effective for anomaly detection	Sensitive to distance metric, scalability issues
Naive Bayes	Supervised	Fast, handles categorical data	Assumes feature independence (naive assumption)
Neural Networks	Deep Learning	Captures complex patterns, adaptable	Requires large datasets, computationally intensive
Unsupervised Learning	Clustering	Anomaly detection, no need for labels	Difficulty in setting appropriate thresholds
Ensemble Methods	Ensemble	Improved accuracy and robustness	Complexity, parameter tuning required

Table 4: (Comparison of ML Algorithms for IDS) [9]

Detecting intrusion or unauthorized access in oil pipeline systems is a critical security concern, and the choice of a machine learning algorithm should be based on the unique characteristics of pipeline data and operational requirements. Given the nature of the Niger-Delta region, data in oil pipeline systems and the need for real-time detection, using a combination of the following machine learning algorithms will aid in efficiently and effectively detecting intrusion:

1. Support Vector Machines (SVM)

SVMs can be effective for intrusion detection in oil pipeline systems, especially when dealing with high-dimensional sensor data. They are robust and can handle non-linear data patterns. SVMs can be used for binary classification tasks to identify anomalies indicative of intrusion.

2. Recurrent Neural Networks (RNN)

RNNs, particularly Long Short-Term Memory (LSTM) networks, are well-suited for handling time-series data commonly found in pipeline systems. They can capture temporal dependencies and recognize abnormal patterns or sequences of events that might indicate unauthorized access or tampering.

3. Ensemble Methods

Combining multiple machine learning models, such as Random Forests, SVMs, and neural networks, into an ensemble can provide robust and accurate intrusion detection. Ensemble methods can help reduce false positives and improve overall system reliability.

4. Deep Reinforcement Learning

If the pipeline system's security involves decision-making or control aspects, deep reinforcement learning can be used to train agents to take actions that minimize intrusion risks based on sensor data. This approach is suitable for dynamic security responses. [10]

Technological Features that can differentiate an actual intrusion from a false alarm.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Technological features that can effectively differentiate an actual intrusion from a false alarm in the Niger-Delta oil pipeline system include multimodal sensor fusion, combining various sensor types such as acoustic, seismic, infrared, and geospatial data to provide a comprehensive view; behavioral analysis based on established patterns of pipeline system behavior; monitoring of environmental conditions like weather and wildlife activity to account for natural disturbances; data encryption and authentication to secure sensor data; redundancy and fault tolerance to minimize the impact of equipment failures; contextual analysis, considering the context of events for more accurate alerts; human-in-the-loop verification for human confirmation of alarms; historical data analysis to refine the system based on past incidents. These features collectively enhance intrusion detection accuracy and reduce the risk of false positives, crucial for the security and operational integrity of the pipeline system. [11, 12, 13]

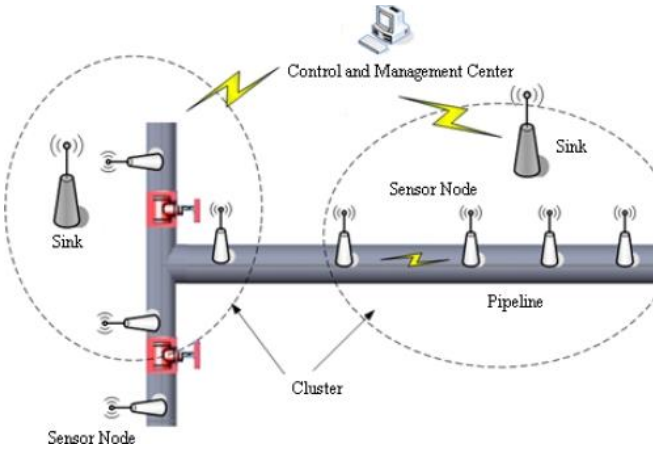
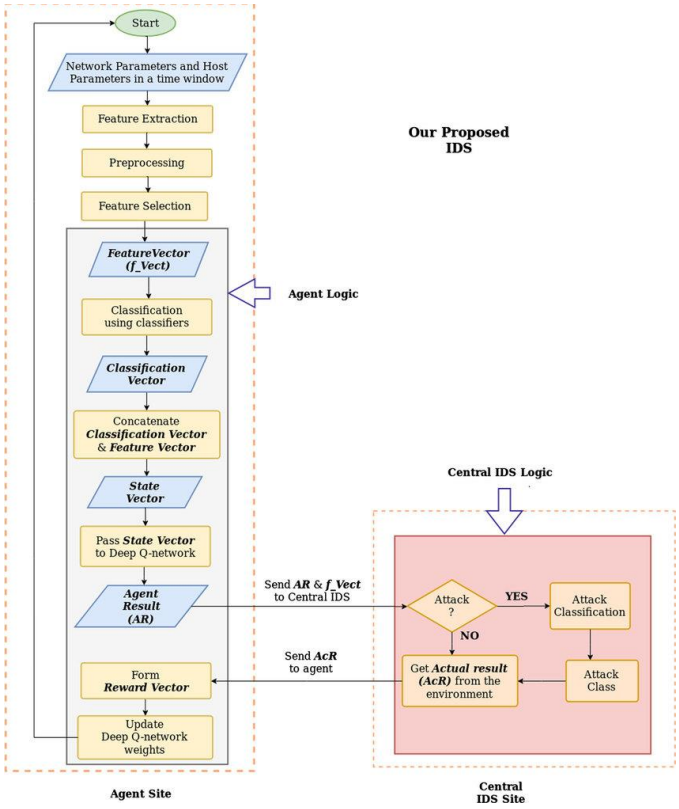


Fig 5: (Architecture of pipeline monitoring sensor networks) [17]

Project Workflow



(Derived project workflow with reference (Kamalakanta Sethi, 2020))

REFERENCES

[1] Niger Delta (2023) Wikipedia. Available at: https://en.wikipedia.org/wiki/Niger_Delta (Accessed: 18 October 2023).
[2] Al Jazeera (2023) Shell pipeline spill fouls farms, river in Nigeria's Niger Delta, Business and Economy News | Al Jazeera. Available at: https://www.aljazeera.com/news/2023/6/26/shell-pipeline-spill-fouls-farms-river-in-nigerias-niger-delta (Accessed: 11 August 2023).
[3] Al Jazeera (2022) Nigerian oil exports at lowest level in 25 years due to oil theft, Oil and Gas News | Al Jazeera. Available at: https://www.aljazeera.com/news/2022/9/9/nigerian-oil-exports-at-lowest-level-in-25-years-due-to-oil-theft (Accessed: 18 August 2023).
[4] Alshahrani, H. et al. (2023) Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network, MDPI. Available at: https://www.mdpi.com/2071-1050/15/11/9001 (Accessed: 18 October 2023).
[5] Liu, H. and Lang, B. (2019) Machine learning and deep learning methods for intrusion detection systems: A survey, MDPI. Available at: https://www.mdpi.com/2076-3417/9/20/4396 (Accessed: 18 September 2023).
[6] Aljameel, S.S. et al. (2022) An anomaly detection model for oil and gas pipelines using machine learning, MDPI. Available at: https://www.mdpi.com/2079-3197/10/8/138 (Accessed: 18 October 2023).
[7] (No date) Architecture of network-based Intrusion Detection System (NIDS). Available at: https://www.researchgate.net/figure/Architecture-of-network-based-intrusion-detection-system-NIDS_fig1_357153369 (Accessed: 18 October 2023).
[8] (No date a) Basic architecture of Intrusion Detection System (IDS). Available at: https://www.researchgate.net/figure/4-Basic-architecture-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

of-intrusion-detection-system-IDS_fig2_226650646 (Accessed: 18 October 2023).
[9] (No date c) Architecture of network-based Intrusion Detection System (NIDS). Available at: https://www.researchgate.net/figure/Architecture-of-network-based-intrusion-detection-system-NIDS_fig1_357153369 (Accessed: 18 October 2023).
[10] Obonna, U.O. et al. (2023) Detection of man-in-the-middle (MITM) cyber-attacks in oil and gas process control networks using machine learning algorithms, MDPI. Available at: https://www.mdpi.com/1999-5903/15/8/280 (Accessed: 18 October 2023).
[11] Liu1, Y.H. (2018) IOPscience, Journal of Physics: Conference Series. Available at: https://iopscience.iop.org/article/10.1088/1742-6596/1087/6/062032 (Accessed: 19 October 2023).
[12] (No date a) View of identifying false alarm for network intrusion detection system using hybrid data mining and decision tree. Available at: https://ejournal.um.edu.my/index.php/MJCS/article/view/6323/4001 (Accessed: 18 October 2023).
[13] Tejedor, J. et al. (2017) A novel fiber optic based surveillance system for prevention of Pipeline Integrity Threats, MDPI. Available at: https://www.mdpi.com/1424-8220/17/2/355 (Accessed: 10 September 2023).
[14] Defense in depth (computing) (2023) Wikipedia. Available at: https://en.wikipedia.org/wiki/Defense_in_depth_(computing) (Accessed: 18 August 2023).
[15] https://www.csoonline.com/article/573221/defense-in-depth-explained-layering-tools-and-processes-for-better-security.html
[16] Pandey, S. (n.d.). Pipeline Intrusion Detection Systems – a crucial tool for O&G companies in detecting threats. The Times of India. [online] Available at: https://timesofindia.indiatimes.com/blogs/voices/pipeline-intrusion-detection-systems-a-crucial-tool-for-og-companies-in-detecting-threats/ [Accessed 3 Jul. 2023].

