SRG International Journal of Recent Engineering Science
ISSN: 2349–7157 / https://doi.org/10.14445/23497157/IJRES-V8I5P104

Volume 8 Issue 5, 21-26, Sep-Oct, 2021

Research Article

Generation of Surveillance Networked Nodes for Oil Pipelines' Theft

Rahmon Ariyo Badru[1], Azeez Ajani Waheed[2], Oluseye Ayobami Akinmoluwa[3], Olaniyi Ralph Obayemi[4]

[1]*Department of Information and Communication Technology, Cooperative Information Network (COPINE), National Space Research and Development Agency(NASRDA), Obafemi Awolowo University, Ile-Ife, Osun State.*
[2]*Department of Mathematics & LeadCity University Ibadan, Oyo State, Nigeria.*
[3,4]*Department of Computer Science & LeadCity University Ibadan, Oyo State, Nigeria.*

Received: 26 August 2021 Revised: 29 September 2021 Accepted: 11 October 2021 Published: 22 October 2021

Abstract *- Despite the use of military task forces and some old detection systems along oil pipelines, sabotage is on the rise, especially in developing countries. This has led to various socio-economic losses and damage to the ecosystem via oil spills. To solve this problem, the research study generated low-cost surveillance networked nodes for oil pipelines theft via real-time monitoring and reporting. The prototype was simulated along the Lagos-Ilorin pipeline (259km) divided into nodes (26m apart interfaced to a central webserver) based on field view computation of the prototype device (resolution 4618 × 3465 pixels). The model software was developed using a web application, tunneling server, and mobile app. The mobile app at each node sends detected faces using feature detection and tracking via Constrained Local Models Algorithm (CLMA), each image having a unique I.D and location, which will be forwarded to a surveillance email. These images were transmitted immediately (1-2 seconds) and uploaded on the webserver. An email of this report was generated and forwarded to the admin indicating human activity on the pipeline infrastructure. The prototype was evaluated using the manual software non-functional Black Box Testing having a response time of 90%, 80% stability, and 90% reliability.*

Keywords *- Node, Oil, Pipeline, Prototype, Server, Surveillance.*

1. Introduction

Nigeria's economy was heavily reliant on agricultural products such as groundnut, rubber, cocoa, cotton, coffee, and so on for revenue and foreign exchange before crude oil was discovered [l]. Oil was discovered in Nigeria in 1956 at Oloibiri in the Niger Delta, which was discovered by Shell-BP [l]. Nigeria became an oil producer in 1958 when the first oil field began producing 5,100 barrels a day. Other international firms were granted mining rights onshore and offshore located close to the Niger Delta after 1960 [l]. These products, therefore, need to be transported from one point to another, which later gave birth to the first pipeline construction in 1955[2].

Pipeline transportation is widely regarded as a reliable, cost-effective, and fast method of transporting oil and gas in Nigeria. In the early exploitation and crude oil transportation, pipeline incidents are very rare in the country. As a result, pipeline security was not a regular occurrence. Oil spills from pipelines were also monitored for natural causes, including corrosion and accidents. Recently, pipeline security and surveillance have become a major concern for oil and gas-producing countries as sabotage and vandalism have spread around the world. Over 95 percent of pipeline leaks in the last decade were caused by artificial (human) disruption, according to statistics[2]. Pipeline networks transport extremely volatile goods such as crude oil, natural gas, and industrial chemicals; on the line may result in the destruction of lives, property and damage to the environment via oil spills. In recent years, militants and terrorists have carried out a number of pipeline attacks in different countries.[3]

2. Oil Pipeline Attacks in Nigeria

Oil pipelines have recently been subjected to three major issues: vandalism, sabotage, and terrorism. These issues have negative consequences for the government, pipeline owners, and host communities in terms of the ecosystem, economy, health and safety, and security. Between 2010 and 2012, Nigeria had around 2,787 pipeline damages, but between 2002 and 2012, the total was reported to be about 15,685 [4]. According to the Nigerian National Petroleum Corporation, 45,347 pipeline explosions have occurred in the last 18 years, with vandalism accounting for around 80% of the causes [5].

These pipeline incidents have resulted in significant economic loss, socio-cultural harm, and environmental contamination. They also resulted in many deaths and health issues, mainly in the local residents, as a result of poisoning of water sources, environmental destruction, and explosions, among other things, with over 2,500 lives lost over a 15-year

stretch [6]. In view of the above, several studies have attempted to find a workable approach to these big issues.

According to the Nigerian National Petroleum Corporation's (NNPC) Monthly Financial and Operations Reports for January 2019, a total of 231 pipeline points were vandalized throughout the region. The Mosimi-Ibadan and Ibadan-Ilorin row, respectively, accounted for 67 and 62 vandalized points. Aba-Enugu row accounted for 30 vandalized points or 13% of total vandalized lines, while line breaks in other places accounted for the remaining 31% of total line breaks across the country[7]. Many studies have been conducted, and many more are currently being conducted in order to identify a long-term solution to the growing pipeline theft problem. Some scholars, on the other hand, called for measures to reduce pipeline attacks and to force pipeline owners to spend more on pipeline security and environmental safety [8].

Oil pipeline facilities monitoring is very important for our dear country and its citizen. This is because crude oil is the major source of the Nigerian economy. If the oil infrastructures are not properly monitored, this could lead to theft, sabotage, and other criminal vices by scrupulous individuals, leading to social-economic loss, biodiversity loss, damage to the ecosystem, loss of revenue, and destruction of lives and property. Hence, poverty, diseases, hunger, and environmental disasters will dominate society. The increase in the rate at which pipeline infrastructures are being damaged has cost Nigeria losses running to Billions of dollars annually, not only for the theft but also for repairs and cleanup. Therefore, the government needs to see as a matter of urgency the need to secure our pipelines in order to forestall future occurrences, thereby improving our economy, saving the environment, protecting lives and property, and reducing biodiversity loss.

In view of this, the use of surveillance network nodes for pipeline theft is of utmost importance in order to curb the continual damage of pipelines in the county, which must be seen as a matter of urgency because damages to the pipeline facility are causing the country loss of revenue, loss of lives and property and great damage to the ecosystem leading to biodiversity loss. The environment is no more friendly and conducive for both the aquatic and land species, especially in the Niger Delta, where this activity of pipeline vandalism is rampant. Swift action is needed, and all hands should be on the desk to reduce vandalism activities.

3. Statement of Research Problem

Despite the use of military task forces and some old detection systems along oil pipelines, incessant damage to pipeline facilities by unscrupulous individuals leading to various socio-economic losses, sabotage, and damage to the ecosystem via oil spills, has continued to increase tremendously. To cub this problem, real-time monitoring and reporting of this act would be technologically explored using a low-cost device.

4. Literature Review

Various researchers have carried out different works and improvements on pipeline security and surveillance. Discussed in the table below are a few among recent publications on this subject based on their adopted methodology and gaps

Authors	Method	Results	Gap
[9]	ATmega328, GSM, and GPS based on the Internet of Things	Sensor nodes, geographic locations, and distances were transmitted via SMS to alert security operatives.	No visual evidence, expensive to implement, and installation and design need expertise. A prototype
[4]	Sensing units (SUs), geophones, Arduino Mega Board, a GSM/GPRS/GPS shield, a Lora Communication Shield, and a Lithium Battery	Seismic signals are processed by the Arduino Mega board. After detecting a threatening activity, the SU sends an alert.	No images of vandals, integration of a line of sight drone, expensive, complex to implement, generation of false alerts
[10]	They used a wired network, wireless network, sensor technology, database, and smart terminals, which were integrated to collect, process, analyze, and transmit data and information in real-time for monitoring crude oil pipelines.	Data and information, e.g., abnormal noise, vibration, pressure changes, and flow changes, were detected by the sensors, cameras, and RFID will be transmitted to the cloud storage center by the communication network.	Possibility of false alerts from nearby noises or vibration, No visual proof of vandalism, images of vandalism
[11]	A review of the use of unmanned aerial vehicles (UAVs) and	It was used under three scenarios and worked as expected;	Expensive and conspicuous, and hence it could be

	different monitoring scenarios are also proposed and illustrated.	Proximity Survey/visual identification of pipe damage, Short Distance Survey/visual identification of leak, and Long Distance Survey/automatic sensing of soil properties.	compromised.
[12]	A Light Tracking Automated Guided Vehicle was used For Oil Pipeline Leakage Detection.	Mobile Robots are coordinated by centralized or computer-based control. The AGC has the ability to sense light and track it, then sends the GPS location of the light, which represents a leakage in the pipeline as a Google map link to a registered phone number (GSM).	A camera or video module can be attached for real-time streaming and for taking pictures which is the major limitation.

In comparison with the proposed prototype with reference to [4], [9], [10], [11], [12], most of the existing works do not have visual pieces of evidence of theft activities on the pipeline, and there could be the possibility of false alerts, the existing systems are complex to design and expensive. The developed prototype is easy to design, cheap, and gives real-time data transmission of activities on the pipeline via an email notification

5. Methodology

This section discussed the research methodology utilized in developing the networked surveillance nodes for theft and other interference along the oil pipelines. The surveillance detection node was prototyped using a mobile phone (with camera detection capability of 26m at coverage of 180^{o} and 4618×3465 pixels resolution), Laptop, and pipelines interference model software developed and installed in the Laptop and mobile phone. Lagos-Ilorin pipeline transport system (259km) was simulated for the real-time scenario. The total network nodes computed on the transport system are 9,962 nodes at 26m range and networked using JavaScript codes. The model software was developed using a web application, a tunneling server, and a mobile app. The tunneling server generated an active https link between the server and the mobile application. Hence, the mobile app accessed the server's content and sent detected images with unique identities and locations, using feature detection and tracking via Constrained Local Models Algorithm (CLMA). These images [274 kB to 280 kB(RGB) in size] were transmitted within 1-2 seconds and uploaded on the webserver. Subsequently, an email of this report was generated, saved on the web app as a backup, processed to obtain facial features (using Matrix Laboratory software), and forwarded to the pipeline network administrator for indication of interference. Following this, Hence, interference results from any or combination of the nodes would show; a unique identity, the field of view, the interference's time, the image captured and size, and its spatial location.

6. Flowchart of the Design

The proposed prototype design consists of the webserver, tunneling server, a mobile phone where the mobile app was installed, and active internet connectivity. The web server is a WAMP (Windows, Apache, MySQL, and PHP) server, and the tunneling server is "ngrok.io," while the mobile was designed using flutter.

The tunneling server initializes and wraps the web app in the mobile app. The camera initializes, thus monitoring and checking the interference status of the pipeline. Once interference is detected, the camera captures the image and prepares it as an input for CLM (Constrained Local Model) algorithm, which monitors the inputs [13]. Immediately a face is detected, CLM captures the face and prepares an image file which is analyzed and generates the date, time-domain name & gps location of interference. The images are saved on the web server, which is now transmitted to a pipeline network administrator email for necessary actions.

7. Methodology

7.1. Design of an Electronic Intrusion and Theft Detection Prototyped System

The prototype system was developed using electronic architecture installed with developed web, tunnel, and mobile application software. The hardware Specification for the prototype system consists of a processor Intel®Pentium®CPU, Random Access Memory RAM of 4GB capacity, and Read-Only Memory ROM of 250G. The Android phone used for the mobile app is a Kernel Version 4.9.190+, Android Version 10 with 3 GB RAM. Also, the software specification consists of an operating system OS with Windows 10 of 64bit. The Web App was a WAMP Server built on Laravel. The tunnel server is Ngrok.io, and the mobile app is developed using Flutter.

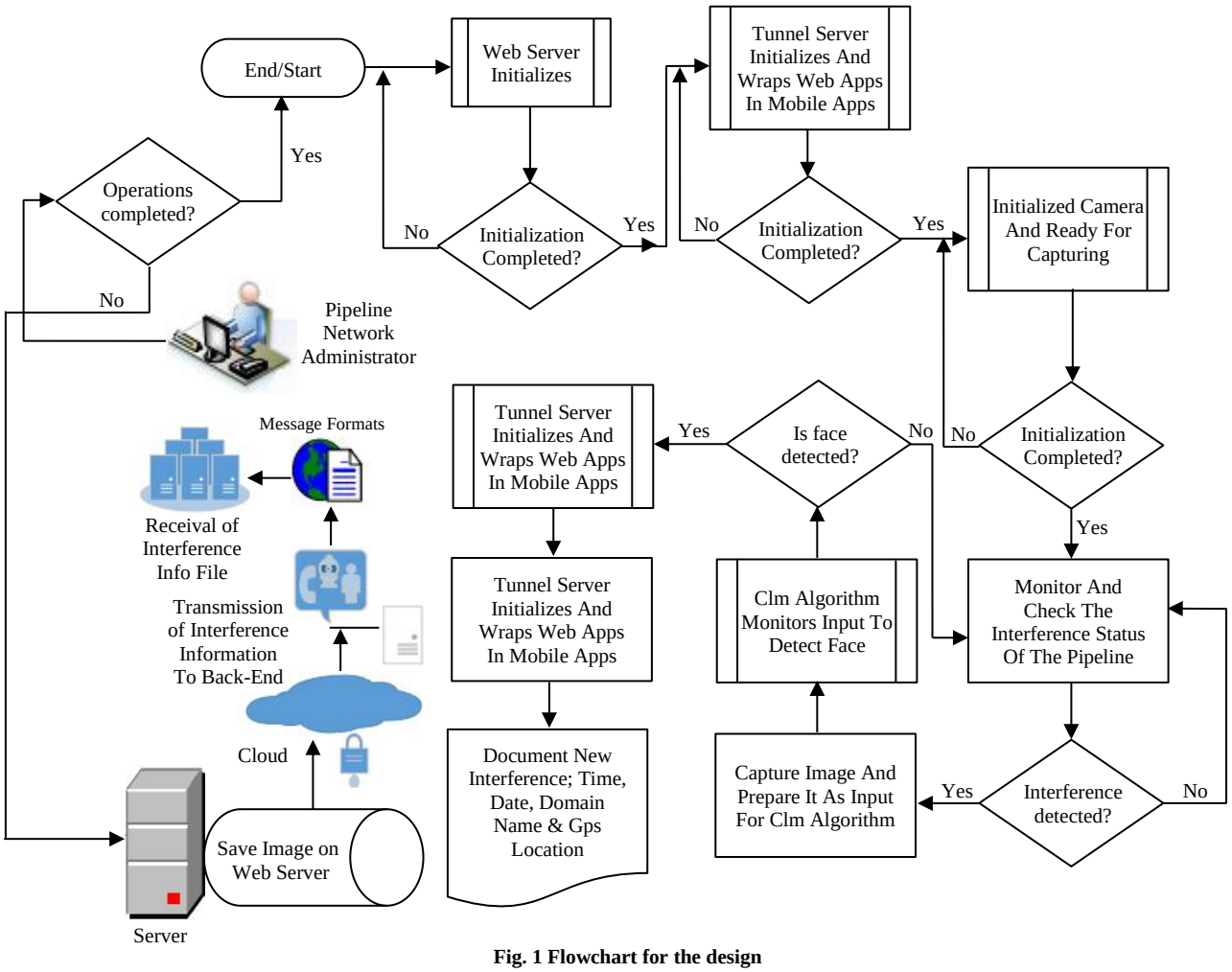

Fig. 1 Flowchart for the design

7.2. Simulation of Real-Time Oil Pipeline for Generating Surveillance Network Nodes

The generation of network nodes was simulated using the Lagos-Ilorin Pipeline axis, which is 259,000m (259km), 4", 6" and 16" pipeline transport system [14]. Also, the prototype camera used has a 16Mp camera having a resolution of 4618 × 3465 pixels. However, to know the distance the mobile phone camera will access, a field view formula was adopted to calculate the distance where the face of the intruder can be identified. The computation of the field view was obtained using equation 1[15].

$$\text{Field View} = \frac{\text{Horizontal Resolution}}{\text{Pixel per feet}} \quad (1)$$

The entire pipeline distance was divided into nodes based on the distance the phone camera could cover (field view).

$$\text{Number of Nodes} = \frac{\text{Total Pipeline Length}}{\text{Field View}} \quad (2)$$

At each node, the prototype device should be installed for the detection of intrusion. Hence, the total networking nodes for the design are shown below:

$$Total\ Number\ of\ Networking\ Nodes\ N_{NT} = \sum_{n=1}^{m} N_n$$
$$= N_1 + N_2 + N_3 + \cdots + N_m$$

Additionally, each node was numbered and given a unique ID on the database for transmission identification.

8. Result

8.1. Result of Electronic Intrusion and Theft Detection Prototype System

A command "ngrok http 8000 was written on the tunneling server to replace the http 80. This will then generate a secured tunnel. When ngrok runs an HTTP tunnel, it opens endpoints for both HTTP and HTTPS traffic. The connection tunnel established by ngrok is secure and can only transmit data to the local host when the port is open.

The https URL will be copied so as to access the application from the mobile app. Immediately after the next page tab is clicked, as shown in Figure 3, the mobile app begins to capture. It then pops up a face detection module, as shown in Figure 8, and sends images captured to the video tag. On the video tag player, the CLM (Constrained Local Models) starts and begins to process and analyze the image using feature detection and tracking.

After analyzing, the CLM sends the detected image to a file(blob) which gives the details on the date, time, and year of the image that will be sent directly to the surveillance mail via a web server.

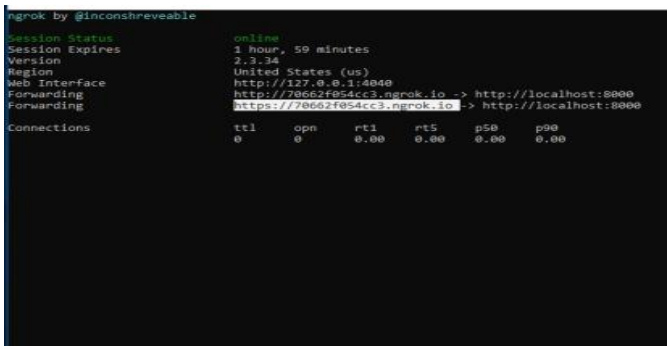

Fig. 2 Newly Generated Https from the Tunnelling Server, Which Will be Inputted on the Mobile App

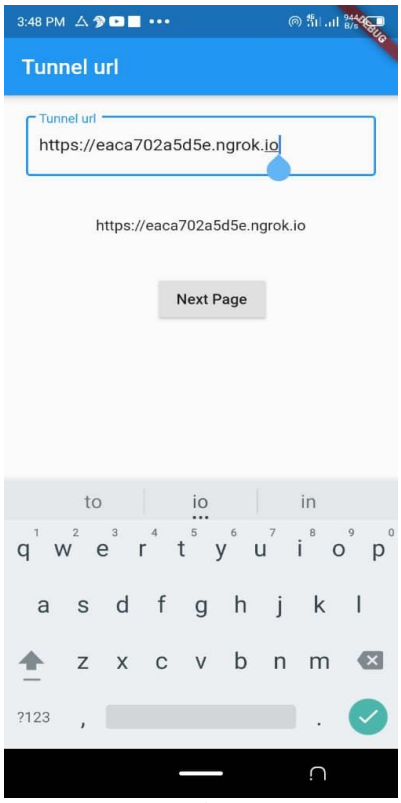

Fig. 3 Tunnel Url Input Section of the Mobile APP Where Secured Tunnel URL Will be Copied

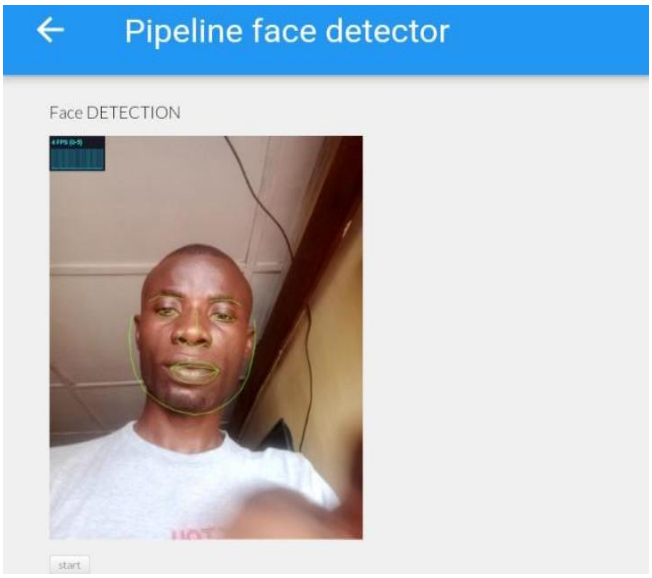

Fig. 4 Face detection module showing the CLM algorithm for Face tracking

8.2. Result on Simulated Surveillance Network Nodes in a Real-Time

From Equation 1,

$$\text{Field View} = \frac{\text{Horizontal Resolution}}{\text{Pixel per feet}}$$

Horizontal resolution of the mobile device used = 4765 Pixel
Pixel per ft = 80

$$\text{Field View} = \frac{4765}{80}$$

Field View= 59.6ft =26m

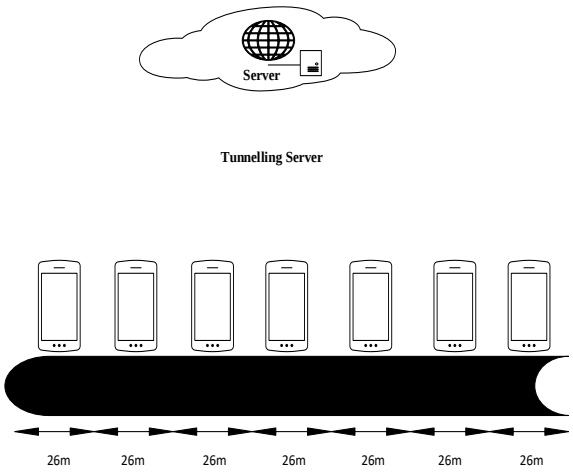

Fig. 5 Simulation of generating network nodes at 26m apart for oil pipeline theft

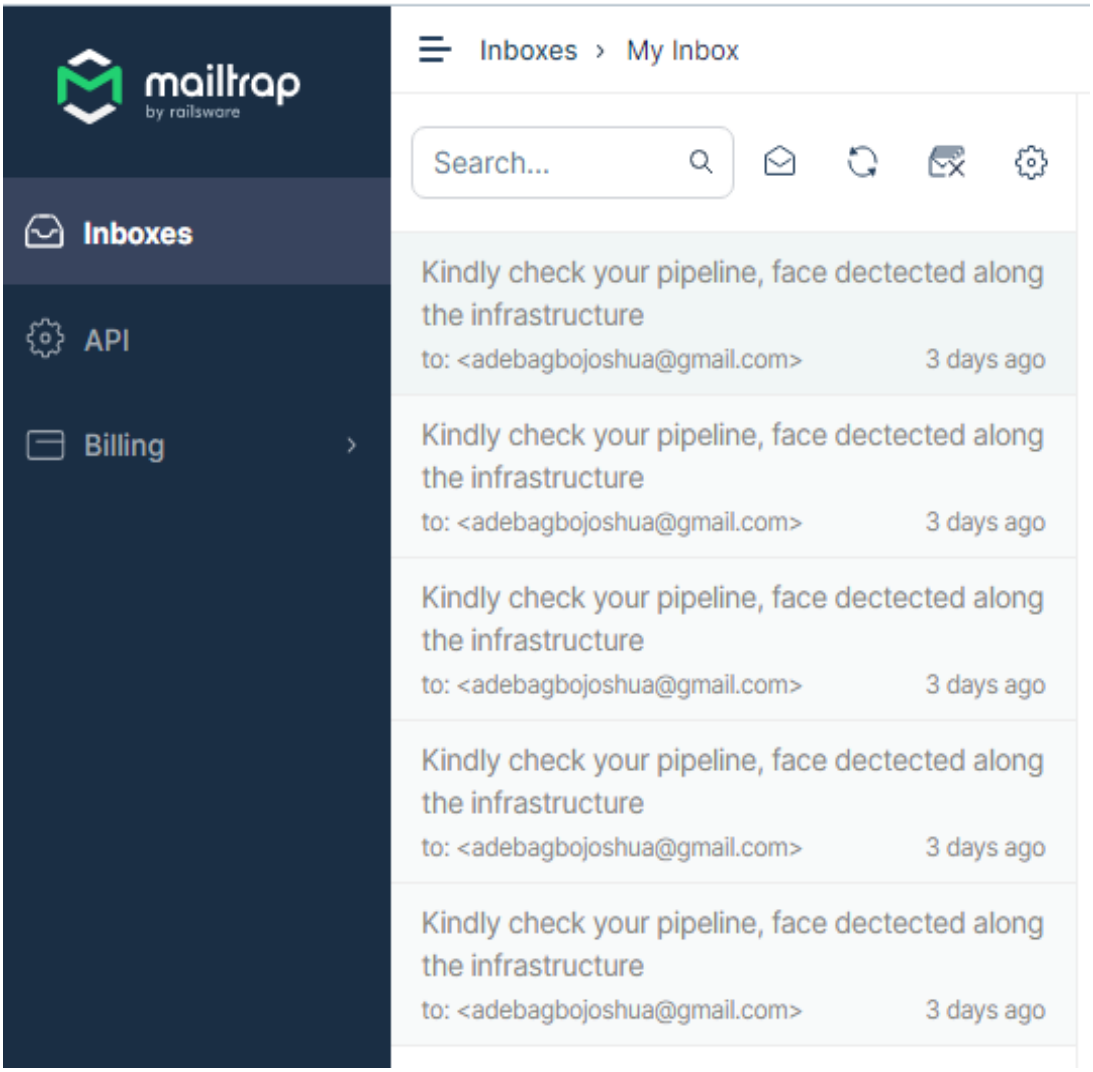

Fig. 6 Snapshot of image sent to the pipeline administrator's mailtrap address

Table 1. Table of results of images sent to the central web server from each nodes

Unique ID	Field of View	Time of Capture	Date	Size of Data	Location (Lat/Long)
Ibadan_Alakia_Cam1	26m	17:00 hrs	2021924	274KB	7.3831N,3.965E
Ibadan_Alakia_Cam1	26m	17:00 hrs	2021924	273KB	7.3831N,3.965E
Ibadan_Alakia_Cam1	26m	17:01 hrs	2021924	279KB	7.3831N,3.965E
Ibadan_Alakia_Cam1	26m	17:02 hrs	2021924	279KB	7.3831N,3.965E
Ibadan_Alakia_Cam1	26m	17:03 hrs	2021924	227KB	7.3831N,3.965E
Ibadan_Ojoo_Cam2	26m	13:00 hrs	2021925	280KB	7.85N, 3.933E

Some screenshots of the email generated from the email trap images downloaded are detailed below.

Fig. 7 Image downloaded from the pipeline administrator's mailtrap address

9. Evaluation of the Design

The developed system was evaluated using the manual software testing technique such as Response Time, Stability, Reliability, Usability Testing (Easy to understand, easy to access, Faster Access, Effective Navigation), Compatibility, and Reliability Testing (Software, Hardware. Network, Mobile).

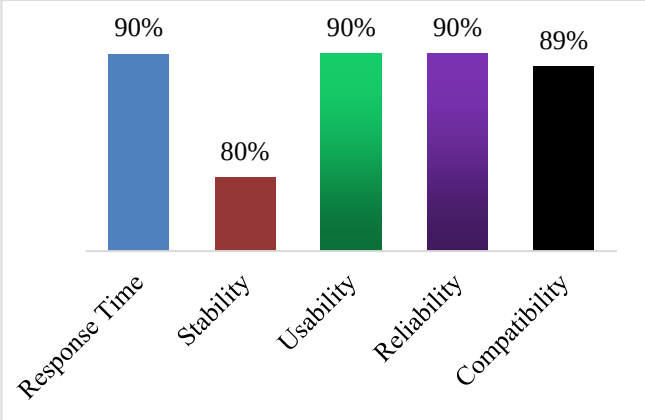

Fig. 8 Evaluation chart of the prototype design

From Figure 8 above, the response time of the developed is 90%, data was transmitted within 1-3 seconds, and the prototype design was tested by applying some load with reference to the stability factor. The system was stable. Also, the design was reliable at a good network speed with attenuation. Hence a score of 90%.

The design is easy to understand; it requires little or no basic training and can be used even if one is not a professional. Easy to access since the component required are not expensive and are mostly open source. The design is compatible with different operating systems, both for forward compatibility and backward compatibility, having a score of 95%, and also with different browsers like Google Chrome, Firefox, and Internet Explorer.

10. Conclusion

This work investigated the generation of networked surveillance nodes for oil Pipelines' theft. The system is significant in cutting costs of security management along the pipeline, efficient in operation due to response time, and reduction in the use of manpower. The main emphasis of this design is to provide efficient surveillance and intrusion notifications for pipeline infrastructure against sabotage or theft. The developed model will be able to perform its required functions for a long time without a change of features. The developed system can also be used to monitor the environmental condition of pipeline facilities, giving details of the environment per second depending on the time range programmed for capturing and sending.

For this system, capturing and sending are every second. The developed system was able to capture intrusion in a simulated pipeline facility, and mail was sent to the surveillance mail as expected. The system had a good response time, scalability, and reliability. Hence, the system will provide a simple, cheaper, and durable pipeline surveillance system to monitor and report real-time operations on a pipeline facility.

References

[1] Robin Cartwright, and Nicholas Atampugre, Delta field Interviews Coordinated by Chris Newsom and Timipere Allison, Organised Oil Crime in Nigeria. [Online]. Available: http://enact-africa.s3.amazonaws.com/site/uploads/2020-11-26-organised-oil-crime-in-nigeria.pdf

[2] Jiedi Sun, Jinquan Zhang, and Xiaojun Wang, "Feature Extraction and Multi-Sensor Data Fusion in Monitoring and Pre-Warning System for Security of Pipeline Based on Multi-Seismic Sensors," *IEEE International Conference on Mechatronics and Automation*, pp. 2595-2600, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[3] G.N Ezeh et al., "Pipeline Vandalization Detection Alert with Sms," *International Journal of Engineering Research and Applications*, vol. 4, no. 4, pp. 21-25, 2014. [Google Scholar] [Publisher Link]

[4] Godswill Ofualagba, O'tega Ejofodomi, "Automated Oil and Gas Pipeline Vandalism Detection System," *SPE Nigeria Annual International Conference and Exhibition*, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Fakoyejo Olalekan, Pipeline explosion: Over 45,000 incidents recorded in 18 years – NNPC, 2020. [Online]. Available: https://nairametrics.com/2020/01/21/pipeline-explosion-over-45000-incidents-recorded-in-18-years-nnpc/

[6] Al Chukwuma Okoli, and Sunday Orinya., "Oil Pipeline Vandalism and Nigeria's National Security," *Global Journal of Human Social Science*, vol. 13, no. 5, pp. 67-75. 2013. [Google Scholar] [Publisher Link]

[7] [Online].Available:https://nnpcgroup.com/NNPCBusiness/BusinessInformation/Pages/MonthlyPerformance-Data.aspx

[8] Ahmed, Tukur Umar, Moh'D. Shahwahid Hajj Othman, Miao Wang, "Causes and Consequences of Crude Oil Pipeline Vandalism in the Niger Delta region of Nigeria: A Confirmatory Factor Analysis Approach," *Cogent Economics & Finance*, vol. 5, no. 1, 2017.[CrossRef] [Google Scholar] [Publisher Link]

[9] AJAO Lukman et al., "An Anti-Theft Oil Pipeline Vandalism Detection: Embedded System Development," *International Journal of Engineering Science and Application*, vol. 2, no. 2, pp. 55-64, 2018. [Google Scholar] [Publisher Link]

[10] Jinfeng Sun, Zhiyue Zhang, Xiaoli Sun, "The Intelligent Crude Oil Anti-Theft System Based on IoT Under Different Scenarios," *Procedia Computer Science*, vol. 96, pp. 1581-1588, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[11] Gómez, Cristina, and David R. Green, "Small Unmanned Airborne Systems to Support Oil and Gas Pipeline Monitoring and Mapping," *Arabian Journal of Geosciences*, vol. 10, no. 202, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] Nwazor O Nkolika, and Romanus Obagidi, "A Light Tracking Automated Guided Vehicle for Oil Pipeline Leakage Detection," *International Journal of Scientific & Engineering Research*, vol. 10, no. 3, pp. 250-256, 2019. [Google Scholar] [Publisher Link]

[13] Tadas Baltrušaitis, Peter Robinson, Louis-Philippe Morency, "Openface: An Open-Source Facial Behavior Analysis Toolkit," *IEEE Winter Conference on Applications of Computer Vision*, pp. 1-10, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[14] [Online].Available: https://thedora.com/pipeline/Nigeria-oil-gas_and_products_pipeline_map.html.

[15] Kintronics IP Security Solution, Calculating What You Can See with Your IP Camera, 2015. [Online].Available: https://kintronics.com/calculating-can-see-ip-camera/