ABUAD Journal of Engineering Research and Development (AJERD)
ISSN (online): 2645-2685; ISSN (print): 2756-6811

Volume 8, Issue 1, 140-150

Investigation of Cybersecurity Vulnerabilities and Mitigation Strategies in Nigeria's Oil and Gas Industry

Christopher Ubaka EBELOGU, Rajesh PRASAD, Hashim Ibrahim BISALLAH, Baba Mohammed HAMMAWA, Israel MUSA

Department of Computer Science, University of Abuja, Abuja, Nigeria
christopher@uniabuja.edu.ng/prasad@aust.edu.ng/mbhammawa@uniabuja.edu.ng/hashim.bisallah@uniabuja.edu.ng/israelmusa9@gmail.com

Corresponding Author: christopher@uniabuja.edu.ng, +2348039394866
Date Submitted: 14/11/2024
Date Accepted: 22/02/2025
Date Published: 23/02/2025

Abstract*: As Africa's largest oil producer, Nigeria heavily relies on its Oil & Gas (O&G) sector, which significantly contributes to the nation's GDP, export profits, and government revenue. However, this sector faces substantial challenges due to its susceptibility to cyberattacks, which exploit the vast amounts of sensitive data generated across its operations. These threats have become more prominent with the integration of digital technologies, increasing the sector's vulnerability. Despite efforts like the Nigerian Data Protection Regulation, cyber incidents like ransomware and Advanced Persistent Threats (APTs) continue targeting critical infrastructure, leading to severe financial, operational, and environmental impacts. The rising frequency of such attacks highlights the urgent need for enhanced cybersecurity measures within Nigeria's O&G industry. This study aims to investigate the cybersecurity landscape in the sector, focusing on identifying prevalent cyber threats and assessing the effectiveness of current control measures. Through systematically analyzing existing research and data, the study seeks to provide insights into the evolution of cyber threats and propose strategies for strengthening the sector's cybersecurity posture.*

Keywords: *Cybersecurity, Nigerian O & G Sector, Information Security, Cyber Threats, Advanced Persistent Threats (APTs), Vulnerabilitie*

1. INTRODUCTION

Nigeria is the largest oil producer in Africa and ranks among the top 10 globally [1]. The Oil & Gas (O &G) sector has served as the major driver of Nigeria's economy, since the discovery of crude oil in commercial quantity in Oloibiri in present-day Bayelsa State in the year 1956 [2]. It plays a major role in the country's income, contributing considerably to its Gross Domestic Product (GDP), export profits, and government revenue [3]. Over 70% of Nigerian government revenue and more than 90% of foreign exchange gains are generated by the O & G Sector [4]. However, this sector grapples with security breaches; given the tones of data generated within a short period from the upstream, midstream, and downstream operations, coupled with the sensitive nature of these data, it is a hotspot for cyber attackers [5]. Information security is described by Microsoft InfoSec [6], as an assortment of security practices and instruments used to safeguard sensitive business data against exploitation, illegal access, interruption, or destruction. InfoSec, taken broadly, includes cybersecurity, control over access, and environmental and physical security. This implies that attempts at information breaches, such as social engineering, could occur even without technology [7].

In 2019, it was reported that the Nigerian Data Protection Regulation would take effect in 2020. This regulation shares similarities with the GDPR introduced in Europe in 2018, and it has not been properly discussed from a regulation perspective in the Nigerian O and G sectors. With the COVID-19 pandemic, many businesses in the O and G sectors migrate to remote work. However, Nigeria has been facing a 90% increase in cybercrime since the start of the pandemic. This has caused severe strain on the cybersecurity ecosystem, and as of now, Nigeria only has an estimated 50,000 professionals in the cybersecurity field. There is a large need for more efficient tactics in dealing with information security threats [8].

According to the analysis of the industry watchdog of THISDAY, the billions of Naira paid to Non-state Actors by the Nigerian Upstream Petroleum Regulatory Commission (NUPRC), to enhance security outfits, did not yield desirable results [9]. The issue of cyber-attack is not peculiar to the Nigerian O & G sector, a report released by Tenable, cited 32 cybersecurity incidents in the global O & G sector in the year 2022. The oil business ranks as the tenth most susceptible industry to cybersecurity risks out of the 29 industries covered in the report [10]. Cybercriminals have found this industry to be a lucrative target in recent years [11]. There are several different causes for this. First off, cybercriminals looking to profit from extortion, theft, or sabotage find the industry profitable due to its high-value assets and vital infrastructure [12]. Secondly, the attack surface has grown due to incorporating sophisticated digital technologies into operational procedures [13]. This has made it simpler for hackers to identify weaknesses to take advantage of.

Cyberattacks have far-reaching and complex effects on Nigeria's O & G industry. These assaults have the potential to cause large financial losses due to money theft, intellectual property theft, and company interruptions [14]. Catastrophic environmental effects are possible, particularly if cyberattacks target operational controls and result in explosions or oil spills that harm ecosystems over time. The chain of energy supply vulnerabilities is demonstrated in Figure 1. The diagram shows the crucial locations vulnerable to sabotage.

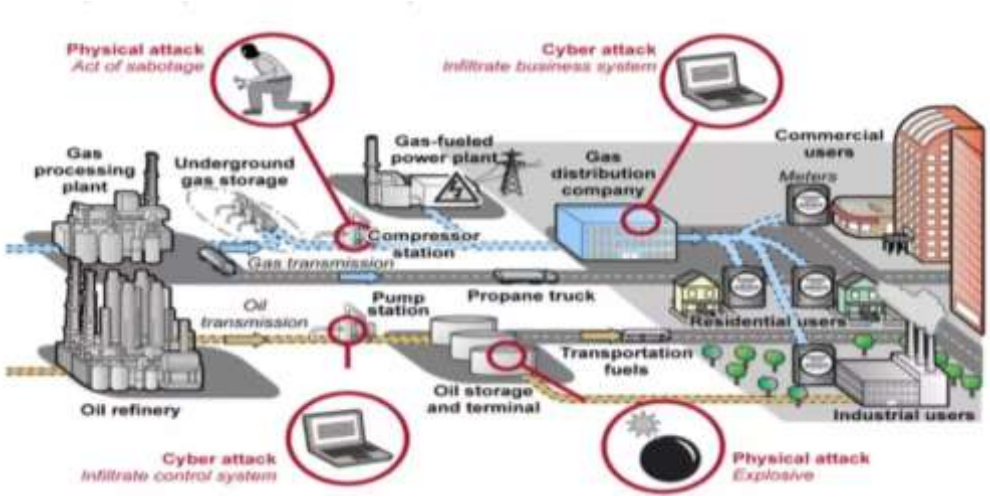

Figure 1: Vulnerabilities in the Energy Supply Chain (U.S. Government Accountability Office, 2020)

Therefore, to keep ahead of these risks, Nigeria's O & G industry must implement cutting-edge management systems and consistently improve its cybersecurity posture [15]. In a bid to mitigate the security challenges, this study aims to investigate and summarize the body of knowledge on cyber threats in Nigeria's O & G industry. The study collects Data on information security breaches, including event logs in the Nigerian O &G sector to identify the most predominant types of attacks, and systems or departments that are more vulnerable.

Summarily, this study offers a detailed survey of the currently existing cyber threats in the Nigerian O&G industry cyber threats, their nature, sources, impacts, and also cybersecurity mitigation techniques implemented currently. Further, it makes suggestions to improve their cybersecurity resilience. The study also identifies international best practices that can be tailored to suit Nigeria's digital and industrial environment. This research provides a systematic view of cyber risks to assist policymakers, practitioners, and cybersecurity experts in reinforcing the active defenses of the sector against emerging cyber threats.

2. RELATED WORKS

Cybercriminals are using more advanced techniques, and the threat landscape is always changing [16]. Techniques including ransomware assaults, Advanced Persistent Threats (APTs), and insider threats are now being used in addition to traditional risks like malware and phishing [17]. Beyond conventional defenses, creative and flexible security solutions are needed to counter these dynamic threats. People and organizations continue to be extremely concerned about data breaches. A ransomware assault on software company Kaseya in July 2021 affected over a thousand firms [18]. In a separate incident, a data breach in August 2021 revealed the personal information of millions of T-Mobile customers. In March 2021, there was a notable breach in data security when hackers gained access to the personal information of over 533 million Facebook users [19]. The attackers took possession of names, phone numbers, and email addresses, among other data that may be used for phishing and other fraudulent activities. The incident demonstrated the significance of data privacy and the need for companies to protect customer information [18].

The report by BBC News [20] indicated that hackers demanded $50 million from Saudi Aramco after leaking company data from one of its contractors in the year 2021. Similarly, Saudi Aramco was attacked in the year 2012. The virus was employed to erase the contents of the hard drives and display an image of a burning American flag on the screens [21]. The attack was attributed to a group called “Cutting Sword of Justice,” which claimed political motives, highlighting the vulnerability of national infrastructure to politically motivated cyberattacks.

Just days after the attack on Saudi Aramco, RasGas, one of the world’s largest liquefied natural gas producers, was hit by a similar virus [22]. The attack took down the company’s website and email servers but did not affect production systems. Like the Aramco incident, it appeared designed more for disruption than financial gain, emphasizing the geopolitical risks in cybersecurity.

A ransomware attack caused Colonial Pipeline to shut down approximately 5,500 miles of pipeline, leading to a significant disruption of fuel distribution across the East Coast of the United States [21]. The FBI attributed the attack to the DarkSide ransomware group, which is believed to be based in Eastern Europe. The rapid payment of the $4.4 million ransom underscored the critical nature of operational uptime in this sector.

The attack at Norsk Hydro 2019 utilized the LockerGoga ransomware, which locked out users and encrypted files across 170 sites in 40 different countries [23]. Norsk Hydro's transparent response to the attack, including regular press briefings and choosing not to pay the ransom, was widely praised and is often cited as a model for handling ransomware incidents.
Similarly, a ransomware attack on Pemex in the year 2019 locked out employees and froze systems, aiming to disrupt oil production [24].

Shell data breach in the year 2021 was part of a global campaign exploiting vulnerabilities in the Accellion FTA server [21]. Sensitive data stolen included business documents and personal information. The incident highlighted the risks associated with third-party services in cybersecurity frameworks.
An attack on Energy Transfer Partners (ETP) in the year 2018 targeted a third-party communications system used by ETP for transporting natural gas and propane [25].

3. METHODOLOGY

The methodology employed in this research study involved a systematic and comprehensive approach to identify, analyze, and synthesize relevant research on cybersecurity in the Nigerian O & G sector. The process was designed to ensure the inclusion of high-quality and pertinent sources, providing a robust foundation for understanding the current landscape of cyber threats and the effectiveness of control measures. To gather the necessary data, a multi-step search strategy was employed:

3.1. Database Selection

1. Academic databases: Key academic databases such as IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar were utilized to find scholarly articles and conference papers.
2. Industry reports: Repositories of major Nigerian O & G sector stakeholders such as the Government Entities, International Oil Companies (IOCs), National Oil Companies (NOCs), and industry associations were consulted for industry reports and local newspapers.

3.2. Keyword Identification

Keywords were chosen based on their relevance to the study's objectives. These included "cybersecurity," "O & G," "Nigeria," "control measures," and "cyber-attacks." Boolean operators (AND, OR) were used to combine keywords and refine the search queries. For example, "cybersecurity AND O & G AND Nigeria" or "cyber-attacks OR control measures AND Nigerian oil sector."

3.3. Inclusion and Exclusion Criteria

1. Inclusion criteria: Sources were included if they were published within the last decade (2014-2024), focused on cybersecurity in the O & G sector, and had a specific emphasis on Nigerian operations or provided applicable insights.
2. Exclusion criteria: Sources were excluded if they were not available in English and the sources that did not address the O & G sector directly.

3.4. Collection and Analysis

1. Initial screening: Titles and abstracts of identified sources were reviewed to determine their relevance. This initial screening helped in filtering out irrelevant studies quickly.
2. Full-text review: Full texts of the selected articles and reports were then reviewed comprehensively. Notes were taken on key findings, methodologies used, types of cyber threats discussed, and control measures proposed or evaluated.

3.5. Data Extraction

A data extraction form was developed to systematically collect information from the reviewed sources. Key data points included: Type of Cyber Threat includes; Phishing, malware, ransomware, APTs, and insider threats.

3.5.1. Impact on the sector: Financial losses, operational disruptions, environmental damage, and national security threats.

3.5.2. Control measures: Traditional measures like firewalls and IDS, emerging technologies like AI and blockchain, and specific case studies demonstrating successful implementations.

3.5.3. Geographic relevance: Specific focus on Nigerian operations and any comparative analysis with other regions.

3.5.4. Synthesis of findings: The extracted data were synthesized to identify common themes, trends, and gaps in the existing literature. This synthesis helped in forming a coherent narrative on the evolution of cyber threats and the effectiveness of control measures in the Nigerian O & G sector.

3.5.5. Critical appraisal: Each source was critically appraised for its methodological rigor, relevance, and contribution to the field. Sources were evaluated based on their study design, data validity, and reliability of findings.

3.5.6. Limitations: While efforts were made to be comprehensive, some relevant studies might have been missed due to language barriers or database access restrictions.

3.6. Key Attributes for Analyzing Cybersecurity in the Nigerian Oil & Gas Sector

To analyze the cybersecurity landscape in the Nigerian Oil & Gas sector, we focused on key attributes such as the types of cyber threats, including ransomware, Advanced Persistent Threats (APTs), phishing, and insider threats. Assess the impact of these threats, such as financial losses, operational disruptions, environmental damage, and national security risks. Evaluate the effectiveness of control measures like traditional security systems and emerging technologies, using case studies where applicable. Comparisons of different incidents, based on severity, frequency, and response effectiveness, alongside visual representations, will enhance understanding of the sector's cybersecurity challenges and solutions.

4. DISCUSSIONS AND ANALYSIS

4.1. Cyberthreat Landscape in the Nigerian O & G Sector

The report by Jaiyeola [26] stated that between January and September 2022, Nigeria experienced a significant number of industrial cyberattacks, with 38.7% of industrial control system (ICS) computers being targeted by various types of malicious objects. The O & G sector was the most affected, with 39.3% of its ICS computers coming under attack. Experts predict an increase in sophisticated Advanced Persistent Threat (APT) attacks and ransomware targeting critical industrial infrastructure through 2022 and into 2023.

ICS computers in Africa experienced an increase in malware attacks, with Nigeria at 32.6%, Kenya at 34.5%, and South Africa at 29.1% [26]. The energy sector, engineering and integration, and building automation were the most targeted, with all detected attacks successfully blocked. Jeremiah [27] reported 32 cyber-attacks, signifying the vulnerability of the oil sector.

Cyber risks to Nigeria's O & G industry are varied and constantly changing [14]. It is essential to comprehend these risks to create defensive plans that work. This section delves into the primary cyber-attack categories that target this vital sector, offering comprehensive insights into their mechanics and consequences.

Achunike & Egbuna [14] provided a foundational overview of network-related threats. They categorize network attacks into intrusions, web defacement, and Denial-of-Service (DoS) attacks. Furthermore, they identify network abuse issues such as phishing, forgery, and spam, which continue to challenge cybersecurity efforts. The study also highlights the prevalence of malicious codes, including viruses, worms, Trojan horses, spyware, key loggers, and BOTs. Importantly, they note the significant threat posed by corporate insiders who may misuse their access to sensitive information.

Obonna et al., [28] focused specifically on the Nigerian O & G sector, detailing various types of cyberattacks prevalent in this industry. They emphasize the occurrence of DoS attacks, Distributed Denial-of-Service (DDoS) attacks, and Man-in-the-Middle (MitM) attacks. These types of attacks can severely disrupt operations and pose significant risks to critical infrastructure.

Onuntuei [29] expanded on this by including ransomware attacks, Advanced Persistent Threats (APTs), SCADA system attacks, insider threats, and DoS attacks. These threats are particularly concerning given the reliance on SCADA systems for operational technology within the O & G industry. Further, Obonna et al., [30] discussed unstructured cyber-attacks, which are characterized by their variability and difficulty in detection. These attacks pose significant threats to the integrity of process control networks and the overall security of O & G installations, complicating efforts to maintain secure operations.

Gidado [31] identified phishing attacks and malicious software as prominent threats, alongside DoS attacks. These types of cyber threats are prevalent and can cause substantial damage to both the security infrastructure and operational efficiency. Adebayo [32] highlighted the prevalence of ransomware attacks, particularly noting that 39% of such attacks in the energy sector are attributed to ransomware. These attacks involve encrypting data and demanding payment for the decryption key, causing significant operational disruptions and financial losses.

Davis [33] discussed Advanced Persistent Threats (APTs), which aim to gain unauthorized access to valuable intellectual property such as drilling technologies, reservoir data, or strategic plans. APTs represent a sophisticated level of threat that targets high-value information within the O & G sector. The study also addresses vulnerabilities within Industrial Control Systems (ICS), including Distributed Control Systems (DCS) and SCADA systems. These operational technology systems are crucial for O & G operations but are susceptible to cyber threats that can compromise their safety and security.

The report by THISDAY [34] on the increasing instances of malware and crypto-jacking attacks. These attacks can lead to data breaches and financial losses, further emphasizing the need for robust cybersecurity measures in the O & G sector. Figure 3 illustrates the distribution of various cyber threats in Nigeria, as identified in the literature. The most prominent threat is Denial of Service. Phishing, insider threats, and malicious codes such as viruses, worms, and Trojan horses are also identified as significant attack types within the sector. Significant portions of the chart are also dedicated to ransomware attacks, which are particularly prevalent in the energy sector. Other notable threats include Distributed Denial-of-Service (DDoS) attacks, Man-in-the-Middle (MitM) attacks, Advanced Persistent Threats (APTs), SCADA system attacks, and vulnerabilities in Industrial Control Systems (ICS). Emerging threats like cryptojacking and unstructured cyber-attacks also feature prominently, underscoring the diverse and evolving nature of the cybersecurity landscape in Nigeria. The cyber threats presented in Figure 2 can be categorized into three broad categories: Network Attacks, Malware and Malicious Code, and Insider and Advanced Persistent Threats.

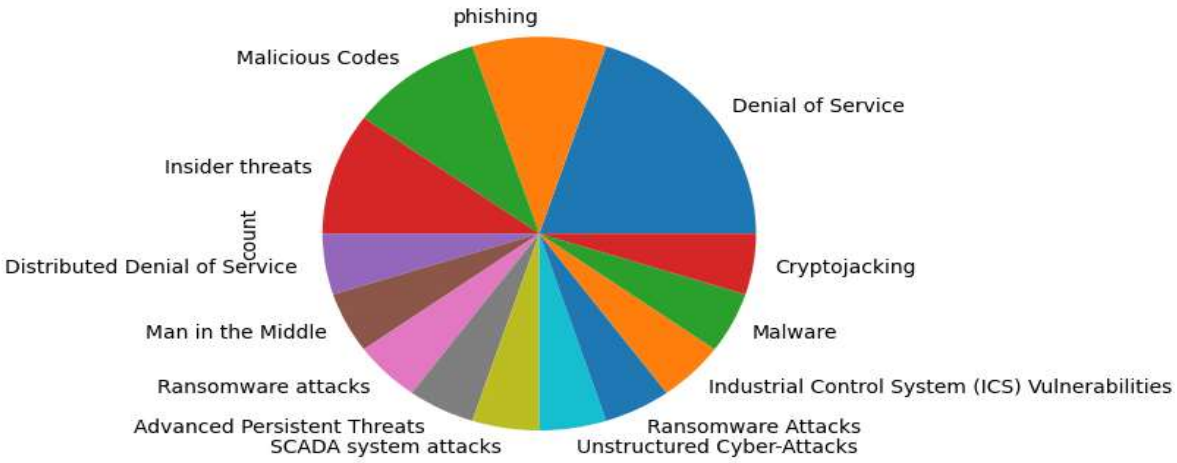

Figure 2: Distribution of Cyberattacks Based on Appearance in Literature

4.2. A Case Study of a Cyber Attack on Nigerian National Petroleum Corporation (NNPC)

In Nigeria, a well-known cyber-attack is the one that happened in 2021 involving the ransomware attack against the Nigerian National Petroleum Corporation (NNPC). In this case, cybercriminals attacked the company by hacking its systems and encrypting sensitive operational information while demanding a ransom for its release. This not only affected NNPC's supply chain management processes but also delayed the transportation of crude oil as well as refinery activities. Furthermore, leaked sensitive corporate data elevated the threat of espionage as well as industrial espionage. These are the few implications of the attack in Nigeria.

i. **Financial Losses:** NNPC lost a huge amount of money due to system downtime, operational disruption, and ransom agreements that were made, impacting the entire economy due to a halted oil exportation.
ii. **Operational Disruption:** Due to the attack, the entire system and all of the components made it extremely difficult to function as an organization and out constant problems that were created from the monsoon of information that was maintained, due to environmental problems.
iii. **Environmental Risk:** As a result of cyberattacks, one of the main operational control systems implemented was the one that could oil spills or explosions - in either circumstance, years of damage is expected to be undergone as an outcome of these attacks, at the distinctly systems operational level.
iv. **Reputation Damage:** A lot of trust in Nigeria, as well as in the oil and gas industry, dropped, with many concerns being made by investors around the world and stakeholders claiming that Nigeria lacks cybersecurity in the sector.

4.3. Global Context and Application to Other Regions

An obvious focus of the attack by the NNPC is the cybersecurity gaps that exist within critical infrastructure sectors globally. Such attacks have previously been carried out in other O&GN sectors which include the Saudi Aramco Shamoon attack which wreaked havoc on a corporate network by deleting data from 30,000 devices in 2012 and the US Colonial Pipeline ransomware cyber-attack that crippled the fuel supply across the eastern US in 2021. These incidents underline the following lessons:

i. **Implementing Cybersecurity Strategies:** All governments need to enforce multilayered cybersecurity frameworks, such as encryption and modern intrusion detection systems if they want to be effective.
ii. **Effective Incident Response Duplication:** Organizations must create and routinely rehearse cyber incident response plans to reduce losses to recovery downtime and financial expenditures.
iii. **International Alliances:** Sharing cybersecurity strategies between nations and private industrial participants can neutralize possible future threats.
iv. **Investment in Cybersecurity Talent:** The gap between cybersecurity professionals makes it increasingly difficult to deal with potential cyber threats; hence, creating training programs and building initial capacity would be a great starting point.

4.4. Emerging Control Measures

As cyber threats evolve in complexity and sophistication, the strategies employed to combat these threats must also advance. [35] recommended continuous updates and evaluations to maintain robust cyber security defenses. Emerging control measures leverage cutting-edge technologies and innovative approaches to bolster cybersecurity defenses [36], particularly in critical sectors like the Nigerian O&G industry. This discussion explores key emerging control measures, which include Artificial Intelligence (AI), Machine Learning (ML), and Blockchain. The analysis of the themes around emerging control measures for cyber-attacks is presented in Figure 3.

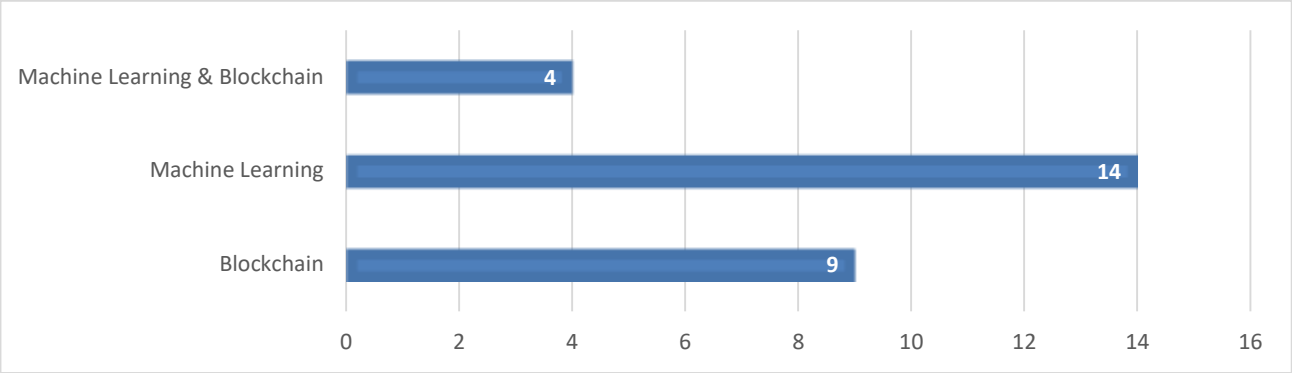

Figure 3: Analysis of emerging techniques for cyberattack control

The study explores 27 papers based on the search term; it focuses on only papers that provide empirical results on the use of these techniques in the control of cyberattacks. The sources of the analyzed papers are presented in Figure 4, and the frequency of the publications based on the themes is presented in Figure 5.

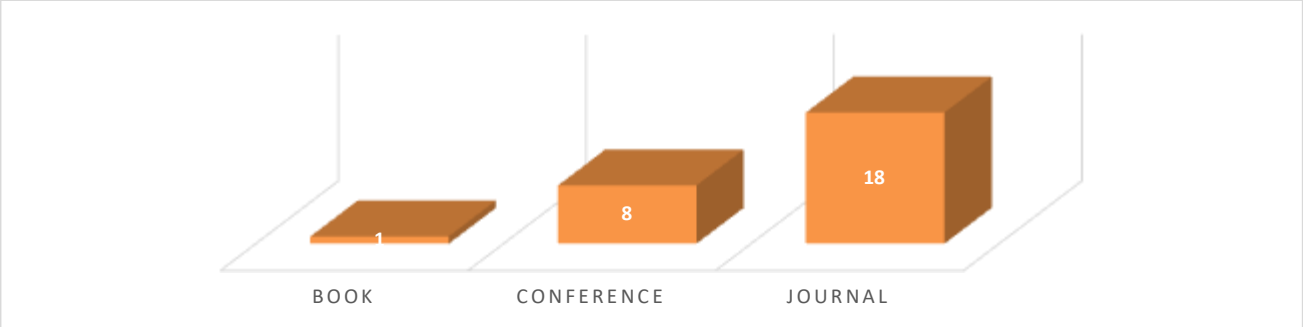

Figure 4: Sources of information on the emerging control measures

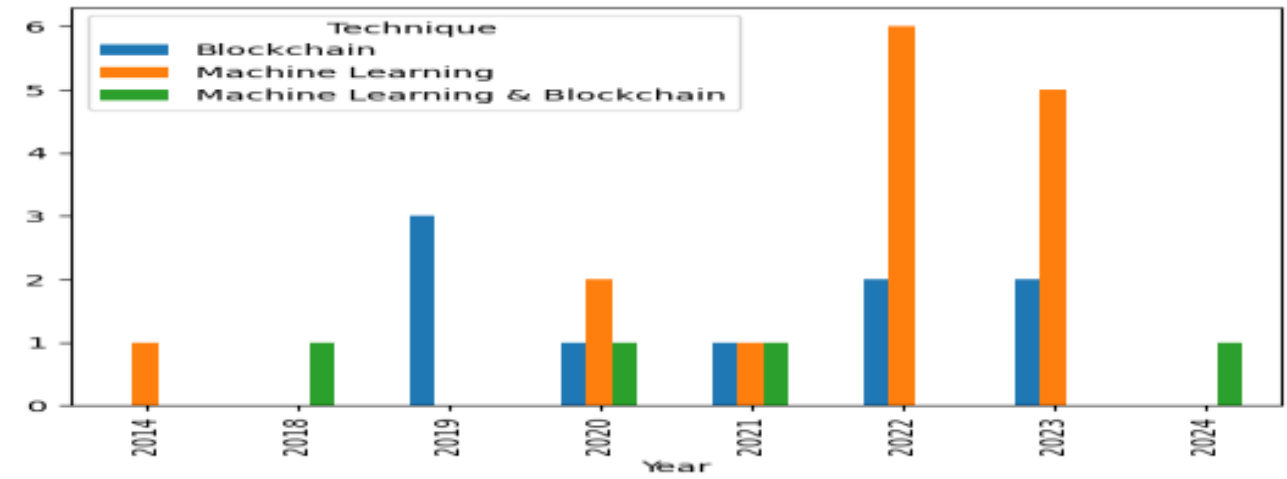

Figure 5: Frequency of publications based on the papers utilized

The proposed novel by Al-majed et al., [37] is a detection framework integrating AI and ML to enhance cybersecurity in CPS. They emphasize the use of a Self-tuned Fuzzy Logic-based Hidden Markov Model (SFL-HMM) combined with Heuristic Multi-Swarm Optimization (HMS-ACO). Their approach demonstrates superior performance in terms of detection rate, false positive rate, and computational efficiency compared to traditional methods. This study highlights the potential of combining fuzzy logic with heuristic optimization for enhanced cyberattack detection.

Uyyala [38] discussed the effectiveness of Support Vector Machine (SVM) algorithms in detecting port scan attempts using the CICIDS2017 dataset. The study achieves high accuracy and suggests exploring other algorithms such as Random Forest, Convolutional Neural Network (CNN), and Artificial Neural Network (ANN) for potentially better results. This work underscores the need for continuous algorithmic innovation to cope with evolving cyber threats.

Semwal & Handa [39] focused on supervised machine learning techniques for detecting cyberattacks in a CPS water treatment plant. They compare K-Nearest Neighbors (KNN), SVM, Decision Tree (DT), and Random Forest (RF) models, finding that DT performs the best with an overall accuracy of 99.9%. This comparative analysis illustrates the variability in performance across different ML algorithms and the importance of model selection in specific application contexts.
Aragonés et al., [40] addressed the challenge of zero-day attacks by designing a scalable threat-hunting system based on ML. They advocate for the strategic application of ML techniques like NLP, C-RNN-GAN, and GNN to distinguish between benign and malicious data in real-time. This study highlights the importance of adaptability in ML techniques to suit various threat scenarios in critical infrastructure protection.

Arora et al., [41] evaluated multiple ML algorithms, including Random Forest, SVM, DT, ANN, and KNN, for detecting cyberattacks in Industrial IoT systems. Their findings reveal the high efficacy of ML in identifying attacks with minimal false alarms. This paper reinforces the notion that the selection of appropriate ML algorithms is crucial for effective intrusion detection in industrial environments.

Avcı et al., [42] proposed an ML-based intrusion detection system using feature selection techniques to enhance detection accuracy. Their study shows that the Random Forest technique outperforms others, achieving an accuracy of 99.72%. This research emphasizes the critical role of feature selection in improving the performance of ML-based cybersecurity systems.

Öztürk et al., [43] explored the use of ML for attack detection in SCADA systems within CPS. They perform attack classification and performance evaluation using various ML algorithms. The study illustrates the applicability of ML in safeguarding SCADA systems, which are integral to critical infrastructure.

Zarandi & Sharifi [44] focused on the detection of deception attacks in CPS using deep neural networks (DNN). Their method includes resilient control algorithms to isolate compromised agents within a leader-follower network structure. This approach demonstrates the advanced capabilities of DNNs in identifying and mitigating sophisticated cyber threats.

Arya & Gupta [45] proposed an ensemble filter-based feature selection approach to enhance the detection accuracy and computational efficiency of ML models for IIoT cybersecurity. Their methodology achieves impressive accuracy rates, demonstrating the value of ensemble techniques in feature selection and attack detection.

Raza et al., [46] discussed the challenges and future directions in CPS security, highlighting the inadequacy of traditional security systems against advanced cyber threats. They review various ML techniques, such as unsupervised anomaly detection, SVM, and CNN, underscoring the need for sophisticated ML solutions to protect CPS.

Singh & Silakari [47] proposed a Cyber Attack Detection System (CADS) using Generalized Discriminant Analysis (GDA) for feature reduction and an ensemble approach for classification. Their system shows high detection accuracy across various attack types, demonstrating the effectiveness of hybrid classifier approaches.

Alqahtani et al., [48] evaluated multiple ML algorithms for intrusion detection, highlighting the effectiveness of AI-driven systems in cybersecurity. Their comparative analysis across various datasets and performance metrics underscores the importance of algorithm selection in developing robust IDS.

Al Ogaili et al., [49] addressed malware detection using a modified whale optimization algorithm for feature selection. Their system achieves high accuracy and low false positive rates, demonstrating the potential of optimization algorithms in enhancing ML-based cybersecurity solutions.

Bhardwaj et al., [50] explored the detection of various cyberattacks using different ML approaches, such as CNN for XSS attacks and logistic regression for SQLI attacks. Their study reveals the strengths and limitations of different ML techniques in detecting specific types of cyber threats.

Zakariah et al., [51] proposed a novel IDS based on Artificial Neural Networks (ANN) for detecting network intrusions. Their custom ANN model outperforms traditional methods, highlighting the advanced capabilities of ANNs in cybersecurity applications.

Cybersecurity remains a pivotal concern across various domains due to the increasing sophistication and frequency of cyberattacks. With the advent of advanced technologies such as blockchain, innovative approaches to enhancing security measures have emerged.

Ghiasi et al., [52] focused on detecting false data injection attacks (FDIAs) in DC microgrids (DC-MGs) by utilizing Hilbert-Huang transform methodology along with blockchain-based ledger technology. Their approach enhances security by analyzing voltage and current signals in smart sensors and controllers, extracting signal details to detect FDIAs. Simulation results demonstrate the proposed model's precision and robustness, significantly improving data exchange security in smart DC-MGs. This study underscores the importance of blockchain's immutable ledger in securing critical infrastructure.

Yu et al., [53] presented a blockchain technology-assisted networked predictive secure control approach for networked control systems (NCSs). The approach inherently boosts the resilience of NCSs against cyberattacks without relying on prior system knowledge. However, blockchain-induced time delays could compromise real-time performance. To mitigate this, a networked Kalman filter-based predictive control is introduced. The effectiveness of this integrated approach is validated through an experimental prototype of a photovoltaic (PV)--based power generation system subjected to random cyberattacks. This study highlights the balance between enhancing security and maintaining real-time performance in NCSs through blockchain integration.

Singh et al., [54] explored blockchain-enabled secure access control mechanisms for the Internet of Things (IoT). The study emphasizes blockchain's decentralization, auditability, transparency, and immutability as key factors in improving IoT security. By reviewing current research trends, Singh et al. identify the most utilized blockchains for secure access control solutions and discuss the improvements and challenges in building decentralized access control systems. This research underscores the transformative potential of blockchain in addressing IoT's security and privacy concerns.

Ajayi & Saadawi [55] proposed a blockchain-based solution to ensure the integrity and consistency of attack characteristics shared in a cooperative intrusion detection system (CIDS). Their architecture effectively detects and prevents fake feature injections and compromised IDS nodes. The evaluation of security and latency demonstrates scalability and low latency, proving the robustness of the proposed approach in preventing compromised nodes and malicious feature manipulation. Similarly, Dang et al., [56] introduced a novel blockchain-based CIDS with a reputation-based consensus protocol, incentivizing service providers to evaluate attack instances and punishing malicious evaluators. The inclusion of a redactable blockchain technique for dynamic instance updates further enhances real-time intrusion detection capabilities.

Dawit et al., [57] investigated collaborative intrusion detection with blockchain to enhance security in peer-to-peer networks. Their study categorizes major vulnerabilities and current enhancements for mitigating these challenges. By leveraging blockchain's transparency, immutability, decentralization, and provenance, the research demonstrates the suitability of blockchain for collaborative intrusion detection systems. Ajayi et al., [58] similarly proposed an architecture that securely stores and distributes attack signatures in CIDS, leveraging blockchain's distributed ledger technology, data immutability, and tamper-proof abilities to ensure prompt detection of attacks.

Li et al., [59] developed CBSigIDS, a collaborative blockchain signature-based IDS framework for IoT environments. This framework allows incremental building and updating of a trusted signature database in a collaborative IoT environment without a trusted intermediary. Evaluation results show enhanced robustness and effectiveness of signature-based IDSs under adversarial scenarios. Laufenberg et al., [60] also introduced an architecture for a blockchain-enabled signature-based CIDS, addressing trust management and consensus-building challenges in CIDS through blockchain's built-in immutability and consensus-building capabilities.

The integration of machine learning (ML) and blockchain technologies is increasingly seen as a promising approach to enhancing cybersecurity mechanisms. Meng et al., [61] provided a comprehensive review of the integration of IDSs and blockchain technology. They discuss the background and applicability of blockchain in intrusion detection, emphasizing blockchain's ability to protect data integrity and ensure process transparency. Despite the potential benefits, Meng et al. identify key challenges, including data and trust management, that need to be addressed to enhance the effectiveness of collaborative IDSs. This study sets the stage for exploring how blockchain can mitigate existing limitations in IDS architectures.

Hazman et al., [62] described a unique blockchain-based hybrid intrusion detection system (IDS) that employs blockchain architecture to exchange signatures between nodes in decentralized IDSs. This approach addresses the difficulties in identifying attacks that impact the overall surveillance system and network performance. By utilizing both detection methods and blockchain technology, the proposed system secures data transmission across the network. The study highlights blockchain's role in improving the efficacy of IDSs by providing a decentralized, secure method for data exchange, thus eliminating the need for an external trusted party.

Alkadi et al., [63] proposed a deep blockchain framework (DBF) designed to offer distributed intrusion detection and privacy protection in IoT networks. The framework employs a bidirectional long short-term memory (BiLSTM) deep learning algorithm to process sequential network data, leveraging datasets like UNSW-NB15 and BoT-IoT for assessment. The DBF integrates privacy-based blockchain and smart contracts using the Ethereum library to ensure data privacy. Experimental results demonstrate that DBF outperforms peer privacy-preserving intrusion detection techniques, highlighting its potential to securely migrate data and protect IoT networks.

5. CONCLUSION

Despite being the major driver of the Nigerian economy, the O & G sector grapples significantly with information breaches. These breaches pose severe risks, not only to the security and confidentiality of operational data but also to the overall stability and reputation of the industry. However, effective research aimed at mitigating these challenges is hindered by a substantial dearth of information within the sector. The lack of comprehensive data and detailed studies specific to the management of information breaches in Nigeria's O & G sector creates a significant gap in the existing body of knowledge.

Current research on information security within the O & G sector is sparse, particularly within the Nigerian context. This scarcity leaves a critical void in understanding the unique challenges and vulnerabilities faced by this industry in Nigeria. Without robust and detailed research, it is challenging to develop tailored strategies and solutions to address these breaches effectively. The current state of play regarding information breach management in Nigeria's O & G sector remains largely unknown, rendering the sector vulnerable to persistent and evolving cyber threats.

Due to the extensive research and successful implementation of emerging technologies to curb information breaches in similar sectors globally, there is a strong case for adopting these technologies within the Nigerian context. Technologies such as blockchain, machine learning, and advanced intrusion detection systems have shown promising results in

enhancing data security and mitigating breaches in various industries. Leveraging these technologies, the Nigerian O & G sector could significantly improve its information security infrastructure.

This research suggests that Nigeria's O & G sector could benefit from adopting these emerging technologies to mitigate issues related to information breaches. Implementing advanced cybersecurity measures and leveraging the potential of blockchain for secure data transactions, machine learning for predictive threat detection, and collaborative intrusion detection systems can provide a robust defense against cyber threats. Tailoring these technologies to the specific needs and challenges of the Nigerian O & G industry could lead to more effective management of information breaches, ultimately contributing to the sector's stability and security.

REFERENCES

[1] Oluniyi, A. E. (2017). Nigeria's oil and gas production and Niger Delta militant: The need of oil resources to stop oil reliance for sustainable development. Global Journal of Human Social Science, 17(5), 22-34.
[2] Ogbuigwe, A. (2018). Refining in Nigeria: history, challenges, and prospects. Applied Petrochemical Research, 8, 181-192.
[3] Donwa, P., Mgbame, C., & Ekpulu, G. (2015). Economic growth: oil and gas contributions. Sci-Afric Research Journal of Accounting and Monetary Policy, 1(2), 102-108.
[4] Owan, V. J., Ndibe, V., & Anyanwu, C. C. (2020). Diversification and economic growth in Nigeria (1981–2016): An econometric approach based on ordinary least squares (OLS). European Journal of Sustainable Development Research, 4(4).
[5] The Guardian. (2023a). 32 Cyber-attacks leave the oil sector vulnerable. The Guardian. https://guardian.ng/energy/32-cyber-attacks-leave-oil-sector-vulnerable/
[6] Microsoft InfoSec, (2023). What is information security (InfoSec)? Microsoft. Retrieved December 13, 2022, from https://www.microsoft.com/en-ww/security/business/security-101/what-is-information-security-infosec.
[7] Siddiqi, M.A.; Pak, W.; and Siddiqi, M.A. (2022). A Study on the Psychology of Social Engineering- Based Cyberattacks and Existing Countermeasures. Appl. Sci. 12, 6042. https://doi.org/10.3390/app12126042.
[8] Sampson, A. S., & Ojen, I. M. (2021). Perception analysis of COVID-19 pandemic, cybercrime and well-being of online fraud victims in Calabar, Nigeria. International Journal of Public Administration and Management Research, 6(4), 29-35.
[9] THISDAY (2023, September 19). Despite the multi-billion Naira spending on oil asset protection, Nigeria recorded the least crude output in four years. This Day Live. https://www.thisdaylive.com/index.php/2023/09/19/despite-multi-billion-naira-spending-on-oil-assets-protection-nigeria-records-least-crude-output-in-four-years
[10] Tenable. (2022). Industrial Cybersecurity to Secure Oil and Gas Operations. Tenable. https://www.tenable.com/solutions/oil-and-gas. *Accessed* October 22, 2024.
[11] Mc Ewan, K. A. (2020). Cyber-threats as political risk: increased risk for the oil and gas industry (Doctoral dissertation, Stellenbosch: Stellenbosch University).
[12] Broadhurst, R. (2017). Cybercrime: Thieves, Swindlers, Bandits, and Privateers in Cyberspace. In The Oxford Handbook of Cyber Security. Oxford, UK: Oxford Handbooks Press.
[13] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., & Lopez, J. (2018). A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials, 20(4), 3453-3495.
[14] Achunike, V. U., & Egbuna, F. C. (2016). Synopsis of Cyber-attacks Incidents and Impacts on Oil and Gas Critical Infrastructures: A Nigerian Perspective. International Journal of Advances in Engineering and Management (IJAEM). 2(3), 335-343
[15] Lu, H., Guo, L., Azimi, M., & Huang, K. (2019). Oil and Gas 4.0 era: A systematic review and outlook. Computers in Industry, 111, 68-90.
[16] Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing. Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017).
[17] Jabar, T., & Mahinderjit Singh, M. (2022). Exploration of mobile device behavior for mitigating advanced persistent threats (APT): a systematic literature review and conceptual framework. Sensors, 22(13), 4662.
[18] Duffy, C. (2021) A massive ransomware attack hit hundreds of businesses. Here's what we know CNN business, CNN. Available at: https://www.cnn.com/2021/07/06/tech/kaseya-ransomware-what-we-know/index.html (Accessed: 14 June 2024).
[19] Faircloth, C., Hartzell, G., Callahan, N., & Bhunia, S. (2022). A study on brute force attack on T-Mobile leading to SIM-hijacking and identity theft. In 2022 IEEE World AI IoT Congress (AIIoT) (501-507). IEEE.
[20] BBC News. (2021, July 22). Hackers reportedly demand $50m from Saudi Aramco over data leak. BBC. https://www.bbc.com/news/business-57924355. *Accessed* October 22, 2024.
[21] Mikkelsen, D. (2024, May 24). Decade of danger: The Top 10 cyberattacks on the Oil & Gas Industry. Oilandgasmiddleeast.com. http://w.oilandgasmiddleeast.com/listing/decade-of-danger-the-top-10-cyberattacks-on-the-oil-gas-industry. *Accessed* October 28, 2024.

[22] Morrison, S. (2021, May 10). How a major oil pipeline got held for ransom. Vox. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices. *Accessed* October 18, 2024.
[23] Briggs, B. (2019, December 16). Hackers hit Norsk Hydro with ransomware. The company responded with transparency. Source. https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/. *Accessed* October 22, 2024.
[24] Stillman, A., & Sebenius, A. (2019, November 12). Pemex Faces Payment Problems After Cyber Attack Shut System. Bloomberg.com. https://www.bloomberg.com/news/articles/2019-11-11/pemex-workers-barred-from-computers-after-unexpected-shutdown. *Accessed* October 20, 2024.
[25] Walton, R. (2018, April 4). Hackers hit communications system of Energy Transfer Partners pipeline. Utility Dive. https://www.utilitydive.com/news/hackers-hit-communications-system-of-energy-transfer-partners-pipeline/520531/. *Accessed* October 21, 2024.
[26] Jaiyeola, T. (2022, November 24). Hackers attack 39% Nigeria's oil sector computers – Report. Punch Newspapers; Punch Newspaper. https://punchng.com/hackers-attack-39-nigerias-oil-sector-computers-report/. *Accessed* October 18, 2024.
[27] Jeremiah, K. (2023, March 8). 32 cyber attacks leave oil sector vulnerable. The Guardian. https://guardian.ng/energy/32-cyber-attacks-leave-oil-sector-vulnerable/. *Accessed* October 22, 2024.
[28] Obonna, U. O., Opara, F. K., Mbaocha, C. C., Obichere, J.-K. C., Akwukwaegbu, I. O., Amaefule, M. M., & Nwakanma, C. I. (2023a). Detection of man-in-the-middle (MitM) cyber-attacks in oil and gas process control networks using machine learning algorithms. Future Internet, 15(8), 280. https://doi.org/10.3390/fi15080280
[29] Onuntuei, E. (2018). Safety, Risk, and Reliability of Cyber Network in Oil and Gas Industry. PUPIL: International Journal of Teaching, Education, and Learning, 2(2),81-97.DOI-https://dx.doi.org/10.20319/pijtel.2018.22.8197
[30] Obonna, U. O., Opara, F. K., Mbaocha, C. C., Obichere, J.-K. C., Nwakanma, C. I., Ahakonye, L. A. C., & Kim, D.-S. (2023b). Coarse tree algorithm-based detection of unstructured cyber-attacks in oil and gas process control networks. 2023 IEEE AFRICON.
[31] Gidado, S. (2020, January 8). Cyber security in Nigerian oil & gas sector. Linkedin.com. https://www.linkedin.com/pulse/cyber-security-nigerian-oil-gas-sector-sirajo-Gidado. *Accessed* October 22, 2024.
[32] Adebayo, C. (2021, May 12). Cybersecurity in Nigeria's energy sector: Lessons from the "DarkSide." Nairametrics. https://nairametrics.com/2021/05/12/cybersecurity-in-nigerias-energy-sector-lessons-from-the-darkside/. *Accessed* October 22, 2024.
[33] Davis, D. (2022, November 1). 5 big cyberattacks in oil and gas. Oil & Gas IQ. https://www.oilandgasiq.com/digital-transformation/articles/5-big-cyber-security-attacks-in-oil-and-gas. *Accessed* October 22, 2024.
[34] THISDAY (2023b, September 19). Despite the multi-billion Naira spending on oil asset protection, Nigeria recorded the least crude output in four years. This Day Live. https://www.thisdaylive.com/index.php/2023/09/19/despite-multi-billion-naira-spending-on-oil-assets-protection-nigeria-records-least-crude-output-in-four-years. *Accessed* October 22, 2024.
[35] Chukwuemeka, A., & Ngozi, M. (2017). Securing Nigeria's Crude Oil and Gas Pipelines–Change in Current Approach and Focus on the Future. *Scientific Research Journal (SCIRJ)*, *5*(1), 1-9.
[36] Saravanan, S., Menon, A., Saravanan, K., Hariharan, S., Nelson, L., & Gopalakrishnan, J. (2023). Cybersecurity audits for emerging and existing cutting-edge technologies. In 2023 11th International Conference on Intelligent Systems and Embedded Design (ISED) (1-7). IEEE.
[37] Al-majed, R., Ibrahim, A., Abualkishik, A., Mourad, N., & Almansour, F. (2022). Using machine learning algorithm for detection of cyber-attacks in cyber-physical systems. Periodicals of Engineering and Natural Sciences (PEN), 10(3), 261. https://doi.org/10.21533/pen.v10i3.3035
[38] Uyyala, P. (2022). DETECTION OF CYBER ATTACK IN NETWORK USING MACHINE LEARNING TECHNIQUES. Journal of Interdisciplinary Cycle Research, 14(3), 1903-1913.
[39] Semwal, P., & Handa, A. (2022). Cyber-attack detection in cyber-physical systems using supervised machine learning. Handbook of Big Data Analytics and Forensics, 131-140.
[40] Aragonés L. M., Pérez Llopis, I., & Esteve Domingo, M. (2023). Threat hunting system for protecting critical infrastructures using a machine learning approach. Mathematics, 11(16), 3448.
[41] Arora, P., Kaur, B., & Teixeira, M. A. (2021). Evaluation of machine learning algorithms used on attack detection in industrial control systems. Journal of The Institution of Engineers (India): Series B, 102(3), 605-616.
[42] Avcı, İ., & Koca, M. (2023). Cybersecurity Attack Detection Model, Using Machine Learning Techniques. Acta Polytechnica Hungarica, 20(7), 29-44.
[43] Öztürk, T., Turgut, Z., Akgün, G., & Köse, C. (2022). Machine learning-based intrusion detection for SCADA systems in healthcare. Network Modeling Analysis in Health Informatics and Bioinformatics, 11(1), 47.
[44] Zarandi, Z. N., & Sharifi, I. (2020, December). Detection and identification of cyber-attacks in cyber-physical systems based on machine learning methods. In 2020 11th International Conference on Information and Knowledge Technology (IKT) (107-112). IEEE.

[45] Arya, L., & Gupta, G. P. (2023, March). Ensemble filter-based feature selection model for cyber-attack detection in industrial Internet of Things. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 1, 834-840.
[46] Raza, A., Memon, S., Nizamani, M. A., & Shah, M. H. (2022, June). Machine learning-based security solutions for critical cyber-physical systems. In 2022 10th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 1-6.
[47] Singh, S., & Silakari, S. (2014). An ensemble approach for cyber attack detection system: a generic framework. International Journal of Networked and Distributed Computing, 2(2), 78-90.
[48] Alqahtani, H., Sarker, I. H., Kalim, A., Minhaz Hossain, S. M., Ikhlaq, S., & Hossain, S. (2020). Cyber intrusion detection using machine learning classification techniques. In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1, Springer Singapore, 121-131.
[49] Al Ogaili, R. R. N., Alomari, E. S., Alkorani, M. B. M., Alyasseri, Z. A. A., Mohammed, M. A., Dhanaraj, R. K., ... & Karuppayah, S. (2023). Malware cyberattack detection using a novel feature selection method based on a modified whale optimization algorithm. Wireless Networks, 1-17.
[50] Bhardwaj, A., Chandok, S. S., Bagnawar, A., Mishra, S., & Uplaonkar, D. (2022). Detection of cyber-attacks: XSS, SQL, phishing attacks, and detecting intrusion using machine learning algorithms. In 2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT), IEEE, 1-6.
[51] Zakariah, M., AlQahtani, S. A., Alawwad, A. M., & Alotaibi, A. A. (2023). Intrusion Detection System with Customized Machine Learning Techniques for NSL-KDD Dataset. Computers, Materials & Continua, 77(3).
[52] Ghiasi, M., Dehghani, M., Niknam, T., Kavousi-Fard, A., Siano, P., & Alhelou, H. H. (2021). Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and Hilbert Huang transform. Ieee Access, 9, 29429-29440.
[53] Yu, Y., Liu, G. P., Zhou, X., & Hu, W. (2022). Blockchain protocol-based predictive secure control for networked systems. IEEE Transactions on Industrial Electronics, 70(1), 783-792.
[54] Singh, R., Kukreja, D., & Sharma, D. K. (2023). Blockchain-enabled access control to prevent cyber-attacks in IoT: Systematic literature review. Frontiers in Big Data, 5, 1081770.
[55] Ajayi, O., & Saadawi, T. (2020). Blockchain-based architecture for secured cyber-attack features exchange. In 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), IEEE, 100-107
[56] Dang, T., Tian, G., Wei, J., & Liu, S. (2023). Blockchain-based collaborative intrusion detection scheme. International Journal of Computational Science and Engineering, 26(4), 418-429.
[57] Dawit, N. A., Mathew, S. S., & Hayawi, K. (2020). Suitability of blockchain for collaborative intrusion detection systems. In 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC), IEEE, 1-6.
[58] Ajayi, O., Cherian, M., & Saadawi, T. (2019). Secured cyber-attack signatures distribution using blockchain technology. In 2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), IEEE, 482-488.
[59] Li, W., Tug, S., Meng, W., & Wang, Y. (2019). Designing collaborative blockchained signature-based intrusion detection in IoT environments. Future Generation Computer Systems, 96, 481-489.
[60] Laufenberg, D., Li, L., Shahriar, H., & Han, M. (2019). An architecture for blockchain-enabled collaborative signature-based intrusion detection system. In Proceedings of the 2019 ACM Southeast Conference, 169-169, https://doi.org/10.1145/3349266.3351389
[61] Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: a review. Ieee Access, 6, 10179-10188.
[62] Hazman, C., Amaouche, S., Abdedaime, M., Guezzaz, A., Benkirane, S., & Azrour, M. (2024). A collaborative intrusion detection approach based on deep learning and blockchain. 112-124). Chapman and Hall/CRC.
[63] Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal, 8(12), 9463-9472