AI-Assisted Crude Oil Bunkering and Illegal Theft Detection in the Oil and Gas Industry

AFOLABI RIDWAN BELLO[1], GODWIN EKUNKE ODOR[2], IDRIS ADEYINKA BUSARI[3], ABDUSSAMAD IDRIS ALI[4], ABDULLAHI ABUBAKAR GIREI[5], JOY OPEYEMI ALABI[6], VICTOR IKECHUKWU STEPHEN[7]

[1]*Department of Chemical Engineering, Ladoke Akintola University of Technology, Nigeria.*
[2]*Department of Mechanical Engineering, University Of Portharcourt, Nigeria.*
[3]*Department of Computer Engineering for Robotics and Smart Industry, University of Verona, Italy.*
[4]*Department of Computer Engineering, King Fahd University of Petroleum and Minerals, Saudi Arabia.*
[5]*Department of Intelligence and Security Studies, Nigerian Defence Academy, Nigeria.*
[6]*Department of Mathematics, University of Lagos, Nigeria.*
[7]*Department of Electrical and Electronics Engineering, Michael Okpara University of Agriculture, Nigeria.*

Abstract- ***Crude Oil bunkering and illegal siphoning remain a threat in the oil and gas industry, with its associated mind-boggling economic loss, environmental degradation, and hours of production losses. Traditional surveillance and monitoring systems have failed to provide real-time detection and intervention as they are manual surveillance-based. This review reports the application of Artificial Intelligence (AI) in oil theft prevention and detection via machine learning, computer vision, and predictive analytics. Case studies centered on high-risk oil producing areas where these activities are often carried out. These include the Gulf of Mexico in North America, Niger Delta regions of Nigeria and Anambra State Nigeria, confirm the effect of AI-based surveillance in preventing these crimes. In Anambra State, studies recorded a 25% reduction in theft, 30% in vandalism, and 20% in sabotage after the installation of AI-based security facilities. These confirm the positive effect of AI theft detection capacity. Similarly, AI-based predictive analytics in the Niger Delta improved real-time detection of anomalies, where the response time improved and meaningful reductions were recorded in the illegal siphoning of oil. In the Gulf of Mexico, AI-based monitoring of pipelines were effective in detecting and preventing unauthorized entry, with the enhancement of asset security. The findings of this review include the confirmation of the revolutionary effect of AI in the safeguarding of oil and gas infrastructures, recommending investment in intelligent surveillance devices and the implementation of strong regulatory frameworks in fighting the threat of illicit activities in the oil and gas industry.***

Indexed Terms- ***Artificial Intelligence (AI); Oil Bunkering; Illegal Theft Detection; Machine Learning; Pipeline Surveillance.***

I. INTRODUCTION

[1] Oil bunkering and theft have emerged as major concerns in the global energy industry. The illegal siphoning of crude oil and refined petroleum products from pipelines, storage tanks, and transportation systems results in billions of dollars in annual losses. This illicit activity is not limited to any specific region; it occurs in oil-producing countries across Africa, Latin America, and the Middle East [2]. In some cases, criminal networks operate sophisticated operations involving advanced siphoning equipment, bribery, and even violence to sustain illegal oil extraction. Oil theft has existed for decades, often linked to political instability, economic hardship, and weak governance. During conflicts, militant groups have used stolen crude oil to finance their operations [3]. In the Niger Delta, oil theft became a full-fledged industry in the early 2000s, driven by militant groups and corrupt officials [4]. Methods of Oil Theft and Illegal Bunkering include Pipeline Tapping: Criminals drill illegal taps into pipelines, siphoning crude oil into

tankers; Ship-to-Ship Transfers: Vessels offload stolen oil to other ships in international waters, making it difficult to track; Storage Facility Break-ins: Thieves target refineries, depots, and storage tanks; Corrupt Documentation: Falsification of shipping manifests and oil movement records to disguise stolen oil as legal shipments. Oil theft is not a minor criminal activity, it has become a multi-billion-dollar industry affecting economies, governments, and oil companies. The direct impact includes revenue loss, increased security costs, and damage to infrastructure [1, 2, and 4]. Case Studies of Oil Theft in Major Oil-Producing Countries include Nigeria (The Epicenter of Oil Theft) - Africa's largest oil producer, loses approximately 400,000 barrels per day to oil theft, amounting to billions in lost revenue annually. The Nigerian National Petroleum Corporation (NNPC) estimates that over $3 billion worth of crude is stolen annually. Organized crime networks, backed by corrupt officials, operate illegal refineries in remote areas [5]; Mexico (Fuel Theft from PEMEX Pipelines) - PEMEX, Mexico's state-owned oil company, reported significant losses due to fuel theft (locally known as "huachicolero"). In 2019, a pipeline explosion in Hidalgo killed over 130 people, highlighting the dangers of illegal bunkering. Criminal cartels in Mexico have taken control of illegal fuel distribution [6]; Venezuela: Smuggling and Black Market Operations - Venezuela, with the world's largest proven oil reserves, suffers from rampant fuel smuggling the collapse of the country's economy led to widespread oil siphoning from refineries and tankers, corruption within the state oil company PDVSA has fueled oil diversion to illegal markets [7]. Illegal oil siphoning not only affects economic stability but also has severe environmental and security implications such as Oil Spills from Illegal Pipeline Taps - When thieves tamper with pipelines, they often cause leaks that contaminate water bodies and farmland. In the Niger Delta, oil spills have devastated marine ecosystems, killing fish populations and poisoning drinking water sources [1].Toxic Emissions from Illegal Refineries - Crude oil processed in makeshift refineries releases hazardous chemicals into the air and soilHealth consequences include respiratory diseases, skin conditions, and cancer among local populations [8]. Security Challenges and Armed Conflicts such as Militant Group Financing - Terrorist organizations and rebel groups use oil theft as a funding mechanism. Examples include the Niger Delta militants in Nigeria and armed groups in Libya.Violence and Crime in Oil-Producing Regions - Armed gangs often control bunkering operations, leading to violence against law enforcement and oil workers, Governments struggle to combat these groups due to corruption and lack of resources [1]. The Limitations of Traditional Theft Detection Methods include Manual Surveillance and Security Patrols - Security guards and military forces patrol pipeline routes, but thieves often evade detection. Criminal networks operate with inside information, making it difficult for authorities to intervene effectively [9], Use of CCTV and Sensor-Based Monitoring - Many oil companies use closed-circuit television (CCTV) and basic sensors to detect pipeline intrusions. However, CCTV cameras can be tampered with or disabled, and basic pressure sensors often fail to detect slow siphoning [10]. Delays in Theft Detection and Response - By the time authorities detect a theft, criminals have already transported the stolen oil. The lack of real-time monitoring and predictive analytics means that response times are slow [11].

1.2 The Role of Artificial Intelligence (AI) in Combating Oil Bunkering and Theft [1, 2 and 4]

Artificial intelligence (AI) offers a transformative solution to the challenges posed by oil bunkering. Unlike traditional methods, AI-powered systems can provide real-time monitoring, predictive analysis, and automated threat detection. AI combines machine learning, computer vision, and IoT-based monitoring to detect suspicious activities and alert security teams in real time. Machine Learning for Anomaly Detection - AI can analyze pipeline flow data and identify irregularities that indicate theft. Unlike conventional pressure sensors, AI algorithms can detect even small leaks or slow siphoning attempts.Computer Vision for Surveillance - AI-powered video analytics can identify unauthorized personnel, suspicious vehicles, and abnormal activities near pipelines. Drones equipped with AI-enhanced vision can monitor vast pipeline networks and remote oil facilities. AI-Integrated IoT for Smart Pipelines - Smart sensors placed along pipelines can continuously transmit data to AI systems. AI can differentiate between normal operations and theft activities, reducing false alarms.

1.3 Research Objectives and Significance

This study aims to explore how AI can enhance oil theft prevention through Real-time threat detection and monitoring using AI-powered surveillance and IoT sensors. Predictive analytics to anticipate theft attempts before they occur. Automated decision-making to improve response times and security interventions. Integration of AI with blockchain for transparent tracking of oil movement and supply chain security. By addressing these objectives, AI has the potential to revolutionize oil security, reduce economic losses, and enhance environmental protection.

II. LITERATURE REVIEW

2.1 Overview of Oil Theft and Bunkering Trends [1, 2 and 4]

Oil bunkering is a broad term that encompasses both legal and illegal activities related to the transportation, storage, and siphoning of crude oil and refined petroleum products. While legal bunkering refers to the legitimate refueling of vessels at sea, illegal bunkering involves unauthorized tapping of oil pipelines, illegal ship-to-ship transfers, and the operation of unregistered refineries. The scope of illegal oil theft varies by region and method. These include; Pipeline siphoning: Criminal networks tap into pipelines to extract crude oil, which is then transported to hidden storage facilities or illegal refineries. Oil smuggling: Stolen crude or refined products are transported across borders, often disguised as legitimate shipments. Corrupt refining and distribution: In some cases, stolen oil is refined in makeshift facilities before being reintroduced into the market through black-market channels. Oil theft is a global challenge, with varying trends based on geography, economic conditions, and regulatory frameworks.

2.1.1 Case Study: Oil Theft in Nigeria [1, 5, 13, 32]

Nigeria, as Africa's largest oil producer, faces one of the highest rates of oil theft. The Nigerian National Petroleum Corporation (NNPC) estimates that over 400,000 barrels per day (bpd) are lost to theft, amounting to billions of dollars in annual revenue loss. Key drivers of oil theft in Nigeria include: Political instability: Militants in the Niger Delta have historically used oil theft as a form of economic protest. Corruption: Some government officials and security personnel are complicit in illegal bunkering operations. Lack of technological oversight: Traditional surveillance methods have failed to detect sophisticated theft techniques. An Anambra study also showed that AI-based security systems resulted in a 25% reduction in theft, a 30% decrease in vandalism, and a 20% drop in sabotage [32].

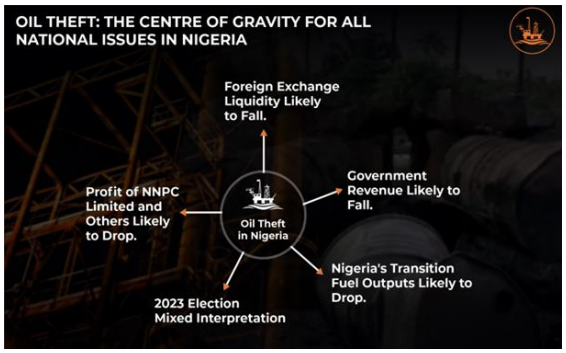

Figure 1: Oil theft as the cemter of gravity for all national issues in Nigeria [14].

2.1.2. Case Study: Mexico's Oil Theft Crisis [15, 16]

Mexico's state-owned oil company, PEMEX, has faced increasing losses due to fuel theft, locally referred to as "huachicolero" activities. Criminal groups drill illegal taps into pipeline networks, siphoning off gasoline and diesel for resale. The Mexican government has implemented military crackdowns, but corruption within the industry hampers efforts to eliminate theft. Oil Smuggling in Venezuela and Libya - In Venezuela, the collapse of the oil industry has led to increased fuel smuggling, often with government insiders involved. Libya, with its fragmented political landscape, sees illegal oil exports controlled by warlords and armed militias.

2.2 Existing Technologies for Oil Theft Detection [17, 18]

Historically, using Traditional Security Measures, oil companies and governments have relied on physical security, surveillance cameras, and manual monitoring to prevent oil theft. Surveillance Patrols involves Security teams regularly inspecting pipelines and storage facilities. However, these efforts are often compromised due to insider collusion and logistical challenges in monitoring vast oil networks. Basic Sensor-Based Monitoring where some pipelines have been equipped with pressure sensors to detect sudden

leaks, but slow siphoning techniques often bypass these detection systems. Satellite and Aerial Surveillance - while satellite imagery has been used to detect illegal ship-to-ship transfers and large-scale oil spills, real-time monitoring is expensive and requires significant human interpretation. Limitations of Conventional Detection Methods include; Delayed Response Times - Oil theft is often discovered after significant losses have already occurred. False Alarms - Traditional leak detection systems sometimes trigger false positives due to natural fluctuations in pressure and flow rates. Inadequate Coverage - Remote pipeline locations make it difficult to maintain continuous monitoring.

2.3 AI Applications in Oil and Gas Security [19, 20]

Machine Learning for Anomaly Detection in Pipelines - Machine learning (ML) models can analyze vast amounts of pipeline flow data to identify unusual patterns that indicate possible theft. Supervised Learning Models: AI algorithms trained on historical pipeline data can recognize typical operational behaviors and flag anomalies in real time. Unsupervised Learning Models: These models can identify theft patterns without pre-labeled data, making them useful for detecting previously unknown methods of oil siphoning. Neural Networks for Pattern Recognition: Deep learning techniques can differentiate between natural fluctuations and illicit activities, reducing false positives. Real-World Example include; Saudi Aramco has integrated AI-driven leak detection systems to reduce oil theft by identifying irregular flow patterns in real time. Computer Vision for Surveillance and Threat Detection - Computer vision, powered by AI, enhances surveillance capabilities by: Analyzing real-time footage from CCTV cameras and drones to detect unauthorized activities, Recognizing suspicious behavior, such as masked individuals near pipelines or tankers parked in restricted areas, Using facial recognition technology to identify known criminals involved in oil theft. AI-Powered Drone Surveillance - Autonomous drones equipped with AI algorithms can patrol pipeline routes and offshore facilities. Thermal imaging cameras detect nighttime theft attempts, which are typically hard to spot with traditional surveillance. AI and IoT for Smart Pipeline Monitoring - The integration of AI and the Internet of Things (IoT) allows for real-time pipeline security. Smart Sensors: AI-driven IoT sensors continuously monitor oil pressure, temperature, and flow rate to detect irregularities. Automated Alerts: When an anomaly is detected, AI systems can send real-time alerts to security teams, enabling faster intervention. Case Study: BP's Smart Pipeline Network - BP has implemented AI-integrated IoT solutions to track oil movement and prevent siphoning along key pipelines. AI-Powered Blockchain for Supply Chain Security - Blockchain, combined with AI, provides an immutable record of oil transactions, preventing fraudulent activities. AI analyzes blockchain data for anomalies, detecting irregular shipping patterns or inconsistencies in oil movement logs. Tamper-proof transaction records ensure that stolen oil cannot be easily laundered into the legal supply chain.

2.4 Challenges and Limitations of AI in Oil Theft Detection [21]

Despite its potential, AI implementation in oil theft prevention faces several challenges such as High Implementation Costs - AI-powered monitoring systems require substantial investment in hardware (sensors, cameras, drones) and software. Many oil-producing nations, especially in Africa and Latin America, lack the budget for full-scale AI deployment. Cybersecurity Risks - AI-based security systems are vulnerable to cyberattacks, where hackers can manipulate data to conceal theft activities. Blockchain vulnerabilities, such as 51% attacks, pose risks to oil supply chain transparency. Need for Regulatory Frameworks - Governments and oil companies need to establish data privacy laws and AI governance policies to regulate AI applications in security. Ethical concerns surrounding AI-powered surveillance, especially facial recognition, require legal scrutiny.

Table 1.0 : Comparism between the findings of relevant literatures

Papers (10)	Objectives	Results	Findings	Practical Implications
[22]	Analyze energy theft methods Propose AI solutions for detection	Overview of energy theft methods and AI detection challenges. Emphasis on need for further research in detection systems.	Overview of energy theft methods and AI detection challenges. AI methods can enhance energy theft detection effectiveness.	AI methods can enhance energy theft detection efficiency. Integration with smart meters improves detection systems.
[23]	Explore machine learning in detecting anomalous contracts. Identify key research and challenges in the field.	Identified key research and challenges in ML applications. Highlighted significant contributors in contract anomaly detection.	Machine learning detects anomalous contracts in oil and gas. Key contributors include China, Indonesia, and major universities.	Enhances contract audits for market stability and transparency. Promotes machine learning for fraud detection and risk mitigation.
[24]	Develop a method to extract bunkering operations quantitatively. Analyze and compare bunkering operations across three port areas.	Variations in vessel types and service times observed. Tokyo Bay has shorter service times for certain vessels.	Variations in vessel types and service times observed. Tokyo Bay has shorter service times for certain vessels.	Develops quantitative methods for analyzing bunkering operations. Compares bunkering characteristics across different port areas.
[25]	Review AI applications for safety and reliability. Analyze Machine Learning techniques for fault detection and diagnosis.	Analyzed 308 papers on AI for safety and reliability. Highlighted challenges and future directions for improvement.	308 papers analyzed, mostly using supervised learning frameworks. Highlights challenges like data availability and trust issues.	Highlights potential for improved operational safety in industrial plants. Discusses challenges like data quality and interdisciplinary collaboration.
[26]	Identify irregularities and anomalies in electricity consumption. Showcase AI algorithms' effectiveness in detecting non-technical losses.	ANN identifies consumer types with 7.62% frequency error. K-means and ANFIS show higher frequency errors of 9.26% and 11.11%.	AI algorithms effectively identify non-technical losses and energy theft. ANN shows 7.62% frequency error in consumer type identification.	AI enhances detection of energy theft and irregularities. Smart meter data improves distribution network security.
[27]	Remove biases from geo-spatial trajectories using AIS.	Two methods reduce biases in geo-spatial trajectories.	Two methods remove biases from AIS geo-spatial trajectories.	Improved behavior detection from AIS data. Enhanced machine learning model

	Enable behavior detection like moored, underway, or drifting.	Comparison of machine learning models for behavior detection.	Behavior detection models include random forests and LSTMs.	generalization in untrained areas.
[28]	Enhance safety and security in oil and gas pipelines. Implement a lightweight IIoT system for data transmission.	N/A	Proposed a secure OGP transportation system using IIoT architecture. Validated security objectives and demonstrated efficiency in computational costs.	Enhances safety and security in oil and gas transportation. Reduces operational costs and improves asset efficiency.
[29]	Review ETD methods and dataset limitations. Discuss generative AI potential in enhancing ETD robustness.	N/A	Review of energy theft detection methodologies and limitations. Emphasis on generative AI for dataset enhancement and ETD robustness.	Highlights limitations of current energy theft datasets. Emphasizes generative AI's potential in enhancing ETD robustness.
[30]	Ensure ship safety using AI and 5G technology. Protect vessels from risky zones with geofencing.	The network security approach of this paper surpasses other studies. The suggested approach ensures AIS network security and vessel safety.	Network security approach surpasses other studies in performance analysis. Geofencing technology effectively protects vessels from risky zones.	Enhances vessel safety through AI and 5G technology. Implements geofencing to avoid risky sailing zones.
[31]	Detect and prevent supply chain fraud using ML and AI. Analyze dataset to identify consumer-based fraud in supply chain.	Top-performing algorithms: AI sequential, CatBoost Top features: delivery status, payment type, late delivery risks	ML and AI effectively detect supply chain fraud. Top features include delivery status and payment type.	Enhancing fraud detection in supply chains using ML and AI. Importance of human oversight in interpreting technology-generated results.

III. DISCUSSION

3.1 The Need for AI-Driven Solutions in Oil Theft Prevention

Oil theft has evolved into a sophisticated industry, with criminal networks employing advanced techniques to bypass traditional security measures. The limitations of manual patrols, CCTV monitoring, and basic sensor-based leak detection have necessitated the adoption of Artificial Intelligence (AI) to enhance security, improve real-time detection, and minimize losses. Key Drivers for AI Adoption include Increased Oil Theft Losses: Countries like Nigeria, Mexico, and Venezuela lose billions of dollars annually due to oil theft, Ineffectiveness of Conventional Security Measures: Security forces and basic surveillance fail to detect slow siphoning techniques and insider fraud, Advancements in AI and IoT: The rise of machine learning, computer vision, and blockchain technology enables real-time threat

detection, Integration with Existing Infrastructure: AI-based solutions can be integrated with legacy security systems to enhance surveillance and threat response.

3.2 AI-Based Solutions for Combating Oil Theft

Machine Learning for Real-Time Anomaly Detection - Machine learning (ML) algorithms can analyze vast amounts of pipeline data to detect anomalous behaviors associated with oil theft. These include Pressure drops caused by siphoning, Sudden changes in oil flow rates, Unusual transportation patterns in oil tankers. Types of ML Models Used such as Supervised Learning Models: Trained on historical oil flow data, these models identify known theft patterns. Unsupervised Learning Models: These detect new and previously unknown theft techniques by recognizing deviations from normal pipeline behavior. Reinforcement Learning: AI systems learn from past theft incidents to continuously improve detection accuracy. Case Study: AI Deployment in Saudi Aramco - Saudi Aramco implemented AI-based leak detection systems that use predictive analytics to identify potential theft zones before actual siphoning occurs. AI-Powered Computer Vision for Surveillance - Computer vision enhances real-time monitoring by: Analyzing live CCTV footage to detect unauthorized access, Using facial recognition to identify known criminals and Deploying drones with AI-enhanced vision to monitor remote pipelines. AI-Powered Surveillance works by Object Recognition - AI detects suspicious movements near pipelines, Facial Recognition: Identifies individuals with prior oil theft records, License Plate Recognition (LPR): Tracks unauthorized vehicles near oil facilities.Case Study include AI Surveillance in Mexico's PEMEX Facilities - PEMEX adopted AI-integrated security cameras with motion tracking and anomaly detection, significantly reducing fuel theft in high-risk areas. AI and IoT-Enabled Smart Pipeline Monitoring - The Internet of Things (IoT) allows oil companies to deploy smart sensors along pipelines, feeding real-time data to AI systems for monitoring. Key IoT Technologies Used include Acoustic Sensors: Detect illegal pipeline tapping, Pressure and Flow Sensors: Identify unauthorized extraction points, Geospatial IoT: Tracks oil movement in real time to detect diversions. Case Study include BP's AI-Driven Smart Pipeline Monitoring - BP uses AI-powered IoT solutions that integrate sensor networks with machine learning to detect pipeline intrusions before significant theft occurs, AI-Integrated Blockchain for Oil Supply Chain Security. AI combined with blockchain technology enhances transparency by recording all oil transactions on an immutable ledger, tracking oil movement to prevent laundering of stolen crude, using AI to analyze blockchain data for suspicious activities. Case Study include Blockchain Implementation in Shell's Oil Tracking System - Shell deployed AI-enhanced blockchain networks to verify the legitimacy of oil shipments, reducing fraudulent documentation.

Table 2.0. Comparative Analysis of AI-Based Oil Theft Prevention Methods

AI Solution	Strengths	Weaknesses
Machine Learning (ML) for Anomaly Detection	- Detects unusual pipeline activity in real-time - Reduces false alarms compared to traditional sensors	- Requires high-quality training data - High computational cost
Computer Vision for Surveillance	- Monitors large areas with AI-driven cameras - Drones cover remote locations	- AI models can be fooled by disguises - Privacy concerns regarding facial recognition
IoT-Based Smart Pipelines	- Continuous monitoring without human intervention - Reduces need for manual inspections	- Expensive to deploy on a large scale - Vulnerable to sensor tampering
AI-Blockchain Integration	- Provides tamper-proof tracking of oil transactions - Enhances supply chain security	- Blockchain networks require extensive adoption to be effective

3.3 Challenges in Implementing AI for Oil Theft Prevention

These include; High Implementation Costs - AI-based security solutions require significant financial investment, making them less accessible for developing nations. Cybersecurity Vulnerabilities - Hackers can manipulate AI data to disguise theft activities, Blockchain systems can suffer from smart contract vulnerabilities. Lack of AI Regulations in Oil Security - Governments must create legal frameworks to ensure ethical AI usage. Privacy concerns over AI-powered facial recognition need regulation.

3.4 Future Directions for AI in Oil Theft Prevention

AI-Powered Predictive Analytics for Theft Prevention - Future AI models will predict oil theft patterns before they occur, allowing for proactive interventions. Autonomous Drones for Continuous AI Surveillance - AI-powered drones will be able to track oil thieves in real time and relay intelligence to law enforcement. AI-Driven Smart Contracts for Automated Oil Transactions - Blockchain-based smart contracts will ensure only verified oil shipments are processed, reducing fraud.

IV. CONCLUSION

4.1 Summary of Key Findings

The implementation of Artificial Intelligence (AI) in oil bunkering and theft prevention has emerged as a transformative approach, significantly enhancing the security and monitoring of oil infrastructure. This review has explored the current landscape of oil theft, the limitations of traditional security measures, and the cutting-edge AI technologies being deployed to mitigate illegal activities in the oil and gas industry.Oil theft remains a global crisis, affecting both developing and developed nations. In Nigeria, over 400,000 barrels per day (bpd) are lost to theft, resulting in billions of dollars in annual revenue loss. Mexico's PEMEX suffers from widespread pipeline siphoning by organized crime networks.Venezuela and Libya face smuggling and illicit refining issues, fueled by political instability. Limitations of Traditional Oil Theft Prevention Methods include Ineffective Physical surveillance - Armed patrols are often compromised by insider collusion and logistical challenges. CCTV monitoring has blind spots: Criminals exploit poorly monitored sections of oil infrastructure. Basic pressure sensors fail to detect slow siphoning: Theft techniques have evolved, making traditional leak detection unreliable. AI-Based Solutions for Oil Theft Prevention include Machine Learning (ML) for anomaly detection - AI models analyze real-time oil flow data to detect irregularities linked to theft. Computer Vision for AI-powered surveillance: AI-driven CCTV and drone-based monitoring enhance detection in high-risk areas. IoT and Smart Pipelines - AI-integrated sensors continuously track oil movement, alerting authorities to unauthorized access. AI-Blockchain integration: Blockchain ensures tamper-proof transaction records, making it harder to launder stolen oil. Studies have proven that AI-based security systems resulted in a 25% reduction in theft, a 30% decrease in vandalism, and a 20% drop in sabotage. Hence, it is the future.

4.2 Policy and Strategic Recommendations

For AI to be effectively implemented in combating oil theft, governments, oil companies, and regulatory bodies must collaborate on policy frameworks and technological advancements by Strengthening AI Integration in National Security Strategies - Governments should prioritize AI adoption in oil security policies, AI-driven oil theft prevention should be integrated into law enforcement operations, Public-private partnerships (PPP) should be encouraged to fund AI-powered security systems, Cybersecurity Measures for AI-Based Systems, AI security frameworks must be established to prevent cyberattacks on oil surveillance networks. Blockchain-based oil tracking systems must include multi-factor authentication and encrypted transaction protocols. AI security algorithms should be regularly updated to counter evolving hacking techniques. Regulatory Frameworks for AI-Based Surveillance and Data Privacy - Governments must introduce legislation governing AI-powered surveillance, ensuring that facial recognition systems do not violate human rights. Strict data privacy laws should be enacted to protect oil companies and individuals from AI surveillance misuse. AI-Powered International Collaboration to Combat Oil Theft - Oil theft is a transnational issue, requiring cooperation between nations, security agencies, and technology firms. Oil-producing countries must share AI-driven intelligence on illegal bunkering trends. Interpol and energy

security organizations should develop an AI-powered global oil theft monitoring network.

4.3 Future Research Directions

These include; Enhancing AI Algorithms for Proactive Theft Prevention - Future research should focus on: Predictive AI models that forecast oil theft trends based on historical data, AI-driven criminal behavior analysis, identifying patterns in oil theft networks, Self-learning AI algorithms that continuously evolve to detect new siphoning methods. Autonomous AI Drones for 24/7 Surveillance - Drones equipped with AI-powered motion detection and thermal imaging can which can detect oil theft in real time, even in remote areas, reduce reliance on human surveillance teams, provide high-resolution evidence for law enforcement agencies. AI and Blockchain for Smart Oil Contracts, AI-driven smart contracts on blockchain networks can prevent fraudulent transactions. Automated verification systems ensure that only legally extracted oil enters global supply chains. AI-based fraud detection can analyze blockchain for irregular oil shipment patterns. AI-Enhanced Underwater Monitoring for Offshore Oil Theft - Underwater AI robots can monitor oil theft from subsea pipelines. AI-powered sonar technology can detect illegal pipeline tapping in deep-sea environments. Oil companies should invest in AI-driven underwater surveillance drones.

4.4 Ethical and Societal Considerations

As AI plays an increasing role in oil theft prevention, ethical concerns must be addressed. These concerns include; Ethical Use of AI-Powered Surveillance - AI must not be used for mass surveillance beyond oil security. Governments should create ethical guidelines for AI monitoring. Public awareness campaigns should educate communities on AI surveillance benefits and risks. Addressing AI Bias and False Positives - AI algorithms must be trained on diverse datasets to avoid bias in threat detection. AI systems should have human oversight to reduce wrongful accusations. Continuous AI model updates will enhance accuracy and minimize errors. The Impact of AI on Employment in Oil Security include AI-driven automation may reduce jobs in manual security monitoring. Governments should train security personnel in AI-based systems to prevent job losses. AI implementation should be gradual, allowing for workforce adaptation.

4.5 Final Thoughts

This review has demonstrated that AI is revolutionizing oil theft prevention through machine learning, IoT, computer vision, and blockchain technology. However, successful AI deployment requires multi-stakeholder collaboration, regulatory oversight, and continuous technological advancements. Key Takeaways - AI provides a transformative solution to oil theft but requires large-scale investment, Cybersecurity and regulatory frameworks are crucial for AI-powered security systems, Future AI advancements, including predictive analytics and autonomous drones, will shape oil theft prevention. Call to Action: Governments, oil companies, and AI researchers must accelerate AI adoption to prevent billions of dollars in annual oil losses. Through strategic investments and ethical AI deployment, oil-producing nations can safeguard their resources and enhance global energy security.

REFERENCES

[1] Romsom, E. (2022). Global oil theft: impact and policy responses. UNU-WIDER Working Paper, 16, 147-1.

[2] Eaton, T. (2021). Theft and smuggling of petroleum products. In The Routledge Handbook of Smuggling (pp. 260-271). Routledge.

[3] Balogun, W. A., & Adesanya, O. P. (2022). “A Sea of Troubles”: Oil Theft, Crude Economy and the Business of Organised Energy Crime in the Gulf of Guinea. African Journal of Stability and Development (AJSD), 14(1&2), 1-36.

[4] Watts, M. J. (2021). Hyper-extractivism and the global oil assemblage. Our extractive age: Expressions of violence and resistance, 207-248.

[5] Ailemen, A. (2024, June 16). Nigeria losing 400,000 barrels of crude oil daily — Nextier. BusinessDay. https://businessday.ng/news/article/nigeria-losing-400000-barrels-of-crude-oil-daily-nextier/

[6] AnotherDay. (2023, September 5). The fuel theft epidemic and its consequences in Mexico.

AnotherDay. https://www.another-day.com/resources/the-fuel-theft-epidemic-and-its-consequences-in-mexico

[7] Venezuela Investigative Unit. (2022, February 2). The smuggler's dilemma – Black market oil from Venezuela or Colombia. InSight Crime. https://insightcrime.org/news/smugglers-dilemma-black-market-oil-from-venezuela-or-colombia/

[8] Onuh, P. A., Omenma, T. J., Onyishi, C. J., Udeogu, C. U., Nkalu, N. C., & Iwuoha, V. O. (2021). Artisanal refining of crude oil in the Niger Delta: A challenge to clean-up and remediation in Ogoniland. Local Economy, 36(6), 468-486.

[9] Nte, N. D., Enoke, B. K., & Abubakar, I. (2022). Technical intelligence and security management within the Nigerian territorial waters: The Nigerian navy challenge. Unnes Law Journal, 8(1), 179-206.

[10] Selvam, A. P., & Al-Humairi, S. N. S. (2023). The impact of iot and sensor integration on real-time weather monitoring systems: A systematic review.

[11] Ekeu-wei, B. F., & Ekeu-wei, I. T. (2024). Crude Oil Spillage in the Niger Delta-Causes, Impact and Detection Approaches.

[12] Martin, A., & Smith, B. (2022). A New AI-Driven Risk Assessment Tool for Investigating Insider Theft and Associated Maritime Crimes in a Southeast Asian Energy Company—A Case Study. International Journal of Maritime Crime & Security, 2(02).

[13] Romsom, E. (2022). Countering global oil theft: Responses and solutions. United Nations University World Institute for Development Economics Research.

[14] Proshare. (2022, September 12). The anatomy of crude oil theft in Nigeria: Understanding the graft, impact, and implications. Proshare. https://proshare.co/articles/the-anatomy-of-crude-oil-theft-in-nigeria-understanding-the-graft-impact-and-implications

[15] Vivoda, V., Krame, G., & Spraggon, M. (2023). Oil theft, energy security and energy transition in Mexico. Resources, 12(2), 30.

[16] Starr, S. (2022). AMLO and Huachicoleo: The Effects and Implications of the Fuel Theft Crackdown in Mexico.

[17] Dada, K. S. J., & Akila, J. (2021). The utilization of unmanned aerial vehicles incombating illegal bunkering activities in the Niger Delta regions of Nigeria. Journal of Advances in Military Studies, 4(1), 101-126.

[18] Mohammed, A., & Ahmed, A. (2024). EFFECTS OF CRUDE OIL VANDALISM ON CRUDE OIL TERMINALS INNIGERIA: 1999-2020. IDENTITY, SOCIAL INCLUSION AND SUSTAINABLE DEVELOPMENT IN NIGERIA, 669.

[19] Okon, E. N., Ojakorotu, V., & Iwara, I. E. (2024). Criminal Entrepreneurs and the Security Crisis in African Sahel. Journal of Somali Studies: Research on Somalia and the Greater Horn of African Countries, 11(2), 27-48.

[20] Ekeu-wei, B. F., & Ekeu-wei, I. T. (2024). Crude Oil Spillage in the Niger Delta-Causes, Impact and Detection Approaches.

[21] Kwari, Hussaini, Using Artificial Intelligence to Combat Oil Theft in Nigeria (March 21, 2023). Available at SSRN: https://ssrn.com/abstract=4395954 or http://dx.doi.org/10.2139/ssrn.4395954

[22] Stracqualursi, E., Rosato, A., Di Lorenzo, G., Panella, M., & Araneo, R. (2023). Systematic review of energy theft practices and autonomous detection through artificial intelligence methods. Renewable & Sustainable Energy Reviews. https://doi.org/10.1016/j.rser.2023.113544

[23] Palacio, L., Guzmán-Luna, J. A., & Restrepo-Carmona, J. A. (2024). Bibliometric Analysis of Intelligent Systems for Early Anomaly Detection in Oil and Gas Contracts: Exploring Recent Progress and Challenges. Sustainability, 16(11), 4669. https://doi.org/10.3390/su16114669

[24] Watanabe, E., & Shibasaki, R. (2023). Extraction of Bunkering Services from Automatic Identification System Data and Their International Comparisons. Sustainability. https://doi.org/10.3390/su152416711

[25] Tamascelli, N., Campari, A., Parhizkar, T., & Paltrinieri, N. (2024). Artificial Intelligence for Safety and Reliability: A Descriptive,

Bibliometric and Interpretative Review on Machine Learning. Journal of Loss Prevention in The Process Industries. https://doi.org/10.1016/j.jlp.2024.105343

[26] Žarković, M., & Dobrić, G. (2024). Artificial Intelligence for Energy Theft Detection in Distribution Networks. Energies, 17(7), 1580. https://doi.org/10.3390/en17071580

[27] Sturgis, R., Emiya, V., Couetoux, B., & Garreau, P. (2024). Beyond geofencing: Behavior detection using AIS. Ocean Engineering. https://doi.org/10.1016/j.oceaneng.2023.116630

[28] Dutt, R., Sharma, R. K., & Villanyi, B. (n.d.). Safe and secure oil and gas pipeline transportation system based on Industrial Internet of Things. IEEE Sensors Journal. https://doi.org/10.1109/jsen.2024.3353595

[29] Kim, S. H., Sun, Y. G., Lee, S., Seon, J., Hwang, B.-S., Kim, J., Kim, J., Kim, K., & Kim, J. (2024). Data-Driven Approaches for Energy Theft Detection: A Comprehensive Review. Energies, 17(12), 3057. https://doi.org/10.3390/en17123057

[30] Chen, M. Y., & Wu, H.-T. (2023). An Automatic-Identification-System-Based Vessel Security System. IEEE Transactions on Industrial Informatics, 19, 870–879. https://doi.org/10.1109/TII.2021.3139348

[31] Lokanan, M., & Maddhesia, V. (2024). Supply chain fraud prediction with machine learning and artificial intelligence. International Journal of Production Research, 1–28. https://doi.org/10.1080/00207543.2024.2361434