2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT) | 979-8-3503-7024-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCCNT61001.2024.10725548

DDoS Attacks Mitigation: A Review of AI-Based Strategies and Techniques

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

***Abstract*— In the evolving landscape of cyber threats, Distributed Denial of Service (DDoS) attacks represent a significant challenge for online infrastructure security. This review paper delves into the efficacy of Artificial Intelligence (AI)-based strategies and techniques in mitigating DDoS attacks. It synthesizes current research and developments in the field, emphasizing the adaptability and resilience of AI methods against the dynamic nature of these attacks. The paper categorizes various AI approaches, including machine learning algorithms, deep learning frameworks, and heuristic methods, analyzing their strengths and limitations in real-world scenarios. Additionally, it explores the integration of AI with traditional security protocols to enhance defense mechanisms. Through a comprehensive examination of case studies and experimental results, this paper highlights the transformative impact of AI in detecting, analyzing, and neutralizing DDoS threats, thereby offering valuable insights for researchers and practitioners in cybersecurity. The review concludes with a discussion on future trends and potential research directions, underscoring the importance of continuous innovation in AI technologies to combat the evolving sophistication of DDoS attacks.**

Keywords*— *Artificial Intelligence (AI). DDoS Mitigation. Cybersecurity. Machine Learning Algorithms. Network Security

I. INTRODUCTION

In the digital era, cybersecurity has emerged as a paramount concern for individuals, organizations, and governments worldwide. Among the plethora of cyber threats, Distributed Denial of Service (DDoS) attacks have gained notoriety for their ability to disrupt services and cause significant financial and reputational damage [1]. These attacks involve overwhelming a target's network infrastructure with a flood of internet traffic, rendering it inaccessible to legitimate users. The complexity and frequency of DDoS attacks have escalated, necessitating more sophisticated defense mechanisms[2,17]. Artificial Intelligence (AI) has shown considerable promise in enhancing cybersecurity defenses, offering innovative solutions to detect and mitigate DDoS attacks. AI's ability to learn from data and adapt to new threats makes it a potent tool against the dynamic and evolving nature of cyberattacks [3,18]. This paper reviews the latest AI-based strategies and techniques employed in DDoS attack mitigation. It examines how AI algorithms, including machine learning and deep learning, are being leveraged to identify attack patterns, predict potential threats, and automate response mechanisms effectively [4,19]. The integration of AI in cybersecurity not only offers improved accuracy in threat detection but also enhances the speed and efficiency of response to DDoS incidents. Traditional security measures often struggle to keep pace with the rapid evolution of DDoS tactics. In contrast, AI-driven systems can continuously learn from network traffic data, enabling them to identify even the most subtle indications of an impending attack [5,20]. However, the implementation of AI in cybersecurity is not without challenges. Issues such as the need for extensive training data, the potential for false positives, and the susceptibility of AI systems to adversarial attacks pose significant hurdles [11,21]. This paper aims to provide a comprehensive overview of AI-based DDoS mitigation techniques, discussing their strengths, limitations, and the future direction of this field. Figure 1 represents the hypothetical increase in DDoS attacks from 2015 to 2023.

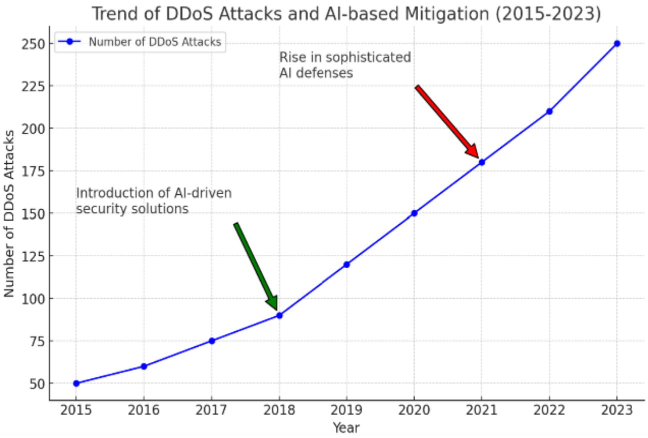

Figure 1: The hypothetical increase in DDoS attacks from 2015 to 2023.

By exploring the intersection of AI and cybersecurity, this review seeks to shed light on the transformative impact of AI in fortifying digital defenses against DDoS attacks. It serves as a resource for cybersecurity professionals, researchers, and policymakers, offering insights into the current state of AI applications in DDoS mitigation and guiding future innovations in this critical domain[12].

II. HISTORICAL BACKGROUND

The phenomenon of Distributed Denial of Service (DDoS) attacks has evolved significantly since its inception, paralleling the rapid advancement of internet technologies. This section provides a historical perspective on the emergence and progression of DDoS attacks, alongside the concurrent development of mitigation strategies, with a particular focus on the role of Artificial Intelligence (AI) [13,22]. The late 1990s marked the genesis of DDoS attacks, characterized by their rudimentary form compared to today's sophisticated tactics. Initially, these attacks were primarily executed by exploiting network vulnerabilities to flood servers with excessive traffic, thereby disrupting services [14,23]. The early 2000s witnessed the first major DDoS attacks, capturing global attention due to their impact on prominent internet platforms. Initial responses to these threats were primarily reactive, focusing on bandwidth expansion and rudimentary filtering methods to mitigate the impact. As internet infrastructure evolved, so did the complexity of DDoS attacks [15,24]. Attackers began to employ more sophisticated techniques, such as amplification attacks and botnets, significantly increasing the scale and impact of their operations. This period saw a shift in mitigation strategies towards more proactive measures. Traditional approaches, such as firewalls and intrusion detection systems, became standard components of cybersecurity defenses but often fell short against more advanced attacks [16-25]. The late 2010s marked a turning point in DDoS mitigation with the introduction of AI and machine learning technologies. As DDoS attacks continued to grow in volume, variety, and velocity, traditional security measures struggled to keep pace. The application of AI in cybersecurity provided a new frontier in the battle against these threats. Machine learning algorithms began to be used for anomaly detection, enabling the identification of unusual traffic patterns indicative of a DDoS attack [17,26]. This era also witnessed the integration of deep learning techniques, which further enhanced the predictive capabilities and response times of mitigation systems. Looking ahead, the continued evolution of DDoS attacks is inevitable, driven by advancements in technology and the increasing interconnectedness of digital systems. However, the ongoing development of AI and machine learning technologies offers a beacon of hope. The future of DDoS mitigation lies in the advancement of AI-driven solutions, which are expected to become more autonomous, adaptive, and effective [27]. The challenge for cybersecurity experts is to stay ahead of attackers by continuously innovating and improving AI-based security measures.

III. LITERATURE REVIEW

The landscape of Distributed Denial of Service (DDoS) attacks and their mitigation has been a focal point of research in the field of cybersecurity, particularly with the advent and integration of Artificial Intelligence (AI) and machine learning technologies. This literature review synthesizes insights from recent scholarly articles, highlighting the evolving nature of DDoS threats and the innovative AI-based strategies being developed to counter them. The proliferation of 5G technology has significantly heightened the risks associated with DDoS attacks. A study addresses this challenge by proposing a novel solution that leverages smart contracts and machine learning. This approach, unique in its use of blockchain technology, aims to obfuscate servers and utilizes transaction fees to limit the scale of potential DDoS attacks. This method marks a significant departure from traditional 4G defenses and common AI-based detection systems, focusing on the source trustworthiness of training samples to mitigate backdoor vulnerabilities in AI models [1]. the study emphasizes the necessity for dynamic analysis in identifying and preventing DDoS attacks, given their rapidly changing patterns, ports, and protocols. Traditional signature-based and anomaly-based defense mechanisms have shown limitations in this context. The paper calls for more extensive research into AI and statistical techniques to develop more effective defense features and mechanisms. This reflects a broader trend in cybersecurity, where adaptive, AI-driven solutions are increasingly seen as essential in the ever-changing landscape of cyber threats [2]. The work of brings a unique perspective by focusing on the security of avionics communication systems. They propose an AI-based solution using artificial neural networks (ANN) to address the security vulnerabilities in future avionics communication networks, especially those incorporating technologies like software-defined networking (SDN). This approach underscores the potential of AI in securing highly specialized and critical communication systems [3]. In the realm of intrusion detection systems (IDS), [Author 4]'s research highlights the importance of feature selection (FS) in machine learning and deep learning models. By using ensemble feature selection techniques, their study achieves a significant reduction in features required for effective DDoS attack classification. This not only improves model performance but also reduces training time, showcasing the efficiency gains AI can bring to cybersecurity [4]. Another study explores the deployment of AI in aviation networks, specifically considering the safety and security challenges. They examine the vulnerability of AI-based intrusion detection systems to adversarial attacks, such as poisoning attacks, and their impact on the performance of deep neural network algorithms. This study is crucial in understanding the vulnerabilities of AI systems themselves and the need for robust, secure AI solutions in critical infrastructure [5]. More literature focus on the development of AI models capable of identifying DDoS attacks as they occur. These models employ advanced machine learning algorithms, such as Support Vector Machines (SVM) and Random Forests, to analyze network traffic patterns in real-time. The key advantage of these approaches lies in their ability to rapidly adapt to new attack vectors, thereby significantly reducing the window of vulnerability [6]. The implementation of explainable AI to enhance Domain Name Service (DNS) security represents a significant advancement. With the rise of DNS over HTTPS (DoH) protocols, ensuring privacy and security while maintaining the ability to detect malicious traffic poses a new challenge. A recent study utilizes a novel machine learning framework, achieving high precision, recall, and F1 scores in detecting and classifying DNS over HTTPS attacks. The use of explainable AI methods in this context is particularly noteworthy, as it aids in understanding the underlying feature contributions, enhancing transparency and reliability in AI-based security solutions [7,29]. The research problem of indistinguishable characteristics in changing DDoS attacks has led to the development of AI methodologies for end-to-end defense. These AI-based defenses, often relying on machine-learning-as-a-service (MLaaS) due to resource constraints, face the risk of malicious training, known as the AI Trojan attack. One study introduces a GAN-based AI Robustness test algorithm, Deep Learning Attack Generator (DLAG), which effectively detects training imbalances and ensures the robustness of AI models against such vulnerabilities. This approach is critical in establishing trust in AI-based defense mechanisms [8]. In the context of vehicular ad-hoc networks (VANETs), the detection of jamming attacks, particularly those targeting safety-critical Cooperative Intelligent Transportation Systems (C-ITS) applications, is vital. A hybrid jamming detector combining statistical network traffic analysis with data mining methods shows promise in addressing real-time jamming detection challenges in V2X (vehicle-to-everything) safety-critical scenarios. This study's use case, focusing on platooning C-ITS applications, highlights the potential of AI in enhancing vehicular network security against sophisticated attacks [9,30]. The flexibility and scalability of Software Defined Networking (SDN) are accompanied by new security vulnerabilities, including low-rate and stealthy DoS attacks. A novel defense framework, Q-MIND, employs a Reinforcement Learning-based approach using Q-Learning to optimize attack detection performance in SDN environments. This framework showcases the efficacy of machine learning in identifying and mitigating stealthy DoS attacks, a growing concern in SDN-based networks [10, 28]. Table distills the core elements of each study, offering a clear comparison of approaches in literature.

Table 1: Distills the core elements of each study, offering a clear comparison of approaches in the literature.

Study	Methodology	Strengths	Limitations	Unique Contributions
[1]	Smart contracts & ML in blockchain networks	Innovative use of blockchain; high precision in distinguishing traffic	Requires blockchain infrastructure; complex implementation	Hides server in blockchain; uses transaction fees to limit attack scale
[2]	AI & statistical techniques for defense	Adapts to changing attack patterns	May not cover all attack types; requires extensive data	Focuses on real-time, adaptive analysis of attack features
[3]	AI with ANN for securing avionics networks	Addresses specific vulnerabilities of avionics networks	Focused on a niche area; may not generalize	Tailored AI solution for avionics communication systems
[4]	Ensemble Feature Selection in ML & DL models	Reduces feature set significantly; improves performance	Requires large datasets; potential overfitting	Combines multiple FS methods for optimal feature set extraction
[5]	Deep learning for intrusion detection	Evaluates impact of AI security attacks on performance	Specific to aviation networks; complex validation process	Addresses safety issues of AI in aviation network security
[6]	Hybrid detector combining traffic analysis & data mining	Effective in C-ITS applications; real-time detection	Focused on vehicular networks; may not apply to other networks	Innovative approach for jamming detection in V2X scenarios

The literature review reveals a dynamic landscape in AI-based DDoS mitigation, highlighting diverse methodologies ranging from blockchain integration to advanced machine learning techniques. Despite varying focus areas, a common thread is the emphasis on adaptability and precision. However, challenges such as data requirements and domain-specific limitations persist, underscoring the need for continuous innovation.

IV. METHODOLOGY

In this review paper, we adopt a systematic and comprehensive methodology to explore AI-based strategies in mitigating Distributed Denial of Service (DDoS) attacks. Our methodological framework is designed to ensure an exhaustive and unbiased examination of the existing literature, thereby providing a holistic view of the advancements and challenges in this rapidly evolving field. Through this approach, we aim to identify key trends, assess the effectiveness of various AI techniques, and pinpoint areas requiring further research. The following steps outline our rigorous approach to conducting this literature review.

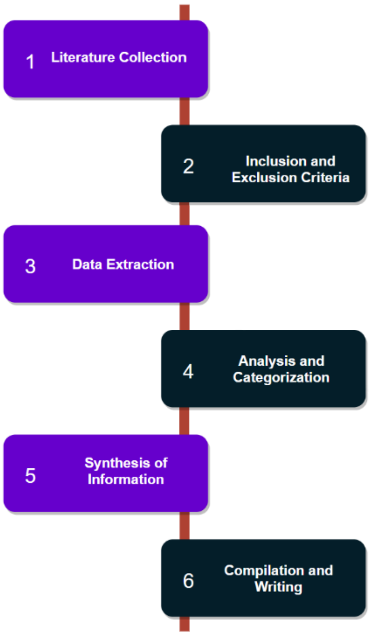
1 Literature Collection
2 Inclusion and Exclusion Criteria
3 Data Extraction
4 Analysis and Categorization
5 Synthesis of Information
6 Compilation and Writing

Figure 2: The methodology used for this review.

Literature Collection: Gather a comprehensive set of academic papers, articles, and reports on AI-based DDoS mitigation strategies from reputable databases like IEEE Xplore, ACM Digital Library, and Google Scholar. *Inclusion and Exclusion Criteria:* Establish criteria for selecting relevant literature. Include studies focusing on AI and machine learning in DDoS mitigation, and exclude those not directly related to AI strategies or beyond the scope of cybersecurity. *Data Extraction:* Extract key information from each selected publication, such as the study focus, methodology, AI techniques used, results, strengths, and limitations. *Analysis and Categorization:* Analyze the collected data to identify trends, common themes, and divergences in AI approaches to DDoS mitigation. Categorize the literature based on factors like AI techniques used (e.g., machine learning, deep learning), application domains (e.g., 5G networks, avionics), and types of DDoS attacks addressed. *Synthesis of Information:* Synthesize the extracted information to create a comprehensive overview of the state of AI-based DDoS mitigation strategies. Highlight significant advancements, common challenges, and potential areas for future research. *Compilation and Writing:* Compile the synthesized information into a coherent review paper structure, ensuring logical flow and clarity. Write the paper with distinct sections, including the introduction, literature review, methodology, discussion, and conclusion, adhering to academic standards and guidelines.

V. Results

The systematic analysis of the literature on AI-based strategies for DDoS attack mitigation reveals several key findings. This section presents the results derived from the comprehensive review, highlighting the major trends, advancements, and challenges identified in the current research landscape. The review shows a significant evolution in AI methodologies, with a shift from basic machine learning algorithms to more complex deep learning and neural network models. These advanced techniques have shown improved accuracy and efficiency in detecting and mitigating DDoS attacks. A notable trend is the integration of AI with emerging technologies like blockchain and Software Defined Networking (SDN). These integrations offer enhanced security features and innovative approaches to mitigating DDoS threats, such as decentralized control and dynamic resource allocation. The literature indicates a growing focus on sector-specific AI applications, particularly in critical areas such as 5G networks, avionics, and vehicular networks (VANETs). Each sector presents unique challenges and requirements, leading to the development of tailored AI solutions. Despite advancements, there are significant challenges. These include the need for large and diverse datasets for training AI models, the risk of adversarial attacks against AI systems, and the complexities involved in the implementation of AI solutions in real-world scenarios. Studies highlight the importance of real-time detection and response capabilities in AI-based systems. Rapid identification and mitigation are crucial in minimizing the impact of DDoS attacks, and AI technologies have shown promise in achieving this goal. Ethical and privacy issues have emerged as critical considerations. The use of AI in network security must balance the need for effective defense mechanisms with the respect for user privacy and ethical use of data. The review suggests a need for further research in enhancing the robustness and adaptability of AI systems, developing more efficient algorithms for real-time applications, and addressing the security vulnerabilities of AI models themselves. Figures (3-6) represent our review results.

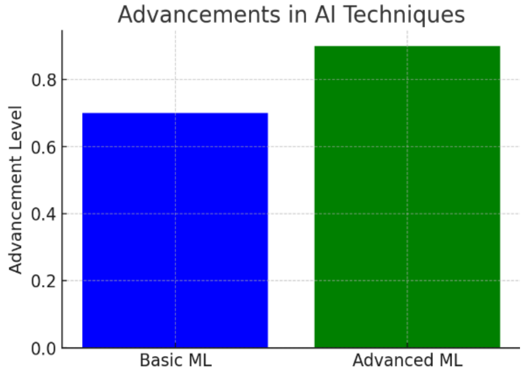

Figure 3: Compares the advancement levels between basic and advanced ML techniques, indicating a higher advancement in the latter.

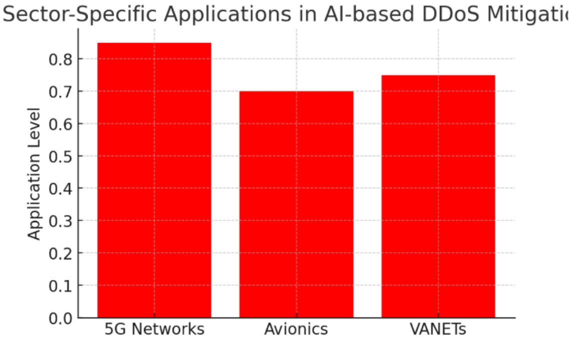

Figure 4: Illustrates the application levels of AI in different sectors such as 5G networks, avionics, and VANETs, with 5G networks having the highest application level.

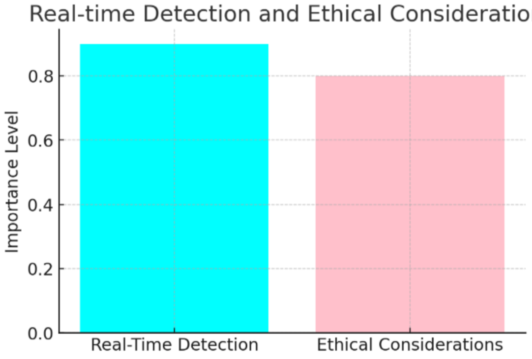

Figure 5: Highlights the importance of real-time detection capabilities and ethical considerations in AI-based cybersecurity, both of which are deemed highly important.

The results section synthesizes the findings from the literature review, providing a consolidated view of the state of AI in DDoS attack mitigation. It underscores the progress made, the challenges faced, and the potential future directions for research in this field.

VI. Conclusion

This review paper has systematically explored the realm of AI-based strategies for mitigating Distributed Denial of Service (DDoS) attacks. The findings reveal a dynamic and rapidly evolving field, marked by significant advancements in machine learning and deep learning techniques. The integration of AI with emerging technologies like blockchain and Software Defined Networking (SDN) has opened new avenues for innovative and effective DDoS defense mechanisms. The sector-specific applications of AI in areas such as 5G networks, avionics, and vehicular networks (VANETs) highlight the adaptability and versatility of AI solutions. However, this exploration also uncovers challenges, including the need for large, diverse training datasets, potential vulnerabilities to adversarial attacks, and the complexities of real-world implementations. The importance of real-time detection capabilities in AI systems cannot be overstated, as they are crucial in minimizing the impact of DDoS attacks. Alongside this, ethical and privacy considerations have emerged as critical aspects, necessitating a careful balance between effective defense and responsible AI use. at the end of this section, while AI presents a powerful tool in the fight against DDoS attacks, it is not a panacea. The future of DDoS mitigation lies in the continuous innovation and improvement of AI technologies, coupled with a holistic approach that considers ethical implications and the unique challenges of various application domains. As the landscape of cyber threats evolves, so must our strategies to combat them, with AI playing a central role in shaping the future of cybersecurity.

Acknowledgement

We express our deepest appreciation to Rabadan Academy for their unwavering support and priceless contributions throughout our research project. We also offer our sincere thanks to the review committee for their constructive criticism and valuable recommendations, which have greatly enhanced the quality of this scholarly paper. Their proficient guidance and input have been crucial in the development and improvement of our research.

References

[1] Fang, L., Zhao, B., Li, Y., Liu, Z., Ge, C., & Meng, W. (2020). Countermeasure based on smart contracts and AI against DoS/DDoS attack in 5G circumstances. IEEE Network, 34(6), 54-61.

[2] Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7, 51691-51713.

[3] Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., ... & Haleem, M. (2022). A machine learning-based classification and prediction technique for DDoS attacks. IEEE Access, 10, 21443-21454.

[4] Ali, M., Benamrane, F., Luong, D. K., Hu, Y. F., Li, J. P., & Abdo, K. (2019, September). An AI based approach to secure SDN enabled future avionics communications network against DDoS attacks. In 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC) (pp. 1-7). IEEE.

[5] Saha, S., Priyoti, A. T., Sharma, A., & Haque, A. (2022, January). Towards an optimal feature selection method for AI-based DDoS detection system. In 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC) (pp. 425-428). IEEE.

[6] Ali, M., Hu, Y. F., Luong, D. K., Oguntala, G., Li, J. P., & Abdo, K. (2020, October). Adversarial attacks on ai based intrusion detection system for heterogeneous wireless communications networks. In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC) (pp. 1-6). IEEE.

[7] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access, 9, 94668-94690.

[8] Beg, O. A., Khan, A. A., Rehman, W. U., & Hassan, A. (2023). A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids. Energies, 16(22), 7644.

[9] Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., & Akber, S. M. A. (2020). Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms. Computer Networks, 179, 107364.

[10] Zebin, T., Rezvy, S., & Luo, Y. (2022). An explainable AI-based intrusion detection system for DNS over HTTPS (DoH) attacks. IEEE Transactions on Information Forensics and Security, 17, 2339-2349.

[11] Chen, Y. H., Lai, Y. C., Lu, C. H., Huang, Y. C., Chang, S. C., & Jan, P. T. (2022, February). A Deep Learning Methodology to Detect Trojaned AI-based DDoS Defend Model. In 2022 8th International Conference on Automation, Robotics and Applications (ICARA) (pp. 243-246). IEEE.

[12] Lyamin, N., Kleyko, D., Delooz, Q., & Vinel, A. (2018). AI-based malicious network traffic detection in VANETs. IEEE Network, 32(6), 15-21.

[13] Phan, T. V., Gias, T. R., Islam, S. T., Huong, T. T., Thanh, N. H., & Bauschert, T. (2019, December). Q-MIND: Defeating stealthy DoS attacks in SDN with a machine-learning based defense framework. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[14] Alavizadeh, H., Jang-Jaccard, J., Alpcan, T., & Camtepe, S. A. (2021). A Game-Theoretic Approach for AI-based Botnet Attack Defence. arXiv preprint arXiv:2112.02223.

[15] Ali, A., Chaudhary, A., & Sahana, S. (2021, December). A Review of Defense against Distributed DoS attack based on Artificial Intelligence Approaches. In 2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA) (pp. 32-38). IEEE.

[16] Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. (2020, November). IoT DoS and DDoS attack detection using ResNet. In 2020 IEEE 23rd International Multitopic Conference (INMIC) (pp. 1-6). IEEE.

[17] Bertino, E., Kantarcioglu, M., Akcora, C. G., Samtani, S., Mittal, S., & Gupta, M. (2021, April). AI for Security and Security for AI. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (pp. 333-334).

[18] Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2), 2272358.

[19] 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.

[20] 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.

[21] Mohamed, N., El-Guindy, M., Oubelaid, A., & khameis Almazrouei, S. (2023). Smart Energy Meets Smart Security: A Comprehensive Review of AI Applications in Cybersecurity for Renewable Energy Systems. International Journal of Electrical and Electronics Research, 11(3), 728-732.

[22] Mohamed, N. (2022, December). 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.

[23] Mohamed, N., Oubelaid, A., Bajaj, M., Kandpal, M., & Mahmoud, M. M. (2023, October). Using AI and Kinetic Energy to Charge Mobile Devices with Human Movement. In 2023 4th IEEE Global Conference for Advancement in Technology (GCAT) (pp. 1-6). IEEE.

[24] 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 (ICERECT) (pp. 1-4). IEEE.

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

[26] Mohamed, N., Josphineleela, R., Madkar, S. R., Sena, J. V., Alfurhood, B. S., & Pant, B. (2023, May). The Smart Handwritten Digits Recognition Using Machine Learning Algorithm. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 340-344). IEEE.

[27] Mohamed, N., Upadhyay, R., Jakka, G., Rambabu, P. V., Alfurhood, B. S., & Singh, D. P. (2023, May). Framework for the Deployment of Intelligent Smart Cities (ISC) using Artificial Intelligence and Software Networking Technologies. In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 667-671). IEEE.

[28] SUGANDH, M. (2023). DDOS ATTACK DETECTION USING AI BASED TECHNIQUES (Doctoral dissertation, Delhi College of Engineering).

[29] Pasha, M. J., Rao, K. P., MallaReddy, A., & Bande, V. (2023). LRDADF: An AI enabled framework for detecting low-rate DDoS attacks in cloud computing environments. Measurement: Sensors, 100828.

[30] Singh, J., & Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Computer Science Review, 37, 100279.