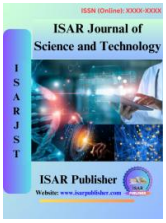
OPEN ACCESS



ISAR Journal of Science and Technology

Volume 2, Issue 12, 2024, Page: 29-36

Abbriviate Title- ISAR J Sci Tech

ISSN *(Online)*- 2584-2056

https://isarpublisher.com/journal/isarjst

AI AND PERFORMANCE CAPABILITIES OF CYBERSECURITY IN THE ENERGY INDUSTRY

Aziboledia Frederick Boye[1*], Onate Egerton Taylor[1] and Deepak Bhagat[2]

[1]Rivers State University, Department of Computer Science, Port Harcourt, Nigeria.

[2]Indorama Fertilizer Limited (IFL), Eleme, Instrumentation Department, Port Harcourt, Nigeria.

***Corresponding Author**

Aziboledia Frederick Boye

Rivers State University, Department of Computer Science, Port Harcourt, Nigeria.

Article History

Received: 19.10.2024
Accepted: 15.11.2024
Published: 23.12.2024

Abstract: The energy industry is significant by digitalization, renewable integration, and automation, making it increasingly reliant on interconnected systems. This evolution exposes the sector to sophisticated cyber threats targeting critical infrastructure, operational technologies (OT), and supply chains, enhancing the cybersecurity landscape of the energy industry, offering several opportunities in the industry. This article explores dual role of AI in shaping the energy industry's cybersecurity framework, emphasizing its impact on threat prevention and performance optimization. Key aspects such as the integration of AI-driven anomaly detection systems, real-time response capabilities, and secure energy grid operations are analyzed. The article also examines the challenges of implementing AI-based cybersecurity, including ethical concerns, data privacy, and the risk of adversarial AI attacks. The article shows the necessity for a fair approach to harness AI's potential while ensuring robust, secure, and efficient energy operations.

Keywords: Artificial Intelligence, Cybersecurity, Energy Industry, Critical Infrastructure, Operational Technology, Threat Detection, Renewable Integration, Adversarial AI.

Cite this article:

Boye, A.F., Taylor, E.O. and Bhagat, D., (2024). AI AND PERFORMANCE CAPABILITIES OF CYBERSECURITY IN THE ENERGY INDUSTRY. *ISAR Journal of Science and Technology*, *2*(12), 29-36.

1. Introduction

The energy industry, a cornerstone of modern civilization, is undergoing a paradigm shift fueled by advancements in technology and a global push toward sustainable energy. From smart grids and distributed energy resources to automated operations in oil and gas, the sector has embraced digitalization to enhance efficiency and reliability. However, this interconnectedness also increases exposure to cyber threats, with potential impacts on safety, financial stability, and national security. The implementation of AI into cybersecurity presents an unprecedented advantage to mitigate these cyber threats and attacks while enhancing the performance of energy systems. However, the landscape has changed. Cyberattacks are becoming more sophisticated, and OT systems are increasingly integrated into broader IT networks. Industries must now leverage data-driven insights and remote monitoring capabilities to safeguard these critical systems. And this is where the convergence of OT and IT comes into play.

2. AI in the Energy Industry: Opportunities and Challenges

The opportunity of leveraging AI techniques in the energy industry, [16] improved the efficiency and reliability performance for more automated and intelligent cyber defense because legacy systems have been replaced and integrated with more advance technologies. In deploying AI in cybersecurity in the energy industry comes with new technical innovations [3]. The integration of AI-driven technologies brings about great opportunities, and developed challenges inn various sectors, energy, oil & gas, etc.

2.1 Energy Industry: Opportunities

There are a lot of opportunities by deploying and implementing AI-driven technologies in the energy industry. The following opportunities are provided with AI-powered solutions to the energy sector for optimization, efficient and reliable system operations.

2.1.1 Enhanced Threat Detection (ETD)

One of the opportunity of implementing and integrating AI-driven solutions in the energy industry by enhancing threat detection. Threat detection was one of the earliest applications of cyber AI. [9] It can augment existing attack surface management techniques to reduce noise and allow scarce security professionals to zero in on the strongest signals and indicators of compromise. AI-powered systems can identify subtle anomalies in vast datasets, enabling early detection of threats. For instance, deep learning as a subset of machine learning allows the algorithms to learn from vast data sets and discover even tiny patterns. That may suggest possible risks

are one of the most important aspects of AI-based threat detection [35]

Depending on the type of data and algorithms utilized, threat detection systems based on AI can detect a variety of dangers. These technologies for example can recognize malware, phishing scams, and other online risks [37]. Artificial intelligence (AI) can detect suspicious activity or behavior in video surveillance footage such as unauthorized access or theft in the context of physical security.

2.1.2 Predictive Maintenance (PM)

Author [33] highlight that AI-driven predictive maintenance relies on sophisticated algorithms that continuously monitor, analyze, and predict the condition of machinery. AI plays in cybersecurity grows more prominent and [3] for instance, like machine learning models that forecast equipment failures, reducing unplanned outages and maintenance costs. So, [33] the value of AI in predictive maintenance is immense, offering both cost avoidance and cost savings. For example, in high-stakes industries like automotive manufacturing, where downtime can cost millions of dollars per hour, the ability to prevent unexpected failures is invaluable. Furthermore, [35] AI's predictive analytics can foresee potential vulnerabilities before they are exploited, offering a proactive form of security rather than a reactive one. AI empowers cybersecurity with advanced analytical tools, making it an indispensable ally in the battle against cybercrime [35].

2.1.3 Real-Time Decision-Making (RTDM)

AI-driven technology and deployment cybersecurity will aid organizations identify and correct potential deficiencies in their security strategy. It imperative as quick real-time quick decision-making will aids safe operations of interconnected systems in the energy industry. In this way, they can implement formalized procedures that can result in more secure IT environments [16]. This is where AI algorithms analyze data streams from energy systems, supporting faster and more informed responses to threats. These results on real-time will give energy related industries the leverage of higher budget implementation.

2.1.4 Adaptive Security

AI-driven solutions evolve to counteract emerging threats and attacks, offering dynamic defense mechanisms. According [50] highlight that AI-driven technology at least information on emerging threats, improves its detection and response capabilities. Furthermore, having the following key features, continuous learning, behavioural analytics, automated response and scalability, this makes it well suited for cybersecurity [50]. Each of these key features plays a role when adaptive security is mentioned in a AI-driven technology in the energy industry.

2.2 AI Challenges in Energy Industry

The implementation of AI-driven technologies [3] has grown across all sectors, including the energy industry, and the integration of cybersecurity is no exception. This becomes so crucial for addressing the escalating speed, complexity, and frequency of cyber threats. The author [4] said ensuring safety remains paramount in the energy, where the repercussions of accidents can be catastrophic. AI offers a transformative solution by leveraging predictive analytics to anticipate potential hazards and preemptively mitigate risks, meaning integrating AI with other modern techniques is imperative.

2.2.1 Complex Implementation

Integrating AI with legacy systems in the energy industry requires significant investment and expertise. Organizations face a significant challenge in integrating these legacy systems with AI-powered platforms [5], but modern AI platforms leverage distributed computing, machine learning algorithms, and real-time data analytics to generate actionable insights [6]. That is [4] the reason according a recent survey conducted by IBM, 80% of managers within the chemical industry acknowledge the imminent transformative influence of artificial intelligence on their business operations within the next three years. [7] identifies three (3) key issues when integration AI-driven technology into legacy systems, organizational (work adaptation issues), technical (compatibility issues) and financial issues (the initial investment required for integrating AI technologies can be substantial, making it a significant barrier for many organizations [8].

2.2.2 Data Privacy and Security

Data privacy and security is one the key security issues in industrial IoT systems which has on the campaign for system integration in the energy industry. Ensuring the integrity of data used by AI models is critical to prevent exploitation. Meanwhile, [9] the cost of cybercrime continues to climb; it’s expected to double from US$3 trillion in 2015 to US$6 trillion by the end of 2021 and grow to US$10.5 trillion by 2025. It an issue also, that numerous studies have highlighted the difficulties organizations face in integrating legacy systems with AI-based platforms or solutions, particularly in terms of data compatibility, interoperability, and migration costs [5]. Because AI simplifies tasks, increases efficiency and enables innovation, companies cannot afford to ignore AI when upgrading old software [11].

2.2.3 Adversarial AI Risks

Malicious actors may use AI to manipulate or evade detection systems, creating new vulnerabilities. APIs will be a growing security concern and that is why the need for legacy system upgrade is imperative in the energy or related industries deploying AI-driven technology for their production operations and engineering. The AI module enhances situational awareness and the sensory data quality through eliminating background noise, isolating important security events, and using machine learning to determine abnormal patterns' recognition [10]. The method leads to use of updated and modified security systems tailored to handle various scenarios effectively, enhancing overall threat mitigation effectiveness.

3. Cybersecurity Threats in the Energy Industry

The platform of integrating legacy systems (LS) and AI-driven platform make these systems vulnerable to cyber-attacks or threats. Authors [47] highlighted that the historical overview of cybersecurity challenges in the energy industry points a complex landscape marked by evolving threats and the sector's increasing reliance on digital technologies Cybersecurity [46] has traditionally been viewed as a technology issue, but is now also regarded as a key environmental, social and governance (ESG) concern. Energy

companies can experience severe reputational damage and be fined if information network is not adequately protected [46].

3.1 Targeted Cyberattacks

With the deployment integration of AI-driven technologies in the energy and all its related industries, cyberattacks and attacks against the energy industry becomes prevalent and can lead to widespread power outage to physical infrastructural damages. Ransomware is one of the major cyber threats and attacks that the energy [48]. In this research we explore recants cyber threats and attacks in the industry.

3.1.1 Ransomware in the Energy Industry

When we consider cyber-attacks in the industry, ransomware is one of the most prevalent and sophisticated. The year 2024 has already seen a steady rise in the number of cyberattacks and ransoms demanded by hackers [53]. In recent years, the digital landscape has been marred by a growing and pervasive threat is ransomware attacks and being on the radar of ransomware groups is akin to swimming in shark infested waters; the longer you're there, the higher the chances of an attack [15]. It is an important threat to cybersecurity, a form of malware that encrypts victim's files. The attacker demands a ransom from the victim to restore access to the files [9]. Ransomware attacks on energy companies can halt operations and demand large payouts [9]. Kojima industries corporation fell victim to a ransomware attack on its file server, forcing the world largest automotive manufacturer to temporarily shut down all 14 factories in Japan, compromising 28 production lines [12]. The German-owned company said [13] it became aware of the attack on January 28, 2022, and it immediately took steps to contain the attack. A letter from KP Snacks sent to store owners February 2, 2022, said its systems had been, "compromised by ransomware," and they, "cannot safely process orders or dispatch goods [13]. The industry, which leads with over a thousand ransomware victims, faces unique challenges due to the operational disruption that halts production lines, causing significant financial and reputational damage [15]. Organization in the US are the business most likely to be affected by ransomware, accounting for 47% of attacks in 2023 [53].

The most notable attacks in the industry is the SolarWinds attacks of 2020, which enabled the attackers unauthorized access into the company systems by injecting trojan code into their Orion software updates [48]. The data as reveal by [15] serves as a critical metric of cybersecurity challenges, calling for strategic responses in threat mitigation. With this year's count reaching 4,893, up from 2,708 the previous year of ransomware victims.

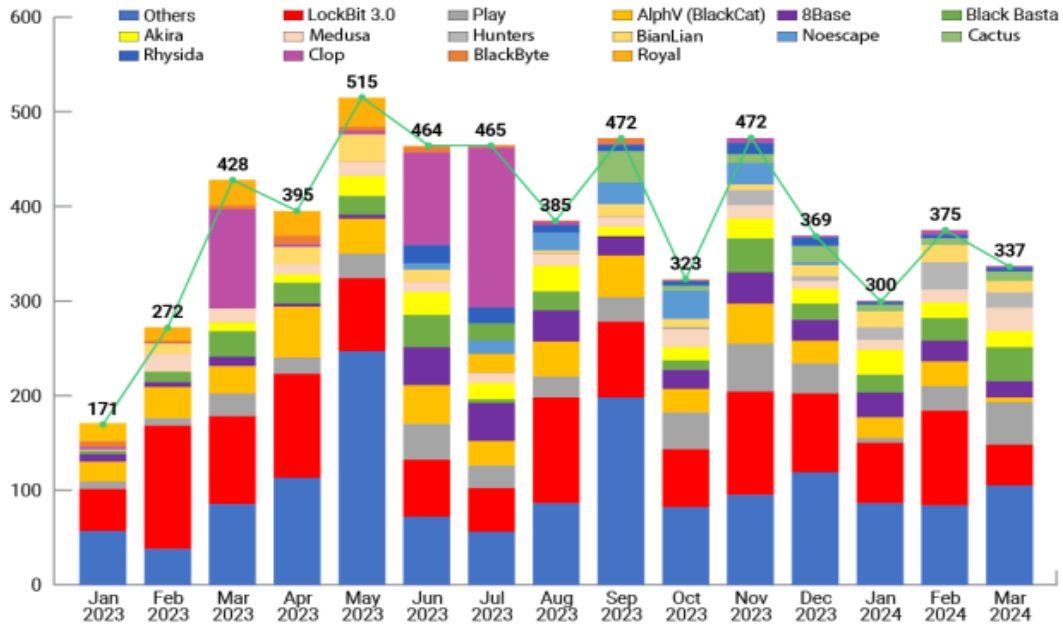


Figure 1:Number of Ransomware Victims Announced [Source: 15]

The article [53] recommended steps in mitigating the impact of ransomware with reducing your blast radius, meaning by limiting access to critical data so that only those who requires access have it. Also, implement a zero-trust security model and finally use user and entity behavior analysis (UEBA). With this tool detection and alert can be received by users (admin) or devices behave abnormally and implement automatic responses to stop threats in their tracks [53].

3.1.2 Grid Manipulation

Threat actors can disrupt energy grids, leading to blackouts or grid instability. The issues related to the electric power grids are a priority to each state's security, energy industry the source of the state economic financial growth. The possible development of so called "smart grids", grids with digital technology that allows two-way communication between the utility and the consumers, represented a big step in the development and the reliability of electricity. However, the digitalization of the grid has raised the vulnerability to cyber-attacks, as it blurred the lines between operational, informational and communication technologies [19]. In a publication [20] if the Smart Meter (SM) is compromised by a cyber-attack, the hacker will be in control of the household power supply and use the SM as an entry point to further attacks to the system's network. The following are features of future grid and cybersecurity challenges, opportunities mentioned by [21] in figure 2 below

Features of future grid		Cybersecurity challenges
Distributed Authority	→	Distributed attack surface
Interconnected Communications	→	Many attacker pivot options
Hierarchal and Coordinated Operation	→	Cascading impacts and failures
Autonomous Operation	→	Trust in autonomous decisions
Scale of number of devices	→	Larger attack surface
Diversity of vendors and devices	→	Supply chain risks

Figure 2: Features of future Grid and Cybersecurity Challenges [Source: 21]

The power system researcher [21] expounded the AI research opportunities available, such as:

i. Distributed Attack Surface: AI for threat correlation across entities and geographies

ii. Multiple Attack Entry Points: Hybrid Intrusion Detection for Energy System

iii. Scale of number of devices: AI for attack anticipation using large datasets [21].

Finally, with grid manipulation, authors in [34] highlight that AI-driven integration can enhance operations by detecting faults, scheduling maintenance and analyzing usage data. This can reduce maintenance costs and required infrastructure investment. It AI can be used for more accurate management of grid voltage and frequency levels [34].

3.1.3 Supply Chain Exploits

Vulnerabilities in third-party software can compromise entire systems. This can lead to loss of energy related industry valuable data with the hope of patching the exploits experience by the firm. While supply chain threats are already high, and threat groups becomes more sophisticated, the situation is amplified when organizations have a lack control of their code. As highlighted by [49] that when established organization use open-source code to deliver solutions and services they put their customers at risk.

3.2 Real-World Incidents

Cyberattacks like ransomware attackers that targeted energy industry is more than double in 2022, with defenders recording 21 attacks through the past October[52], which agree with that ransomware attacks are risen by 13% in the last five years, with an average cost of $1.85 million per incident in 2023 [53]. Several oil storage and transport terminals worldwide-including Oiltanking in Germany, SEA-Invest in Belgium, and Evos in the Netherlands-experienced IT system disruptions. The total number of affected terminals was in the dozens [52].

On February 15, 2023, threat actor group Medusa claimed to have stolen data from PetroChina Indonesia. The hacker group posted some brief information about the oil & gas company on their Dark Web blog and demanded a ransom to delete the victim's data. After extending the deadline of payment by $10,000/day. Medusa also demanded $400,000 from the victim to prevent Medusa from leaking, and another $400,000 for them the recover it [52].

Portugal's EDP, was the victim of a ransomware attack in April of 2020 by [41]. EDP serves 11 million customers and employs 11,500 million people. The cyberattacks stole 10 terabytes of data including sensitive customers information's and credentials in addition demanding $11 million in ransom.

In February 2021, hackers tried to poison the water suppl of a small water treatment in Florida. [31] highlighted that hacker logged into the SCADA remotely**.** Luckily, and employee was stop the attack once they realized the system was being, manipulated-but the threat actors still gain access to the system.

Author [30] added that cyberattacks on energy and commodities infrastructure rose sharply in the third quarter of 2022, with a record high of major incidents. Author [42] highlight that the attack targeted systems at Oiltanking and Mabanaft in Germany, SEA-Invest in Belgium and Evos in the Netherlands. A total of 17 terminals (11 in Germany and six in ARA) were affected, according to Platts. Operational processes, which meant that product couldn't be loaded or uploaded from barges, jammed up while the companies sought to resolve the attack.

The author [30] highlighted a ransomware attack by hackers on Saudi Aramco in 2021, the world's largest single exporter of crude, which involved a data leak and an attempt to extort $50 million from the state-controlled oil producer. The colonial Pipeline Ransomware Attack (2021): Disrupted fuel supplies across the Eastern United States, emphasizing the financial and societal impact of cyber breaches.

The article [52] highlighted that August 2022, the Italian multinational oil company Eni S.P.A disclosed a cyberattack on its computer networks. The attempted ransomware attacks only caused minor damage to affected systems. The company internal systems identified unauthorized network activity in the days before the attacks.

The author [42] highlighted that Triconex Controller Attack at Saudi Aramco, One of the biggest and most sophisticated attacks targeted Triconex controllers at the Saudi Arabian company's oil and gas facilities in 2017. attack was designed to cause severe damage to Saudi Aramco's oil and gas operations. Luckily, a bug in the attacker's computer code shut down the plant's production systems before it could cause severe damage to operational assets and infrastructure [42]. Ukraine Power Grid Attack (2015)**:** A cyberattack left over 230,000 people without power, highlighting the vulnerability of critical infrastructure.

In 2012, 2014, 2017, the researcher [42] highlighted that Shamoom Malware Wipes Data at Saudi Aramco and Other Saudi Arabian

Targets, with reports of a data-destroying virus that was completely wiping out the hard drives of tens of thousands of computers at Saudi Aramco. The author [42] said the hacker took down the world largest oil producers and delayed production. The hack took place with a virus known as "Shamoon" which was "modular and multi-faceted like Stuxnet, but had only one purpose, to find and destroy data.

Expert have warned that cyberattacks on IT infrastructure-like bill payment systems-can have an impact on operations and provided services, meaning that even if an attack only affects the IT side of the business, critical services like energy generation and transmission can be impacted. There is a preponderance of older technologies configured to enable remote management without modern security control like encryption and multifactor authentication [54].

4. AI-Driven Cybersecurity Capabilities

Implementing AI-driven approach in cybersecurity offers a wide range of benefits for related energy industry looking to manage their risk and it capabilities constantly improve as it learns from new data. Techniques like deep learning and machine learning enable AI to recognize patterns, establish a baseline of regular activity, and discover any unusual or suspicious activity that deviates from it [16].

4.1 Threat Detection and Mitigation

The interconnectivity between IT and OT systems, while enhancing operational efficiency, also broadens the attack surface for cyber threats [18]. The 2024 global cyber outlook findings indicate that organizations are paying attention and reacting quickly to mitigate the risks of adopting emerging technology like AI and other advance technologies [17]. AI has significantly enhanced threat detection, [3 scales easily as an organization's digital footprint grows. As cyber threats become more sophisticated.

4.1.1 Anomaly Detection Systems

The implementation of AI-driven technologies with ADS [3] can uncover subtle signs of cyber threats, such as unusual network activity or suspicious user behavior, and identifies deviations in energy consumption or operational patterns indicative of potential breaches. The author [36] highlighted that AI-driven techniques can detect trends and anomalies in network traffic and user behavior that may indicate a potential cyberattack using machine learning algorithms and advanced data analysis. This allows security personnel to respond to potential attacks quickly and proactively. Furthermore, adaptive AI excels in real-time anomaly detection.

4.1.2 Behavioral Analysis

Machine learning models detect unusual user or system behavior, flagging potential insider threats. [36] describes UEBA as an AI-based approach that uses machine learning algorithms, it can detect malicious insiders or compromised accounts which are challenging to detect with traditional security methods. The article [16] highlighted that with behavioral analytics, organizations can identify evolving threats and known vulnerabilities. Traditional security defenses rely on attack signatures and indicators of compromise to discover threats. However, with the thousands of new attacks that cyber criminals launch every year, this approach is not practical. With the implementation of [16] behavioral analytics by any firm will enhance their threat-hunting processes. It uses AI models to develop profiles of the applications deployed on their networks and process vast volumes of device and user data.

4.2 System Resilience

The capability of a system, whether it's engineered, organizational, or software-based to handle disruption and keep functioning is an imperative mechanism. [51] added that system resilience is paramount for several reasons, which include Maintaining continuous operations, minimizing disruption and downtime, protecting against cyber threats, ensuring data integrity and recovery, and adapting to change and scaling. Furthermore, SR as a system design, exhibit several characteristics, which includes: redundancy, fault tolerance, scalability, self-healing capabilities, which is discuss in 4.2.2, isolation and containment, continuous monitoring and analysis etc. [51]

4.2.1 Automated Incident Response

AI-enabled tools can isolate affected systems, neutralize threats, and restore operations with minimal downtime. The authors [40] highlighted that AI-based incident response systems can automate the response to cyber threats that reduced the time required to respond to an attack. These systems can analyze data from various sources and provide actionable insights to the security team to take appropriate action quickly. The article [16] AI-driven security tools are based on rules and algorithms that define how the system should respond based on the circumstances of the event, [3] lead to swift and effective action, significantly reducing response time and helping teams scale and accelerate response efforts.

4.2.2 Self-Healing Networks

With the advent of AI-driven solutions systems can automatically monitor, detect and prevent intrusions without human intervention. AI technologies in the energy industry will enable energy grids to autonomously reroute power and recover from disruptions and [51] this aid each network to automatically detect, diagnose, and resolve issues without human intervention. They lead the system to further initiate corrective actions, such as restarting failed industrial components in the system (PLCs, SCADA, DCS etc.) or reallocating resources, to restore, to normal operation [51]. The health and performance of the self-network depends on the historical analysis of the system provided by AI-driven solution.

4.3 Secure Renewable Integration

The integration of cybersecurity with AI-driven approaches has become paramount to safeguard the critical infrastructure against a myriad of cyber threats and attacks [24] By focusing on the protection systems' cybersecurity, which is crucial for grid reliability, this framework offers a novel strategy for aiding the resilience of renewable energy systems against cyber-attacks [22]. With the rising adoption of renewables, and AI-driven implementation in the industry will enhance the security of distributed energy resources (DERs) by ensuring secure communication between devices, preventing unauthorized access and managing grid stability. It will offer promising solutions to the sector's unique challenges poses by AI deployment. The researchers [27, 28] highlight the significant of machine learning (ML), in enhancing the security of renewable energy systems [26].

A recent research by [25] also give an impressive performance metric accuracy of 92% and false positive rate (FPR) of 2.2% using Kaggle IIoTset dataset. The author [25] IIoT system using ML approach also give general system detection rate of 0.0156 seconds.

5. Performance Capabilities of AI in Cybersecurity

The importance of implementing AI-driven solutions is the driven force behind performance capabilities in the energy industry. AI in cybersecurity with efficient and performance capability can help address the challenges faced by the industry. The integration of AI into cybersecurity for the energy sector delivers measurable benefits, Because AI-driven technologies can process large datasets quickly, detect subtle patterns, and adapt to new threats, it offers a powerful level of efficiency and continuous learning that complements human capabilities and can act as a force multiplier said [3].

5.1 Faster Threat Response

The energy industry with the integration of AI-powered solutions enhances the speed of response in terms of plant optimization and efficient system. Author [28] contributed that AI-driven solution helps improve information security response through rapid and accurate diagnosis of threats and attacks. AI models can analyze behavioral patterns and historical data to identify potential future attacks and take early corrective actions. AI reduces the time required to identify and mitigate attacks, minimizing disruptions during industry plant operations. With AI-driven implementation [16] organizations can detect threats more quickly, faster and resolve some issues automatically.

5.2 Scalability

In the dynamic landscape of AI, scalability faces a formidable challenge with the escalating sophistication of AI models, scalability is achieved by parallel processing, cloud computing, and containerization and microservices architectures, pivotal components that contributes to the achieving scalable AI solutions [43]. With AI can effectively handle and trained large volumes of data, ensuring comprehensive monitoring the industry grows [2].

6. Ethical Considerations and Future Directions

While AI offers significant benefits, its deployment in cybersecurity raises ethical and operational questions. To ensure ethics is the field of cybersecurity, frequently cybersecurity specialist adheres to codes of ethics. These codes aim to promote ethical behavior, responsibility, and integrity in the handling of information and system security [45].

6.1 Bias in AI Models

The conformity of different models depends on the algorithm used for it development which leading to discriminatory outcomes. The use of biased models in cybersecurity has ethical implications [44], model bias in AI can also arise from various sources, including training of data, algorithm design, or interception of results. Authors in [45] highlighted that complying with ethical constraints and sound ethical principles as a software practitioner, trust in AI application in cybersecurity is fostered.

6.2 Transparency and Accountability

AI-driven cybersecurity techniques also have some challenges, [36], one of them is the lack of transparency in AI algorithms [38]. It is imperative to know and comprehend on how an AI system makes judgements, which makes it tough to have dependence in these systems. Another issue is the potential for false positives from AI systems, which could result in pointless alarms and causes disruption in production operations, distract panel operators. Therefore, firms implementing innovative technologies such as AI-driven to stay ahead of the curve as cyber risks evolve [39]. Ensuring explain ability in AI decision-making is critical for regulatory compliance and stakeholder trust. transparency and transparency: Author [29] imperatively added that AI algorithms can be complex, making it difficult to understand how they reach their decisions. This lack of transparency can raise concerns about bias, accountability, and potential misuse.

7. Methods

The method used was the qualitative research method, where pools of past and presents related articles, journals, books and other online materials where systematically studied and explore to effectively drive a detailed information's about topic. The stepwise results and discussions on the topic gives a better understanding on the related pools from the research method deployed etc and successfully points out the challenges and opportunities, performance capabilities of how artificial Intelligence (AI) impact is revolutionizing cybersecurity in the energy industry, addressing the growing complexities and risks associated with digitalization.

8. Conclusion

Artificial Intelligence (AI) is revolutionizing cybersecurity in the energy industry, addressing the growing complexities and risks associated with digitalization. By enhancing threat detection, system resilience, and operational efficiency, AI-driven technologies contribute to the secure and reliable functioning of critical energy infrastructure (EI). However, to fully realize these benefits, stakeholders must address the challenges of implementation, ethical concerns, and evolving threat landscapes. A balanced approach that combines AI innovation with robust cybersecurity frameworks will be essential in ensuring the sustainable and secure growth of the energy industry.

References

1. Siemens (2022), Cybersecurity for Industry, siemen.com/industrial security (Online)
2. Txone network (2024), Securing digital manufacturing, essence of ISA/IEC-62443 implementation (Online)
3. Lucia Stanham (2024), The Role of AI in Cybersecurity**,** (www.crowdstrike.com/cybersecurity-101/artificial-intelligence/).
4. Womack, D.; Krishnan, V.; Lin, S. (2020): Optimizing the chemicals value chain with AI. AI champions are creating more business value and outperforming their peers. https://www.ibm.com/thought-leadership/institute-businessvalue/en-us/report/chemicals-value-chain-ai (Retrieved: 10.03.2024).

5. Khondoker, R., Patwary, M., & Islam, R. (2016) "A comprehensive study on big data issues and challenges", *International Journal of Advanced Computer Science and Applications*, *7*(2), pp. 427-433. https://doi.org/10.14569/IJACSA.2016.070255
6. Marz, N., & Warren, J. (2015) Big Data: Principles and best practices of scalable real-time data systems, Manning Publications.
7. Singh, N., Adhikari, D., (2023), Challenges and Solutions in Integrating AI with Legacy Inventory Systems. *International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2321-9653, 11* (XII).
8. Zokaee, M., Nazari, A., Aghsami, A., & Jolai, F. (2021). An inventory system with coordination among manufacturers and retailers under buyback contract, vertical integration, retailer's effort and carbon footprint constraint. https://doi.org/10.1080/19397038.2021.1986591
9. Ed Bowen, Wendy Frank & Deborah Golden (), Deloitte Insight Cyber AI: Real defense**,** Augmenting security teams with data and machine intelligence, www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html
10. Sundeep Reddy Mamidi (2024), Integrating AI into Legacy Security Systems, International Journal of Enhanced Research in Management & Computer Applications ISSN: 2319-7471, Vol. 13 Issue 8, Impact Factor: 8.285
11. Gnani Prathap Naik Mude (), The Role of Ai In Legacy Software Application Modernization, *International Journal of Marketing and Technology*, *14* (03).
12. Txone Network (2022), In-depth analysis of cyber threats to automotive factories. (Online).
13. Sanjay Fuloria, IBS, Hyderabad (2022), Cybersecurity and Ransomware, Academia Letters, https://doi.org/10.20935/AL4820.
14. Peter Lund (2022), OPSWAT ISS Issue, Cybersecurity: Simplifying Complexity, See All Your OT Assets and Understand How to Protect Them.
15. Ferhat Dikbiyik, Ferdi Gul, Gokcen Tapkan, Yavuz Han, Yunus Dogan, Ozcan Akdora (2024), State of Ransomware: 2024, A Year of Surging and shuffling, Black Kite.
16. CrowdStrike (2024), Indicators of Attack vs Indicators of Compromise, (Online).
17. Jeremy Jurgens & Paolo Dal Cin (2024), Global Cybersecurity Outlook 2024, Insight Report, in collaboration with Accenture. World Economic Forum.
18. Takepoint Research (TPR) (2023), Industrial Cyber Critical Infrastructure Handbook, Industrial Cyber
19. Oracle. (2012). Mitigating Cyber-Security Risk of Smart-Grid AMI. Oracle. Retrieved from www.oracle.com/us/technologies/bpm/mitigate-cyber-security-risk-1533517.pdf.
20. Mahmud R., V. R. (2015). A survey on smart grid metering infrastructures: Threats and solutions. 2015 IEEE International Conference on Electro/Information Technology (EIT) (p. 386–391). IEEE.
21. Richard Macwan & Ryan King (2021), Artificial Intelligence for Energy Systems Cybersecurity, NREL/PR-5R00-81098.
22. Bretas, A., & Dutta, A. (2023). Cyber-Physical power systems protection: the byzantine cybersecurity framework. In 2023 IEEE Kansas Power and Energy Conference (KPEC), 1-5. IEEE. . https://doi.org/10.1109/KPEC58008.2023.10215452
23. Adama, H. E., & Okeke, C. D. (2024). Comparative analysis and implementation of a transformative business and supply chain model for the FMCG sector in Africa and the USA. Magna Scientia Advanced Research and Reviews, 10(02), 265–271. DOI: https://doi.org/10.30574/msarr.2024.10.2.0067
24. Joel O. T., & Oguanobi V. U. (2024). Leadership and management in high-growth environments: effective strategies for the clean energy sector. International Journal of Management & Entrepreneurship Research, 6, 1423-1440, May 2024. DOI: 10.51594/ijmer.v6i5.1092.
25. Boye A. Frederick (2024), Cyberattacks Intrusion Detection and Prevention in Industrial IoT Ecosystem Using CNN and Fuzzy Logic: A Case Study on Kaggle IIoTset Dataset, AITP-ITEP 2024-153.
26. Mohammed, M. S. A. A. (2023). Utilization of Artificial Intelligence (AI) and Machine Learning (ML) in the field of energy research. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 305–318. https://doi.org/10.17762/ijritcc.v11i3.9774.
27. Familoni, B. T., & Babatunde, S. O. (2024). User Experience (Ux) design in medical products: theoretical foundations and development best practices. Engineering Science & Technology Journal, 5(3), 1125-1148.
28. Odimarha, A. C., Ayodeji, S. A., & Abaku, E. A. (2024). The role of technology in supply chain risk management: Innovations and challenges in logistics. Magna Scientia Advanced Research and Reviews, 10(2), 138-145.
29. Mariam Aldhamer (2023), The Impact of Artificial Intelligence on the Future of Cybersecurity, *Multi-knowledge Electronic Comprehensive Journal for Education and Science Publication (MECSJ)*, issue 71, 2616-9185.
30. Eklavya Gupte (2022), 2022 a record year for cyber security incidents targeting oil and energy, Energy Security Sentinel tracks 45 cyberattacks on energy since 2017, US most targeted by hackers, Europe also heavily earmarked, www.spglobal.com
31. Ranold Heil (2024) KPMG, Cybersecurity considerations 2024: Energy and natural resources sector, kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2024-energy-and-natural-resources-sector.html
32. Diana Davies (2022), 5 Big Cyberattacks in Oil and Gas, www.oilandgasiq.com/digital-transformation/articles/5-big-cyber-security-attacks-in-oil-and-gas (Online).
33. Siemens (2024), Leveraging AI for Predictive Maintenance: The Future of Industrial Efficiency,

blog.siemens.com/2024/08/leveraging-ai-for-predictive-maintenance-the-future-of-industrial-efficiency/

34. Henri V. S, Ismael A. R., Hye M. P, Bryden S., Austin W., Harper F., Joshua S., M. L (2024) , The use of AI in improving the Energy Security. visit www.rand.org/t/RRA2907-1.
35. Hua Li J. (2028), Cyber security meets artificial intelligence: a survey. Front Inf Technol Electron Eng. 2018;19(12):1462–74. https://doi.org/10.1631/FITEE.1800573.
36. Mohammed Rizvi (2023), Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention, International Journal of Advanced Engineering Research and Science (IJAERS), Vol-10, Issue-5, Article DOI: https://dx.doi.org/10.22161/ijaers.105.8
37. Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things, 1(1). https://doi.org/10.1007/s43926-020-00001-4
38. de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial IntelligenceBased Cyber Security in the Context of Industry 4.0—A Survey. Electronics, 12(8), 1920. https://doi.org/10.3390/electronics12081920.
39. Harel, Y., Gal, I. Ben, & Elovici, Y. (2017b). Cyber security and the role of intelligent systems in addressing its challenges. ACM Transactions on Intelligent Systems and Technology, 8(4). https://doi.org/10.1145/3057729.
40. Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019b). The Role of Artificial Intelligence in Cyber Security (pp. 170–192). https://doi.org/10.4018/978-1-5225-8241-0.ch009.
41. Dashlane (2022), Real-World Examples of Hackers and Breaches in the Utilities and Energy Industry, dashlane.com (Online).
42. Jacob Fox (2024), 11 Biggest Cybersecurity Attacks in History. Cobalt.
43. Mausam M. Kaur (2023) Comprehensive Guide to Scalability in Artificial Intelligence (AI), blog.accredian.com (Online).
44. Besnik Limaj (2023), Ethical Consideration in AI-powered Cybersecurity, medium .com (Online).
45. Ariel Lopez G., Mailyn M., Ariadna C.M.R., Yahima H.F. & Nayma C. P (2024), Ehics in Artificial Intelligence: Am Approach to Cyberscurity, *Journal Liberamia.org, 27*(73), 38-54, ResearchGate.
46. Kristen Madler & Jamila Amodeo (2024), Counting Energy Cybersecurity Threats, USAID.(Online).
47. Adebimpe B. I., Eseoghene K. & Oluwatosin I. (2022), Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources, International Journal of Science and Research, 12(01), 2978–2995.
48. Barlow, E., (2023), A Surge of Cyber Security for the Energy Sector. Securityhq.com (Online)
49. Barlow, E., (2021), How to mitigate against supply chain attacks. Securityhq.com (Online}
50. Jason S. (2024), Adaptive AI in Cybersecurity: Threat Detection and Response, parangel.medium.com.
51. Resilience System-System Design (2024) geeksforgeeks.com, (Online).
52. Resecurity (2024), Oil, Gas, Energy, Ransomware, Nuclear Energy, Cyber Threats, Cyber Attacks. Rescurity.com. (Online) .
53. Sobers, R., (2024), Ransomware Statistics, Data, Trends and Facts [updated 2024], varonis.com. (Online).
54. Vasquez, C., (2024), Ransomware attacks are hitting energy, oil and gas sectors especially hard, cybercop.com (Online).