iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60409

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Enhancing DDoS Attack Classification: Ensemble of ANN Models with SDN-Based Network Analysis

Jeevitha R[1], Prabhu T[2]
[1]*Research Scholar,* [2]*Associate Professor, Department of Computer Applicatios, Dr. MGR Educational and Research Institute, Chennai, TamilNadu, India*

Abstract: ***In this survey optimization of Distributed Denial of Service (DDoS) attack classification has been explored. Dealing with the increasing frequency, and complexity of such attacks presents a substantial challenge to contemporary network infrastructures. An ensemble approach leveraging Artificial Neural Network (ANN) models is proposed to enhance accuracy and robustness. The integration of multiple neural network architectures, combined with the introduction of Software-Defined Networking (SDN), is emphasized as a crucial element for efficient network data analysis. SDN provides dynamic and programmable network management with real-time response capabilities. The fusion of ANN models and SDN-based analytics aims to improve DDoS attack detection precision while minimizing false positives. Thoroughly scrutinizing the strengths and weaknesses of diverse ANN architectures to assess their suitability for DDoS attack classification, the study has highlighted the impact of SDN on adaptability and responsiveness in network security. Positioning the ensemble approach as a comprehensive defense mechanism against the evolving DDoS threat landscape, the research illuminates not only the then-current state of DDoS attack classification, but also a proposed forward-looking methodology laying the groundwork for intelligent and adaptive security solutions aimed at safeguarding network infrastructures against persistent DDoS onslaughts.***
Keywords: DdoS attacks, Artificial Neural Network (ANN) models, Ensemble Approach, Optimization, Software-Defined Networking (SDN).

I. INTRODUCTION

The Software-Defined Networking (SDN) framework is an advanced architectural design comprising various layers and components designed to revolutionize traditional network management[1]. At its core lies the Infrastructure Layer, forming the foundation including both physical and virtual network equipment, such as network routers, switches, and connectivity points. This layer is the cornerstone for dynamic flow of data packets in the network. Connecting this infrastructure to the intelligent control layer are the Southbound APIs (Application Programming Interfaces)[2]. These APIs serve as the communication bridge, facilitating instructions and the SDN controller manages the set ups and manages the networks and the connections within the Infrastructure Layer. The Control Layer, housing the SDN controller, is the nerve center of the framework, where decisions regarding traffic management, policy implementation, and real-time network adjustments take place. Utilizing Southbound APIs, the controller orchestrates the behavior of the network devices, ensuring seamless data flow. Above the control layer, Northbound APIs provide an interface for external applications and services to interact with the SDN controller[3]. This layer serves as a gateway for applications seeking to leverage the programmability and adaptability of the SDN framework. As the SDN framework progresses towards the top, the Applications and Services Layer comes into play[4]. This layer comprises a diverse range of software applications and services that capitalize on the programmable nature of SDN. From network analytics to security applications, these services use Northbound APIs to communicate with the SDN controller, contributing to the overall intelligence and functionality of the network. Within this framework, SDN-enabled Network Devices play a pivotal role, embodying devices in the Infrastructure Layer that align with SDN principles. These components enable the separation of both control and data planes, enabling programmable configurations by the SDN controller[5]. They act as the hands and feet of the controller, executing decisions to optimize network performance. Enabling the communication across the SDN framework is the SDN Protocol, often embodied by OpenFlow[6]. This protocol standardizes the exchange of information between the controllers for SDN and networked equipment/s, fostering interoperability and allowing for a cohesive, multi-vendor environment. Altogether, the SDN framework is a carefully orchestrated symphony of layers and components. It isolates the control plane from the data plane while still adding flexibility and centralization, previously unattainable in traditional networking[7]. The modular design and standardized protocols empower organizations to adapt and scale their networks efficiently, meeting the demands of modern, dynamic, and complex networking environments[8]. In essence, the SDN framework is a transformative paradigm that empowers networks to be more agile, responsive, and intelligently managed in the ever-evolving landscape of information technology.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

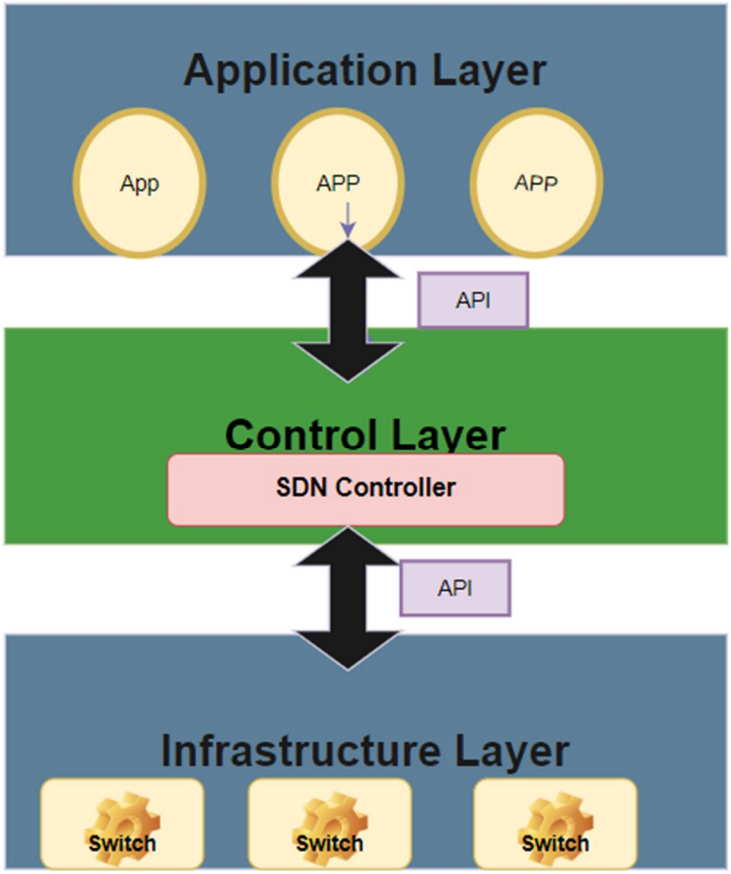


Fig. 1 SDN Architecture

A. Essential Characteristics of SDN

SDN is characterized by several essential features that distinguish it from traditional networking approaches[9]. These characteristics contribute to the flexibility, efficiency, and programmability of network infrastructures. Some of the essential characteristics of SDN include:

1) *Separation of Data Plane and Control Plane:* In the software-defined network field, the distinction among the Control Planes and Data Planes is essential. The idea is to divide the data plane, which transmits data packets physically from the control plane, from the control plane which decides what traffic to route over the network. This split has resulted in a centralised control system, which promotes a more flexible and configurable method toward Network Management.
2) *Centralized Network Control:* Centralized network control has played a crucial role. The SDN controller is the software program that integrates all the control plane operations. This centralized control mechanism facilitateds streamlined management, effective policy enforcement, and optimization of network resources.
3) *Programmability and Automation:* Programming ability and automation emerge as standout qualities. SDN networks show a high level of programmability, allowing administrators to design and control network behavior using the software. This programming ability facilitates task automation, allowing for greater responsiveness to changing internet conditions and evolving demands of applications.
4) *Open Standards and APIs:* Software-Defined Networking (SDN) is notable for its devotion to open standards and the availability of accessible Application Programming Interactions. This commitment to accessibility not only facilitates compatibility, but also fuels the development of a diverse ecosystem that include SDN-compatible apps, switches, and controls.
5) *Network Virtualization:* One prominent characteristic of the Software-Defined Networking (SDN) environment is its support for the virtualization of networks. This capability enabled the creation of many online networks inside a shared physical framework. In previous examinations, this quality was associated with increased utilization of assets, flexibility, and the capacity to separate and strengthen various network operations.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

6) *Dynamic Resource Allocation:* SDN, with its centralized oversight and programming ability, has previously enabled adaptive allocating of resources depending on immediate time infrastructure situations, hence improving network performance and response.
7) *Agility and Flexibility:* SDN architectures were intentionally designed for flexibility, enabling swift adjustments to evolving network demands. This adaptability is crucial in cloud environments, ensuring dynamic scalability, and facilitating the integration of technologies like IoT and 5G. In the dynamic IT landscape, SDN's design philosophy remains vital, supporting seamless technology integration and effective network administration.
8) *Improved Network Visibility:* SDN offers improved visibility into network traffic and performance via centralized monitoring. This heightened visibility facilitates more effective troubleshooting, optimization, and informed decision-making, contributing to overall improved network efficiency and reliability.
9) *Vendor Neutrality:* SDN's open architecture reduces dependence on proprietary hardware and allows organizations to choose networking equipment and software from different vendors. This vendor neutrality promotes competition and innovation in the networking industry.

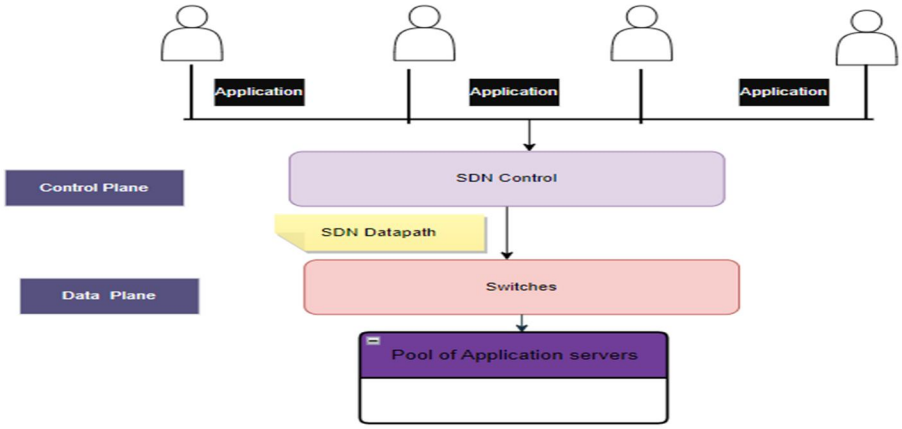


Fig. 2 Essential Components of SDN

B. Mitigating DDoS Attacks within SDN Environments

DDoS compromise SDN by depleting resources and impeding communication between valid hosts and the SDN controller, causing significant impact on the performance and behavior of programmable networks[10]. More specifically, distributed denial-of-service (DDoS) attacks consume the SDN controller, OpenFlow switches, and secure channels in an SDN environment by flooding the network with several new flows, disrupting valid servers. It's noteworthy that, distinct from traditional networks, DDoS poses unique threats to programmable networks like SDN. For instance, attackers might exploit low-volume traffic flows, creating a multitude of ingress messages to inundate both the ingress switch and the controller.

The emphasis on improving DDoS (Distributed Denial of Service) attack classification arises from the growing threat landscape in cybersecurity[11]. DDoS attacks pose a serious threat because they render a target system or network unavailable to authorized people by flooding it with excessive traffic. The need to improve classification techniques arises from the evolving sophistication of DDoS attacks, making it more challenging to identify and address them.

1) *Growing Complexity of DDoS Attacks:* DDoS attackers continually evolve their tactics, employing advanced methods to obfuscate their activities. Traditional classification mechanisms struggle to effectively identify and differentiate these complex attack patterns.
2) *Impact on Network Resilience:* Adequate categorization is necessary to precisely identify DDoS attacks. Enhancements in this area contribute directly to bolstering the resilience of networks, ensuring rapid response and mitigation measures.
3) *Evolving Attack Vectors:* DDoS attacks manifest through various vectors, such as volumetric, protocol, and application layer attacks. Improving classification capabilities allows for a nuanced understanding of these diverse attack types, enabling tailored defense strategies.

4) *Importance of Prompt Response:* Swift detection and classification of DDoS attacks are paramount to minimize downtime and mitigate potential damage. Enhancing classification methods facilitates quicker response times, reducing the impact of attacks on network availability.
5) *Integration of Advanced Technologies:* The integration of advanced technologies, such as Artificial Neural Networks and Software-Defined Networking offer new possibilities for improving classification accuracy. These technologies provide adaptive and intelligent approaches to control the DDoS assaults' dynamic characteristics.
6) *Protection of Critical Infrastructure:* Due to their significant threat to critical infrastructure, DDoS attacks require heightened attention. including financial institutions, healthcare systems, and government services, there is a pressing need to enhance classification methods to safeguard these essential services from disruption.
7) *Continuous Adaptation to Threats:* The cybersecurity landscape is dynamic, with attackers constantly refining their techniques. Enhancing DDoS attack classification is an ongoing process that involves adapting to emerging threats, ensuring that defensive measures remain effective against the latest attack vectors.

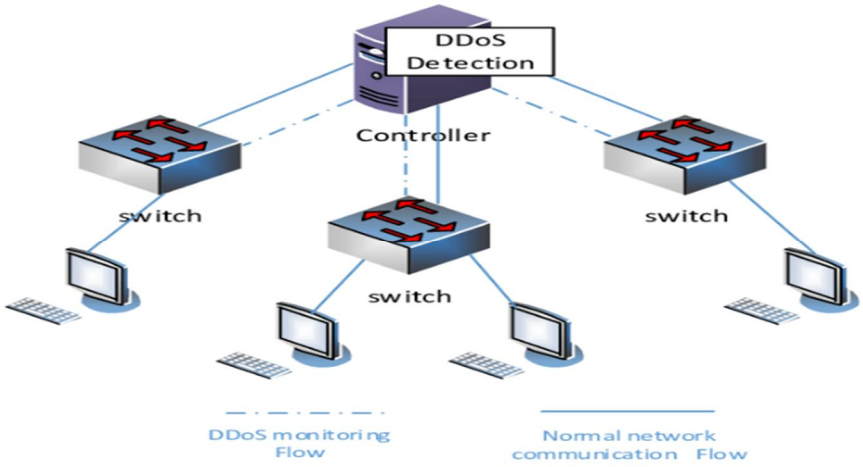


Fig. 3 Architectural Design of DDoS Detection System for SDN.

Utilized as a control program, the DDoS detection function operates by enabling periodic communication between the controller and the switch to gather and analyze network flows. Upon detecting a flow indicative of a DDoS attack, the controller adjusts the forwarding rules in the flow table and alerts the switch to address the anomaly. Throughout this survey, we embark on an exploration of various ANN architectures, scrutinizing their individual strengths and limitations in the context of DDoS attack detection[13]. Additionally, we investigate the integration of SDN, emphasizing its role in augmenting the adaptability and responsiveness of the classification framework. The proposed ensemble approach not only seeks to bolster the accuracy of DDoS detection but also strives to minimize false positives, a crucial aspect in ensuring the efficacy of any security solution.

II. LITERATURE REVIEW

In the literature review, a comparative analysis of two DDoS detection schemes employing a thresholding approach and a Machine Learning approach Indicates that the machine learning-driven approach demonstrates performance in terms of both detection precision and computational complexity expenditure (R. Fouladi et al). The focus on SDN security, among other challenges, has drawn the interest of both academia and industries, as emphasized by Dayal et al. (2016). The expanding IT infrastructure processes introduced ensures the integrity, confidentiality, authentication, and availability of information within the IT infrastructure present complexities, as discussed by Singh and Behal (2020). In the domain of SDN security, Distributed Denial of Service Attacks (DDOS) emerges as a notable apprehension, aiming to render systems or network resources unusable or inaccessible, motivated by various factors such as financial profits, political incentives, and service disruption, as detailed by Bawany et al. (2017).
Zhijun et al. proposed a DDoS detection technique employing factorization machines (FM) specifically tailored for low-rate DDoS attacks on the data plane within SDN framework, achieving a accuracy through fine-grained detection techniques. Liu et al. suggested a DDoS attack detection approach incorporating information entropy and Deep Learning (DL). Information entropy identified spoofed switch ports., and a Convolutional Neural Network model was utilized to differentiate between suspicious and regular traffic.

TABLE I OUTCOME AND CHALLENGES OF VARIOUS RESEARCH STUDIES

s.no	Author	Methodology	Challenges	Outcomes
1	K. Sundar *et al [13]*	The paper employs Decision Tree and Support Vector Machine (SVM) machine learning techniques for detecting malicious traffic.	Accurately detecting malicious traffic	Study demonstrates that Decision Tree and SVM algorithms outperform others, achieving superior accuracy and detection rates in identifying malicious network traffic.
2	Kannan,C *et al [14]*	The study utilizes the Ryu controller and Mininet tool to address the impact of Denial of Service (DoS) attacks on Software-Defined Networking (SDN). Machine learning (ML) algorithms, implemented through Ryu and Mininet, are employed for DoS attack detection. Various ML techniques are applied to identify and drop malicious traffic in real-time, preventing network congestion.	Overcoming challenges associated with SDN controller vulnerabilities to DoS attacks and effectively implementing ML-based detection methods.	Simulated in Mininet, demonstrates effective DoS attack detection with notable accuracy, showcasing its potential for enhancing SDN security.
3	Obaid Rahman *et al [15]*2019	The study looks at how to prevent DDoS attacks in Software Defined Networking (SDN) by using methods based on machine learning such J48, Random Forest (RF), Support Vector 4Machine (SVM), and K-Nearest Neighbors (K-NN).	Tackling security threats, particularly DDoS attacks, in SDN networks and selecting the most effective machine learning algorithm for detection.	J48 outperforms other evaluated algorithms, demonstrating superior performance, especially in regards to training and testing time, rendering it a promising option for DDoS detection and prevention in SDN environments.
4	V.Deepa *et al [16]*2019	An ensemble technique is employed, which combines K-Nearest Neighbor (KNN), Naive Bayes, Support Vector Machine (SVM), and Self-Organizing Map (SOM) machine learning algorithms. detecting anomalous behavior in Software Defined Network (SDN) traffic.	Addressing challenges related to Distributed Denial of Service (DDoS) attacks in SDN, particularly in handling large-scale traffic floods and coordinating responses across the network.	Experimental findings demonstrate that the ensemble approach in machine learning surpasses the performance of individual algorithms. demonstrating superior accuracy, detection rates, and lower false alarm rates. This highlights the efficacy of the proposed ensemble technique in enhancing SDN security against anomalous data traffic behavior.
5	S. Sumathi *et al [17]*2022	A hybrid optimization algorithm, blending Harris Hawks Optimization (HHO) and Particle Swarm Optimization (PSO), fine-tunes network parameters such as weight vectors and bias coefficients. This approach, integrating Long Short-Term Memory (LSTM) recurrent neural network with autoencoder and decoder architectures, aims to address the shortcomings of existing Intrusion Detection Systems (IDS) for detecting Distributed Denial of Service (DDoS) attacks.	challenges in traditional IDS models, including delayed convergence, local stagnation, and trapping issues, particularly in the context of DDoS attacks in cloud computing environments.	The LSTM and deep learning model, enhanced by the hybrid HHO-PSO algorithm, demonstrates superior performance compared to existing models in the literature. Results affirm its effectiveness in detecting DDoS attacks, underscoring the efficacy of the hybrid optimization and deep learning methodology.

III. RESEARCH GAP

Table 1 in the survey visually represents the existing research gaps that were not adequately addressed or explored by prior researchers in the surveyed literature. The survey uncovered several significant research gaps in the realm of enhancing DDoS attack categorization through the Ensemble Approach of ANN Models and SDN-Based Networking Data Analysis. While prior research had made tremendous progress in providing ensemble approaches for DDoS identification, a key research gap existed in the lack of real-world application and efficacy assessment[19]. Extensive investigations evaluating the actual efficacy of the suggested ensemble technique in a variety of network contexts and settings were clearly required. Furthermore, more research was needed into the scalability issues and potential performance consequences of adopting this technology in large-scale networks. Another research need was the development of hybrid techniques, which combines machine learning, rule-based systems, and anomaly detection to deliver a more holistic defense against attacks. that use DDoS. The survey underscores the imperative to address the ongoing proliferation of DDoS threats, highlighting the necessity for research dedicated to identifying and classifying novel attack vectors, while also pointing out the previously unexplored avenue of integrating the proposed ensemble approach with real-time threat intelligence feeds; the study's focus is on investigating the behavioral patterns in Software Defined Network (SDN)-based network data concerning DDoS attacks and their types, utilizing various Exploratory Data Analysis (EDA) techniques, with the overarching goal of constructing an Ensemble model utilizing the Artificial Neural Network (ANN) algorithm for the classification of attack events and their types.

IV. SOLUTION AS DISCUSSION

The research was driven by the increasing sophistication of DDoS attacks, posing challenges for detection. The proposed solution, outlined in "Survey on Optimizing DDoS Attack Classification: Ensemble Approach of ANN Models with SDN-Based Network Data Analysis," addresses the limitations of existing optimization techniques for countering DDoS attacks.[20]

A. Dataset Collection and Preprocessing

The research commenced with the meticulous collection and preprocessing of datasets, laying the foundation for a robust analysis.

B. Optimized AI Model Training

The core of the solution involves training an Artificial Neural Network (ANN) model, optimizing its hyperparameters to improve accuracy and effectiveness in DDoS attack detection.

C. Benchmarking ANN Models

Benchmarking of various ANN models is being conducted, providing insights into their comparative performance and aiding in the selection of an effective ensemble approach by leveraging these capabilities, the developed ANN model notably enhances the precision and efficacy of DDoS detection systems, reinforcing the resilience and security of network infrastructures. The paper makes substantial contributions to SDN security by shedding light on optimizing ANN models for DDoS detection.

Furthermore, this review emphasizes the importance of hybrid techniques, combining Deep learning, rule-based systems for a more robust defense against DDoS attacks. Integrating the proposed ensemble approach with real-time threat intelligence feeds is identified as an underexplored avenue, promising enhanced system responsiveness.

V. CONCLUSION

This survey has delved into the critical domain of optimizing DDoS attack classification, focusing on the innovative Ensemble Approach that integrates Artificial Neural Network (ANN) models with Software-Defined Networking (SDN)-based network data analysis. The exploration of this ensemble methodology has revealed its potential to substantially improve the precision and efficacy of DDoS attack detection and classification, thus an improved counter-response system. The integration of ANN models brings a layer of intelligence to the system, enabling more nuanced analysis and pattern recognition in the detection of DDoS attacks. Simultaneously, the utilization of SDN-based network data analysis provides a centralized and dynamic control mechanism, allowing for adaptive responses to emerging threats. Throughout the survey, it became evident that this ensemble approach not only improves the precision of DDoS attack classification but also aligns with the contemporary trends in networking, where the segregation of control and data planes is a foundational principle. The comprehensive review of related literature has provided insights into the strengths and constraints of different methodologies, underscoring the necessity for a comprehensive and adaptable approach to tackle the changing landscape of DDoS attacks.

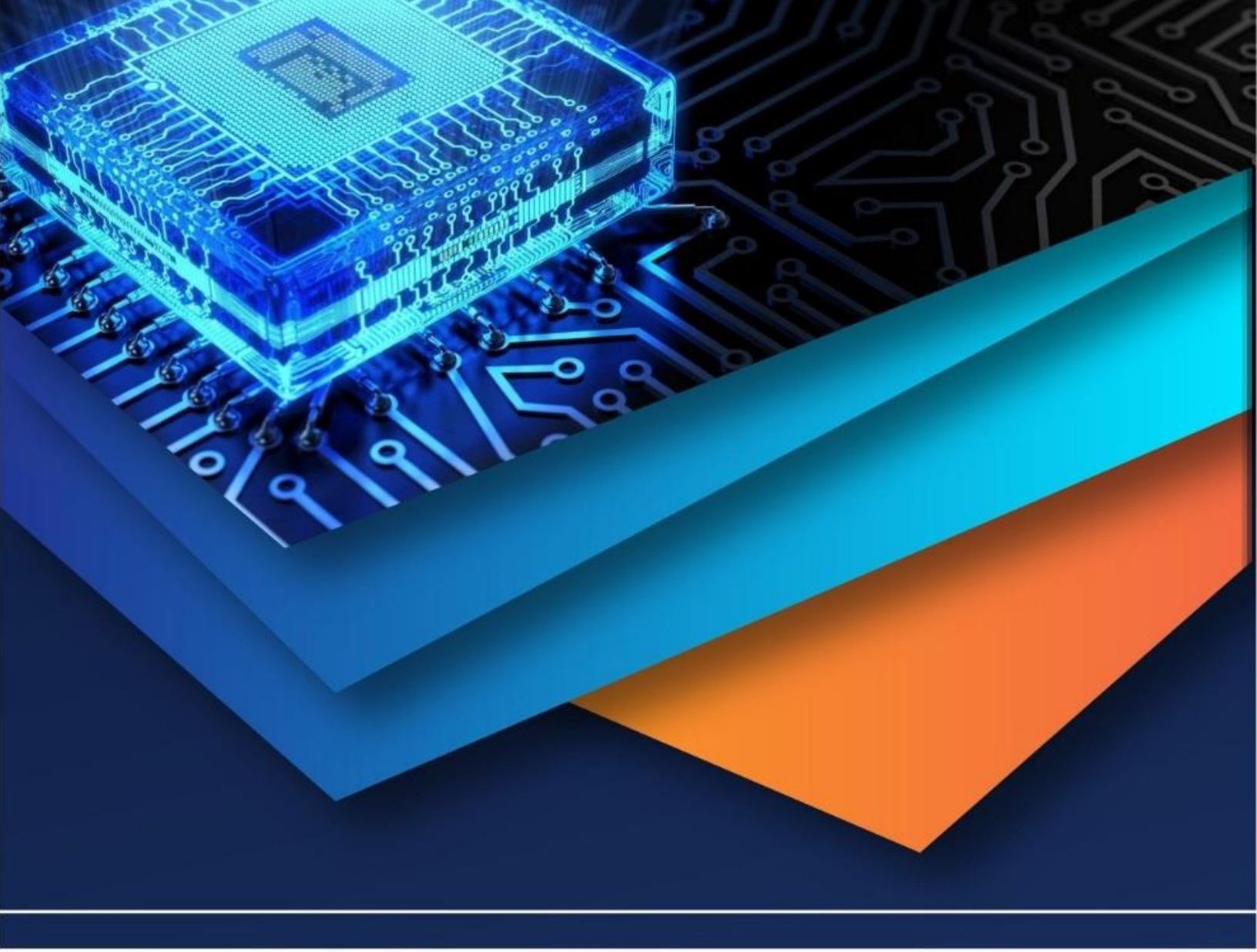
©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The synergy between advanced technologies, such as ANN models and SDN, demonstrate the potential for a robust and intelligent defense against DDoS attacks. However, it is crucial to acknowledge the ongoing evolution of cyber threats, necessitating continuous research and development to stay ahead of emerging challenges. This survey lays the groundwork for future investigations, encouraging the exploration of novel techniques and the integration of emerging technologies to further enhance the resilience of networks against DDoS attacks given the ever-changing digital landscape, the insights derived from this survey can be instrumental in the ongoing discourse on bolstering cybersecurity measures and thus ensuring the integrity of network infrastructures in the face of dynamic and sophisticated threats.

REFERENCES

[1] Vickramasingam, Deepa & Sudar, K. Muthamil & Deepalakshmi, P.. (2019). Design of Ensemble Learning Methods for DDoS Detection in SDN Environment. 1-6. 10.1109/ViTECoN.2019.8899682.
[2] M. I. Sayed, I. M. Sayem, S. Saha and A. Haque, "A Multi-Classifier for DDoS Attacks Using Stacking Ensemble Deep Neural Network," 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 2022, pp. 1125-1130, doi: 10.1109/IWCMC55113.2022.9824189.
[3] J. F. Cañola Garcia and G. E. T. Blandon, "A Deep Learning-Based Intrusion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks," in IEEE Access, vol. 10, pp. 83043-83060, 2022, doi: 10.1109/ACCESS.2022.3196642.
[4] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane and I. B. Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," in IEEE Access, vol. 11, pp. 119862-119875, 2023, doi: 10.1109/ACCESS.2023.3327620.
[5] Ahmad, R., Alsmadi, I., Al-Hamdani, W. A., & Tawalbeh, L. (2022). A deep learning ensemble approach to detecting unknown network attacks. Journal of Information Security and Applications, 67, 103196. https://doi.org/10.1016/j.jisa.2022.103196
[6] Mohammed, A., & Kora, R. (2023). A comprehensive review on ensemble deep learning: Opportunities and challenges. Journal of King Saud University - Computer and Information Sciences, 35(2), 757–774
[7] Alghamdi, R., Bellaiche, M. An ensemble deep learning based IDS for IoT using Lambda architecture. Cybersecurity 6, 5 (2023)
[8] Saha, S.; Priyoti, A.T.; Sharma, A.; Haque, A. Towards an Optimized Ensemble Feature Selection for DDoS Detection Using Both Supervised and Unsupervised Method. Sensors 2022, 22, 9144.
[9] Arshad, A. M., Jabeen, M., Ubaid, S., Raza, A., Abualigah, L., Aldiabat, K., & Jia, H. (2023). A novel ensemble method for enhancing Internet of Things device security against botnet attacks. Decision Analytics Journal, 8, 100307.
[10] S. Sumathi, R. Rajesh, Sangsoon Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection", Journal of Sensors, vol. 2022, Article ID 8530312, 21 pages, 2022.
[11] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. Wang, and Y. Liu, “A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges,” IEEE Communications Surveys & Tutorials, vol.21, no. 1, pp. 393-430, 2019.
[12] H. K. Lim, J. B. Kim, J. S. Heo, K. Kim, Y. G. Hong, and Y. H. Han, “Packet-based network traffic classification using deep learning,” International Conference on Artificial Intelligence in Information and Communication, IEEE Press,February 2019, pp. 046-051.
[13] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402517.
[14] Kannan, C., Muthusamy, R., Srinivasan, V., Chidambaram, V., & Karunakaran, K. (2023). Machine learning based detection of DDoS attacks in software defined network. Indonesian Journal of Electrical Engineering and Computer Science. DOI:10.11591/ijeecs.v32.i3.pp1503-1511
[15] O. Rahman, M. A. G. Quraishi and C. -H. Lung, "DDoS Attacks Detection and Mitigation in SDN Using Machine Learning," 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019, pp. 184-189, doi: 10.1109/SERVICES.2019.00051
[16] V.Deepa et al., “Design of Ensemble Learning Methods for DDoS Detection in SDN Environment” 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) DOI:10.1109/ViTECoN.2019.8899682
[17] S. Sumathi et al., Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection Hindawi Journal of Sensors Volume 2022, Article ID 8530312, 21 pageshttps://doi.org/10.1155/2022/8530312
[18] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane and I. B. Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," in IEEE Access, vol. 11, pp. 119862-119875, 2023, doi: 10.1109/ACCESS.2023.3327620
[19] R. Fadaei Fouladi, O. Ermis and E. Anarim, "A Comparative Study on the Performance Evaluation of DDoS Attack Detection Methods," 2022 30th Signal Processing and Communications Applications Conference (SIU), Safranbolu, Turkey, 2022, pp. 1-4, doi: 10.1109/SIU55565.2022.9864872.
[20] W. Zhijun, X. Qing, W. Jingjie, Y. Meng and L. Liang, "Low-rate DDoS attack detection based on factorization machine in software defined network", IEEE Access, vol. 8, pp. 17404-17418, 2020.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)