International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 11 Nov. 2025, pp: 252-259 www.ijaem.net ISSN: 2395-5252

An Iot Based Oil and Gas Pipeline Monitoring Using Wireless Sensor and Fog Computing

[1]Sirajo Abdullahi Bakura, [2]Zayyanu Yunusa
Federal University Birnin Kebbi
Bayaro University Kano.

Date of Submission: 29-09-2025 Date of Acceptance: 09-10-2025

ABSTRACT: Oil and gas pipelines are critical infrastructure at the heart of oil and gas industry, almost all of the processes of exploration, distribution and storage of gas and refined petroleum products relied heavily on these pipelines, in refineries these pipelines lies between a few to hundred meters long connecting several wells to storage tanks. In the case of the distribution of refined products, the pipelines lie thousands of kilometers long. This critical infrastructure is vulnerable to both damage in the case of vandals and natural disaster in case of leakage, as such it requires proper monitoring to maintain safety standards and to avoid catastrophic events as they carry highly flammable products along. Several techniques have been proposed in the past to provide ways of guaranteeing the safety of the pipelines. Nevertheless, some of the techniques focus on detecting leakages while others focus on surveillance. Therefore we proposed a hybrid system of oil and gas pipeline infrastructure monitoring to provide both surveillance and leak detection using internet of Things (IoT), wireless sensors and fog computing.

KEYWORDS: Fog computing, IoT, Wireless sensor network

I. INTRODUCTION

As with any given industry that has several branches which span across geographical distance, the task of co-ordination and managing vulnerable physical infrastructure is tedious and critical one. Infrastructures such as Transmission stations, and power substation in power sector, network mast and towers in telecommunication sector and pipelines in oil and gas sectors serve as backbone of these industries, the steady operation of these industries relies heavily on the infrastructure. Not only that these infrastructures are important to the industries, they are critical to the operational well-being of the companies, a small fault may account for a major damage and disrupt the smooth running of the industry, causing loss of fortunes. Despite the critical nature of these infrastructures, ensuring their safely is not a trivial task as they lie across different locations, some of which are in remote areas, without any form of life activity in the region or security measures.

In Nigeria for example, due to security challenges physical infrastructures are vulnerable to attack by vandals, militants, and the rest of terrorist groups. These groups attack both government and private infrastructures with little or no benefit. It happened many times in Niger/Delta region terrorist group vandalized oil pipelines to steal petroleum products,[1] whereas, in the northeast part of the country Boko Haram militants damages several power transmission stations and cellular network mast stations[2]. To prevent these illicit acts of infrastructure damage, the stakeholders can leverage the power of modern computing tools to provide a low cost and efficient real-time infrastructure monitoring capable of identifying threats in the regions where these infrastructures are deployed. For safety concerns, these infrastructures are also open to natural problems resulting from general system failure or component failure, these needs to be address with a fault detection mechanism, in order to avoid natural disaster which can lead to unnecessary losses or catastrophic events.

Oil and gas industry is a mega industry that has physical vulnerable infrastructures such as storage tanks, pipelines cutting across physical distances, these pipelines carries different petroleum products from one place to another. The pipelines can be categorized into onsite and offsite:

onsite pipelines are typically found in refineries connecting wells and storage tanks while offsite runs across cities distributing the products from refinery to mega stations easier and faster. Both the onsite and offsite pipelines are critical to the industry, as such the design and maintenance of these infrastructures is a challenging one. Some of the challenges are both applicable to the onsite and offsite pipelines such as pipeline leakage, while others are domain specific such as pipeline vandalism which is applicable only to offsite pipelines [3].

In Nigeria specifically, pipeline vandalism is common ill-behaviors found in the regions where the oil pipelines pass through, it's the process of breaking the pipeline forcefully to tap the oil that the pipeline is conveying to be sold in black market. This ill behavior sometimes referred to as oil bunkering poses a lot of dangers to these industries costing them a lot of damage and economic downturn. The act have shun away several investors as the safety of their infrastructure cannot be guaranteed causing major setbacks in the country's economy[4].

The rebels who carryout these dirty businesses are constantly chased and hunted by security operatives, but due to the distances of these pipelines, armed forces cannot cover all the areas and provide real-time surveillance. An automated system needs to be put in place to detect any suspicious movements along these areas and aid security operatives in eradicating the illegal operation of oil bunkering to alert the proper officials for immediate action.

Consequently, these pipelines are prone to natural damage, which caused pipeline ruptures as result of aging and poor maintenance. To prevent such incidents from occurring, the monitoring need to provide a mechanism to cater for natural damage not only human ignited.

The aforementioned problems attributed to the pipelines have been approach by the stakeholders and researchers with different techniques. For example, from the stakeholders point of view uses automated leak detection system, most of which uses pressure sensors, the main drawback of these systems is they cannot identify the exact place where the leak occurs [13]. Other techniques involve the use of CCTV cameras for surveillance, physical inspection and so on. From a research perspective, several works have been done in the past to provide a long lasting solution to this problem, such as the work of [8], [9], [11] all of which used proposed leak detection using different forms of sensor network to address the problem, but failed to take either location or physical distances they span across, as such with recent advances in edge computing it is possible to propose a new solution that is more feasible and cost effective.

Therefore in this paper we proposed a wireless sensor and fog computing based pipeline monitoring that will provide an effective infrastructure monitoring incorporating both surveillance and leak detection.

The rest of the paper is organized as follows: Section II presents surveys of existing literature on the topic. Section III discusses the methodology and simulation experimental setup. Section IV presents the simulation results and discussions. Section V concludes the paper with conclusion and recommendations.

II. LITERATURE REVIEW

A. Definition of terms

Wireless sensor networks (WSN): is a type of distributed systems which employed sensors that are interconnected together referred to as nodes, these sensors communicate wirelessly to collect data about the surrounding environment. Nodes are generally low powered and distributed in an ad hoc decentralized fashion [10].

Internet of Things popularly known as (IoT) is a branch of distributed systems which allow devices to communicate automatically with minimal or no human intervention. IoT is a system of interrelated computing devices, sensors, and CPUs, which are equipped with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction [3]. IoT is a network of embedded systems, Smartphones, and personal computers that communicate through the internet. Data generated from IoT systems are saved and monitored through a server or a broker depending on the design.

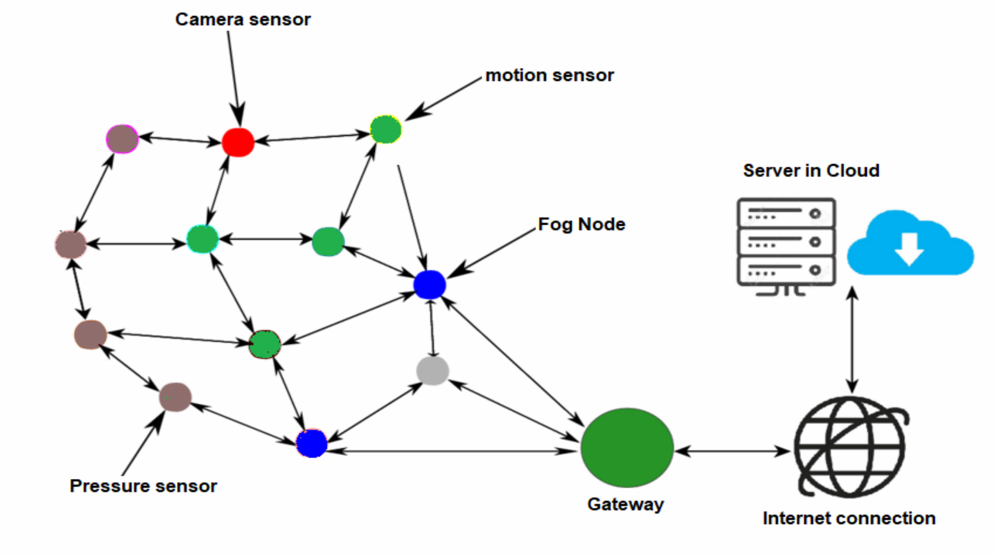

Fig.1 wireless sensor network setup

FOG Computing: Fog computing is a networking paradigm where computing devices known as fog nodes are placed physically closer to the Internet of Things (IoT) devices or WSN. The fog node serves as a middleman between the end device and the cloud. It processes data on behalf of the cloud and/or the WSN nodes. The network administrator can access the processed data directly from the cloud. The Fog and cloud complement each other; they provide interdependent and mutually beneficial services to reduce communication, computing, control, and storage overhead in the system. As such, several tech-giants have embrace fog computing [5].

B. Related works

Several works have been proposed in the past by numerous researchers which automate the process of infrastructure surveillance using WSN, starting with the most common one, Visible (Video) camera is common sensor technology used for surveillance system. It has been used to monitor infrastructures such as buildings, people, events and activities. It is the most commercially available surveillance sensors starting from low cost IP camera to high performance professional CCTV. Security cameras have been placed in everywhere, from private homes, streets, public buildings, as well as in border between countries [6].

Apart from camera sensor, several others sensors have been employed to provide an alternative to camera sensor surveillance in situation where the camera is not deem right. Examples of this sensors include ultrasonic for audio surveillance, passive infrared (PIR), pressure sensor, and so forth. Sometimes combination of more than one sensor improved the performance of the surveillance system, other sensors such as sound, magnetic field, motion can be added to increase more confidence in the decision making which give rise to a hybrid systems [6].

In hybrid systems, some sensors maybe used as primary sensors which will trigger the secondary sensors. Such kinds of setup are used in situation where it has several factors to consider before decision can be made, others simply uses hybrid setup in an effort to achieved power efficiency. He et al[6] employed a magnetic field sensors as primary sensor which sense magnetic field of a moving vehicle and activate camera sensor to verify whether the vehicle is a threat or not. The camera sensors are put into sleep mode prior to activation which reserves the battery usage. The sensors used in primary level are usually sensors that dissipate low energy as compared to those employed in secondary layer as such cutting down the energy consumption as describe in the work of [7].

Bai et al [8] proposed an intelligent home surveillance system based on wireless sensor network, in their work they employed several sensors in an hybrid design, specifically ultrasound sensors was used to capture background sounds such as dog bark, gun shots, broken glass and so on, the ultrasound sensors trigger the camera sensor when a suspicious sound has been sensed. Prior to triggering the camera was asleep saving the power dissipation, while the low power consuming ultrasound was active. The interdependencies between the sensors complement each other and provides a truly energy efficient surveillance system.

L. Gary [14] proposed a real-time monitoring systemparty contact with pipelines (typically caused by contact with a digging or drilling device) can res ult in mechanical damage to the pipe, in addition to coating damage that can initiate corrosion. Because t his type of damage often goes unreported and can le ad to eventual catastrophic failure.

Others such as [9], [10], [11] and [12] focus only on using WSN in detecting pipeline leakage without considering the surveillance part. H. B. Salameh [7] proposed the use of IoT technology in gas pipeline leak detection. The system used pressure sensors to detect the pressure level in the pipelines, whenever a drop of pressure occurs the system signals the controller, the controller then compiles the pressure reading and forward to admin as text SMS for action. The system was able to detect pressure drop and which serve as cause of leak and inform the administrators about the problem, but looking at the nature of distribution pipelines which span across towns and cities to places where there is no cellular network coverage the proposed system will failed to work under this conditions, it is only applicable to onsite leak detection which is available in refinery and the coverage area is equipped with cellular network.

Shen X et al [9] uses wireless sensors in oil pipeline monitoring; the system was design in an energy harvest situation, where the power to be used by the sensors are source from the environment. The system uses vibration sensor to detect the vibration state of the oil pipeline, and transmits the information to the sink node through the low power wireless sensor node which is supplied by wireless energy harvesting and rechargeable battery. Pipeline anomaly can easily be detected by varying vibration data sent by the sensors; the system addresses the safety of the pipelines in energy efficient manner without consideration of hostilities and deliberate attacks. While [9] focus on using energy efficient design. Sindhu, S. and Khan, A.[10] proposed a gas pipeline leakage detection, their work focuses on finding the exact location where the leakage occurs, therefore the sensors used not only sent the data to admin, but along with the location of a given failure. The system used wireless sensors, Microcontrollers and Zigbee protocol. The work provides the means to identify exact location of gas leakage which ensures easy maintenance and enhances safety.

Mohammed, S., and F. Aliyu [12] proposed a transmission pipeline leak detection system using WSN and Fog computing, they overcome the problem associated with [7] by integrating fog computing thus, providing a response to a server even when there was no cellular network in place where the sensors detect the leak. Nevertheless, their solution didn’t account for surveillance or any means to deal with deliberate vandalism of these pipelines, leaving the infrastructure vulnerable to hostile attack.

To the best of our ability, no work in the consulted literature employed both surveillance and detection in ensuring safety of oil and gas pipelines which justify the importance and relevance of our work.

III. METHODOLOGY

The methodology employed in this paper has been described in figure I, which summarizes and highlights the entire architecture of the proposed system. The system uses WSN in an IoT setup where sensors communicate with fog nodes without human intervention and transmit data to cloud layer where users can act based upon the information provided.

The system deploys pressure sensors, gas sensors, along the length of the pipelines in a linear arrangement, this phase caters for the leakage detection, another type of sensors which include thermal and motion sensors will also be integrated to provide surveillance capability, the system will be used in power saving mode, where the motion sensor will be active at all times, given a suspicious motion, the sensors will trigger camera/thermal sensor in order to obtained visual evidence about the motion, the captured information can then be sent to a fog node where a processing will occur, the fog node then transmit these data to server in cloud. The server is equipped with machine learning algorithm that can classify the data received from fog nodes into a threat or none threat activity. For a threat behavior a warning will be sent by the server to admin terminal for emergency action. And for none threat the server will discard the data, thus overcoming the false alarm problem encountered by most surveillance systems.

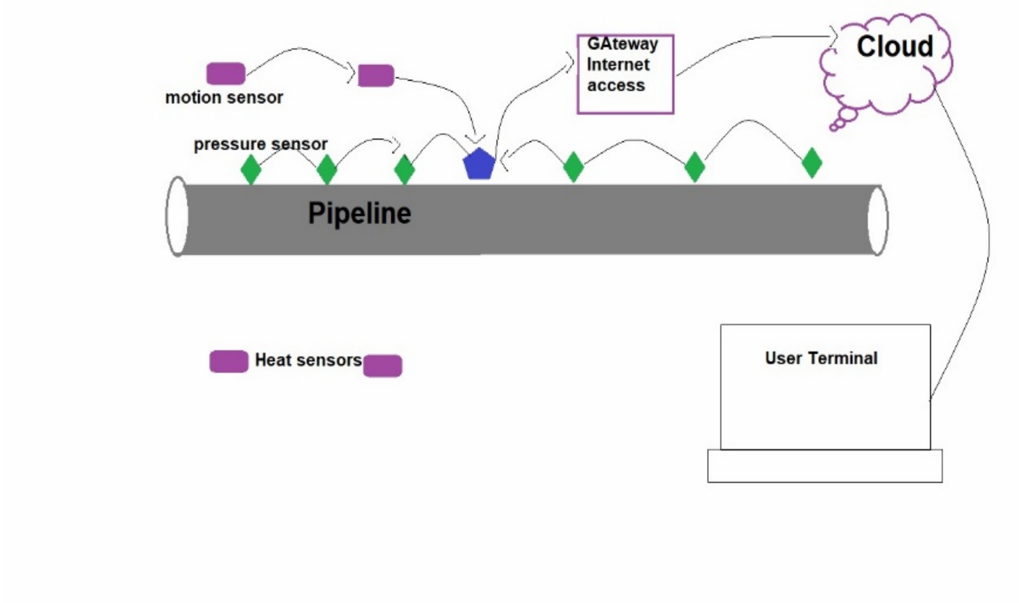

Fig. 2 Proposed System

IV.

V. PROPOSED SYSTEM

The system utilizes Zigbee protocol for communication between sensors-to-sensor and sensor-to-fog node, while communication between fog to cloud make use of internet where both TCP/IP and UDP will be tested to obtained the best result.

The system work in series of steps, from the beginning, the motion sensors are always enabled, and has communication functionality to its neighboring sensors, the neighbors will keep propagating the message from one sensor to another until when it reaches nearest thermal sensor, the thermal sensor will be activated upon receiving the message and scan the environment for heat signature, thermal sensor will forward the signature to the nearest sensor until it reaches fog node, the fog node will then classify the signature as either threat or none threat, where human being signature serve as threat and animal signatures serve as none threat, when a threat signature is confirmed then fog node will send the information to cloud where central admin application is running, the admin can then notify department in charge of mitigating the problem, whether security department in case of threat or maintenance department in case of leak. The proposed methodology can be described in the Algorithm I below:

Algorithm I:

```
1.    Start
2.    Motion sensor, Pressure sensor← Sense data
3.     pressure sensor→ send sense data to nearest sensor
4.     Do until (nearest sensor = fog node)
5.     Motion sensor→ sends the data to nearest sensor
6.    While nearest sensor !=  thermal sensor
7.    Repeat 3
8.     Thermal sensor← sense data
9.     Thermal sensor: scan for heat signature
10.    Motion sensor→ send the heat signature to nearest sensor
11.    Do until (nearest sensor = fog node)
12.   Fog node←heat signature, Sense data
      If (heat signature==human or sense data!= normal)
        Fog node: send heat signature/sense data to Cloud
      Else
        Ignore
```

VI. SIMULATION SETUP

Algorithm described detailed walkthrough of the proposed system, starting from the inputs to the sensors, how the sensors will communicate to neighboring sensors until a fog node is reached, the fog node is equipped with a machine learning algorithm that is capable of classifying the data it received from sensor as either threat or non-threat, for a threat situation the fog node will send an alert to the server in cloud which will be received by system administrator for further action. For non-threat situation the system simply ignore the data as false alarm without sending it to the server.

To further verify the system, the system will be simulated using Cooja simulator, where simulation parameters such as communication module, transmission rate, sensor range, supply voltage and so on, will be supplied and determine the overall behavior of the system when deployed on actual pipeline monitoring.

VII.RESULTS

Raspberry pi with TCP/IP and UDP were used as fog node in the experiment, and finally the setup with less latency and low power consumption has been considered for implementation.

Table I lists the simulation parameters utilized in the proposed system's simulation. The simulation was run using MATLAB and R sofware [15] provided the energy parameters for Zigbee/IEEE 802.15.4, while [16], [17] provided the values for the satellite transceiver module (RockBlock 9603). Each of the 100 sensor nodes sends data to a fog node, which then sends it to the cloud via satellite. The planned system will be installed along a 2,800 kilometer pipeline. Because each sensor node has a range of 100 meters, there must be 28000 sensor nodes.

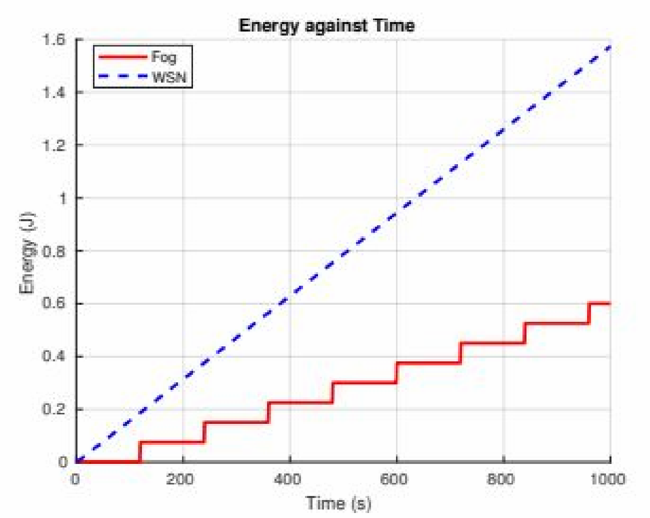

Fig.3 Energy consumption of Fog node and Sensors nodes

TABLE I. SHOWING ENERGY CONSUMPTION

Raspberry pi	Protocols	Metrics	
		Time(s)	Energy(J)
	Fog	1000	1.6
	WSN	1000	0.6

From Table I we can derived that the proposed WSN system uses less energy than that of ordinary fog nodes.

TABLE II. SHOWING LATENCY PROPOSED SYSTEM

S/N	Node	Average Latency in (s)
1	Proposed system with 100 nodes per segment	0.0253
2	Fog at the end of segment	120
3	WSN with 2800 nodes (LSN)	7.21

Finally, the proposed system's latency was evaluated in comparison to LSN's latency. The table II summarizes the findings: Data from any node transferred to the fog node has an average delay of 0.02 seconds, whereas LSN has a latency of 7.2 seconds. However, because fog nodes send data to the cloud on a regular basis, the proposed system's latency is equal to the difference between the latency of the fog node and the latency of the WSN.

TABLE III. Table III SIMULATION PARAMETERS

S/N	Module type	Parameters	Values
1	XBEE Series 1 (Zigbee)	supply voltage	3.3v
2		sleeping mode	12uA
3		awake mode	50mA

4		transmit current	52mA
5		receiving curent	54mA
6		sennsor node range	100m
7		packet size	128 byte
8		Payload	102 byte
9		data rate	250 kbps
10	RockBlock 9603	supply voltage	5v
11		Sleep	200uA
12		Idle	40mA
13		transmitting curent	1.5A
14		transmitting time	10ms
15		packet size	340 bytes
16		Max periodic transmssion	120 s
17		sampling rate	0.016HZ

VIII.

IX. CONCLUSION AND FUTURE DIRECTION

This paper presents an intelligent, WSN-IoT oil pipeline monitoring system using wireless sensor network and fog computing, the paper encompasses both the two aspect of pipeline monitoring, that is surveillance and leak detection. It provides a solution to problems associated with pipeline monitoring especially in areas where oil pipelines are prone to vandalism and bunkering. The paper addressed the issues found in the literature such as high latency and power consumption by employing fog computing to reduce the communication delays between sensors and cloud for a sense data and provides onsite computing capability to eradicate false alarm. The system used a low powered raspberry pi as fog node, the latency of the system using different fog node and protocol was measured to obtained best setup that has lowest latency and energy consumption. However, all the devices and sensors used in this paper are battery powered, which needs to be recharge at regular interval, the main source of power to the system are small solar panels as the areas which the pipeline span across are not connected to national grid, therefore, the main source of power is still vulnerable to thieves and vandals whom they can destroyed the source of power or steal the panels, it is therefore recommended that in future research the source of power be change into something more ubiquitous that cannot be easily identified, or something that is of no any value to the vandals, such as energy harvesting technologies.

REFERENCES

[1]. A. Tukur, M, Shahwahid and M. Wang, “Causes and Consequences of crude oil pipeline vandalism in the Niger Delta region of Nigeria: A confirmatory factor analysis approach,” Cogent Economics & Finance, 2017. doi/full/10.1080/23322039.2017.1353199

[2]. AfricaNews, “Boko Haram cuts off Maiduguri from Nigeria’s national power grid,” Africanews, Jan. 20, 2020. https://www.africanews.com/2020/01/21/boko- haram-cuts-off-maiduguri-from-nigeria-s-national-power-grid// (accessed Mar. 23, 2022).

[3]. T. Bello, “Oil and Gas Problems in Nigeria; The Impending Problems and the Preferable Solutions,” SSRN Electronic Journal, 2017, doi: 10.2139/ssrn.3072236.

[4]. A. Musa, M. Hamada, F. Aliyu, and M. Hassan, “An Intelligent Plant Disease Detection System for Smart Hydroponic Using Convolutional Neural Network,” Presented at the IEEE 14th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), Singapore, 2021, Accessed: Sep. 16, 2021.

[5]. SherryAir, “Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are,” 2015. Accessed: Sep. 16, 2021. [Online]. Available: https://www.cisco.com/c/dam/en_us/solutions/trends/

[6]. S. Warsono Ibrahim, “A comprehensive review on Intelligent surveillance systems,” Communications in Science and Technology, vol. 1, no. 1, 2016, doi: 10.21924/cst.1.1.2016.7.

[7]. T. He et al., “VigilNet:An Integrated Sensor Network System for Energy-Efficient Surveillance,” ACM Transactions on Sensor Networks, vol. 2, no. 1, pp. 1–38, Feb. 2006, doi: 10.1145/1138127.1138128.

[8]. Y.-W. Bai, L.-S. Shen, and Z.-H. Li, “Design and Implementation of an embedded home surveillance System by use of multiple ultrasonic sensors,” IEEE Transactions on Consumer Electronics, vol. 56, no. 1, pp. 119–124, Feb. 2010, doi: 10.1109/tce.2010.5439134.

[9]. Y. Shen, X. Liu, C. Liu, H. Guo, X. Yang, and W. Du, “A Low Power Consumption Wireless Sensor System with Wireless Power Harvesting for Oil Pipeline Monitoring,” 2018 International Conference on Microwave and Millimeter Wave Technology(ICMMT), May 2018, doi: 10.1109/icmmt.2018.8563967.

[10]. K. Sindhu S and A. Khan, “Development on Gas Leak Detection and Location System Based on Wireless

[11]. Sensor Networks: A Review,” International Journal \ of Engineering Trends and Technology (IJETT), vol. 12, no. 6, 2014, Accessed: Sep. 16, 2021.

[12]. S. Mohammed and F. M. Aliyu, “Fog Computing for Leak Detection in On-shore Transmission Pipelines,” Feb. 2020, doi: 10.1109/aect47998.2020.9194193.

[13]. Agbakwuru, Jasper. (2011). Pipeline Potential Leak Detection Technologies: Assessment and Perspective in the Nigeria Niger Delta Region. Journal of Environmental Protection. 02. 10.4236/jep.2011.28121.

[14]. Burkhardt, Gary & Crouch, Alfred. (2022). REALTIME MONITORING OF PIPELINES FOR THIRD-PARTY CONTACT. 10.2172/839568.

[15]. O. O. Kazeem, O. O. Akintade, and L. O. Kehinde, “Comparative study of communication interfaces for sensors and actuators in the cloud of internet of things,” Int. J. Internet Things, vol. 6, no. 1, pp. 9–13, 2017.

[16]. Iridium Communications, “Iridium 9603/9603n sbd transceiver: Developers guide (revision 3.1),” accessed 19th July, 2019. [Online]. Available: https://fccid.io/Q639603N/User-Manual/ Developers- guide-2370311.pdf

[17]. ROCK SEVEN LOCATION COMMUNICATION, “Rockblock 9603: Developer guide,” 2017.