Fuzzy Systems and Soft Computing
ISSN : 1819-4362

A SURVEY OF DISTRIBUTED DENIAL-OF-SERVICE ATTACKS AND DETECTION

Gibi K S, Research Scholar, Department of Computer Science, Park's College, Tirupur
Dr. S.Nithya, Assistant Professor, Department of Computer Science, AVP College of Arts and Science, Tirupur.

Abstract:
Distributed Denial-of-Service (DDoS) attacks pose a significant threat to the availability of internet-based applications, targeting critical resources to disrupt services to legitimate users. A surge in online activity and the proliferation of Internet of Things (IoT) devices provide fertile ground for attackers. The attack surface has expanded exponentially with millions of individuals transitioning to remote work, e-commerce, and entertainment platforms. As we anticipate the trends for 2024, projections indicate a staggering rise to over 15.4 million attacks, highlighting the pressing need for robust security measures [1]. This survey endeavors to find the problem with the current systems and discover the pioneer advancements in DDoS intrusion detection. By examining the current scenario, it will be more efficient and effective if we use a system using artificial intelligence (AI) and machine learning (ML) to detect and block malicious traffic, thereby safeguarding the confidentiality, integrity, and availability (CIA) of network resources.
Key Words: DDoS, machine learning, Artificial Intelligence, IoT, confidentiality, integrity, availability.

INTRODUCTION:

A distributed denial-of-service (DDoS) attack disrupts the functioning of a server, service, or network by overwhelming it with unwanted Internet traffic. At their most severe, these attacks can render a website or entire network inaccessible for prolonged periods. DDoS attacks send malicious traffic to a target through numerous computers or devices. Frequently, these devices are part of a botnet: a collection of compromised devices controlled by a single attacker. Some DDoS attacks involve multiple attackers or specialized DDoS tools, like stress-testing applications or slow-and-steady programs These attacks, which reached 7.9 million in 2018, have escalated in frequency and complexity, particularly during the COVID-19 pandemic. As lockdown restrictions forced a global shift towards remote working and online activities, the reliance on internet services surged, providing ample opportunities for DDoS attackers. By analyzing trends before and after the pandemic, we aim to understand the evolving threat landscape and propose proactive measures to mitigate risks.

The COVID-19 pandemic has catalyzed a dramatic increase in DDoS attacks, fuelled by the unprecedented surge in online activity and the proliferation of IoT devices. The attack surface has expanded exponentially with millions of individuals transitioning to remote work, e-commerce, and entertainment platforms. In 2019 alone, DDoS attacks reached 9.5 million, underscoring the escalating threat landscape. As we anticipate the trends for 2024, projections indicate a staggering rise to over 15.4 million attacks, highlighting the pressing need for robust security measures [1].

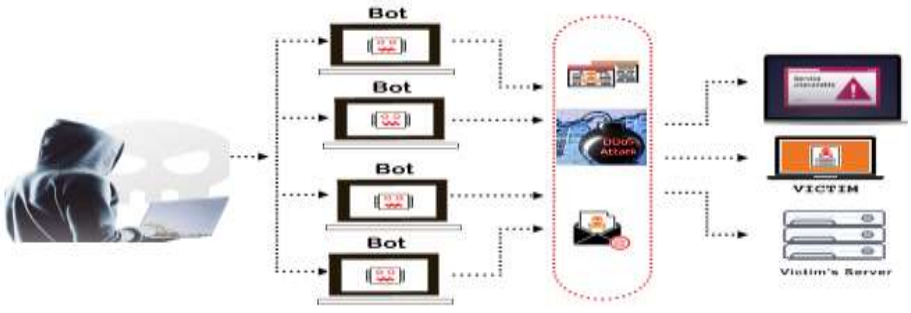

Figure 1: *How DDoS Works.*

Businesses and governments have traditionally used a reactive approach to cyber threats, layering various security solutions on top of each other. This approach is costly and ineffective, as negative

cyber-attacks often make headlines [2]. Boards of directors are now prioritizing cyber security due to recent data breaches. Instead, businesses should consider implementing an automated, integrated Next-Generation Security Platform that offers reliable, prevention-based security across Saab's environments, endpoints, data centers, networks, and public and private clouds [3]. Emphasizing prevention can reduce overall cyber security risk and prevent threats before they affect the network.
The swift advancement of technologies is also increasing the difficulty of cyber security since there are currently no long-term fixes for the issues at hand. Even if we are actively combating and showcasing a variety of frameworks or technologies to safeguard our network and data, none of them offer long-term safety. But with improved security knowledge and sensible tactics, we can lessen the loss of money and reputation while safeguarding trade secrets and intellectual property [4].
The digital storage of vast volumes of data and private documents by federal, state, and municipal governments makes them prime targets for cyber attacks. The majority of the time, inadequate funding, ignorance, and unsuitable infrastructure cause governments to struggle. Government agencies must preserve sensitive data, uphold positive citizen-government relations, and offer dependable services to the public [5]. Different cyber-security strategies are used to combat the wide range of cyber threats. Authentication, Encryption, Digital Signatures, Antivirus, and Firewall are the techniques used for cyber security [6].
Using deep learning to its full potential in cyber-security means using advanced algorithms to automatically recognize and block new and emerging cyber threats [7]. By learning patterns from large datasets, deep learning models like neural networks improve threat detection skills and make it possible for them to adjust to new attack strategies [8]. The malware that is contained in the program can be quickly identified by AI algorithms, which can then take effective action [9]. It is also employed in the processing of the enormous volume of data that users provide every day. To detect these assaults, machine learning (ML) with increased security detection software, encoding, and thread extraction features is needed [10]. However, the idea of deep learning is more effective in identifying cyber-security problems. deep learning systems may effectively process large amounts of data found in cyber-security datasets [11].

2. BACKGROUND STUDY

Preventing Distributed Denial-of-Service (DDoS) attacks is vital for maintaining the stability and accessibility of online services, networks, and servers. Although complete eradication of the threat is unfeasible, organizations can significantly minimize their susceptibility through proactive measures. This involves deploying robust network security measures such as firewalls, intrusion detection, and prevention systems, alongside leveraging specialized DDoS mitigation services provided by ISPs or third-party vendors. Additionally, implementing traffic analysis tools, anomaly detection systems, and content delivery networks (CDNs) enables organizations to monitor and distribute traffic effectively, reducing the impact of potential attacks. By adopting a multi-layered approach encompassing these strategies, businesses can fortify their digital infrastructure against DDoS attacks and ensure uninterrupted service availability. To tackle these issues, Machine learning techniques have been implemented to improve the accuracy and effectiveness of D DoS attack detection in Networks.

Components of ML in DDoS Attack Detection

Data Collection: Collect raw network traffic data from routers, switches, and other network devices. This includes packet captures and flow data. Gather log data from firewalls, intrusion detection/prevention systems (IDS/IPS), and servers.

Data Pre-processing: Filter out irrelevant or redundant information, deal with missing values, and normalize timestamps. Convert raw network traffic into features such as packet size, inter-arrival time, protocol type, source/destination IP addresses, etc. Summarize data over fixed intervals to create a manageable dataset, such as the number of packets per second.

Feature Engineering: Identify relevant features for DDoS detection, such as traffic volume, packet rate, flow duration, and unique source/destination IPs. Create additional features like traffic entropy, percentage of SYN packets, ratio of incoming to outgoing traffic, etc.

Model Selection: Choose appropriate machine learning algorithms suited for anomaly detection, such as clustering (K-means), classification (Random Forest, SVM), or deep learning methods (autoencoders, CNNs, RNNs). Define the structure of models, especially for deep learning (e.g., LSTM networks for sequence data).
Model Training: Use historical data with labeled instances of normal and attack traffic to train the model. Employ optimization techniques to adjust model parameters for the best performance. Adjust hyperparameters such as learning rate, number of layers/neurons in neural networks, and regularization parameters.
Model Evaluation: Utilize metrics like precision, recall, F1 score, true positive rate (TPR), false positive rate (FPR), and area under the ROC curve (AUC) to evaluate model performance. Perform k-fold cross-validation to ensure the model generalizes well to unseen data.
Model Deployment: Deploy the trained model into a network monitoring system for real-time analysis. Expose the model via APIs for integration with existing security infrastructure.
Monitoring and Maintenance: Continuously monitor model performance in detecting new types of DDoS attacks. Regularly retrain the model with new data to adapt to evolving attack patterns.

3.LITERATURE SURVEY

In 2023, Alsirhani *et al.* [12] proposed a novel intrusion detection method for intelligent grids, combining feature-based and DL-based methods. The method used pre-processed datasets, extracted information, arranged features using the African Vulture Optimization Algorithm, and used DBN-LSTM for categorization, proving effective in detecting cybersecurity intrusions.
In 2023**,** Kumar *et al*. [13] combined a Digital Twin technology, Software-Defined Networking (SDN), Deep Learning (DL), and blockchain to design a secure SG network. The secure communication channel uses blockchain authentication, while a new DL architecture enhances attack detection. SDN served as the network backbone, and DT technology was integrated into the SDN control plane. The blockchain implementation demonstrated efficiency and better intrusion detection.
In 2022, Suryotrisongko and Musashi [14] presented a novel deep-learning model for cybersecurity, combining quantum and classical techniques. It used domain generation algorithms (DGA) for botnet detection and compared its performance with classical models. The model's quantum circuit combined Pennylane's embedding and layers circuit. It achieved high accuracy in some cases.
In 2022, Abdiyeva-Aliyeva *et al*. [15] discussed the use of machine learning algorithms, specifically XGBoost, in detecting cybercrime. It highlighted the importance of real-time checking systems and the mathematical background of XGBoost, referencing previous studies on its effectiveness in cybersecurity. The article underscored the potential of machine learning in minimizing cybercrime risks.
In 2023, Kävrestad *et al.* [16] aimed to develop design guidelines for cognitively accessible cybersecurity training, targeting around 10% of users with cognitive disorders. Cybersecurity was perceived as cognitively demanding, and a minimalistic approach is needed to minimize cognitive processing, incorporating accessibility features and minimizing design and informational features.
In 2023, Renaud and Dupuis [17] suggested that cybersecurity can learn from religions to enhance security practices. They explored religions' experience in dealing with human nature and fallibility and highlighted challenges like employee non-compliance. They proposed a vision for cybersecurity based on religious insights, seeking feedback from professionals to create a new era of best practices.
In 2023, Rawindaran *et al.* [18] examined the opinions of SMEs in Wales on collaborating with the government to tackle cybersecurity issues. It focused on the challenges faced by SMEs in implementing effective cybersecurity measures and their perception of government engagement, aimed at improving cybersecurity initiatives.
In 2023, Bozorgchenani *et al*. [19] explored the optimization of cybersecurity levels and IDM selection in 5G networks using multiple Security Agents. It proposed a joint security and QoS utility function, balancing cybersecurity and resource costs, and demonstrated the importance of different parameters through simulations.

In 2023, Chang and Huang [20] highlighted the significance of information sharing in cybersecurity and the establishment of Information-Shared and Analysis Organizations (ISACs) in Taiwan. It discussed factors influencing information sharing, operational practices, and the need for effective governance and policy alternatives.
In 2018, Xin *et al*. [21] proposed a method that uses deep learning techniques to identify malware and pirated software on the Internet of Things. It used TensorFlow deep neural network to detect source code plagiarism, tokenization, weighting feature approaches, and color image visualization to identify viruses. The method outperformed state-of-the-art techniques in classifying cybersecurity threats in IoT networks.

Table 1: Review By Various Authors About Research Gaps.

Authors and citations	**Aim**	**Advantages**	**Limitations**
Alsirhani *et al.* [12]	To suggest a novel approach to cybersecurity intrusion detection for intelligent grids by fusing feature-based and deep learning-based methods.	Effectiveness	It did not assess how well it performed in other scenarios or against a broader variety of intrusions.
Kumar *et al*. [13]	To create a novel Smart Grid (SG) network that combines blockchain, Software-Defined Networking (SDN), Deep Learning (DL), and Digital Twin (DT) technologies to improve cybersecurity in SG environments that are enabled by IoT.	Low latency and real-time services in the SG network. Improves communication with SMs	The scalability was not tested with more smart meters or with various real-time datasets.
Suryotrisongko and Musashi [14]	To assess a hybrid quantum-classical deep learning model's efficacy in cybersecurity botnet domain generation algorithm (DGA) identification.	High accuracy Explores the applicability of the model for current Noisy Intermediate Scale Quantum (NISQ) technology	It did not investigate the various arrangements of layers and quantum circuit embeddings.
Abdiyeva-Aliyeva *et al*. [15]	To examine the potential applications of machine learning algorithms—more especially, classification algorithms—in cybersecurity to lessen the damaging effects of cybercrimes and assaults	Highlights the potential of XGBoost Highlights the significance of providing people with training	It excluded the group learning of many deep learning and machine learning techniques.
Kävrestad *et al.* [16]	To create a design guideline for cybersecurity training that is cognitively accessible	Makes a theoretical addition to the topic of cybersecurity education	The usability problems experienced by people with

	for those with cognitive impairments.	that is cognitively accessible.	cognitive limitations were not addressed.
Renaud and Dupuis [17]	To investigate the cybersecurity lessons that can be drawn from religions in order to enhance cybersecurity procedures, lower staff error rates, and prevent intentional security policy violations.	Offers a better cybersecurity environment within organizations provides a vision for cybersecurity	It didn't concentrate on creating and honing the cybersecurity vision using knowledge from religious activities.
Rawindaran *et al.* [18]	To investigate the viewpoints of Wales' small and medium-sized businesses (SMEs) on their cooperation with the government to address cybersecurity issues.	Gives information about the obstacles and difficulties faced by SMEs	It did not look into creating specialized government assistance programs.
Bozorgchenani *et al*. [19]	To tackle the difficulties of choosing suitable Intrusion Detection Mechanisms (IDMs) and maximizing cybersecurity levels in 5G networks while taking Quality of Service (QoS) and security goals into account.	Highlights the significance of many aspects in the joint problem Security Agent (SA) detection level increases improve security utility but reduce QoS usefulness.	It skipped over the more intricate situation.
Chang and Huang [20]	To investigate the administration of cybersecurity information-sharing networks spanning many sectors, with a particular emphasis on Taiwan's Information Sharing and Analysis Center (ISAC).	Explains the motivation behind and methods by which ISAC members exchange cybersecurity information.	The diverse effects of formal and informal regulations on cooperative information-sharing behaviors were not examined.
Xin *et al*. [21]	To provide a combined deep learning method for identifying files contaminated with malware and illegal applications on IoT networks.	better classification performance	It failed to address the interpretability issue.

DDoS attack detection using various Algorithms:

Detecting Distributed Denial of Service (DDoS) attacks is paramount in safeguarding network integrity. Various algorithms, ranging from statistical analysis to machine learning, have emerged as effective tools in identifying these threats. By analyzing traffic patterns and deviations, these algorithms distinguish between legitimate and malicious traffic. This paper aims to assess the efficacy of different detection algorithms, evaluating their strengths, limitations, and real-world applicability. Through this exploration, we aim to provide insights into enhancing network security against evolving

cyber threats.
In 2023 Wang, Jin, et [22] Proposed CC-Guard, a defense scheme for SDN against DDoS attacks. It features four modules: attack detection trigger, switch migration, detection, and mitigation. Using controller capabilities, it ensures timely defense operations and prevents congestion. Detection employs a two-stage method and multiple IDS for efficient attack identification. Simulations validate CC-Guard's effectiveness, but improvements are needed for accurate attack identification and large-scale experiments. Future work aims to enhance CC-Guard's versatility and scalability through physical SDN experimentation.
In 2020 S. Kiranyaz,[23] proposed an in-depth exploration of 1D Convolutional Neural Networks (CNNs) and their burgeoning role in diverse engineering domains. While 2D CNNs have long dominated image-related tasks, the rise of 1D CNNs presents a compelling solution for processing 1D signals like time series data. By elucidating the architecture and operational principles of 1D CNNs, the paper underscores their capacity to excel in scenarios with limited training data and their suitability for cost-effective, real-time hardware implementation due to their streamlined configuration. Notably, the review highlights the transformative impact of 1D CNNs across various engineering applications, including biomedical data classification, early diagnosis, structural health monitoring, and fault detection in electrical systems. By filling a notable gap in the literature, this paper not only consolidates existing knowledge but also provides essential resources such as benchmark datasets and software tools, thereby facilitating further exploration and adoption of 1D CNNs in practical settings.
In 2020 M. V. O. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença [24], presented a novel defense mechanism for Software-defined Networking (SDN) environments, leveraging deep learning techniques for efficient detection of DDoS and intrusion attacks. By analyzing individual IP flow records, the proposed system, based on Gated Recurrent Units (GRU), offers swift identification of malicious activities, enabling rapid response and minimizing potential disruptions to the network. Evaluation against diverse machine learning methods using public datasets demonstrates promising detection rates. Additionally, the implementation of a lightweight mitigation strategy showcases its potential for real-world deployment. Feasibility tests further underscore the scalability of the approach, indicating its suitability for large-scale networks. Overall, the findings highlight the efficacy and viability of employing GRU-based models in fortifying SDN infrastructures against evolving cybersecurity threats.
In 2021 M. S. ElSayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut [25], prposed a hybrid Deep Learning (DL) approach, employing convolutional neural networks (CNN), for Network Intrusion Detection Systems (NIDSs) in Software-defined Networking (SDN) environments. Highlighting the vulnerability of SDN controllers to attacks, the study introduces a new regularizer, SD-Reg, addressing overfitting issues to enhance model robustness. Evaluation against diverse datasets, including InSDN, demonstrates the superiority of SD-Reg and the efficacy of the hybrid DL technique. Additionally, the study explores lightweight NIDS by training CNN models with reduced feature sets, indicating minimal impact on performance. This research contributes to strengthening SDN security, facilitating wider adoption of SDN technologies.
In 2021 F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina [26], presented a novel paper on an Intrusion Detection Systems (IDS), which monitor network traffic for malicious activity, are crucial for countering these threats and can be host-based or network-based. Recent deep learning-based IDS approaches, while promising, have high false negative rates. To improve performance, we propose a detection model combining Long Short-Term Memory (LSTM) networks with an Attention mechanism and four feature reduction algorithms: Chi-Square, UMAP, PCA, and Mutual Information. Evaluated on the NSL-KDD dataset, our model achieved accuracies of 99.09% for binary classification and 98.49% for multiclass classification, highlighting its effectiveness in enhancing network security.
In 2021 Y. Liu, T. Zhi, M. Shen, L. Wang, Y. Li, and M. Wan [27] proposed Software Defined Networking (SDN) decouples the control plane from the data plane, facilitating new service deployment but introducing the risk of a single point of failure. Attackers often target the SDN controller with distributed denial of service (DDoS) attacks via switches. Traditional DDoS detection methods struggle to balance accuracy and efficiency: statistical methods lack accuracy, while machine

learning methods are inefficient and costly to train. To address this, we propose a two-level DDoS detection method combining information entropy and deep learning. Initially, an information entropy mechanism identifies suspicious components and ports at a coarse level. Subsequently, a fine-grained packet-based detection is performed using a convolutional neural network (CNN) to differentiate normal from suspicious traffic. The controller then executes a defense strategy to block the attack. Experimental results show that our method achieves a detection accuracy of 98.98%, demonstrating its effectiveness in detecting DDoS attacks in an SDN environment.

Algorithm	Type	Characteristics	Effectiveness (1-10)	Resource Overhead (1-10)	Implementation Complexity (1-10)
Rate Limiting	Network Layer	Limits incoming traffic to a threshold level	8	3	4
Blackholing	Network Layer	Diverts attack traffic to a black hole	7	2	3
IP Filtering	Network Layer	Blocks traffic from specific IP addresses	9	5	5
Deep Packet Inspection	Network Layer	Analyzes packet contents for suspicious patterns	9	7	8
Traffic Shaping	Network Layer	Regulates traffic flow to mitigate attacks	6	4	5
Anomaly Detection	Network Layer	Identifies abnormal traffic patterns	7	6	7
Application Firewalls	Application Layer	Filters and inspects traffic at the application level	9	6	7
Content Delivery Networks (CDNs)	Network Layer	Absorbs and filters attack traffic	9	8	6
Scrubbing Centers	Network Layer	Cleans incoming traffic before forwarding it	8	9	8
DNS Rate Limiting	Network Layer	Limits DNS query rate to mitigate reflection attacks	8	5	5

Content Neutrality Network (CNN)	Network Layer	Filters traffic based on behavior and content	8	7	7
Generic Routing Encapsulation (GRE)	Network Layer	Encapsulates and redirects traffic	7	6	6

Table 2: Comparison of various algorithms for mitigate DDoS attacks

In 2022, P. V. Shalini, V. Radha, and S. G. Sanjeevi [28], proposed a novel method for Software Defined Networking (SDN) , which separates the data plane from the control plane, enabling centralized network control and faster data transmission. However, it faces significant security challenges, particularly from Distributed Denial of Service (DDoS) attacks. A major issue with existing SDN DDoS detection models is their tendency to misidentify genuine benign flash traffic as a DDoS attack. To address this, we developed DOCUS (DDoS detection in SDN by modified CUSUM), designed to distinguish between flash traffic and actual DDoS attacks, thus reducing false positives. Emulated experiments demonstrate that DOCUS effectively detects DDoS attacks on web servers and reduces the average detection time by 83.3% compared to recent methods. Furthermore, DOCUS accurately identifies flash traffic as benign and attack traffic as malicious, efficiently mitigating attacks by blocking traffic from identified attackers.

4. **DISCUSSION:**

The critique of the cybersecurity framework brings to light several significant shortcomings. Firstly, it highlights a lack of thorough testing across various scenarios and against a wide range of potential threats. Without this comprehensive assessment, there's a risk of overlooking vulnerabilities that attackers could exploit. Additionally, the limited scalability testing means the system may not be adequately prepared to handle increased data loads or user demands, potentially leading to performance issues or security breaches under heavy usage. Furthermore, the absence of research into quantum computing implications and group learning integration represents missed opportunities to stay ahead of emerging threats and make the system more adaptable and resilient. Moreover, the usability challenges faced by individuals with cognitive limitations point to a lack of inclusivity in the design of cybersecurity measures, underscoring the importance of accessibility considerations in safeguarding digital systems. Additionally, neglecting to leverage insights from religious activities and failing to explore specialized government assistance programs means overlooking potential sources of knowledge and support in enhancing cybersecurity strategies. Finally, the oversight of regulatory impacts on cooperative behaviors and the interpretability issue in security models highlight gaps in understanding how rules and regulations shape information-sharing practices and trust in the cybersecurity ecosystem. Addressing these deficiencies is essential to strengthen cybersecurity defenses and ensure robust protection against evolving threats in an increasingly digital landscape.

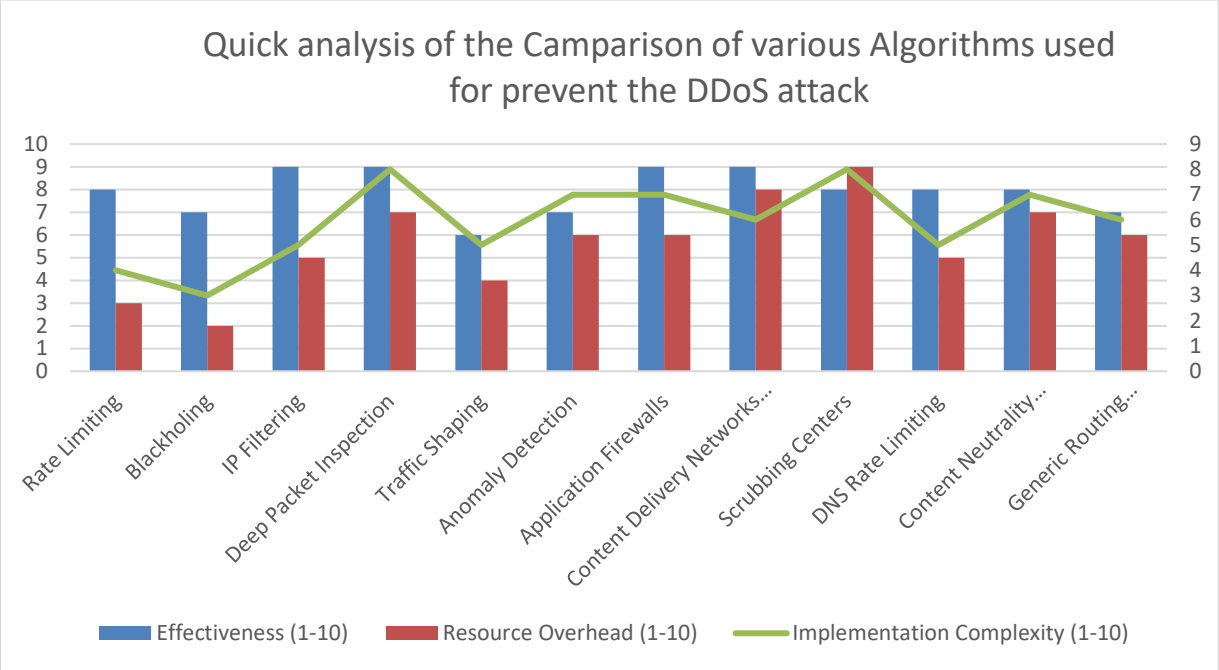

Figure 2: *Performance analysis of algorithms.*

Based on the detailed analysis of DDoS mitigation algorithms, no single method can universally address all attack scenarios effectively. Each technique has its strengths and weaknesses, necessitating a multi-layered defense strategy. For optimal protection, combining rate limiting, IP filtering, and traffic shaping for initial control; deploying deep packet inspection and application firewalls for in-depth analysis; and utilizing content delivery networks and scrubbing centers for high-volume attack absorption is recommended. This layered approach enhances resilience against various attack types, ensuring continuous and reliable service.

5. CONCLUSION AND FUTURE WORK:

The comparison of DDoS mitigation algorithms demonstrates that no single solution can effectively counter all types of DDoS attacks. Each technique, whether it be rate limiting, IP filtering, deep packet inspection, or content delivery networks, has its unique strengths and weaknesses. Therefore, a multi-layered defense strategy is essential. By combining various methods, organizations can better manage initial traffic surges, perform in-depth packet analysis, and absorb high-volume attacks. This comprehensive approach enhances the resilience of network services, ensuring continuous and reliable operations even under DDoS attack conditions. Future work in DDoS mitigation should focus on the integration of advanced technologies and collaborative efforts. Enhancing machine learning techniques for real-time anomaly detection and predictive analysis will be crucial. Additionally, AI-driven adaptive security mechanisms can dynamically adjust defense strategies in response to evolving threats. Collaboration between organizations to share threat intelligence and coordinated defenses will strengthen individual and collective security postures. Exploring blockchain for secure and transparent mitigation, optimizing resource usage, and developing quantum-resistant algorithms are also key areas. Comprehensive testing frameworks that simulate diverse DDoS scenarios will further refine and improve mitigation strategies, leading to more robust and efficient defenses against sophisticated DDoS attacks.

6. REFERENCES:

[1]. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, “Statistical approaches to DDoS attack detection and response,” *IEEE Xplore*, Apr. 01, 2003. https://ieeexplore.ieee.org/abstract/document/1194894

[2]. Seemma, P.S., Nandhini, S. and Sowmiya, M., 2018. Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), pp.125-128.

[3]. Goutam, R.K., 2015. Importance of cyber security. International Journal of Computer Applications, 111(7).
[4]. Pande, J., 2017. Introduction to cyber security. Technology, 7(1), pp.11-26.
[5]. Ustundag, A., Cevikcan, E., Ervural, B.C. and Ervural, B., 2018. Overview of cyber security in the industry 4.0 era. Industry 4.0: managing the digital transformation, pp.267-284.
[6]. Walters, R. and Novak, M., 2021. Cyber security. In Cyber security, artificial intelligence, data protection & the law (pp. 21-37). Singapore: Springer Singapore.
[7]. Sarker, I.H., 2021. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2(3), p.154.
[8]. Ferrag, M.A., Maglaras, L., Moschoyiannis, S. and Janicke, H., 2020. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, p.102419.
[9]. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A. and Marchetti, M., 2018, May. On the effectiveness of machine and deep learning for cyber security. In 2018 10th international conference on cyber Conflict (CyCon) (pp. 371-390). IEEE.
[10].Alazab, M. and Tang, M. eds., 2019. Deep learning applications for cyber security. Springer.
[11].Roopak, M., Tian, G.Y. and Chambers, J., 2019, January. Deep learning models for cyber security in IoT networks. In 2019 IEEE 9th annual computing and communication workshop and conference (CCWC) (pp. 0452-0457). IEEE.
[12].Alsirhani, A., Alshahrani, M.M., Hassan, A.M., Taloba, A.I., Abd El-Aziz, R.M. and Samak, A.H., 2023. Implementation of African vulture optimization algorithm based on deep learning for cybersecurity intrusion detection. Alexandria Engineering Journal, 79, pp.105-115.
[13].Kumar, P., Kumar, R., Aljuhani, A., Javeed, D., Jolfaei, A. and Islam, A.N., 2023. Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity. Solar Energy, 263, p.111921.
[14].Suryotrisongko, H. and Musashi, Y., 2022. Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection. Procedia Computer Science, 197, pp.223-229.
[15].Abdiyeva-Aliyeva, G., Aliyev, J. and Sadigov, U., 2022. Application of classification algorithms of Machine learning in cybersecurity. Procedia Computer Science, 215, pp.909-919.
[16].Kävrestad, J., Rambusch, J. and Nohlberg, M., 2023. Design principles for cognitively accessible cybersecurity training. Computers & Security, p.103630.
[17].Renaud, K. and Dupuis, M., 2023. Cybersecurity insights gleaned from world religions. Computers & Security, p.103326.
[18].Rawindaran, N., Jayal, A., Prakash, E. and Hewage, C., 2023. Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. International Journal of Information Management Data Insights, 3(2), p.100191.
[19].Bozorgchenani, A., Zarakovitis, C.C., Chien, S.F., Ting, T.O., Ni, Q. and Mallouli, W., 2023. Novel modeling and optimization for joint Cybersecurity-vs-QoS Intrusion Detection Mechanisms in 5G networks. Computer Networks, 237, p.110051.
[20].Chang, K. and Huang, H., 2023. Exploring the management of multi-sectoral cybersecurity information-sharing networks. Government Information Quarterly, 40(4), p.101870.
[21].Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. and Wang, C., 2018. Machine learning and deep learning methods for cybersecurity. Ieee access, 6, pp.35365-35381.
[22] J. Wang, L. Wang, and R. Wang, “A Method of DDoS Attack Detection and Mitigation for the Comprehensive Coordinated Protection of SDN Controllers,” *Entropy (Basel, Switzerland)*, vol. 25, no. 8, p. 1210, Aug. 2023, doi: https://doi.org/10.3390/e25081210.
[23] S. Kiranyaz, “1D convolutional neural networks and applications: A survey,” *Mechanical Systems and Signal Processing*, vol. 151, p. 107398, Apr. 2021, doi: https://doi.org/10.1016/j.ymssp.2020.107398.
[24] M. V. O. Assis, L. F. Carvalho, J. Lloret, and M. L. Proença, “A GRU deep learning system against attacks in software defined networks,” *Journal of Network and Computer Applications*, vol.

177, p. 102942, Mar. 2021, doi: https://doi.org/10.1016/j.jnca.2020.102942.
[25] M. S. ElSayed, N.-A. Le-Khac, M. A. Albahar, and A. Jurcut, "A novel hybrid model for intrusion detection systems in SDNs based on CNN and a new regularization technique," *Journal of Network and Computer Applications*, vol. 191, p. 103160, Oct. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103160.
[26] F. Laghrissi, S. Douzi, K. Douzi, and B. Hssina, "IDS-attention: an efficient algorithm for intrusion detection systems using attention mechanism," *Journal of Big Data*, vol. 8, no. 1, Nov. 2021, doi: https://doi.org/10.1186/s40537-021-00544-5.
[27] Y. Liu, T. Zhi, M. Shen, L. Wang, Y. Li, and M. Wan, "Software-defined DDoS detection with information entropy analysis and optimized deep learning," *Future Generation Computer Systems*, Nov. 2021, doi: https://doi.org/10.1016/j.future.2021.11.009.
[28] P. V. Shalini, V. Radha, and S. G. Sanjeevi, "DOCUS-DDoS detection in SDN using modified CUSUM with flash traffic discrimination and mitigation," *Computer Networks*, vol. 217, p. 109361, Nov. 2022, doi: https://doi.org/10.1016/j.comnet.2022.109361.