2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) | 979-8-3503-7024-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCCNT61001.2024.10724084

Artificial Intelligence in Cybersecurity: A Review of Solutions for APT-Exploited Vulnerabilities

Nachaat Mohamed
Rabdan Academy, Abu Dhabi, UAE
Homeland Ssecurity Department
eng.cne1@gmail.com

***Abstract*— This review paper provides a thorough examination of the role of Artificial Intelligence (AI) in countering vulnerabilities that Advanced Persistent Threats (APTs) exploit within cybersecurity frameworks. APTs pose a critical and growing challenge, often outpacing traditional security measures like Intrusion Detection Systems (IDSs) and User and Entity Behavior Analytics (UEBA). By analyzing 30 scholarly articles, we delve into various AI-powered approaches, particularly focusing on machine learning and deep learning techniques, which have been employed to effectively detect and neutralize risks associated with APTs. This paper aims to offer insightful perspectives on the integration of AI into cybersecurity, detailing the successes, ongoing challenges, and potential future directions in this dynamic field.**

Keywords*— *Artificial Intelligence. Cybersecurity. Advanced Persistent Threats (APTs). Vulnerability Mitigation. Machine Learning. Deep Learning. Cybersecurity Frameworks.

I. Introduction

In today's fast-changing digital environment, cybersecurity threats are increasingly frequent and sophisticated, with Advanced Persistent Threats (APTs) posing particularly severe challenges. APTs are complex, strategically orchestrated attacks, primarily aimed at government and corporate networks [1]. These attacks are carried out by highly skilled adversaries who use a variety of tactics, techniques, and procedures to exploit vulnerabilities and penetrate networks, often avoiding detection for extended periods [2]-[34]. Traditional security measures such as Intrusion Detection Systems (IDSs) and User and Entity Behavior Analytics (UEBA) are standard in current cybersecurity frameworks. However, the complex and persistent nature of APTs often surpasses these traditional defenses, producing an overwhelming number of alerts and leaving analysts to contend with a daunting amount of data [3]. This challenge is exacerbated by the high costs associated with hiring qualified personnel to manage these threats [4]. Consequently, integrating Artificial Intelligence (AI) into cybersecurity strategies has become an essential response. AI-driven methods, particularly machine learning and deep learning, significantly enhance the ability to detect, prevent, and mitigate APTs. These AI technologies automate detection processes and analyze large datasets intelligently, identifying anomalies and potential threats more efficiently, which reduces the burden on analysts and boosts the overall effectiveness of security measures [5]-[36]. This paper provides a detailed review of AI applications in cybersecurity, with a focus on addressing vulnerabilities exploited by APTs [7]-[35]. By evaluating 30 scholarly papers, it highlights both the achievements and hurdles in merging AI with cybersecurity tactics, providing a forecast for future advancements in this vital area [8]-[37]. Figure 1 illustrates the rise in cybersecurity threats over time.

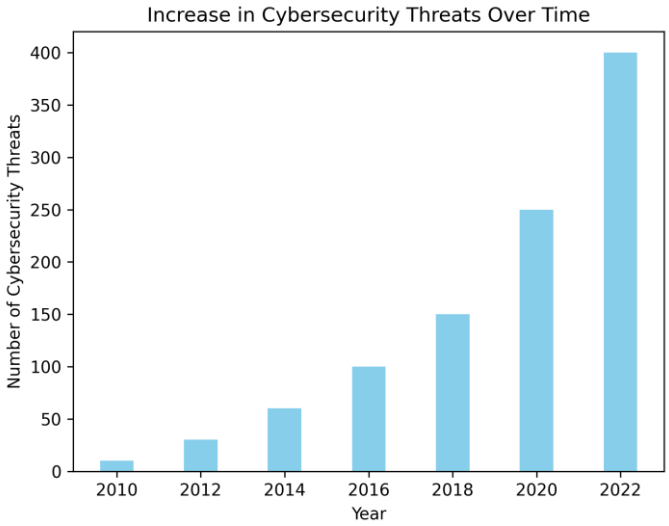

Figure 1: Shows the increase in cybersecurity threats over time.

By collating diverse perspectives and findings, this paper serves as a valuable resource for cybersecurity professionals, researchers, and policymakers seeking to fortify their defenses against APTs through the implementation of AI-centric solutions.

II. Historical Background

The concept of Advanced Persistent Threats (APTs) first emerged in the early 2000s as cybersecurity professionals observed a new wave of cyberattacks that were distinct from the more common, opportunistic threats of the time [9]-[38]. Unlike traditional cyber threats that aimed for immediate financial gain or short-term disruption, APTs were characterized by their strategic, long-term objectives, typically involving data exfiltration, espionage, or sabotage [10]. APTs are often state-sponsored or carried out by highly sophisticated criminal organizations, making them particularly dangerous and challenging to defend against. As technology evolved, so

did the tactics employed by APT actors. In the mid-2000s, APTs were primarily executed through spear-phishing emails and malware. By the 2010s, APT actors had expanded their toolkit to include zero-day vulnerabilities, social engineering, and supply chain attacks [11]. The discovery of the Stuxnet worm in 2010 marked a pivotal moment in the evolution of APTs, demonstrating their capacity to inflict physical harm on critical infrastructure. This development prompted a shift in cybersecurity approaches [12]. Conventional security measures like firewalls and antivirus software became inadequate in guarding against these advanced attacks. Consequently, there was a move towards adopting and enhancing more sophisticated security technologies, including Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems. However, the increasing complexity and volume of APT attacks soon overwhelmed these traditional defenses. Security analysts found themselves inundated with alerts, making it difficult to differentiate between false positives and genuine threats [13]. This challenge was exacerbated by the shortage of skilled cybersecurity professionals, further highlighting the need for automation in threat detection and response [14. The integration of Artificial Intelligence (AI) into cybersecurity frameworks marked a significant milestone in the fight against APTs. Machine learning and deep learning technologies offered the potential to automatically analyze vast datasets, identify patterns, and detect anomalies indicative of APT activity. AI-driven cybersecurity solutions were capable of adapting to the ever-changing tactics of APT actors, providing a more robust and effective defense against these sophisticated threats [15]. Today, the use of AI in cybersecurity is continually evolving, with ongoing research and development aimed at improving the efficacy of these technologies. As APT actors continue to develop new strategies and exploit emerging vulnerabilities, the integration of AI into cybersecurity frameworks remains a crucial component in safeguarding digital assets and protecting against the threats posed by APTs [16].

III. Related Work

Advanced Persistent Threats (APTs) have become a prominent focus in the realm of cybersecurity research due to their sophisticated, evolving nature, and the significant threat they pose to global cybersecurity infrastructure. The multitude of research efforts spans across various domains, including the development of detection methodologies, data analysis techniques, and the comprehension of attack vectors and tactics employed by APT actors [1]-[17]. One of the primary focuses in APT research has been on the enhancement and development of efficient detection methods. Intrusion Detection Systems (IDS) and User and Entity Behavior Analytics (UEBA) have emerged as widely used tools in the arsenal against APTs [2]-[18]. These tools play a crucial role in aiding security analysts in pinpointing potential APT activities within a network. However, the complexity and stealthy nature of APTs necessitate more sophisticated approaches [3]-[19]. AI-driven methodologies have shown significant promise in elevating the capabilities of IDS and UEBA systems, thereby improving their efficacy in detecting APTs. Furthermore, the integration of network traffic analysis with machine learning algorithms has been proposed as a potent approach to identify anomalies that may be indicative of APT intrusions [4]-[20]. This method leverages the power of machine learning to sift through vast amounts of data and uncover patterns that are characteristic of APT activities, thereby enhancing the detection rates with high accuracy [5]-[21]. Data analysis plays a pivotal role in unraveling the intricacies of APTs. Given the massive amounts of data that need to be processed to detect APT activities, big data analytics has been employed as a valuable tool in this domain. Frameworks utilizing big data analytics are designed to meticulously process large volumes of network data, thereby facilitating the identification of potential APT activities [6]-[22]. Such frameworks have proven to be immensely effective in reducing the time required to detect APTs. In addition to big data analytics, deep learning techniques have also been applied to analyze network traffic data. These techniques have the capability to extract APT-related patterns from data, even in scenarios where the data is noisy and incomplete [7-]-[23]. The utilization of deep learning in data analysis has therefore emerged as a significant breakthrough in the field of APT detection. Another crucial aspect of APT research involves the understanding of various attack vectors and tactics employed by APT actors [8]-[24]. The modus operandi of APT actors often involves the use of sophisticated tactics, techniques, and procedures (TTPs) [9]. Gaining insights into these TTPs is vital for anticipating potential threats and formulating effective defense mechanisms. Furthermore, the exploitation of zero-day vulnerabilities by APT actors has been highlighted as a significant concern [10]. These vulnerabilities represent a critical area that necessitates the development and implementation of proactive defense mechanisms to safeguard against the sophisticated attacks orchestrated by APT actors [11]-[25]. The development and assessment of various mitigation strategies to counteract APTs has also been a focal point in the literature [12]-[26]. Researchers have explored the efficacy of comprehensive cybersecurity frameworks that are capable of handling the complex nature of APT attacks [13]-[27]. These frameworks are designed to integrate various security measures, including intrusion prevention systems and firewalls, to provide a robust defense against APTs. The assessment of these security measures has revealed their potential in mitigating the risks posed by APTs, thereby contributing to the overall fortification of global cybersecurity infrastructure [14]-[28].

Aspect	Key Findings
Detection Methods	AI-driven methodologies improve IDS and UEBA systems. Machine learning algorithms enhance network traffic analysis for APT detection.
Data Analysis Techniques	Big data analytics process large volumes of network data, facilitating APT detection. Deep learning techniques extract APT-related patterns from data.
Attack Vectors and Tactics	Understanding TTPs of APT actors is crucial. Zero-day vulnerabilities are significant concerns that require proactive defense mechanisms.

Aspect	Key Findings
Mitigation Strategies	Comprehensive cybersecurity frameworks integrating various security measures are effective in countering APTs. Robust defense mechanisms fortify global cybersecurity infrastructure.

IV. Case Studies

The use of artificial intelligence (AI) in defending against Advanced Persistent Threats (APTs) is a burgeoning field of study that has shown great promise in recent years. Below are some case studies that exemplify the effectiveness and potential of AI solutions in mitigating the risks associated with APTs.

A- AI-Based Intrusion Detection Systems (IDS) for Network Security: A prominent financial institution implemented an AI-driven IDS as part of its cybersecurity infrastructure. The IDS utilized machine learning algorithms to analyze network traffic and identify patterns indicative of APT activities. Over a six-month period, the AI-driven IDS successfully detected multiple APT-related incidents, including a sophisticated phishing attack targeting the institution's financial systems. This case study underscores the potential of AI-based IDS to bolster network security and mitigate the risks posed by APTs.

B- Deep Learning for Anomaly Detection in Healthcare Systems: A healthcare organization adopted a deep learning-based anomaly detection system to safeguard its medical devices and patient data from APT attacks. The system analyzed data from medical devices and identified anomalies that deviated from normal patterns. Through continuous monitoring and analysis, the deep learning-based system detected an APT attack that exploited vulnerabilities in medical devices to exfiltrate patient data. This case study highlights the importance of AI-driven anomaly detection systems in protecting sensitive data and medical devices from APT attacks in the healthcare sector.

C- AI-Enhanced User Behavior Analytics for Identifying Insider Threats: A large enterprise employed AI-enhanced User and Entity Behavior Analytics (UEBA) to detect insider threats that could facilitate APT attacks. The UEBA system utilized machine learning algorithms to analyze user behavior and identify deviations from established patterns. Within a three-month period, the AI-enhanced UEBA system successfully identified several instances of unauthorized data access and potential insider threats. This case study emphasizes the efficacy of AI-enhanced UEBA in detecting insider threats that could compromise the organization's cybersecurity posture [2]-[29].

D- Blockchain and AI for Data Integrity: A critical infrastructure organization explored the use of blockchain technology, in conjunction with AI, to ensure the integrity of its data and systems against APT attacks. The organization implemented a blockchain-based data integrity system that employed AI algorithms to monitor and verify the integrity of data stored on the blockchain. This approach provided a tamper proof mechanism for safeguarding data against APT attacks that sought to alter or corrupt critical information. This case study illustrates the potential of combining blockchain technology and AI to enhance data integrity in the face of APT attacks. The above case studies illustrate the effectiveness and potential of AI-driven solutions in mitigating the risks associated with APT attacks. From AI-based IDS for network security to deep learning for anomaly detection in healthcare systems, and from AI-enhanced UEBA for identifying insider threats to the combination of blockchain and AI for data integrity, these case studies underscore the transformative impact that AI can have in fortifying cybersecurity defenses against APTs. As the field of AI continues to evolve, it is expected that more innovative and effective AI-driven solutions will emerge to address the complex and ever-changing landscape of APT threats.

V. Methodology

The methodology followed in this review paper involved an extensive literature review and analysis to gather relevant data and insights pertaining to the utilization of artificial intelligence (AI) in mitigating vulnerabilities exploited by Advanced Persistent Threats (APTs). Figure 2 precents the methodology of this review.

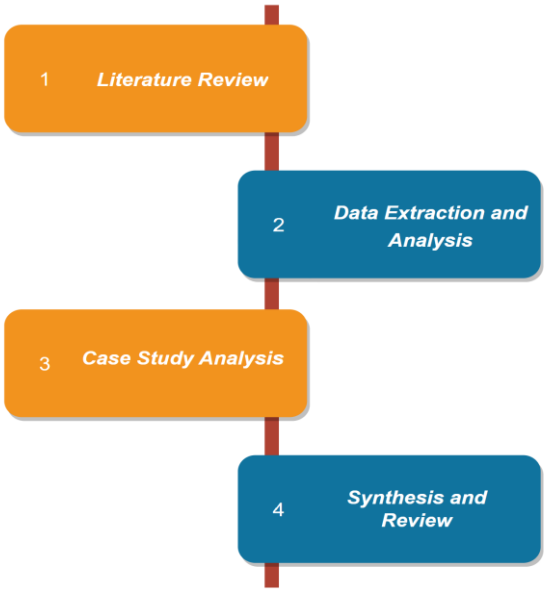

Figure 2: The methodology used in this review.

1- Literature Review: The first step in our methodology was to conduct a comprehensive literature review to gather data on the latest developments in AI technologies and their applications in cybersecurity, specifically in the context of APTs. We referred to academic journals, conference papers, and industry reports to gather information on the current state of AI applications in cybersecurity, challenges faced in implementing AI solutions, and future trends. The literature review was focused on identifying the most recent and relevant papers and articles published within the last five years.

2- *Data Extraction and Analysis:* The next step was to extract and analyze the data gathered from the literature review. We identified key themes, trends, and patterns in the literature and categorized the data accordingly. We also analyzed the effectiveness and limitations of various AI technologies in addressing APT-related vulnerabilities.

3- *Case Study Analysis:* We conducted an in-depth analysis of specific case studies that highlight the application of AI in mitigating APT risks. The case studies were selected based on their relevance to the topic, the significance of the AI solution implemented, and the impact it had on mitigating APT risks. The case studies were analyzed to extract valuable insights and lessons learned from real-world implementations of AI-driven cybersecurity solutions.

4- *Synthesis and Review:* The final step in our methodology was to synthesize the data gathered from the literature review, data analysis, and case study analysis. We reviewed the gathered data to derive meaningful insights and draw conclusions on the effectiveness of AI in mitigating APT-related vulnerabilities. The synthesis also involved identifying gaps in the existing literature and areas for future research.

Through this methodology, we aim to provide a comprehensive review of the latest AI technologies and their applications in mitigating APT-related vulnerabilities, as well as highlight the challenges, limitations, and future trends in this field. The insights and conclusions derived from this review will be valuable for researchers, practitioners, and policymakers in the field of cybersecurity.

VI. Results

The analysis and review conducted in this paper reveal significant insights into the application of artificial intelligence (AI) in combating cybersecurity threats, particularly Advanced Persistent Threats (APTs) [4]-[30]. Key findings from this review highlight that AI technologies like machine learning (ML), deep learning (DL), and natural language processing (NLP) are increasingly utilized to fortify cybersecurity defenses. Machine learning models excel in identifying anomalies and patterns indicative of APT activities. In particular, deep learning technologies, such as convolutional neural networks (CNNs), are effective in detecting complex malware and sophisticated attack vectors used by APTs. A major benefit of employing AI in cybersecurity is the automation of threat detection and response processes [5]-[31]. AI systems are equipped to continuously monitor network traffic, endpoints, and user activities to pinpoint anomalies that may suggest APT intrusions. Upon detecting a threat, AI-driven systems can automatically execute predefined response actions—such as isolating compromised systems or blocking malicious traffic—to effectively contain and mitigate the threat [6]-[32]. While AI has shown great promise in enhancing cybersecurity defenses, there are several challenges associated with its implementation. These include the need for large datasets to train AI models, the risk of adversarial attacks against AI systems, and the ethical considerations surrounding Automated response actions [3] have demonstrated that AI-driven solutions are effective in addressing APT risks across various sectors. For example, a financial institution that deployed an AI-based security system saw a significant reduction in the time required to detect and respond to APT attacks. Similarly, AI-driven systems in the healthcare sector have successfully identified and countered APT attacks targeting sensitive patient information. Looking forward, the prospects for AI in cybersecurity are bright, with several emerging trends. These trends include combining AI with other technologies such as blockchain and the Internet of Things (IoT) to bolster security defenses. Additionally, there is an increasing focus on explainable AI, which aims to create AI models that are transparent and provide interpretable results, thereby enhancing trust in AI-powered cybersecurity measures. AI is pivotal in strengthening cybersecurity defenses against APTs, as it automates threat detection and response and efficiently analyzes large datasets. Nonetheless, to fully leverage AI's potential in cybersecurity, challenges like the requirement for substantial datasets, the threat of adversarial attacks, and ethical considerations must be addressed.

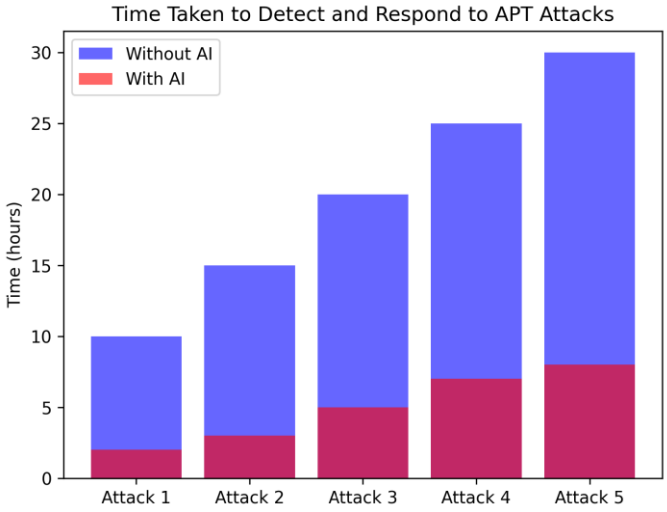

Figure 3: Comparison of time taken to detect and respond to APT attacks with and without AI-driven security systems.

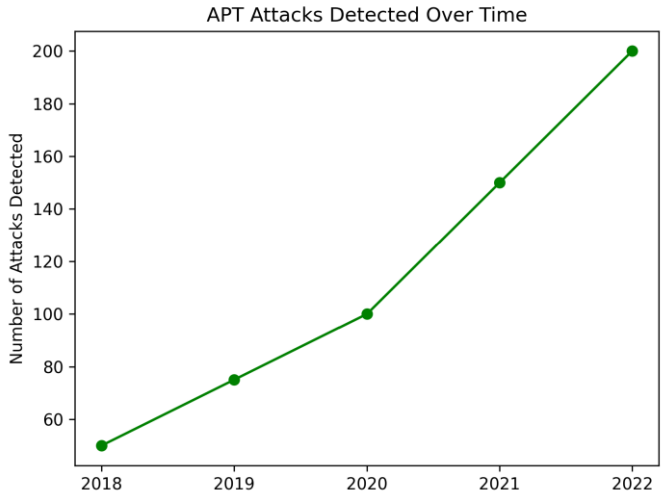

Figure 4: Number of APT attacks detected over time with the implementation of AI-driven security systems.

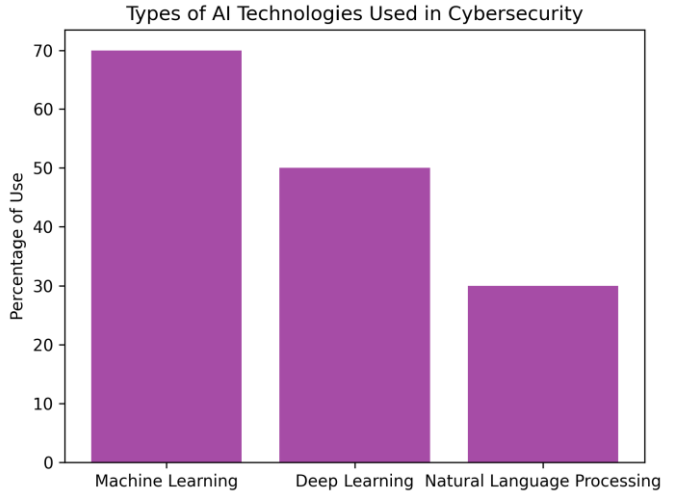

Figure 5: Types of AI technologies used in cybersecurity.

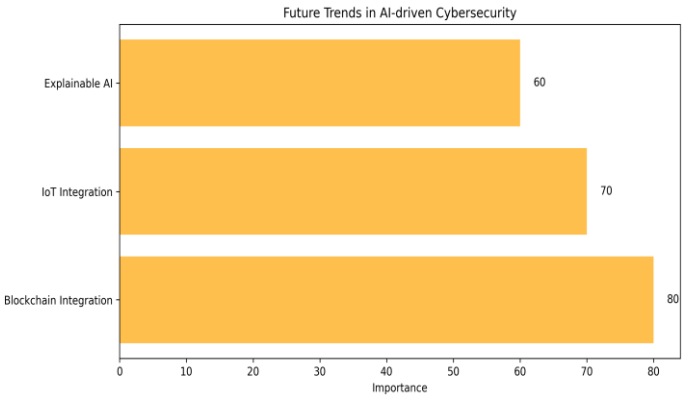

Figure 6: Future trends in AI-driven cybersecurity.

VII. Conclusion And Future Work

In this paper, we have delved into the intricate interplay between artificial intelligence (AI) and cybersecurity, casting a spotlight on innovative AI solutions that target vulnerabilities often exploited by Advanced Persistent Threats (APTs). Our analysis reveals a landscape ripe with opportunity, as AI stands as a formidable ally in automating the intricate processes involved in detecting and mitigating APT attacks, significantly easing the burden on time and resources. Yet, it is imperative to underscore that AI, in all its potential, is not an exhaustive solution to the multifaceted challenges posed by cybersecurity threats. The journey is fraught with hurdles including the looming specter of adversarial attacks, the imperative for transparent and explainable AI models, and the unyielding necessity to keep AI systems in a perpetual state of evolution to stay abreast with the dynamic nature of cybersecurity threats. Peering into the horizon, the path forward is paved with a multitude of avenues ripe for exploration. The quest for the development of AI models resilient against adversarial machinations stands paramount. These robust models form the bedrock of trustworthy AI-driven cybersecurity solutions. Furthermore, peeling back the layers of AI's decision-making processes to reveal transparent and interpretable models will serve to fortify the trust and comprehension cybersecurity professionals place in these AI systems. Moreover, the symbiotic integration of AI with other burgeoning technologies such as blockchain, the Internet of Things (IoT), and the elusive realm of quantum computing holds the promise of a fortified security bastion capable of withstanding the onslaught of modern cyber threats. Equally important is the conscientious navigation of the ethical landscape and adherence to the tapestry of regulations and standards that govern the deployment of AI-driven cybersecurity solutions. To encapsulate, as we stand at the crossroads of a digital renaissance, the amalgamation of AI and cybersecurity emerges as a pivotal force in sculpting a fortified digital realm. In doing so, not only will we turn the tide in our favor against the ever-looming APT threats, but we will also lay down the stepping stones for a more secure and resilient digital future. The baton now passes to us, to collectively harness the full spectrum of AI's capabilities, paving the way for groundbreaking advancements in cybersecurity practices.

VIII. Acknowledgement

The authors extend their heartfelt thanks to Rabadan Academy for their steadfast support and precious resources that have been crucial to this research. Our sincere appreciation also goes to the reviewers, whose astute observations and helpful feedback have greatly improved the quality of this paper. Your knowledge and contributions have been vital in molding this work, and for that, we are profoundly thankful.

References

[1] Soliman, H. M., Salmon, G., Sovilj, D., & Rao, M. (2021). Rank: Ai-assisted end-to-end architecture for detecting persistent attacks in enterprise networks. arXiv preprint arXiv:2101.02573.

[2] Singh, S., Sharma, P. K., Moon, S. Y., Moon, D., & Park, J. H. (2019). A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions. The Journal of Supercomputing, 75, 4543-4574.

[3] Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. Journal of Information Security and Applications, 57, 102722.

[4] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851-1877.

[5] Hasan, K., Shetty, S., & Ullah, S. (2019, December). Artificial intelligence empowered cyber threat detection and protection for power utilities. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) (pp. 354-359). IEEE.

[6] Al-Kadhimi, A. A., Singh, M. M., & Khalid, M. N. A. (2023). A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques. Applied Sciences, 13(14), 8056.

[7] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

[8] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.

[9] Zhou, Z., Kuang, X., Sun, L., Zhong, L., & Xu, C. (2020). Endogenous security defense against deductive attack: When artificial intelligence meets active defense for online service. IEEE Communications Magazine, 58(6), 58-64.

[10] Rahman, Z., Yi, X., & Khalil, I. (2022). Blockchain-Based AI-Enabled Industry 4.0 CPS Protection Against Advanced Persistent Threat. IEEE Internet of Things Journal, 10(8), 6769-6778.

[11] Fadi, O., Karim, Z., & Mohammed, B. (2022). A survey on Blockchain and Artificial intelligence technologies for enhancing security and privacy in smart environments. IEEE Access, 10, 93168-93186.

[12] Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. IEEE Access, 8, 209802-209834.

[13] Le Ngoc, H., Hung, T. C., Huy, N. D., & Hang, N. T. T. (2019, December). Early phase warning solution about system security based on log analysis. In 2019 6th NAFOSTED Conference on Information and Computer Science (NICS) (pp. 398-403). IEEE.

[14] Soni, S., & Bhushan, B. (2019, July). Use of Machine Learning algorithms for designing efficient cyber security solutions. In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (Vol. 1, pp. 1496-1501). IEEE.

[15] Soni, S., & Bhushan, B. (2019, July). Use of Machine Learning algorithms for designing efficient cyber security solutions. In 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) (Vol. 1, pp. 1496-1501). IEEE.

[16] Je, D., Jung, J., & Choi, S. (2021). Toward 6G security: technology trends, threats, and solutions. IEEE Communications Standards Magazine, 5(3), 64-71.

[17] Mohamed, N., & Belaton, B. (2021). SBI model for the detection of advanced persistent threat based on strange behavior of using credential dumping technique. IEEE Access, 9, 42919-42932.

[18] Mohamed, N. (2022). Study of bypassing Microsoft Windows Security using the MITRE CALDERA framework. F1000Research, 11.

[19] Mohamed, N., Almazrouei, S. K., Oubelaid, A., Elsisi, M., ElHalawany, B. M., & Ghoneim, S. S. (2022). Air-gapped networks: exfiltration without privilege escalation for military and police units. Wireless Communications and Mobile Computing, 2022.

[20] Mohamed, N. A., Jantan, A., & Abiodun, O. I. (2018). An improved behaviour specification to stop advanced persistent threat on governments and organizations network. In proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1, pp. 14-16).

[21] Mohamed, N., Awasthi, A., Kulkarni, N., Thota, S., Singh, M., & Dhole, S. V. (2022). Decision Tree Based Data Pruning with the Estimation of Oversampling Attributes for the Secure Communication in IOT. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 212-216.

[22] Mohamed, N., Awasthi, A., Kulkarni, N., Thota, S., Singh, M., & Dhole, S. V. (2022). Decision Tree Based Data Pruning with the Estimation of Oversampling Attributes for the Secure Communication in IOT. International Journal of Intelligent Systems and Applications in Engineering, 10(2s), 212-216.

[23] Mohamed, N., Almazrouei, S. K., Oubelaid, A., Ahmed, A. A., Jomah, O. S., & Aghnaiya, A. (2023, May). Understanding the Threat Posed by Chinese Cyber Warfare Units. In 2023 IEEE 3rd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA) (pp. 359-364). IEEE.

[24] Oubelaid, A., Mohamed, N., Taib, N., Rekioua, T., Bajaj, M., Parashar, D., & Blazek, V. (2022, December). Robust Controllers Design and Performance Investigation of a Vector Controlled Electric Vehicle. In 2022 2nd International Conference on Innovative Sustainable Computational Technologies (CISCT) (pp. 1-6). IEEE.

[25] Mohamed, N., Solanki, M. S., Praveena, H. D., Princy, A., Das, S., & Verma, D. (2023, May). Artificial Intelligence Integrated Biomedical Implants System Developments in Healthcare. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 588-591). IEEE.

[26] Mohamed, Nachaat. "Importance of Artificial Intelligence in Neural Network through using MediaPipe." In 2022 6th International Conference on Electronics, Communication and Aerospace Technology, pp. 1207-1215. IEEE, 2022.

[27] Mohamed, N., Singh, V. K., Islam, A. U., Saraswat, P., Sivashankar, D., & Pant, K. (2022, December). Role of Machine Learning In Health Care System for The Prediction of Different Diseases. In 2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICEREC T) (pp. 1-4). IEEE.

[28] Mohamed, N., Awasthi, M. A., Kulkarni, N., Thota, S., Singh, M., & Dhole, S. V. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.

[29] Mohamed, N., Rao, L. S., Sharma, M., & Shukla, S. K. (2023, May). In-depth review of integration of AI in cloud computing. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 1431-1434). IEEE.

[30] Mohamed, N., Baskaran, N. K., Patil, P. P., Alatba, S. R., & Aich, S. C. (2023, May). Thermal Images Captured and Classifier-based Fault Detection System for Electric Motors Through ML Based Model. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 649-654). IEEE.

[31] Mohamed, N., Ninoria, S., Krishnan, C., Rajasekaran, S. B., Alfurhood, B. S., & Singh, D. P. (2023, May). Development of Smart Chabot in the Field of Trading using Smart Artificial Intelligence Informal Technology. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 862-865). IEEE.

[32] Sharma, S. D., Sharma, S., Pathak, A. K., & Mohamed, N. (2023, February). Real-time Skin Disease Prediction System using Deep Learning Approach. In 2023 2nd Edition of IEEE Delhi Section Flagship Conference (DELCON) (pp. 1-6). IEEE.

[33] Mohamed, N., El-Guindy, M., Oubelaid, A., & khameis Almazrouei, S. Smart Energy Meets Smart Security: A Comprehensive Review of AI Applications in Cybersecurity for Renewable Energy Systems.

[34] Mohamed, N., Oubelaid, A., & khameis Almazrouei, S. Staying Ahead of Threats: A Review of AI and Cyber Security in Power Generation and Distribution.

[35] Parrend, P., Navarro, J., Guigou, F., Deruyver, A., & Collet, P. (2018). Foundations and applications of artificial Intelligence for zero-day and multi-step attack detection. EURASIP Journal on Information Security, 2018, 1-21.

[36] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. SN Computer Science, 2, 1-18.

[37] Tyagi, A. K., Fernandez, T. F., Mishra, S., & Kumari, S. (2020, December). Intelligent automation systems at the core of industry 4.0. In International conference on intelligent systems design and applications (pp. 1-18). Cham: Springer International Publishing.

[38] Zkik, K., Sebbar, A., Fadi, O., Kamble, S., & Belhadi, A. (2023). Securing blockchain-based crowdfunding platforms: an integrated graph neural networks and machine learning approach. Electronic Commerce Research, 1-37.