Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Deep Learning Algorithms for Detecting and Mitigating DDoS Attacks

Soran Abdulrahman Hamad, Shavan Askar, Sozan Sulaiman Maghdid, Farah Sami Khoshaba, Nihad Abdullah
soran.hamad@epu.edu.iq
Information System Engineering , Technical Engineering College, Erbil Polytechnic University

Article Information

Submitted : 21 Mar 2024
Reviewed: 25 Mar 2024
Accepted : 20 Apr 2024

Keywords

DDoS, DDoS tools, DDoS types, machine learning, deep learning, AI

Abstract

Raising the threat of Distributed Denial of Service (DDoS) attacks means that high and adapted detection tools are required now more than ever. This research focuses on exploring the latest solutions in preventing DDoS attacks and emphasizes how Artificial Intelligence (AI) is involved in enhancing end-to-end detection techniques. Through the analysis of several key approaches, this work notes that AI-guided models quickly identify and counteract any unusual traffic patterns that may indicate an oncoming DDoS attack. Essential aspects towards creating more resilient networks against such attacks include machine learning algorithms, sophisticated data analytics together with AI based detection systems for traffic pattern recognition. Importantly, AI does well in behavioral analysis because it can distinguish and adapt to changing attack vectors. Additionally, it puts AI into perspective as making positive mitigation strategies possible that contain quick interferences such as temporary halt of traffic, rerouting and targeted block listing with real time control panel operations. On the contrary, current DDoS detection prevention techniques remain critically addressed of persistent challenges and limitations fundamental to them. From what emerges, they should always be ready for innovation and improvement because of how attacks might evolve over time. This paper aligns itself with the position that AI-driven detection mechanisms are natural to network security against DDoS attacks. It underlines the importance of integrating AI-based solutions with conventional practices in order to enhance network resilience and efficiently counteract cyber threats that are evolving all the time.

A. Introduction

There has been considerable growth in online services and networks of the digital world, making it much more disposed to to cyber threats such as Distributed Denial of Service (DDoS) attacks. These attacks overload networks with flood of data, which can effectively disrupt services to large groups of users all at once and may damage organizations reputations[1, 2, 3]. To tackle these difficulties accurately, it is necessary to develop a broad plan using several approaches and rules that can change as the world evolves in this constant fight against cyber threats. Some of the key methods include action-oriented analytical approaches and numbers oriented approach which utilize network behavioral visuals as well as strange numeric sequences aimed at identifying potential threats. But these approaches can be failing and require frequent updating when dealing with continuous sequences of attacks[5,6, 7,8].

Consequently, network impact level may be decreased to blocking and slowing down of the traffics thereby enhancing protection in the systems. The utilization of AI, deep learning and machine learning has essentially enhanced DDoS protection as it can anticipate new types of online issues coming up while also minimizing false positives[9, 10, 11,12]. The research on the systems that are capable of detecting and halting DDoS attacks involves different types of networks such as IoT, WLAN ,and Cellular . DDoS attacks are thought-out and sophisticated methods that criminals use to intentionally interrupt internet services [7]. They involve carefully selecting possible victims and gathering information about their weaknesses. Attackers then arrange for a botnet, which uses up the target's resources by flooding its network bandwidth or server capacity. Good plans like redirecting traffic and using special DDoS blocking solutions are needed to prevent these attacks[8].

The main purpose of a DDoS attack is to stop people from using online services or networks, causing long periods of no activity or slow speed. DDoS attacks can cost organizations or groups money by disrupting buying and selling online, causing sales to go down, and spending extra cash on prevention measures[15]. Reputation damage can also occur due to extended service interruptions or inaccessibility, while competitors may use DDoS attacks to weaken the market position of targeted organizations. DDoS attacks are often carried out with political or activist intentions, aiming to disorder government or corporation activities[15].

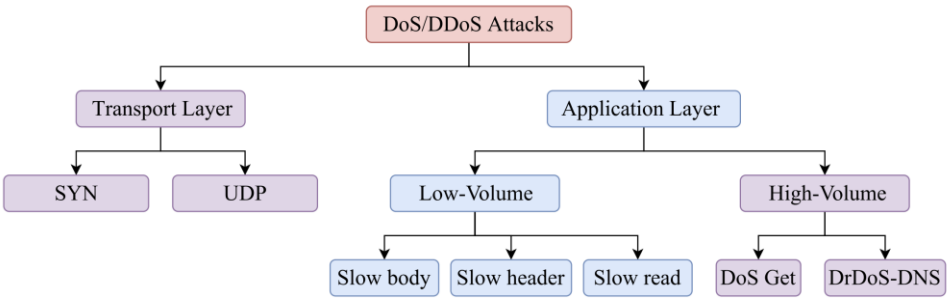

Figure 1. Taxonomy of the studied DoS/DDoS attacks.[19]

B. DD0S Attack Types

There has been a significant increase in the number of reported DDoS attacks worldwide, with hundreds of incidents documented so far. Various methods are being used to initiate a DDoS attack[13] . Nevertheless, several types of DDoS may classify into the following groups.

1. Volumetric Attacks:

Flooding Attacks: These attacks flood the target system or network with excessive traffic, aiming to exhaust available bandwidth or network resources. They include UDP floods, ICMP floods, and other forms of overwhelming traffic[14].

Reflection Attacks: Exploiting vulnerabilities in spoofing, attackers generate requests from numerous devices to transmit traffic to the target, replicating the origin of the requests. This includes techniques like DNS amplification attacks[16].

Amplification Attacks: Small requests are manipulated to generate larger responses, exploiting protocols like DNS, causing servers to overload. This includes attacks like DNS amplification and NTP amplification [5].

2. Protocol Attacks:

SYN Floods: Unnecessarily floods a target with connection requests that never complete the handshake process, filling up resources.

Smurf DDoS: Amplifies a victim's broadcast ping requests to jam the target network.

Fragmented Packet: Manipulated fragmented packets to deplete resources by making devices reassemble the fragments more than they should[17].

3. Application Layer Attacks (Layer 7):

GET/POST Floods: Floods a server with GET/POST requests, overwhelming its capacity to respond to legitimate traffic [4].

Low-and-Slow Attack: Utilizes slow connections or minimal traffic rates to reduce server resources slowly[18].

Exploits Targeting Vulnerabilities: Targeting specific systems or applications based on their known weaknesses, servers with flawed software implementations[13].

In classification of different types of DDoS attacks, these descriptions provide useful messages to describe volumetric, protocol and application layered attack categories which should simplify further insight into them [15]

C. Literature Review

DDoS attacks remain a significant issue in modern networking security, and they have the power to halt essential network functionalities by disabling core services that provide accesses to end-users[9],[20] . Globally disruptive, scientists and computer security experts throughout the world are completely committed to understanding, investigating, overriding in these interferences using innovative

approaches. The aim is to improve digital systems against negative effects experienced by these attacks.

This paper describes a review of observable literature focusing on combining deep learning approaches towards enhancing detection and prevention mechanisms for DDoS attacks[9]. It is based on reviewing a series of scholarly works and improvements that exploit the potentials offered by deep learning techniques to strengthen systems against such malicious cyber threats [19]

This review aims at summing up research efforts as they have been conducted so far to outline a valid picture for methodologies used in deep learning approaches tied with defense strategies aimed. The purpose of this exploration is to illuminate in what ways advancements, difficulties and possible opportunities lie within the utilization deep learning-based methods when it comes to reinforcing defense mechanisms against these cyber threats that are becoming more elaborate every day. Proposing a system that will utilize Support Vector Machine (SVM) classification with SNORT Intrusion Prevention System IPS [26].

This would help safeguard against attackers who attempt to deny service spanning multiple locations simultaneously over the internet. The study indicates that 97% average correctness was found during the network traffic analysis which significantly improved network security. This combined method not only made security in networking more precise, but it also seemed promising for finding threats before they happen.

Nguyen Tan Cam and Nguyen Gia Trung [9], came up with a new way to make finding threats enhanced in connected systems on the internet. They did this by using machine learning tools plus an analysis process called principal component methods. These two scientists came up with this method.

Using their plan made just for overcoming security problems on the Internet of Things (IoT), they obtained really good at finding threats in real time traffic analysis. This lines up with people getting more worried about internet security in these types of environments [26].

Significant contribution made by creating an innovative way to detect Distributed Denial of Service attacks (DDos in SDN)[9], [22, 23, 24, 25]. They used Mininet as well as the Ryu controller. Their new plan worked accordingly, catching 99.99% of malicious network traffic. This shows a big improvement in using deep learning methods to make SDN protection optimized and stronger.

Suggesting a good way to find risky actions called CIFA in named data networking (NDN)[14]. This method is made just for this kind of attacks. Their work was focused on making customers happier and improving network quality by using a smart plan for finding problems and stopping them. This was a big help for the field of computer network security [23].

A new way to find denial-of-service attacks, built it on the Matching Pursuit algorithm as its main part[4]. The new buildings found out unusual attacks on services faster, showing more accuracy with true positive results and few mistake alarms. This shows a big improvement in fighting strong attacks that stop services[27].

A study where they looked into flow-based problem detection in SDNs. They used techniques to pick out important parts and deep learning models for this job. They made their plan work.

This led to fewer false alarms and improved the correctness of systems that find unusual activities. This action was huge step forward to keep the internet availability against new dangers[28]

Attacks involved in using threats that stop services in apps[19+], [18]. These were made with tools anyone can

get easily. The study results showed the need to use machine learning methods with feature selection. This highlights the importance of quickly and completely spotting possible online dangers to minimize them in future.

Combined deep learning method suggested using AE-MLP to find and categorize DDoS attacks. This method tried to handle the limits of simple machine learning methods by dealing with growing complexity and variety of spread denial service attacks (DDoS)[29, 30].

A method to use computer learning for preventing online attacks that slow down or make servers not work[31, 32, 33]. They targeted "DDoS" on Internet of Things networks with stateful Software-Defined Networking (SDN) technology. Their complete way works well in finding high-rate and low-rate attacks that block services, which is important for making security better against different levels of danger from online threats[34].

The study indicates that machine learning, deep learning and advanced algorithms are used in a clear way to make it easier to spot and stop different types of DDoS attacks on large complex networks. These studies have greatly improved safety for networks, but it's still important to keep finding new ideas an always stay tuned[35]. This will help delay ahead of changing computer network threats and make digital systems stronger against attacks.

Table 1. Literature Review

Paper Title	Authors	Year	Methodology	Contribution	Performance/Results	Key Findings/Impact
An Intelligent Approach to Improving the Performance of Threat Detection in IoT	Nguyen Tan Cam, Nguyen Gia Trung	2023	Machine Learning with Principal Component Methods	Rapid threat identification in IoT	Swift threat detection	Addressed internet security concerns within IoT environments
Optimized Artificial Intelligence Model for DDoS Detection in SDN Environment	Y. Al-Dunainawi, B. R. Al-Kaseem, H. S. Al-Raweshidy	2023	Mininet and Ryu controller	99.99% Malicious Traffic Detection	Optimized SDN security	Effective identification of malicious network traffic in SDN
Detecting and Mitigating Collusive Interest Flooding Attacks in Named Data Networking	R. A. Al-Share, A. S. Shatnawi, B. Al-Duwairi	2022	CIFA detection in NDN	Improved customer satisfaction, network quality	Enhanced network reliability	Effective detection and mitigation of Content-Centric Networking Interest Flooding Attacks
A Flow-Based Anomaly Detection Approach with Feature Selection Method Against DDoS Attacks in SDNs	M. S. E. Sayed, N. -A. Le-Khac, M. A. Azer, A. D. Jurcut	2022	Deep Learning models	Enhanced precision in abnormal activity detection	Reduced false alarms	Improved accuracy in identifying anomalous network activities
AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification	Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, S. Compete	2021	AE-MLP combined method	Handling complexity of DDoS attacks	Improved DDoS categorization	Addressing growing complexity and variety of DDoS attacks
An Effective	R. Abubakar et	2020	SVM	Enhanced DDoS	Improved network	Efficient

Mechanism to Mitigate Real-Time DDoS Attack	al.		Classification with SNORT IPS	protection, 97% average correctness	security	protection against internet-wide denial-of-service attacks
Hybrid DDoS Detection Framework Using Matching Pursuit Algorithm	D. Erhan, E. Anarim	2020	Matching Pursuit algorithm	Accurate detection of rare service-disrupting attacks	Reduced false alarms	Improved identification of impactful denial-of-service attacks
Detection of Application-Layer DDoS Attacks Produced by Various Freely Accessible Toolkits Using Machine Learning	D. Mohammed Sharif, H. Beitollahi, M. Fazeli	2023	Machine Learning with Feature Selection	Prompt threat identification	Importance of quickly spotting and mitigating potential online dangers	Urgency of identifying online threats for mitigation
FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks	W. I. Khedr, A. E. Gouda, E. R. Mohamed	2023	Stateful SDN-based IoT network defense	Efficient detection of high-rate and low-rate attacks	Strengthened IoT network security	Effective mitigation against varying levels of online threats
DDOS Attack Detection System Based on Analysis of Users' Behaviors for Application Layer	B. Meng, W. Andi, X. Jian, Z. Fucai	2017	Behavioral analysis	Improved application layer security	Enhanced behavioral analysis	Improved detection of application-layer DDoS attacks
Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-SlowRate-DDoS Dataset	N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, E. Jacob, C. Martinez-Cagnazzo	2023	Physical assessment in SDN-based security	Improved understanding of SDN-based security	Validated SDN-based security framework	Enhanced defense against DDoS attacks
A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks	F. Hussain et al.	2021	Machine Learning for IoT security	Efficient prevention and detection of IoT botnet attacks	Enhanced IoT security	Improved mitigation against IoT botnet threats
An Efficient IDS Framework for DDoS Attacks in SDN Environment	J. E. Varghese, B. Muniyal	2021	Intrusion Detection System	Improved IDS for SDN environments	Enhanced intrusion detection	Strengthened security against DDoS attacks
LSTM-Based Collaborative Source-Side DDoS Attack Detection	S. Yeom, C. Choi, K. Kim	2022	LSTM-based detection	Improved source-side DDoS attack detection	Enhanced source-side attack identification	Strengthened defense against source-side DDoS attacks
SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning	N. M. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz	2021	Machine and Deep Learning in SDN architecture	Improved transport and application layer DDoS attack detection	Enhanced DDoS detection at different layers	Strengthened defense against multi-layered DDoS attacks
A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs	M. S. E. Sayed, N. -A. Le-Khac, M. A. Azer, A. D. Jurcut	2022	Flow-based anomaly detection	Enhanced anomaly detection in SDNs	Improved anomaly detection	Strengthened defense against anomalous behavior in SDNs
ShieldRNN: A Distributed Flow-Based DDoS Detection Solution for IoT Using Sequence Majority Voting	F. Alasmary, S. Alraddadi, S. Al-Ahmadi, J. Al-Muhtadi	2022	Distributed Flow-Based DDoS Detection	Improved IoT DDoS detection	Enhanced IoT DDoS detection	Strengthened IoT defense against DDoS attacks

Source-Based Defense Against DDoS Attacks in SDN Based on sFlow and SOM	M. Wang, Y. Lu, J. Qin	2022	sFlow and SOM-based defense	Enhanced source-based DDoS defense	Improved source-based defense	Strengthened defense against source-based DDoS attacks
Enhancing DDoS Attack Detection Using Snake Optimizer With Ensemble Learning on Internet of Things Environment	M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama, M. A. Hamza	2023	Snake Optimizer with Ensemble Learning	Enhanced DDoS attack detection in IoT	Improved IoT DDoS detection	Strengthened defense against IoT-based DDoS attacks

The evaluated research papers have proven relatively intensive for DDoS attack detection and prevention, thus highlighting the crucial value of AI in enhancing network security. These studies demonstrate distinct advancements: Some focus on the ability of AI to achieve high accuracy rates, improving overall network security through effective differentiation and containment of attacks[36,37]. Other works use AI algorithms to reduce false alarms and improve the accuracy of anomaly detection. Some of the articles show that AI is an effective tool for detecting different intensities of attack while dealing with various threat levels found in modern networks.

Specific studies also highlight AI's ability to identify and mitigate threats quickly, especially within the complex environment of IoT security. Collectively, all these academic attempts highlight the versatile role played by AI in serving as a support to strengthen network defense mechanisms against highly dynamic DDoS threats.

D. Conclusion

DDoS attacks are a kind of attack that will probably never be eliminated. This study explored various approaches, from sophisticated deep learning models to innovative anomaly detection techniques that analyze and counteract DDoS attacks. One of the most crucial findings made in this research is a level sophistication related to DDoS defenses. Deep learning, convolutional neural networks and machine learning algorithms have enabled cybersecurity experts to develop defense mechanisms that are efficient as well as highly flexible. These advanced techniques identify, respond and deactivate DDoS attacks thus reinforcing the protection of network. They improve overall network security and promote active cyber threat defense. These methods support resilience in SDN, IoT and NDN context. Continuous innovation also aims to optimize network defenses withstand DDoS attacks, as these innovative methods could translate into practical solutions. By analyzing, creating and integrating these advanced strategies, cybersecurity specialists may create more reliable, flexible and robust defense mechanisms to fight off far higher and diversified types of cyber-attacks. Investigate and implement these approaches, concentrating on practical realities as well scaling potentials to enhance network infrastructures while keeping organization one step ahead of cyber threats which are contentiously developing.

E. References

[1] S. Naiem, A. E. Khedr, A. M. Idrees, and M. I. Marie, "Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the

Detection of DDOS in Cloud Computing," IEEE Access, vol. 11, pp. 124597–124608, Oct. 2023, doi: 10.1109/access.2023.3328951.

[2] Sulaiman Mohamed Sulaiman, Shavan Askar, "Investigation of the Impact of DDoS Attack on Zakho University", Journal of University of Zakho, Vol 3A, No. 2, 2015.

[3] O. Shirko and S. Askar, "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking," in IEEE Access, vol. 11, pp. 21641-21654, 2023

[4] A. Praseed and P. Santhi Thilagam, "Multiplexed Asymmetric Attacks: Next-Generation DDoS on HTTP/2 Servers," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1790–1800, 2020, doi: 10.1109/TIFS.2019.2950121.

[5] F. Alasmary, S. Alraddadi, S. Al-Ahmadi, and J. Al-Muhtadi, "ShieldRNN: A Distributed Flow-based DDoS Detection Solution For IoT Using Sequence Majority Voting," IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3200477.

[6] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama, and M. A. Hamza, "Enhancing DDoS Attack Detection Using Snake Optimizer With Ensemble Learning on Internet of Things Environment," IEEE Access, vol. 11, pp. 104745–104753, 2023, doi: 10.1109/ACCESS.2023.3318316.

[7] Baydaa Hassan Husain & Shavan Askar, 2021. "Survey on Edge Computing Security," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 52-60.

[8] Kurdistan Ali & Shavan Askar, 2021. "Security Issues and Vulnerability of IoT Devices," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 101-115.

[9] "A_Two Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks".

[10] B. Meng, W. Andi, X. Jian, and Z. Fucai, "DDOS Attack Detection System Based on Analysis of Users' Behaviors for Application Layer," in Proceedings - 2017 IEEE International Conference on Computational Science and Engineering and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, CSE and EUC 2017, Institute of Electrical and Electronics Engineers Inc., Aug. 2017, pp. 596–599. doi: 10.1109/CSE-EUC.2017.109.

[11] Kosrat Dlshad Ahmed & Shavan Askar, 2021. "Deep Learning Models for Cyber Security in IoT Networks: A Review," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 61-70

[12] Zhwan Mohammed Khalid & Shavan Askar, 2021. "Resistant Blockchain Cryptography to Quantum Computing Attacks," International Journal of Science and Business, IJSAB International, vol. 5(3), pages 116-125.

[13] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack," Journal of Computer Networks and Communications, vol. 2019. Hindawi Limited, 2019. doi: 10.1155/2019/1283472.

[14] Vishal and Vasudha, "International Conference on Innovative Computing and Communication DOS/DDOS Attack Detection using Machine Learning: A Review." [Online]. Available: https://ssrn.com/abstract=3833289

[15] N. T. Cam and N. G. Trung, "An Intelligent Approach to Improving the Performance of Threat Detection in IoT," IEEE Access, vol. 11, pp. 44319–44334, 2023, doi: 10.1109/ACCESS.2023.3273160.

[16] M. S. El Sayed, N. A. Le-Khac, M. A. Azer, and A. D. Jurcut, "A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs," IEEE Trans Cogn Commun Netw, vol. 8, no. 4, pp. 1862–1880, Dec. 2022, doi: 10.1109/TCCN.2022.3186331.

[17] V. Degli-Esposti et al., "IEEE Access Special Section Editorial: Millimeter-Wave and Terahertz Propagation, Channel Modeling, and Applications," IEEE Access, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 67660–67666, 2021. doi: 10.1109/ACCESS.2021.3076326.

[18] "Hybrid_DDoS_Detection_Framework_Using_Matching_Pursuit_Algorithm".

[19] D. M. Sharif, H. Beitollahi, and M. Fazeli, "Detection of Application-Layer DDoS Attacks Produced by Various Freely Accessible Toolkits Using Machine Learning," IEEE Access, vol. 11, pp. 51810–51819, 2023, doi: 10.1109/ACCESS.2023.3280122.

[20] D. Nashat, S. Khairy, and M. M. Hassan, "Detection of Application Layer DDoS Attack Based on SIS Epidemic Model," IEEE Access, vol. 9, pp. 159827–159832, 2021, doi: 10.1109/ACCESS.2021.3132130.

[21] "An_Effective_Mechanism_to_Mitigate_Real-Time_DDoS_Attack".

[22] Y. Al-Dunainawi, B. R. Al-Kaseem, and H. S. Al-Raweshidy, "Optimized Artificial Intelligence Model for DDoS Detection in SDN Environment," IEEE Access, vol. 11, pp. 106733–106748, 2023, doi: 10.1109/ACCESS.2023.3319214.

[23] Dezheen H. Abdulazeez; Shavan K. Askar, "Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment" IEEE Accesss Volume 11, 2023.

[24] Saman M. Omer, Kayhan Z. Ghafoor, Shavan K. Askar, "Plant Disease Diagnosing Based on Deep Learning Techniques" ARO journal, 2022.

[25] Shavan Askar & Kosrat Dlshad Ahmed & Shahab Wahhab Kareem, 2021. "Deep learning Utilization in SDN Networks: A Review," International Journal of Science and Business, IJSAB International, vol. 5(6), pages 174-182.

[26] S. Yeom, C. Choi, and K. Kim, "LSTM-Based Collaborative Source-Side DDoS Attack Detection," IEEE Access, vol. 10, pp. 44033–44045, 2022, doi: 10.1109/ACCESS.2022.3169616.

[27] M. Wang, Y. Lu, and J. Qin, "Source-Based Defense Against DDoS Attacks in SDN Based on sFlow and SOM," IEEE Access, vol. 10, pp. 2097–2116, 2022, doi: 10.1109/ACCESS.2021.3139511.

[28] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning," IEEE Access, vol. 9, pp. 108495–108512, 2021, doi: 10.1109/ACCESS.2021.3101650.

[29] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," IEEE Access, vol. 9, pp. 146810–146821, 2021, doi: 10.1109/ACCESS.2021.3123791.

[30] J. E. Varghese and B. Muniyal, “An Efficient IDS Framework for DDoS Attacks in SDN Environment,” IEEE Access, vol. 9, pp. 69680–69699, 2021, doi: 10.1109/ACCESS.2021.3078065.

[31] F. Hussain et al., “A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks,” IEEE Access, vol. 9, pp. 163412–163430, 2021, doi: 10.1109/ACCESS.2021.3131014.

[32] Shavan Askar & Chnar Mustaf Mohammed & Shahab Wahhab Kareem, 2021. “Deep Learning in IoT systems: A Review”, International Journal of Science and Business, IJSAB, Vol. 5(6), pages 131-147.

[33] Zhala Jameel Hamad & Shavan Askar, 2021. “ Machine learning Powered IoT for Smart Applicatoins”, International Journal of Science and Business, IJSAB, Vol 5(3), pages 92-100.

[34] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, “FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks,” IEEE Access, vol. 11, pp. 28934–28954, 2023, doi: 10.1109/ACCESS.2023.3260256.

[35] Enhancing_the_Efficiency_of_Gaussian_Nave_Bayes_Machine_Learning_Classifier_in_the_Detection_of_DDOS_in_Cloud_Computing”.

[36] H. D. Zubaydi, M. Anbar, and C. Y. Wey, “Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller,” in Proceedings - 2017 Palestinian International Conference on Information and Communication Technology, PICICT 2017, Institute of Electrical and Electronics Engineers Inc., Sep. 2017, pp. 10–16. doi: 10.1109/PICICT.2017.26.

[37] D. H. Abdulazeez and S. K. Askar, "A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture Within the Fog-Cloud Environment," in IEEE Access, vol. 12, pp. 39936-39952, 2024