International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 2, Mar-Apr 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Detecting and Mitigating DDoS Attacks: The Role of AI and Machine Learning

Dilip Kumar[1], Yashwant Kumar[2]

[1]Department of Engineering, Snowflake Inc, San Mateo, CA, USA
[2]Engineering Department, Hitachi Rail, GTS, India

ABSTRACT

The growing frequency and complexity of Distributed Denial of Service (DDoS) attacks have necessitated more dynamic and intelligent cybersecurity solutions. This paper explores the transformative role of Artificial Intelligence (AI) and Machine Learning (ML) in detecting, mitigating, and preventing DDoS attacks across modern network infrastructures, especially in the context of IoT environments. Traditional security mechanisms struggle to adapt to the evolving tactics used in multi-vector DDoS attacks. In contrast, AI-driven intrusion detection systems provide adaptive learning, real-time anomaly detection, and improved decision-making through explainable AI. The study also examines AI-enabled methodologies such as deep learning, ensemble models, and blockchain integration, highlighting their potential to enhance the resilience and accuracy of defense mechanisms. Furthermore, the paper addresses the challenges of false positives, scalability, and privacy concerns associated with AI deployment. It concludes by emphasizing the need for continuous research and development in AI-centric security frameworks to ensure future-proof defense against sophisticated cyber threats.

KEYWORDS: *Distributed Denial of Service (DDoS), Artificial Intelligence (AI), Machine Learning (ML), Intrusion Detection Systems (IDS), Explainable AI (XAI), Internet of Things (IoT) Security, Network Anomaly Detection, Deep Learning, Blockchain in Cybersecurity, Adaptive Threat Mitigation, Software Defined Networks (SDN), Cybersecurity*

How to cite this paper: Dilip Kumar | Yashwant Kumar "Detecting and Mitigating DDoS Attacks: The Role of AI and Machine Learning" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-2, April 2025, pp.1017-1024, URL: www.ijtsrd.com/papers/ijtsrd78657.pdf

IJTSRD78657

INTRODUCTION

Currently, innovations such as artificial intelligence (AI) and machine learning become interesting strategies for building cybersecurity architecture as an effort to deal with DDoS attacks. A DDoS attack has an ever-evolving character along with the advancement of technology, so that its level of sophistication continues to increase. This condition affects the ability of DDoS defense mechanisms to deal with ever-evolving attacks. Therefore, organizations need defense mechanisms based on machine learning and AI that can learn and adapt to new attack. Machine learning algorithms also help predict potential DDoS attacks and enhance proactive measures. AI and machine learning systems can provide more efficient, accurate, and faster responses than conventional methods. In this way, AI acts as one of the building blocks to help prevent and reduce DDoS attacks.

AI in cyber security can very well counter the IoT-based DDoS attacks that are rapidly rising as more and more devices are getting connected to the Internet (Abed & Anupam, 2023). The AI-based systems are capable of recognizing abnormal behavior of network traffic that are indicative of the DDoS attacks. With the AI-based technology, the systems can automatically adapt to recognize the new attack patterns as the learning from the historical data of similar attacks is embedded into the security system. The intrusion detection systems can work with a greater accuracy by stringing predictive analytics alongside acknowledging the IoT patterns to recognize where the system may soon fall vulnerable. In conclusion, cyber security systems that shall be using AI will always have their pros and cons, with the benefits outweighing the downfalls. However, research and technology needs to evolve continuously

to keep developing AI-based automated attacks that may risk the nation's critical infrastructure.

Explainable AI is not only important for detection purpose but also beyond that which helps during mitigation phase of DDoS attacks by allowing more educated decisions to be taken (Kalutharage et al., 2023). Explainable AI provides insight to security practitioners why AI took certain decision allowing them to to adjust their course of action based on the particular attack and its source. It will greatly help during mitigation phase to reduce down time and improve recovery. Explainable AI will add to the advantages especially in the case of IoT networks where scale and complexity of devices makes it difficult to understand that how certain network actions were taken. The integration of explainable AI with current network monitoring tools will allow similar flow of information to make decisions on whether the connection is genuine or not and act accordingly. Continuous learning and adaptation will also help in reducing unused connections and reducing the amount of potential connections that could lead to an attack. Overall choke points and redundancy of security mechanisms will be addressed more intelligently further improving its security against attackers using latest technologies in the ever-evolving cyber security threats.

Thus, the integration of explainable AI models within DDoS detection could potentially emerge as a constructive means for optimizing comprehensibility and accuracy in predicting DDoS attacks in IoT networks (Kalutharage et al., 2023). More specifically, leveraging a feature-set that is relevant to a DDoS attack would enable the system to comprehensively map features that influence its functionality to perform anomaly detection capabilities in a precise manner. Consequently, this will facilitate predicting IoT DDoS attacks, as well as providing an explainable reasoning that may instill trusted AI competency based on which security teams could verify AI observations. Additionally, explainable AI architecture would provide a feasible means for addressing one of the core obstacles encountered in utilizing AI models, which is the model's black box functionality, could be overcome as a result of enhanced clarity and traceability regarding how decisions are made. Accordingly, embedding such AI models into DDoS detection systems will significantly contribute to optimizing the overall architecture designed for resisting DDoS attacks, as such yielding a more secure environment.

Understanding DDoS Attacks

Over the years, Distributed Denial of Service (DDoS)attacks have emerged as a major threat to network security. DDoSattacks usually deny service to legitimate users by overwhelming the target or its infrastructure, with a large amount of traffic. They are the result of taking advantage of the large-scale nature of the internet. DDoS attacks typically involve the use of networked devices that have been compromised, called botnets, to send high levels of traffic at low cost to a given target. DDoS attacks are on the rise, probably because attack tools and services are easier to get. Such that those who are not skilled can carry out divided attacks using them. Also, through the layered approach of different attacks, sometimes called multi-vector DDoS, attackers can adapt these layered approaches to make them bypass conventional network security(Markevych & Dawson, 2023). With the prevalence and sophistication of these approaches, there is a greater need for sophisticated network security to develop techniques that would detect them to avoid system disruptions.

The use of AI in intrusion detection systems is crucial in tandem with the evolution of technologies. This enables the development of network security systems capable of identifying and responding to DDoS attacks in a timely manner. In contrast, machine learning and deep learning-based solutions have demonstrated the ability to discriminate between genuine and malicious traffic using extensive datasets in real time (Schmitt, 2023). These AI systems can continuously learn and adapt to new DDoS attack trends, which inflexible systems cannot cope with. However, implementing this solution is not without difficulties – there are issues that require solving, such as the creation of a large labeled dataset for machine learning, as well as the vulnerability of AI itself to DDoS attacks through adversarial learning. Nevertheless, the constant improvement and training of AI algorithms can significantly increase the efficiency of intrusion detection systems, which will subsequently ensure the reliable protection of network infrastructures against new DDoS attack vector schemes (Schmitt, 2023).

Components of DDoS Attacks

Denial of service attack (DdoS attack) has its own components one of them being Botnets, attack Vectors and methodologies. Botnets refers to a group of hijacked computer equipment that send large amounts of messages or requests to the network targeted. Attack vectors refers to method used by attackers to introduce attack to the organization, an example of attack vector would be a DDoS attack on bandwidth. While attack methodology is technique used by an attacker to disrupt the server of a network or systems, an example of these is exploiting and

opening on TCP/IP layer (Park et al., 2022). Component as these mentioned above will help in the design of AI-based application to handle DDoS attack because it will bring the idea of how to identify the various attack methodologies used thereby improving the organization approach to cybersecurity.

Further, attacks can be divided as volumetric, protocol and application attacks which each bring different challenges for cybersecurity mechanisms to recognize and overcome. Volumetric attacks can overload bandwidth of network by sending large data packet which saturates the transmission mediums, resulting in services getting interrupted (Ref-DROyjRxgriED). Protocol attacks try to deplete available resources on a server exploiting specified vulnerabilities in communication protocols, for instance, Table Control Protocol (TCP) which stops the targeted server from executing legitimate operation requests (Rahman et al., 2019). Application attacks work on crawling vulnerabilities from the application and database, and target a particular online service itself, making it undetectable in conventional manner, which is defined as weakened later under application (Schmitt, 2023). Discrimination of these threat categories is fundamental in designing a strategy based riding computing technologies such as AI to detect and overcome them individually and effectively.

Impact on Network Infrastructure

DDoS attacks overwhelm networks and cause critical failures that lead to monetary losses. These attacks can fully crash servers by consuming allocated resources making it impossible for genuine users to access the network and related services. DDoS attacks can have serious financial implications, not only due to the possible compromise of network infrastructure but also due to registration of lost revenue and damage to the organization's reputation (Rahman et al., 2019). Furthermore, preventive measures against DDoS attacks can have a significant financial impact as organizations may deploy sophisticated security networks in a bid to secure their network infrastructure. DDoS attacks pose multiple challenges across network infrastructure that threaten service accessibility, thus, crippling financial security, posing the dire need to understand the diverse impacts of such attacks to minimize the implications.

Moreover, the long-term effects of distributed denial-of-service (DDoS) attacks on the reliability of networks can also erode trust and threaten communication across industries. The nature of DDoS attacks as long-term threats would force many entities to carry out constant monitoring and continue pouring resources into developing frameworks for cybersecurity. Ultimately, the impact on network reliability can undermine operational effectiveness and erode stakeholder trust in the system's ability to endure and recover from sieges (Rahman et al., 2019). Such a loss of trust would lead to fines, breach of partnerships, and reduced user interaction, which further emphasizes the need for security systems that are not only resilient but also adaptive to emerging threats. In light of these factors, the incorporation of artificial intelligence is necessary to model, forecast, and adjust to emerging security risks and threats across networks to create a safer digital space.

Apart from predicting threats, AI's implementation in network monitoring can prevent DDoS attacks over networks by improving network operations infrastructure. AI can utilize predictive analytics whereby the system predicts hardware failure (Bushuev, 2024). This avails the network to maintain its resiliency during a DDoS attack. Besides, this reduces downtime and the economic implications that come with reactive measures aimed at restoring network operations. As such, network operations continue unhindered in the face of attacks. AI is also economically favorable to network operations with predictions estimating that 75% of companies adopting the technologies are likely to gain economically (Bushuev, 2024). Overall, AI has become a vital element for establishing cybersecurity strategies in its continuous growth due to its economic value in securing systems.

AI-Driven Intrusion Detection

The use of AI to improve intrusion detection systems will provide crucial advantages to today's cyber protection systems, compared to traditional approaches, due to the unique ability of artificial intelligence to learn its algorithms and architectures to recognize new patterns of possible threats. The use of AI provides substantial advantages over classical approaches, based on previously defined rules, including the identification of network and user behavior anomalies by machine learning algorithms. This allows improving the response and detection of a certain level of threats (Schmitt, 2023). AI-based systems are capable of continuous learning and training processes during operation, increasing the accuracy of threat detection predictions across large data sets and significantly enhancing the quality of the system's results. An explainable AI-based system provides better transparency to security personnel, allowing them to comprehend and validate the AI-based results, which are essential to ensuring the trustworthiness of automated processes (Kalutharage et al., 2023). Therefore, the use of AI as the main technology to improve intrusion detection systems will significantly increase their efficiency at all stages

of threat detection, response, and elimination, allowing an adaptive approach to minimize cyber threats.

Role of Machine Learning in Detection

Traditional detection mechanisms, the use of machine learning algorithms in the detection of potential DDoS attacks and threat anomalies, have been found to be effective and more accurate than previously adopted techniques. As highlighted in a research study assessing DDoS detection and mitigation techniques, fast learning algorithms can analyze significant volumes of network traffic data captured over time to develop normal behavior patterns for the system, and if new detections divert from established patterns, then individual packets can be classified as harmful. Through supervised learning algorithms and clustering of benign and harmful data packets, as with machine learning, the detection speed and accuracy in identifying potential threats is improved in Software Defined Network (SDNs) systems (Rahman et al., 2019) . Adopting machine learning algorithms for intrusion detection systems allows for adaptive response to threat environment developments. Additionally, threats can be preemptively mitigated, improving the accurate prediction of the network-targeted attacks with establishment of normal behavior patterns.

In addition, the techniques of supervised and unsupervised learning would significantly improve the ability to identify anomalous patterns standard for DDoS attacks. Supervised learning models, including decision trees and neural networks, use labeled datasets to verify the differences between standard and malicious traffic and are characterized by high accuracy of detection (Rahman et al., 2019). Supervised learning approaches enable continuous adaptation of models to new types of DDoS attacks as new labeled data appears, which improves the robustness of models against new threats. Unsupervised learning approaches, including clustering and anomaly detection, do not use labeled datasets, thus leading to the ability to detect DDoS attacks and explore new patterns in unmarked datasets that are different from the current standard-specific base. The systematic use of supervised and unsupervised learning approaches in AI-based DDoS intrusion detection models provides a proper compromise solution by adopting the ideal features of predictive tools (supervised learning) and exploratory tools (unsupervised learning), which would effectively improve detection accuracy and minimize false-positive rates (Schmitt, 2023).

Recent Advancements in AI Techniques

AI techniques are providing a promising future for the DDoS attacks detection improvement. Deep learning can detect complex patterns within large datasets, which increases the efficiency in separating the normal network traffic from the malicious one (Rahman et al., 2019). Convolutional and recurrent neural networks can model the sequences and time access patterns from the network traffic data, which increase the granularity in the attacks understanding through their features extraction (Schmitt, 2023). The Generative Adversarial Networks (GANs) can generate the normal and abnormal network traffic data, which can be used to test and improve the intrusion detection systems. This will allow to simulate the various attacking situations in order to improve the defensive strategies even when we simulate some of them (Park et al., 2022).

One promising use case of AI to countering DDoS threats is in Software Defined Networks (SDNs) that integrates machine learning algorithms. One instance in this regard is the use of ensemble online machine learning models to counter various attack types, which is also seen to be effective (Alashhab et al., 2024). Also worthy to mention, is a system that applies blockchain and machine learning, which is capable of improving tracking and mitigation against DDoS attacks (Manikumar & Maheswari, 2020). Also, the application of AI techniques in this environment can aid in prompt detection of anomalies and effective employment of counteractive measures based on the type of attack. Hence, this serves as an evidence that AI has the potential to revolutionize how networks and systems can be secured, through the improvement and adaptive capacity of an infrastructure even to sophisticated threats.

Mitigation Strategies Using AI

As part of the proficient utilization of AI in devising DDoS mitigation strategies, adaptive security responses are improved due to the superior learning ability of AI. The use of machine learning algorithms in identifying trends in network traffic is the underlying principle of notable algorithms so that the potential attacks can be realized before occurring (Rahman et al., 2019). The remarkable use of AI in Software Defined Networks (SDNs) is the ability to alter policies dynamically so that the networks become more resilient and adaptive to DDoS attacks (Alashhab et al., 2024). Some methodologies also consider the collaborative use of blockchain technology and AI to be able to track and mitigate DDoS more efficiently, thus providing a comprehensive framework to cope with many vectors of attack (Manikumar & Maheswari, 2020). Learning

from the above mentioned highlights, the employed DDoS mitigation strategies due to AI superiority have improved the accuracy and efficiency of the network DDoS damage reaction mechanisms and promote the adaptability of the basic network infrastructure against advanced cyber threats.

Artificial Intelligence (AI) is playing an important role in intrusion detection systems (IDS) to enhance the detection and prevention mechanisms against DDoS attacks on complex networks (Rajapaksha et al., 2023). AI based IDS are equipped with advanced algorithms that can easily analyze the network traffic and identify the anomalies that may pose DDoS attacks. By employing historical data and adaptive learning, AI-based IDS can evolve and improve their detection mechanisms for accuracy and reduced false alarms. The evolution of AI-based techniques will strengthen the IDS and will help to evolve them against new attacks and ensure security of network infrastructures. Cybersecurity models should be focused on the role of AI in IDS to protect the network against complex cyber threats.

Enhancing Network Security

Adaptive learning algorithms have played a vital role in real-time threat detection through AI-enabled solutions. The solutions used in AI have been able to analyze the entire network statistics and identify the unusual patterns in the network activities that are indicative of a DDoS attack at the network-layer. As per the findings of the research, the AI-based solutions of network security effectively address DDoS attacks through the usage of machine learning-based models that analyze the network data to promote predictions and adaptive measures (Kalutharage et al., 2023). also, the implementation of AI for delivering network security within different frameworks promotes dynamic response mechanisms that ensure immediate actions against potential threats through the process of real-time analysis and decision-making (Park et al., 2022). AI mechanisms deliver requisite intelligent and rapid accuracy for ensuring the advancements in detecting malicious network activity and upgrading the network systems and infrastructures against critical DDoS threats. As a result, the incorporation of these AI-based solutions ensures the security, safety, and integrity of crucial data information in computer networks.

Furthermore, artificial intelligence technology employs real-time threat analysis and response, which dramatically improves the ability to quickly counteract the Distributed Denial of Service (DDoS) attacks. The introduction of AI technology into threat detection systems empowers them to analyze network data traffic for patterns and instantly identify any irregularities. This functionality allows organizations to respond to security breaches quickly and selectively. Recent studies indicate that AI-based methods combining machine learning algorithms can effectively analyze abnormal traffic patterns and respond promptly, shortening the time needed to follow up on suspicious events (Schmitt, 2023). In addition, the integration of such technology in network security enhances performance through quick decision-making and allows systems to adjust security measures to new attack patterns adaptively, making it a reliable defense system against constantly of emerging cyber threats (Sarker et al., 2021). The application of AI in real-time threat analysis permits an organization to preserve business continuity by preventing DDoS attacks from adversely affecting critical infrastructure.

Privacy Concerns and Solutions

While the application of artificial intelligence into network security systems has potential benefits, privacy risks should be critically evaluated. Machine learning requires enormous, detailed data sets to train algorithms in identifying aberrant behaviors and threats (Devineni, 2024). The primary privacy risk at stake here is the possibility, albeit unintentional, of exposing personally identifiable information (PII) as contained in the data sets machine learning algorithms utilize when making decisions. This poses an ethical dilemma for organizations intending to integrate artificial intelligence into their security frameworks. Organizations may mitigate privacy risks by adopting privacy-preserving methods such as data anonymization and federated learning models. When machine learning algorithms are trained, the centralized entities from which they collect sensitive data do not need to expose their private data to external parties. A model-centered training method achieves this as it does not expose the raw data if information transfer is inevitable (Castro et al., 2023). This method optimizes protection, prevents raw data access, and ensures comprehensive data accuracy. Organizations can enjoy the benefits of swift threat detection through enhanced cybersecurity with artificial intelligence without compromising user privacy.

Methodologies for DDoS Mitigation

The methodologies in this research can significantly contribute towards the AI-based security development, strengthen future systems towards DDoS attacks, and protect infrastructural integrity. Building upon the existing solutions via AI algorithms is a proven and successful methodology to enhance the capabilities of the systems. AI and Machine Learning approaches used in this study are

categorized under various methodologies. The examples of enhanced approaches include the use of machine learning within Software Defined Networks (SDNs), which adjusts the configuration to shift the priorities from the attacked ones to the genuine when a DDoS attack is identified (Tuan et al., 2020). Other methodologies that improve the accuracy and speed of existing protection systems considered in the study are ensemble learning models. The latter applies different machine learning models that improve detection and protection functions (Alashhab et al., 2024). The innovative approach proposed in the reviewed studies is considered to be the integration of AI with blockchain technology in protecting against a DDoS attack. This complex development would perform decentralized tracking and responding, allowing the attacked system to react to changes much faster (Manikumar & Maheswari, 2020). In summary, the modern AI and Machine Learning methodologies aimed towards improving DDoS mitigation can significantly strengthen the developments.

Network Monitoring Techniques

The new AI enabled network monitoring systems based mechanisms are use full in identifying the DDoS attacks on time. These systems are based on AI techniques, such as machine learning (ML) based anomaly detection and clustering algorithms which can analyze the ongoing traffic patterns using their advanced learning capabilities. These algorithms can learn the normal behavior of traffic on the network. After that, they can identify the anomalies and abnormal behavior in the traffic that can indicate the possible DDoS security threats (Research paper: AI-enabled network security). The machine learning algorithms can learn continuously from the changes in network environment. Hence, they can identify the security threats with more efficiency and accuracy. The AI mechanisms provide an option of using explainable AI (XAI) based models which provide enhanced decision-making processes to their users along with better understanding and reliability. This allows network administrator to validate and verify the identification of security threats and take the relevant actions for securing the IT infrastructure (Research paper: AI-enabled network security). Hence, this form of AI based network monitoring will help in early identification of DDoS attacks.

In addition, learning continuously and adapting are essential for the efficiency of monitoring systems aimed at identifying Distributed Denial of Service (DDoS) attacks (Sarker et al., 2021). With the help of continuous analytical processes, enhancements of monitoring systems thoroughly adjust their "normal" network behavior model, resulting in the growing accuracy of their further anomaly detection (Sarker et al., 2021). Through that iterative process, machine learning models could be improved, adapting to the ongoing changes in the climate of the DDoS attack methods and the environments where they occur. Adaptive algorithms incorporated in the monitoring systems decrease false positives and help to make objects more secure (Rahman et al., 2019). Data, obtained from the learning processes, ensures the relevance of monitoring systems, increasing their robustness against contemporary threats (Sarker et al., 2021). The ability of monitoring systems to learn continuously makes them core components in the stable cybersecurity strategies in the contemporary context.

Malware Mitigation Approaches

Moreover, AI-based solutions are becoming more and more important in protecting malware that is often part of DDoS attacks. Machine learning algorithms can deviate from normal behavior, a signature of the malware, even in large datasets with complex behavior. The deep learning algorithm is an AI technology that aids in distinguishing between understandable and harmful behavior and improves the efficiency and speed of the detection (Schmitt, 2023). Secondly, the application of AI for malware attacks allows adaptive learning to change the detection parameters according to the changes in the nature of the threat (Rahman et al., 2019). Therefore, using these options with AI services to improve the networking gives additional protection against the malware, and at the same time, it encourages the general processes of safe net workflows.

In the same manner, AI has proved to be highly efficient in differentiating legitimate and malicious network traffic due to its high-level analytics. In a conventional manner, machine learning is used to analyze and classify traffic from various resources. It is capable of analyzing significant volumes of network data and recognizing patterns that characterize normal and abnormal operation (Schmitt, 2023). As a result, a timely identification of threats is based on their analysis, which increases the accuracy of malicious network traffic recognition and reduces false positive results. Malicious network traffic is effectively differentiated by using AI-based systems due to their high level of network traffic analysis and classification with the use of neural networks (Park et al., 2022). As a result, this enables more accurate mitigation of potential DDoS attacks. The explanation ability of AI models results in increased awareness of security experts on the reasons for threatening detections, thus ensuring the accuracy and

transparency of such models in exploiting high-level network traffic classifications (Kalutharage et al., 2023).

Challenges and Future Directions

Regardless of the innovations in DDoS mitigation through AI applications, many concerns affect their full capabilities. One common challenge is the high false positive rate that many AI systems still demonstrate, allowing non-malicious traffic to be falsely flagged as a threat to the service (Sarker et al., 2021). Furthermore, scalability is still a challenge, where AI systems must efficiently handle increasing amounts of network traffic data without losing effectiveness. Future explorations must improve the sophistication of AI models to efficiently maintain DDoS detection accuracy while minimizing false positive rates through combination learning of deep and other AI models that facilitate more effective learning of network structure (Schmitt, 2023). Furthermore, explainable AI will be crucial in the integration of trustable frameworks of DDOs mitigation, allowing security professionals to understand specific model actions, thus providing them with the confidence to adopt these alternatives and integrate them alongside existing security protocols in the network infrastructure (Kalutharage et al., 2023).

Limitations in Current Systems

The existing Artificial Intelligence (AI) solutions have several constraints with respect to DDoS attack detection and prevention. One of the major constraints is the high false positive rate which results in normal network traffic to be flagged up as malicious traffic (Sarker et al., 2021). This entails reliance on IT staff to validate the alerts which not only defeats the objective of AI but adds on the operational overhead on IT teams. Another constraint with the existing AI models is scalability wherein the models need to ensure the efficiency across the increasing volume of network traffic while detecting and preventing DDoS attacks (Schmitt, 2023). One of the current strategies to improve the existing AI models is through the implementation of explainable AI. This could improve the confidence of the security operation teams in network behavior anomaly detection (NBAD) and model based intrusion detection mechanisms to act on model predictions (Kalutharage et al., 2023).

Future Research Opportunities

For the enhancement of AI to further enhance its potential for its purpose to fight against DDoS, future research should focus on creating more advanced ML algorithms that are able to understand complex data pattern. One of the most interesting research area to pursue is the development of AI-based intrusion detection system using hybrid learning, which makes use of both deep learning and statistical based algorithm in order to achieve the best decision-making output in terms of accuracy and speed (Schmitt, 2023). The use of edge computing with AI is another research area that can promote improvement through scaling and latency reduction and AI can achieve this by performing real-time threat detection entirely at the entry points of the network (Sarker et al., 2021). Likewise, creating an AI infrastructure that upholds explainability is a promising research pursuit that can invite improvement through allowing the security personnel to question and verify the outcome of the AI-based decision (Kalutharage et al., 2023). The cybersecurity industry will gain its defense against DDoS and similar attacks through strengthen of these avenues in research.

References

[1] Abed, A. K., & Anupam, A. (2023). Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*, *6*(3), e285. https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.285

[2] Alashhab, A. A., Zahid, M. S., Isyaku, B., Elnour, A. A., Nagmeldin, W., Abdelmaboud, A., Abdullah, T. A., & Maiwada, U. (2024). Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model. *IEEE Access*. https://ieeexplore.ieee.org/abstract/document/10489935/

[3] Bushuev, S. (2024). Application of AI for monitoring and optimizing IT infrastructure: economic prospects for implementing predictive analytics in enterprise operations. *Международный Журнал Гуманитарных и Естественных Наук*, *8-3 (95)*, 125–129. https://cyberleninka.ru/article/n/application-of-ai-for-monitoring-and-optimizing-it-infrastructure-economic-prospects-for-implementing-predictive-analytics-in

[4] Castro, O. E. L., Deng, X., & Park, J. H. (2023). Comprehensive survey on AI-based technologies for enhancing IoT privacy and security: Trends, challenges, and solutions. *Human-Centric Computing and Information Sciences*, *13*(39). http://hcisj.com/data/file/article/2023080005/13-39.pdf

[5] Devineni, S. K. (2024). AI in data privacy and security. *International Journal of Artificial*

Intelligence & Machine Learning (IJAIML), *3*(01), 35–49. https://lib-index.com/index.php/IJAIML/article/view/IJAIML_03_01_004

[6] Kalutharage, C. S., Liu, X., Chrysoulas, C., Pitropakis, N., & Papadopoulos, P. (2023). Explainable AI-based DDOS attack identification method for IoT networks. *Computers*, *12*(2), 32. https://www.mdpi.com/2073-431X/12/2/32

[7] Manikumar, D. V. V. S., & Maheswari, B. U. (2020). Blockchain based DDoS mitigation using machine learning techniques. In *2020 Second international conference on inventive research in computing applications (ICIRCA)* (pp. 794–800). IEEE. https://ieeexplore.ieee.org/abstract/document/9183092/

[8] Markevych, M., & Dawson, M. (2023). A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). In *International conference knowledge-based organization* (Vol. 29, Issue 3, pp. 30–37). sciendo.com. https://sciendo.com/pdf/10.2478/kbo-2023-0072

[9] Park, C., Lee, J., Kim, Y., Park, J. G., Kim, H., & Hong, D. (2022). An enhanced AI-based network intrusion detection system using generative adversarial networks. *IEEE Internet of Things Journal*, *10*(3), 2330–2345. https://ieeexplore.ieee.org/abstract/document/9908159/

[10] Rahman, O., Quraishi, M. A. G., & Lung, C. H. (2019). DDoS attacks detection and mitigation in SDN using machine learning. In *2019 IEEE world congress on services (SERVICES)* (Vol. 2642, pp. 184–189). IEEE. https://ieeexplore.ieee.org/abstract/document/8817237/

[11] Rajapaksha, S., Kalutarage, H., Al-Kadri, M. O., Petrovski, A., Madzudzo, G., & Cheah, M. (2023). Ai-based intrusion detection systems for in-vehicle networks: A survey. *ACM Computing Surveys*, *55*(11), 1–40. https://dl.acm.org/doi/abs/10.1145/3570954

[12] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173. https://link.springer.com/article/10.1007/s42979-021-00557-0

[13] Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, *36*, 100520. https://www.sciencedirect.com/science/article/pii/S2452414X23000936

[14] Tuan, N. N., Hung, P. H., Nghia, N. D., Tho, N. V., Phan, T. V., & Thanh, N. H. (2020). A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN. *Electronics*, *9*(3), 413. https://www.mdpi.com/2079-9292/9/3/413