IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Smart Monitoring and Control System for Crude Oil Pipeline Vandalism

Eloho Goodluck Okeno[1], Prof. Olabode O.[2], Frank Okaro[3]
Lecturer, Department of Computer Science, Federal University of Technology, Akure, Nigeria[1,2]
Researcher, IT Department, Whitedovewebworld, Abraka, Nigeria[3]
goodluckokrno@gmail.com[1], olabodeo@futa.ng.org[2], info@whitedovewebworld.com[3]

Abstract: *Crude oil pipeline vandalism, theft, and unauthorized interference present a significant challenge to the oil industry's security, profitability, and sustainability. Despite initial measures such as security patrols, traditional methods have proven inadequate, particularly in difficult terrains and aquatic regions. These methods often fail to promptly detect and prevent vandalism and theft, which results in significant economic, environmental, and safety risks. This study developed and implemented a smart monitoring and control system to address these challenges by improving the detection of oil pipeline vandalism, including incidents in aquatic environments. The Prototyping methodology was adopted, allowing for continuous testing and improvements throughout the development process. The system was built using C#.NET under the .NET Framework, with Microsoft SQL Server as the database, incorporating an encryption layer for database security. To enhance its effectiveness, an oil theft detection algorithm was integrated with a web-based interface to facilitate real-time monitoring, visualization, and reporting. Testing scenarios demonstrated that the system successfully detected threats and ensured seamless data flow from sensors to the central system. This solution marks a significant advancement in the security and sustainability of oil infrastructure, contributing to environmental protection and the safety of stakeholders*

Keywords: Crude Oil Pipeline Vandalism, Oil Theft Detection, Internet of Things (IoT), and Smart Monitoring System

I. INTRODUCTION

Crude oil pipelines are vital components of the global energy infrastructure, playing a key role in the transportation of oil from extraction sites to refineries and distribution points. Despite their importance, these pipelines face increasing threats from vandalism, theft, and unauthorized tampering. Such criminal activities compromise the structural integrity of the pipelines and lead to significant economic, environmental, and safety concerns [1]. The growing prevalence of oil theft, in particular, has become a major challenge for the oil and gas industry, resulting in substantial financial losses, environmental degradation, and interruptions in the oil supply chain [2].

Oil theft encompasses a wide range of illicit activities, from small-scale siphoning to highly organized operations involving direct hacks into pipelines. These incidents often contribute to environmental pollution, as oil spills caused by vandalism damage ecosystems and threaten public safety. The criminal networks involved in these operations exacerbate security concerns, making it clear that current monitoring and control methods are inadequate to fully prevent such breaches [3].

To address these challenges, there is an urgent need for advanced, technology-driven solutions capable of detecting and preventing oil theft. The rise of the Internet of Things (IoT) offers a promising approach to overcoming these issues. IoT technology, which connects various devices and sensors over a network, enables real-time data collection and monitoring. This technology has the potential to transform crude oil pipeline security by providing continuous surveillance, anomaly detection, and immediate alerts [4]. With IoT, the need for periodic inspections can be reduced, as systems continuously monitor pipeline activity, collecting data on temperature, pressure, flow rates, and other critical parameters [5].

This research is motivated by the need to enhance the security and resilience of crude oil pipelines. It aims to develop a Smart Monitoring and Control System that integrates IoT technology with advanced monitoring strategies to detect and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

prevent oil theft more effectively. By leveraging IoT devices, real-time data analytics, and a centralized control system, the proposed solution offers a comprehensive approach to mitigating pipeline vandalism. The system not only ensures early detection of theft and tampering but also facilitates a swift and coordinated response to security breaches. This research seeks to provide the oil and gas industry with a more robust, efficient, and scalable solution to protect its critical infrastructure and minimize the risks associated with oil theft.

II. RESEARCH MOTIVATION

The ongoing and increasing incidents of crude oil pipeline vandalism pose a significant threat to the stability and security of the global energy supply chain. These acts of sabotage and theft result in considerable economic losses for the energy sector and create serious risks to environmental integrity, public safety, and national security [1]. The oil industry, as a cornerstone of the global economy, faces persistent challenges, particularly from oil theft, which encompasses a range of illicit activities, including pipeline vandalism and unauthorized access to oil facilities. These challenges not only undermine the profitability and sustainability of oil companies but also lead to environmental contamination and safety hazards for surrounding communities [2].

While innovative systems like the Ground Robotics Oil Spill Surveillance (GROSS) have emerged, they also face limitations, particularly regarding their applicability to aquatic environments where a significant portion of oil theft occurs. The GROSS system is primarily designed for ground-level surveillance and lacks the real-time monitoring and visualization capabilities essential for effective decision-making by security personnel [6].

Given these pressing challenges, there is an urgent need to develop a more sophisticated and adaptive Smart Monitoring and Control System that can effectively address the multifaceted issues posed by crude oil pipeline vandalism. By leveraging advanced technologies and integrating robust monitoring and response strategies, this research aims to enhance the security and resilience of oil infrastructure, ultimately contributing to the protection of economic interests and environmental safety.

III. REVIEW OF RELATED WORK

[7] presented an "Integrative Systems Model for Oil and Gas Pipeline Data Prediction and Monitoring Using a Machine Intelligence and Sequence Learning Neural Technique." Their research proposed the use of the Hierarchical Temporal Memory (HTM), a machine intelligence system designed for real-time monitoring and prediction of pressure signals in oil and gas pipelines. The HTM system enhances the security and efficiency of pipeline operations by outperforming the Online Sequential Extreme Learning Machine (OS-ELM) in terms of Mean Absolute Percentage Error (MAPE). Notably, while the OS-ELM requires extensive training data and numerous parameter adjustments, the HTM technique necessitates tuning of only one parameter, making it more suitable for real-time applications. The research contributes significantly by combining machine intelligence and machine learning techniques for monitoring pipeline data effectively.

[8] developed a low-cost prototype system for detecting pipeline operational issues and vandalism spillages, aimed at addressing the financial and technical challenges that often accompany more advanced systems. Their study, published in Advances in Internet of Things, proposed a framework for detecting and validating pipeline spillages, providing a cost-effective alternative for smaller oil firms, particularly in regions like the Niger Delta. Their research demonstrated how technological innovation, especially low-cost sensor systems, could be integrated into spillage detection while maintaining accuracy. The validation framework they introduced is essential for confirming the legitimacy of detected anomalies, thus improving system efficiency.

[9] proposed an innovative and cost-effective approach to address oil pipeline vandalism through the utilization of Earth observation systems, specifically Small Satellites (CubeSats) in Low Earth Orbit. Their research introduced a surveillance system leveraging the cost-effectiveness, quick development, and continuous real-time monitoring capabilities of CubeSats. The proposed system comprises a constellation of 12 CubeSats designed to monitor infrastructure comprehensively across Nigeria. Additionally, their ground segment employs a novel method inspired by car airbag systems, where crash/vibration sensors trigger alerts upon detecting anomalies. While their approach shows promise, it also has limitations, including insufficient details on sensor specifications and potential challenges in real-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

world deployment. Further research and field trials are necessary to validate the practicality and scalability of their proposed system.

[6] introduced the Ground Robotics Oil Spill Surveillance (GROSS) system aimed at early detection of oil spills from crude oil pipelines. While the GROSS system relies on an autonomous ground mobile robot for continuous surveillance, it faces challenges, particularly as many oil theft incidents occur in aquatic environments where the system is less effective. Furthermore, the lack of real-time monitoring and visualization capabilities hampers effective decision-making for security personnel. This highlights the urgent need for an advanced Smart Monitoring and Control System capable of addressing these multifaceted challenges.

Together, these studies emphasize the critical need for innovative technological solutions to combat the pervasive issue of pipeline vandalism, highlighting various approaches, from machine learning models to low-cost sensor systems, and advocating for integrated strategies that consider both technological advancements and regulatory frameworks.

IV. METHODOLOGY ADOPTED

The study adopted the Prototype Development Methodology to develop and implement a smart monitoring and control system for crude oil pipeline vandalism. This methodology was particularly suitable for projects requiring iterative refinement and real-time feedback, allowing for the integration of IoT sensors, a web-based monitoring platform, and an oil spill detection algorithm. The approach facilitated continuous testing and improvement, ensuring optimal system performance before final deployment.

Initially, the project began with requirement gathering, identifying the necessary hardware (IoT sensors) and software (ASP.NET C#, SQL Server) components. Key performance metrics, including detection accuracy, response time, and false alarm rate, were established to ensure operational efficacy.

Following this, a preliminary system design was developed, outlining the overall architecture of the monitoring system. This design included a web-based platform for real-time data visualization and the oil spill detection algorithm for aquatic environments. The prototype development phase involved creating a functional version of the system, integrating IoT sensors, and implementing the detection algorithm within the GROSS framework. This prototype served as a baseline for further refinement.

The testing and evaluation phase involved using simulated sensor data to assess performance, measuring key indicators such as latency and detection accuracy. Based on these evaluations, the system underwent several refinements. The spill detection algorithm was enhanced to improve accuracy, and the platform was optimized for better user interaction and data visualization.

After iterative testing and refinement, the final version of the system was developed and integrated, undergoing comprehensive testing to confirm that it met the project objectives. The final step involved deploying the system for real-time monitoring, enabling it to detect oil spills and alert relevant stakeholders about potential pipeline vandalism.

Overall, the Prototype Development Methodology was instrumental in this project, enabling continuous improvement and ensuring the final system effectively addressed the needs of the oil and gas industry for enhanced pipeline security and environmental protection.

V. PROPOSE SYSTEM

The proposed Smart Monitoring and Control System, powered by Internet of Things (IoT) technology, marks a significant enhancement over the existing GROSS system. This advanced solution utilizes the capabilities of IoT sensors to detect incidents of oil theft, particularly in aquatic environments, while facilitating real-time monitoring. By employing a web-based platform, the system achieves immediate anomaly detection, effectively minimizing human error through automation. It also ensures rapid response times through real-time alerts, proving to be a cost-effective alternative by reducing the need for constant human oversight.

The comprehensive system harnesses intelligent sensors, data analytics, cloud-based platforms, and remote monitoring to enhance security within oil facilities. It is comprised of a range of seamlessly integrated components that work in unison to continuously monitor critical parameters, detect anomalies, and generate real-time alerts. This functionality enables prompt and effective responses to potential threats. Central to the system is a monitoring and data processing hub specifically designed to aggregate data from the IoT sensors deployed throughout the oil facility.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Tailored to combat oil theft, this sophisticated system has the potential to revolutionize security protocols within the oil industry, significantly enhancing its ability to protect assets and effectively deter theft. It is designed to collect data from IoT sensors strategically positioned across the oil facility, ensuring comprehensive coverage and monitoring.

Key components of the proposed system include IoT sensors, a robust communication infrastructure, a user-friendly web-based platform, automated alerting mechanisms, and various security measures. Additionally, the system features real-time monitoring and visualization capabilities, alongside data storage and logging functionalities, and user access control systems. Each of these components plays a crucial role in the overall effectiveness of the proposed system, guaranteeing real-time monitoring, thorough data analysis, proactive security measures, and enhanced user access, ultimately improving the security and operational efficiency of the oil facility.

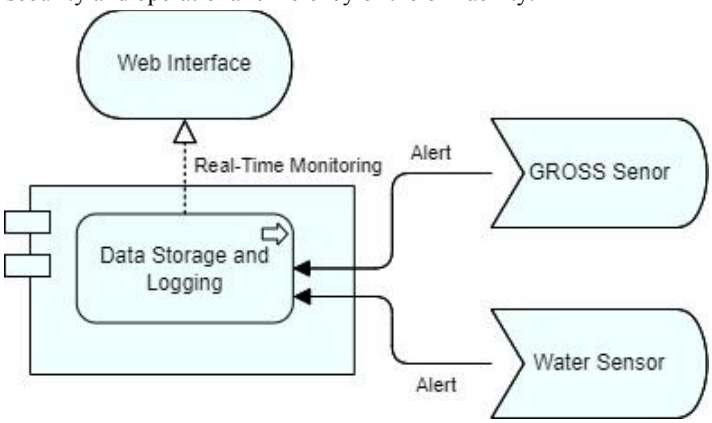

Fig. 1. Proposed system architecture

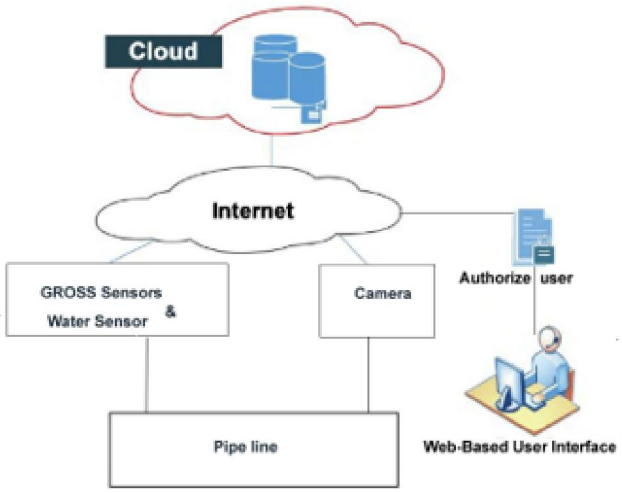

Fig. 2. High-level model diagram of the proposed system

The algorithm of the proposed system is given thus:

i. Oil Theft Detection in Water

Input:

Sensor data from water sensors (e.g., water level, pressure, temperature)

Threshold values for anomaly detection

Output:

Alert if an anomaly indicating potential oil theft is detected

Procedure: DetectOilTheftInWater

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Step 1: Read sensor data from water sensors.
Step 2: Categorize the data based on sensor type (e.g., water level, pressure, temperature).
Step 3: Analyze the sensor data for anomalies:
Calculate the change in water level, pressure, or temperature compared to the previous reading.
Compare the calculated change against predefined threshold values for anomaly detection.
Step 4: If the change exceeds the threshold values for any sensor:
Record the anomaly with the following details:
Type of anomaly (e.g., water level change, pressure change)
Location and timestamp of the anomaly.
Trigger an alert indicating a potential oil theft incident.
Step 5: If no anomalies are detected, continue monitoring.
End DetectOilTheftInWater.

ii. Algorithm: Anomaly Detection

Input:
SensorData (array of sensor readings)
Mean (μ_X)
StdDev (σ_X)
ThresholdFactor (k)
Output:
AnomalyFlags (array of binary indicators)
Steps:
Begin by initializing AnomalyFlags as an empty array.
For each reading X_i in SensorData:
Compute the Threshold as T_X = ThresholdFactor * StdDev.
If the absolute difference $|X_i - Mean|$ exceeds the threshold T_X:
Append 1 to AnomalyFlags (indicating the presence of an anomaly).
Otherwise:
Append 0 to AnomalyFlags (indicating no anomaly).
Finally, return the AnomalyFlags array.

iii. Algorithm: Risk Assessment

Input:
AnomalyFlags (array of binary anomaly indicators)
Weights (array of weights for each type of anomaly)
RiskThreshold (T_R)
Output:
RiskScore (calculated risk score)
AlertStatus (binary indicator)
Steps:
Begin by initializing RiskScore to 0.
For each index i in AnomalyFlags:
Update RiskScore by adding the product of AnomalyFlags[i] and Weights[i].
If RiskScore exceeds RiskThreshold:
Set AlertStatus to 1 (indicating that an alert is triggered).
Otherwise:
Set AlertStatus to 0 (indicating no alert).
Finally, return RiskScore and AlertStatus.

iv. Algorithm: Risk Assessment

Input:
AnomalyFlags (array of binary anomaly indicators)

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Weights (array of weights for each type of anomaly)
RiskThreshold (T_R)

Output:

RiskScore (calculated risk score)
AlertStatus (binary indicator)

Steps:

Begin by initializing RiskScore to 0.
For each index i in AnomalyFlags:
Add the product of AnomalyFlags[i] and Weights[i] to RiskScore.
If RiskScore exceeds RiskThreshold:
Set AlertStatus to 1, indicating that an alert is triggered.
Otherwise:
Set AlertStatus to 0, indicating no alert.

Finally, return both RiskScore and AlertStatus.

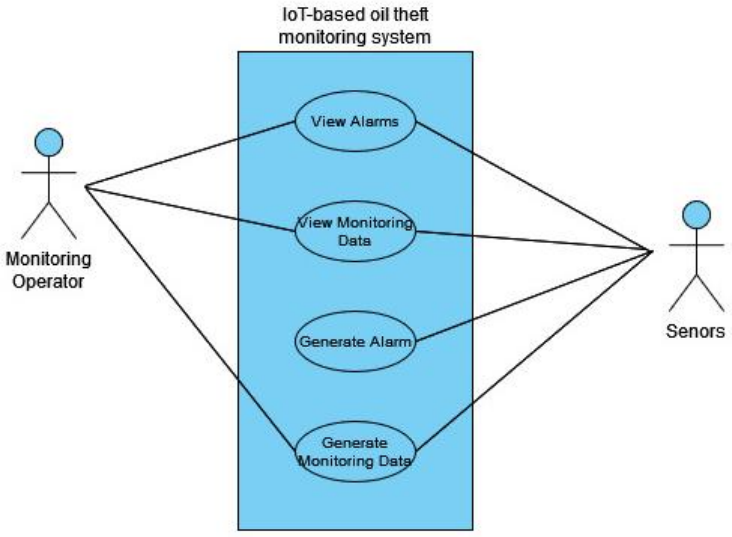

Fig. 3.Use case diagram for smart monitoring and control system

VI. EXPERIMENTAL RESULT

The system operates through two distinct sessions: the user session and the admin session. The user session begins by launching a web browser like Mozilla Firefox, Chrome, or Opera and accessing the application via the hosted URL. This opens the welcome page, which introduces the researcher and provides a help button with system information. The welcome page serves as the starting point for users to familiarize themselves with the application and its purpose. Fig. 4 visually represents the appearance of the welcome page.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

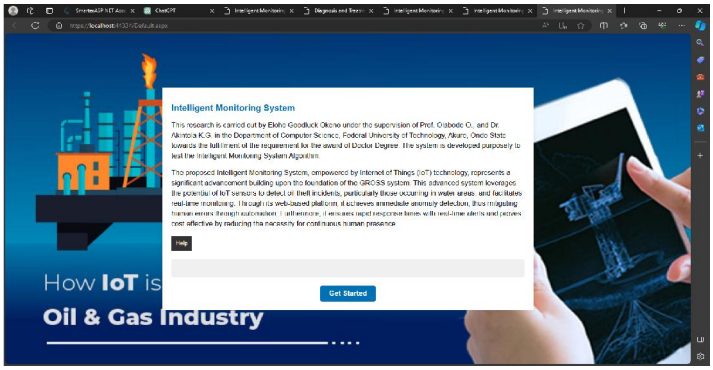

Fig. 4.Welcome page interface

When users click the "Help" button on the welcome page, a pop-up menu appears, providing a detailed instructional message on how to effectively use the system, as visually represented in Fig.5. This user guide outlines the system's prerequisites and offers comprehensive guidelines to help users navigate and operate the system with ease. Its primary goal is to support users by offering clear, concise instructions for maximizing the system's features. By integrating this guide into the interface, the system enhances the user experience, ensuring that users of all expertise levels can confidently use the application.

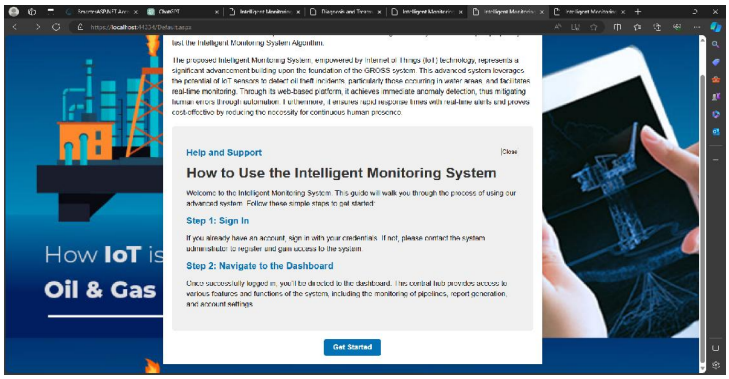

Fig. 5.User guide page

On the login page, users input their username and password to begin the authentication process. The system verifies these credentials by comparing them to stored data. Once successfully authenticated, users are redirected to the system's dashboard, granting access to various features. This secure login process ensures that only authorized users can access the system, enhancing both security and user experience.

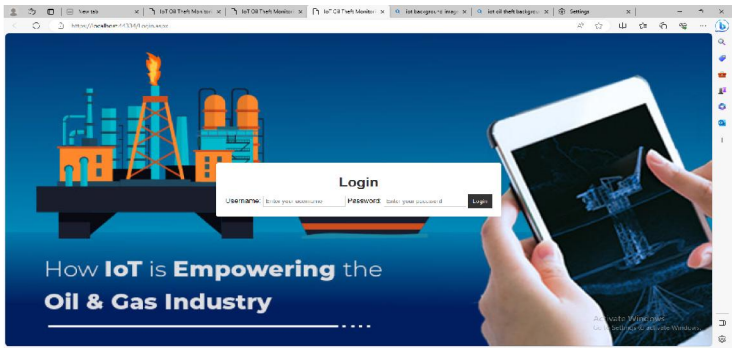

Fig. 6.Login interface

Fig.7 depicted the user dashboard following successful login, where users are redirected to the monitoring page. This interface allows for real-time monitoring of pipelines in both water and land environments, using intuitive visualizations to display the current status. The system provides sensor readings, alerts, and other essential data, while

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

an automated alert system notifies users of any detected anomalies, enabling prompt responses to potential issues and ensuring efficient pipeline monitoring.

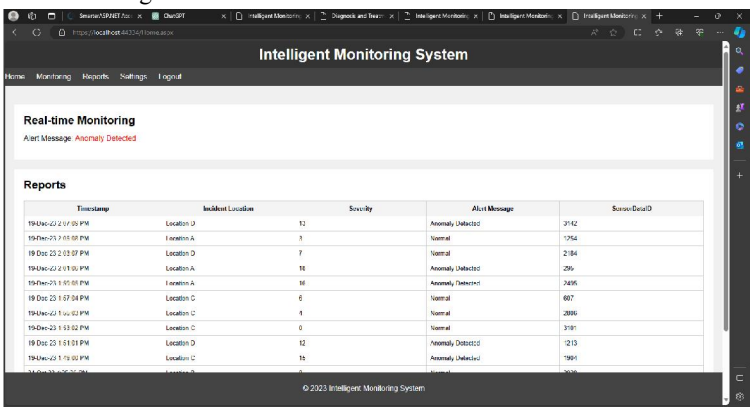

Fig. 7.Dashboard interface

Fig.8. presented the Monitoring Page, a key feature of the system's administrative interface. Designed for administrators, it provides real-time data and a comprehensive view of system operations, enabling precise monitoring of various stations. The page offers insights into both individual station performance and the overall network health, empowering administrators to make informed decisions and respond swiftly to anomalies. Its intuitive design and detailed system information support proactive management and optimization of system performance.

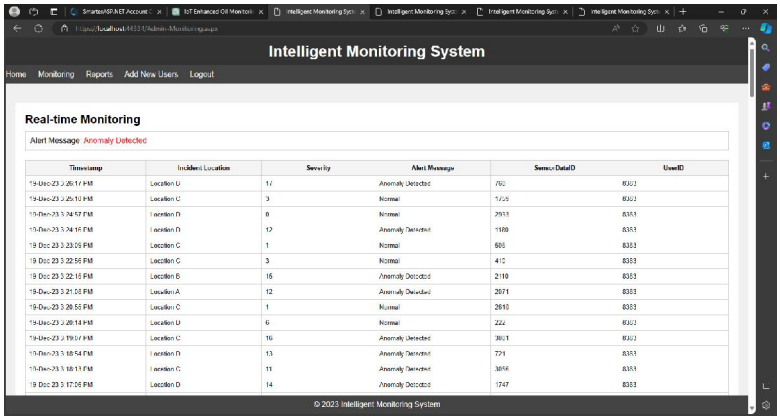

Fig. 8.Admin monitoring page

Table 1: Evaluation metrics for the system's performance

Timestamp	Sensor Reading (X_i)	Actual Anomaly (1/0)	Detection Time (seconds)	Response Time (seconds)	Latency (seconds)
2024-09-01 12:00:00	105	1	1.2	2.5	1.0
2024-09-01 12:01:00	98	0	0.0	0.0	0.0
2024-09-01 12:02:00	115	1	1.5	2.8	1.2
2024-09-01 12:03:00	100	0	0.0	0.0	0.0
2024-09-01 12:04:00	107	1	1.1	2.7	1.0

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

$$Detetion\ Accuracy = \frac{Number\ of\ True\ Postives}{Number\ of\ True\ Positives + Number\ of\ False\ Nagative}$$

True Positives (TP) = 3 (Anomalies correctly detected)

True Positives (TP) = 3 (Anomalies correctly detected)

$$Detetion\ Accuracy = \frac{3}{3+0} = 1.0\ or\ 100\%$$

$$False\ Alarm\ Rate = \frac{Number\ of\ False\ Positivies}{Number\ of\ False\ Positives + Number\ of\ True\ Negatives}$$

False Positives (FP) = 0 (Normal instances incorrectly detected as anomalies) False Positives (FP) = 0 (Normal instances incorrectly detected as anomalies)

$$False\ Alarm\ Rate = \frac{0}{0+2} = 0.0\ 0r\ 0\%$$

$$Average\ Response\ Time = \frac{Sum\ of\ Response\ Times}{Number\ of\ Anomalies}$$

Total Response Time = 2.5 + 2.8 + 2.7 = 8.0 seconds

Number of Anomalies = 3

$$Average\ Response\ Time = \frac{8.0}{3} = 2.67\ seconds$$

$$Average\ Latency = \frac{Sum\ of\ Latency\ Times}{Number\ of\ Anomalies}$$

Total Latency = 1.0 + 1.2 + 1.0 = 3.2 seconds

Number of Anomalies = 3

$$Average\ Latency = \frac{3.2}{3} = 1.07\ seconds$$

The evaluation of the smart monitoring and control system focused on key performance metrics: detection accuracy, false alarm rate, average response time, and average latency. The system achieved a perfect detection accuracy of 100%, successfully identifying all anomalies without missing any, demonstrating the effectiveness of the anomaly detection algorithm. With a false alarm rate of 0%, the system avoided incorrectly flagging normal conditions, ensuring reliable operation without unnecessary disruptions.

The average response time was 2.67 seconds, reflecting the system's ability to quickly notify relevant personnel or trigger automatic responses after detecting an anomaly. The average latency, measuring the time between an anomaly's occurrence and its detection, was 1.07 seconds, indicating a minimal delay in identifying events. While the system performed well, improvements could be made to further reduce response time and latency, enhancing its real-time monitoring capabilities in high-risk environments.

Overall, the system's performance metrics indicate that it is highly effective for real-world pipeline monitoring, though further optimization could improve its responsiveness.

VII. CONCLUSION

The Smart Monitoring and Control System marks a major step forward in addressing the security and sustainability challenges in the oil industry. This research has thoroughly explored the persistent issues of oil theft, such as pipeline vandalism, illegal tapping, and unauthorized access to oil facilities, which have caused significant financial losses, environmental damage, and safety risks. Traditional security methods have proven inadequate, and this system responds with advanced, proactive solutions.

The integration of the Ground Robotics Oil Spill Surveillance (GROSS) system, with its innovative algorithm for detecting water-based theft, tackles the difficult terrains and sophisticated tactics of oil thieves. The web-based centralized monitoring platform further enhances real-time data visualization and decision-making for security teams, making the system both cutting-edge and effective in preventing oil theft.

In conclusion, the Smart Monitoring and Control System offers a comprehensive solution to the complex challenges facing the oil industry. By safeguarding oil infrastructure, it boosts industry profitability, protects the environment, and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

ensures the safety of all stakeholders. This system serves as a model for integrating technology and surveillance in critical infrastructure security, highlighting the essential role of innovation in protecting valuable resources and ensuring the long-term sustainability of the oil sector.

REFERENCES

[1]. Y. Chao, T. Mao, F. Gong, D. Wang, and J. Chen, "An oil film information retrieval method overcoming the influence of sun glitter, based on AISA+ airborne hyper-spectral image," in Proc. SPIE Int. Soc. Opt. Eng., vol. 7825, 2020.

[2]. F. C. Onuoha, "Oil pipeline sabotage in Nigeria: Dimensions, actors and implications for national security," African Secur. Rev., vol. 17, no. 3, pp. 99–115, 2018.

[3]. O. H. Boris, "The upsurge of oil theft and illegal bunkering in the Niger Delta region of Nigeria: Is there a way out?" Mediterranean Journal of Social Sciences, vol. 6, no. 3, pp. 563–573, 2015.

[4]. J. Jeong, O. Han, and Y. You, "A design characteristics of smart healthcare system as the IoT application," Indian Journal of Science and Technology, vol. 9, no. 37, 2016.

[5]. Ambituuni, P. Hopkins, J. Amezaga, D. Werner, and J. Wood, "Risk assessment of a petroleum product pipeline in Nigeria: The realities of managing problems of theft/sabotage," in WIT Transactions on The Built Environment, vol. VI, pp. 49–50, WIT Press, 2021.

[6]. E. Otega and O. Godswill, "Ground Robotics Oil Spill Surveillance (GROSS) System for early detection of oil spills from crude oil pipelines," International Journal of Imaging and Robotics, vol. 20, no. 2, pp. 36–54, 2020.

[7]. O. Chinwe and O. Emmanuel, "An integrative systems model for oil and gas pipeline data prediction and monitoring using a machine intelligence and sequence learning neural technique," Federal University of Technology (FUTO), Owerri, Nigeria; onukwugha2000@yahoo.com, National Open University of Nigeria (NOUN); nd.osegi@sure-gp.co., 2018.

[8]. F. Ekeu-Wei and I. T. Ekeu-Wei, "Development of a low-cost prototype system for pipeline operational and vandalism spillage detection and validation framework," Advances in Internet of Things, vol. 14, no. 02, pp. 21–35, 2024.

[9]. O. S. Nnadih and O. E. Offiong, "Mitigation of oil pipeline vandalism using small-satellites and earth observation systems. A case study-Nigeria," Am. J. Eng. Res., vol. 6, no. 9, pp. 66–70, 2017.