International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 14, Issue 10, October 2025)

A Comprehensive Review of DDoS Cyber Security Threats and Countermeasures

Girraj Kushwah[1], Susheel Kumar Gupta[2]

[1]*M.Tech Scholar, Department of CSE, Lakshmi Narain College of Technology, Bhopal, India*
[2]*Assistant Professor, Department of CSE, Lakshmi Narain College of Technology, Bhopal, India*

***Abstract*— Distributed Denial of Service (DDoS) attacks have become one of the most serious threats to cyber security, causing service disruption, financial loss, and reduced system performance across various sectors. With the increasing use of cloud computing, Internet of Things (IoT), and connected networks, attackers are using more advanced techniques to launch large-scale DDoS attacks. This review provides a comprehensive study of different types of DDoS threats, their impact on modern networks, and the challenges faced in detecting and preventing them. It also highlights various countermeasures, including machine learning, deep learning, and network-based defense strategies, while discussing their strengths and limitations. The paper aims to give researchers and practitioners a clear understanding of the current landscape of DDoS attacks and possible directions for developing more effective defense mechanisms.**

Keywords—MIoT, Deep Learning, Accuracy, Security.

I. INTRODUCTION

In today's digital world, the Internet has become an essential part of our personal, professional, and social lives. From online banking and e-commerce to healthcare systems, education platforms, and smart city infrastructures, almost every sector depends on reliable and secure networks [1]. However, as dependence on the Internet continues to grow, so do the risks associate with cyber threats. One of the most serious and disruptive forms of these threats is the Distributed Denial of Service (DDoS) attack. A DDoS attack aims to make a network, service, or system unavailable to its users by overwhelming it with massive amounts of traffic or requests from multiple compromised devices. These devices are often part of a *botnet*—a network of computers or IoT devices infected with malicious software and remotely controlled by attackers [2].

DDoS attacks are highly dangerous because they can cause severe disruption without directly stealing data. Instead, they target the availability of a service, which is one of the core principles of cyber security, alongside confidentiality and integrity [3]. When successful, such attacks can bring down websites, delay critical online transactions, interrupt communication services, and cause financial and reputational damage to organizations. For example, global e-commerce platforms, banking systems, and cloud services have suffered massive losses due to large-scale DDoS incidents. The increasing reliance on cloud computing and the Internet of Things (IoT) has also provided attackers with more opportunities, as billions of connected devices can be exploited to launch powerful and complex attacks[4].

Over the years, DDoS attack strategies have evolved from simple flooding methods to highly sophisticated and multi-layered techniques. Attackers now use methods such as volumetric attacks, which consume all available bandwidth; protocol-based attacks, which exploit weaknesses in network protocols [5]; and application-layer attacks, which target specific services or applications. Modern DDoS attacks often combine multiple strategies, making them even harder to detect and mitigate. In addition, attackers frequently hide their activities using advanced evasion techniques, further complicating defense efforts[6].

To counter these threats, researchers and organizations have developed a wide range of defense mechanisms. Traditional methods include firewalls, intrusion detection systems, and rate-limiting techniques, which can block or filter malicious traffic. However, these approaches are often insufficient against large-scale or advanced DDoS attacks [7]. In response, more advanced solutions have been proposed, including machine learning and deep learning-based detection systems, which can identify abnormal traffic patterns in real time. Cloud-based defense services and Content Delivery Networks (CDNs) are also commonly used to absorb and filter traffic during an attack.

Moreover,hybrid defense strategies that combine multiple approaches have gained attention for their effectiveness in handling complex attacks [8].

Despite these efforts, several challenges remain. High-speed attacks can still bypass defenses, and distinguishing between legitimate traffic spikes and malicious requests is often difficult [9]. Additionally, the rapid growth of IoT devices and 5G networks has created new vulnerabilities that attackers can exploit. Therefore, continuous research and innovation are required to develop more intelligent, adaptive, and scalable solutions [10].

This review paper aims to provide a comprehensive understanding of DDoS cyber security threats and countermeasures. It explores the different types of DDoS attacks, their impact on critical infrastructures, and the limitations of existing defense mechanisms. It also highlights the role of emerging technologies, such as artificial intelligence and blockchain, in designing stronger and more effective solutions. By presenting an overview of current trends, challenges, and future directions, this paper seeks to assist researchers, practitioners, and organizations in developing better strategies to protect against DDoS threats.

II. LITERATURE SURVEY

S. E. Vadakkethil et al., [1] proposed an Improved Whale Optimization Algorithm (IWOA) integrated with an Optimized Long Short-Term Memory (OLSTM) network for DDoS detection in IoT environments. The IWOA method was used for feature optimization, while OLSTM improved classification performance. Their approach effectively reduced false alarm rates and improved detection accuracy compared to traditional machine learning methods. This hybrid framework demonstrated high scalability and robustness, making it suitable for real-time cyber defense applications.

S. E. Vadakkethil Somanathan Pillai et al., [2] discussed integrating network security into Software Defined Networking (SDN) architectures. They highlighted the benefits of central control and programmability in SDN while addressing the risks posed by DDoS attacks on controllers. The study emphasized the importance of embedding security functions directly into SDN to monitor traffic flow and mitigate threats effectively. Their proposed design showed that SDN can become more resilient when combined with proactive detection and response mechanisms.

Ogini et al., [3] developed a DDoS detection and prevention model for IoT-based computing environments using an ensemble machine learning approach. The study used multiple classifiers to enhance accuracy and reliability in detecting malicious traffic patterns. Results showed significant improvement in precision and recall compared to individual classifiers. The ensemble strategy also proved effective in handling the heterogeneity of IoT traffic and reduced misclassification of normal requests.

Ramzan et al., [4] presented a deep learning-based detection system for identifying DDoS attacks in network traffic. Their model analyzed packet-level features and utilized neural networks to distinguish between legitimate and malicious flows. The experimental evaluation demonstrated high accuracy and low false-positive rates. Moreover, the system was adaptable to dynamic network conditions, showing strong potential for deployment in large-scale infrastructures.

Al Saleh et al., [5] introduced a Bayesian-based CNN framework enhanced with data fusion techniques for cloud DDoS detection. Their approach combined multiple feature sets to improve detection robustness and generalization. The Bayesian component helped in handling uncertainty in decision-making, while CNN captured spatial dependencies in network traffic. Results indicated superior performance compared to conventional CNN models, especially in cloud-based environments with complex attack patterns.

Alduailij et al., [6] proposed a machine learning-based detection method using mutual information and random forest feature importance to select the most relevant attributes for DDoS detection. Their study highlighted that feature selection significantly enhances model efficiency by reducing redundant and irrelevant data. The random forest classifier achieved high accuracy with lower computational cost. This approach provided a balanced trade-off between detection performance and processing speed, making it suitable for real-time security applications.

S. E. Vadakkethil Somanathan Pillai et al., [7] explored SDN-based network security measures to mitigate DDoS attacks. Their research emphasized the centralized control capabilities of SDN, enabling efficient traffic monitoring and real-time attack response. By integrating anomaly detection mechanisms into the SDN controller, the system could identify abnormal flows and apply dynamic mitigation strategies. The approach demonstrated scalability and improved resilience of networks against volumetric DDoS attacks.

Sharifian et al., [8] proposed Sin-Cos-bIAVOA, a novel feature selection method based on an improved African Vulture Optimization Algorithm (AVOA) and a new transfer function for DDoS detection. This evolutionary-inspired technique enhanced the selection of optimal features, reducing redundancy in network datasets. Their

experiments showed that the method achieved better classification accuracy and reduced computational cost compared to traditional approaches. The proposed algorithm proved effective in handling high-dimensional traffic data.

Zhao et al., [9] developed a CNN-AttBiLSTM mechanism for detecting DDoS attacks, which combined convolutional neural networks with attention-based BiLSTM. The CNN extracted spatial features, while BiLSTM captured temporal dependencies in traffic flows. The attention mechanism further improved the model's ability to focus on critical features. Evaluation results showed that the hybrid model outperformed conventional deep learning techniques in both detection accuracy and adaptability to evolving attack patterns.

Ahmim et al., [10] introduced a hybrid deep learning model for DDoS detection in IoT environments. Their framework integrated CNN and LSTM architectures to analyze complex traffic data efficiently. The hybrid approach achieved high precision and recall, even in heterogeneous IoT network conditions. Experimental results highlighted the system's ability to minimize false alarms while maintaining fast detection performance, making it highly suitable for real-world IoT deployments.

Sokkalingam et al., [11] designed an intelligent intrusion detection system for DDoS attacks using a support vector machine (SVM) enhanced with a hybrid optimization algorithm. The optimization technique was used to fine-tune SVM parameters for improved classification performance. Their results indicated significant improvements in detection accuracy compared to conventional SVM models. The study also showed that the hybrid approach provided better generalization across diverse datasets, enhancing the robustness of intrusion detection systems.

Bakro et al., [12] proposed a cloud-based intrusion detection system (Cloud-IDS) utilizing hybrid bio-inspired feature selection algorithms in combination with a random forest model. The bio-inspired optimization helped identify the most relevant features for detecting malicious activity. The random forest classifier further enhanced detection accuracy and reduced computational complexity. Their experimental evaluation revealed that the hybrid Cloud-IDS outperformed traditional detection methods, providing a scalable and effective defense for cloud environments.

Table 1: Summary of literature review

Sr. No.	Author Name & year	Work	Outcome
1	S. E. Vadakkethil et al. 2024	Improved Whale Optimization Algorithm and Optimized LSTM for DDoS Cyber Security Threat	Proposed improved whale optimization + LSTM model, enhancing accuracy in DDoS threat detection.
2	Somanathan Pillai et al. 2024	Integrating Network Security into Software Defined Networking (SDN) Architectures	Presented integration of security mechanisms into SDN for improved resilience against network attacks.
3	Ogini, N.O. et al. 2022	Distributed Denial of Service Attack Detection and Prevention Model for IoT-Based Computing Environment Using Ensemble ML Approach	Developed ensemble ML model improving IoT DDoS detection and prevention efficiency.
4	Ramzan, M. et al. 2023	Distributed denial of service attack detection in network traffic using deep learning algorithm	Utilized deep learning on network traffic to achieve high accuracy in DDoS detection.
5	Al Saleh, I. et al. 2024	Novel ML Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements	Proposed Bayesian-CNN with data fusion, improving detection of DDoS in cloud

			systems.
6	Alduailij, M. et al. 2022	ML-Based DDoS Attack Detection using Mutual Information and Random Forest Feature Importance Method	Combined feature selection with random forest for robust DDoS detection.
7	S. E. Vadakkethil et al. 2024	Mitigating DDoS Attacks using SDN-based Network Security Measures	Suggested SDN-based mitigation techniques, improving network adaptability and security.
8	Sharifian, Z. et al. 2023	Sin-Cos-bIAVOA: Improved African Vulture Optimization for Feature Selection in DDoS Detection	Introduced novel feature selection method, enhancing DDoS detection performance.
9	Zhao, J. et al. 2023	CNN-AttBiLSTM Mechanism: DDoS Detection Using Attention + CNN-BiLSTM	Designed hybrid CNN-AttBiLSTM mechanism, achieving strong detection accuracy.
10	Ahmim, A. et al. 2023	DDoS Detection for IoT using Hybrid Deep Learning Model	Built hybrid DL framework, enhancing IoT-based DDoS attack detection reliability.
11	Sokkalingam, S. et al. 2022	Intelligent IDS for DDoS: SVM with Hybrid Optimization Algorithm	Proposed hybrid SVM-optimization IDS, achieving higher detection precision.
12	Bakro, M. et al. 2024	Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection + Random Forest Model	Developed hybrid cloud IDS with feature selection + RF, improving cloud security performance.

III. CHALLENGES

1. Detection Complexity

One of the major challenges in combating DDoS attacks is the difficulty of detecting them in real-time. DDoS traffic often mimics legitimate user traffic, making it hard to differentiate between normal surges in activity and malicious flooding. Attackers also use distributed sources, botnets, and spoofed IP addresses, which further complicates accurate detection.

2. Scalability Issues

Modern networks, cloud platforms, and IoT ecosystems generate massive amounts of traffic. Existing defense mechanisms often fail to scale effectively under sudden, large-scale DDoS attacks. As attackers launch high-bandwidth and volumetric attacks, many organizations struggle to maintain the availability of services while deploying mitigation strategies.

3. Evolving Attack Techniques

DDoS attacks are constantly evolving. Beyond traditional volumetric attacks, attackers now employ application-layer attacks, multi-vector attacks, and even AI-driven adaptive strategies. This evolution makes static defense mechanisms ineffective and requires continuous innovation in security systems.

4. Resource Constraints

Mitigation of large-scale DDoS attacks demands significant computational resources, high-performance hardware, and robust bandwidth. Small and medium-sized organizations often lack the financial and technical capacity to deploy advanced anti-DDoS solutions, leaving them more vulnerable to prolonged service disruptions.

5. Latency and Performance Trade-Offs

Deploying advanced filtering, traffic scrubbing, or anomaly detection systems can sometimes lead to increased latency, affecting user experience. Striking a balance between security and system performance is a persistent challenge for organizations.

6. IoT and Botnet Proliferation

The rapid expansion of IoT devices, many of which are poorly secured, has significantly increased the attack surface. Compromised IoT devices are commonly used to build massive botnets, such as Mirai, which can launch devastating DDoS attacks. Ensuring IoT security is thus an essential yet highly challenging aspect of defense.

IV. VARIOUS TECHNIQUES

1. Signature-Based Detection

Signature-based methods identify DDoS attacks by comparing incoming traffic patterns with known attack signatures. This approach is fast and effective for detecting previously identified threats, but it struggles against zero-day or evolving attack techniques. Signature-based intrusion detection systems (IDS) are widely used in traditional network security environments.

2. Anomaly-Based Detection

Anomaly-based detection focuses on identifying unusual network behavior by creating a baseline of normal traffic patterns. Any deviation from this baseline, such as sudden traffic spikes or irregular packet flows, is flagged as a potential DDoS attack. This method is highly effective for detecting new and unknown threats but may generate false alarms if the baseline is not properly defined.

3. Machine Learning-Based Techniques

Machine learning (ML) algorithms are increasingly applied to DDoS detection due to their ability to analyze large datasets and classify traffic intelligently. Algorithms such as Support Vector Machines (SVM), Random Forests, and K-Nearest Neighbor (KNN) can differentiate between legitimate and malicious requests. ML-based models improve detection accuracy and adaptability but require high-quality datasets and significant computational resources.

4. Deep Learning Approaches

Deep learning methods, particularly Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) models, provide advanced solutions for detecting complex and evolving DDoS attacks. CNNs can capture spatial features of traffic data, while LSTMs are effective in analyzing sequential traffic patterns. These models improve accuracy in detecting sophisticated and distributed attacks but may suffer from high training time and computational costs.

5. Hybrid Detection Systems

Hybrid approaches combine multiple detection methods, such as integrating signature-based and anomaly-based techniques or blending ML with statistical analysis. These systems offer higher accuracy, lower false-positive rates, and improved adaptability against diverse DDoS attacks. However, they may require complex implementation and integration with existing security frameworks.

6. Traffic Filtering and Rate Limiting

Traffic filtering techniques block or limit suspicious traffic before it reaches critical systems. Rate limiting controls the number of requests allowed within a specific timeframe to prevent flooding. While these methods are straightforward and effective in mitigating attacks, they may also impact legitimate users during high-traffic periods.

7. Cloud-Based Mitigation Solutions

Cloud-based DDoS protection services, such as Content Delivery Networks (CDNs) and traffic scrubbing centers, provide scalable and reliable defenses. They reroute traffic through filtering mechanisms, allowing only legitimate traffic to reach the target server. These solutions are effective for large-scale attacks but may be costly for small and medium organizations.

8. Blockchain-Based Security Frameworks

Emerging blockchain technology offers decentralized methods for mitigating DDoS threats. By distributing verification and authentication processes across multiple nodes, blockchain reduces single points of failure and prevents malicious actors from overwhelming centralized systems. However, blockchain adoption for DDoS protection is still in early research and development stages.

V. CONCLUSION

Distributed Denial-of-Service (DDoS) attacks continue to be one of the most dangerous and persistent cyber threats, posing significant risks to businesses, governments, and individuals. Despite advancements in detection and mitigation, attackers are constantly evolving their methods, making defense strategies increasingly complex. A combination of traditional security mechanisms, such as firewalls and intrusion detection systems, with advanced approaches like machine learning, deep learning, and cloud-based defense models has shown promising results. However, no single solution is completely effective, highlighting the need for a layered, adaptive, and collaborative defense framework. Continuous research, real-time monitoring, and global cooperation are essential to build resilient systems that can withstand the growing scale and sophistication of DDoS threats while ensuring the security and stability of digital infrastructures.

REFERENCES

1. S. E. Vadakkethil, K. Polimetla, S. Velpula, P. Kumar Pareek and D. Sontakke, "Improved Whale Optimization Algorithm and Optimized Long Short-Term Memory for DDoS Cyber Security Threat," *2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, Ballari, India, 2024, pp. 01-05, doi: 10.1109/ICDCECE60827.2024.10549448.

2. Somanathan Pillai, S. E. Vadakkethil and K. Polimetla, “Integrating Network Security into Software Defined Networking (SDN) Architectures,” 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2024, pp. 1–6, doi: 10.1109/ICICACS60521.2024.10498703.

3. Ogini, N.O., Adigwe, W. and Ogwara, N.O., 2022. Distributed Denial Of Service Attack Detection And Prevention Model For Iot-Based Computing Environment Using Ensemble Machine Learning Approach.

4. Ramzan, M., Shoaib, M., Altaf, A., Arshad, S., Iqbal, F., Castilla, A.K. and Ashraf, I., 2023. Distributed denial of service attack detection in network traffic using deep learning algorithm. Sensors, 23 (20), p. 8642.

5. Al Saleh, I., Al-Samawi, A. and Nissirat, L., 2024. Novel Machine Learning Approach for DDoS Cloud Detection: Bayesian-Based CNN and Data Fusion Enhancements. Sensors, 24 (5), p. 1418.

6. Alduailij, M., Khan, Q.W., Tahir, M., Sardaraz, M., Alduailij, M. and Malik, F., 2022. Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method. Symmetry, 14 (6), p. 1095.

7. S. E. Vadakkethil Somanathan Pillai and K. Polimetla, “Mitigating DDoS Attacks using SDN-based Network Security Measures,” 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2024, pp. 1–7, doi: 10.1109/ICICACS60521.2024.10498932.

8. Sharifian, Z., Barekatain, B., Quintana, A.A., Beheshti, Z. and Safi-Esfahani, F., 2023. Sin-Cos-bIAVOA: A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection. Expert Systems with Applications, 228, p. 120404.

9. Zhao, J., Liu, Y., Zhang, Q. and Zheng, X., 2023. CNN-AttBiLSTM Mechanism: A DDoS Attack Detection Method Based on Attention Mechanism and CNN-BiLSTM. IEEE Access, 11, pp. 136308–136317.

10. Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S. and Dhaou, I.B., 2023. Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model. IEEE Access, 11, pp. 119862–119875.

11. Sokkalingam, S. and Ramakrishnan, R., 2022. An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach. Concurrency and Computation: Practice and Experience, 34 (27), p. e7334.

12. Bakro, M., Kumar, R.R., Husain, M., Ashraf, Z., Ali, A., Yaqoob, S.L, Ahmed, M.N. and Parveen, N., 2024. Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model. IEEE Access.