How existing machine learning models for DDoS detection differ in performance and accuracy when applied to synthetic versus real-world network traffic datasets

Abdulqudos Yahya Alnahari[1] and Noor Azurati Ahmad[1]

[1]*Faculty of Artificial Intelligence, University Technology Malaysia, Kuala Lumpur, Malaysia*
abqudos@gmail.com, azurati@utm.my

Article history

Received:
25 November 2025

Received in revised form:
27 November 2025

Accepted:
2 December 2025

Published online:
26 December 2025

*Corresponding author
azurati@utm.my

Abstract

Machine learning–based DDoS detection systems frequently report exceptionally high performance, often exceeding 98–99% accuracy. However, such results are predominantly derived from synthetic, laboratory-generated datasets that fail to capture the complexity, variability, and noise of real operational environments. This phenomenon is not unique to cybersecurity; similar patterns have been observed in applied health technologies such as remote blood pressure monitoring, where machine learning models trained on controlled clinical datasets often demonstrate inflated performance but struggle to generalize to real-world home monitoring conditions. This paper empirically demonstrates how multiple machine learning models achieve near-perfect performance when evaluated on controlled, laboratory-created DDoS datasets. Using two widely adopted benchmark datasets, the evaluated models achieved accuracies close to 99%. However, when the same learning methods were applied to a real-world dataset constructed from 28 months of unsolicited network traffic, model accuracy declined to approximately 92%.

Keywords: *DDoS, Cloud, Security, Real-World Dataset, Synthetic Dataset*

1. Introduction

The rapid evolution of cloud computing and the Internet of Things (IoT) has brought transformative benefits across industries, enabling highly scalable services and pervasive device interconnectivity [1][2]. However, this expansion has also increased the attack surface exposed to cyber threats, particularly Distributed Denial of Service (DDoS) attacks, which aim to exhaust network or computational resources and render services unavailable [3]. *Figure.1* shows the increase in the number of attacks each year.

* *Corresponding author. azurati@utm.my*

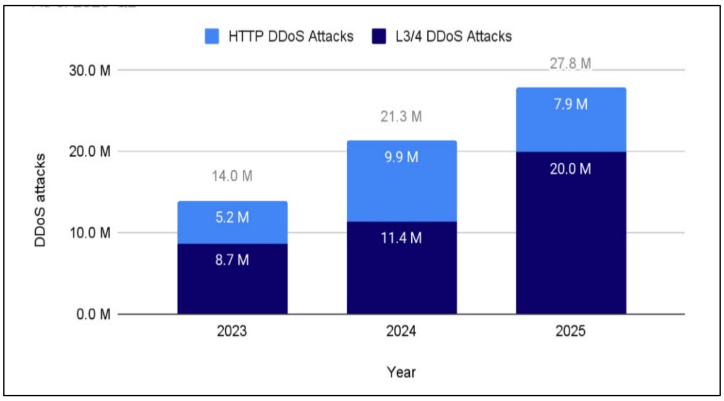

Figure.1. Annual Report for DDoS Attack (source: cloudflare.com)

The growing use of multi-vector DDoS strategies, including low-rate stealthy attacks and protocol-specific floods, has rendered traditional defense mechanisms such as firewalls and signature-based intrusion detection systems largely ineffective [4]. To address these limitations, researchers have proposed numerous machine learning (ML) and deep learning (DL) approaches, which leverage traffic features, flow behavior, and statistical patterns to distinguish legitimate from malicious activity [5][6]. These models have shown promise in simulated environments, particularly when evaluated using benchmark datasets such as CIC-DDoS2019, NSL-KDD, and CICIoT2023 [7][8].

However, a persistent gap in the literature is the lack of validation of these models against real-world, unstructured traffic. Benchmark datasets are typically generated in controlled settings with clearly labeled attack vectors and idealized conditions. While useful for algorithm training and comparison, such datasets do not reflect the ambiguity, noise, and irregularity of traffic seen in operational networks, especially in cloud-hosted services and IoT deployments, where background scanning, botnet reconnaissance, and unsolicited probes are common.

This research addresses that gap by shifting the focus from designing new detection models to assessing the generalizability of existing ones. The study is based on a large-scale, real-world dataset collected over 28 months from a private server with no public-facing services. Despite being unadvertised, the server received a significant volume of unsolicited traffic during daily 12-hour monitoring sessions, suggesting persistent automated scanning or targeting.

The growing reliance on cloud computing and IoT systems has significantly increased the impact of Distributed Denial of Service (DDoS) attacks, which disrupt services by overwhelming target systems with malicious traffic. In cloud environments, DDoS attacks may trigger uncontrolled resource scaling, incur financial losses, and violate SLAs. In IoT ecosystems, insecure and resource-constrained devices are easily compromised to form large-scale botnets that launch persistent, distributed attacks [1][2]. While DDoS attacks are often discussed in the context of cloud computing, they are not exclusive to it and may also target other systems, such as indoor positioning systems [9], which is important to have continuous availability of location-based services that support safety, operational efficiency, and timely decision-making in indoor environments.

To mitigate such threats, many researchers have proposed machine learning (ML) and deep learning (DL) models trained on benchmark datasets like CIC-DDoS2019, NSL-KDD, or CICIoT2023 [10][11]. These datasets are created in controlled environments with clean labels and known attack types. However, models trained in such settings may fail to perform adequately in real-world cloud or IoT deployments, where traffic is noisy, unlabeled, and unpredictable [4][12].

2. DDoS Taxonomy:

Distributed Denial of Service (DDoS) attacks can be classified into various categories based on the attack vector, protocol layer, and techniques used. These classifications are critical for developing appropriate detection and mitigation strategies, particularly in cloud and IoT ecosystems where service continuity is essential.

A commonly accepted taxonomy breaks DDoS attacks into three major categories: volumetric attacks, protocol attacks, and application-layer attacks [13].

a. Volumetric attacks: These are the most traditional and aim to exhaust the bandwidth of a network or server by overwhelming it with massive volumes of traffic. Examples include UDP floods, ICMP floods, and DNS amplification. These attacks often originate from large botnets and are easy to detect but difficult to mitigate due to their scale [14].

b. Protocol attacks (Layer 3/4): Such as SYN floods, ACK floods, and Smurf attacks, target vulnerabilities in the TCP/IP stack. Rather than focusing on raw bandwidth, these attacks aim to exhaust server resources like connection tables and firewall processing capacity [15].

c. Application-layer attacks (Layer 7): These are stealthier and more difficult to detect, as they mimic legitimate user behavior. Attacks like HTTP GET floods, Slowloris, or RUDY (R-U-Dead-Yet) exploit application logic by sending requests at low rates or maintaining open connections for extended periods [16].

Modern DDoS campaigns often involve multi-vector strategies, combining attacks from different layers to evade detection and maximize disruption. In IoT environments, attackers frequently use low-volume flows from large botnets, making volumetric and protocol-layer patterns harder to distinguish from normal behavior [17].

Additionally, researchers have identified new categories such as low-rate (slow) DDoS attacks, which are designed to remain under the radar of volume-based detection systems. These subtle threats are particularly effective in cloud and edge networks due to their ability to trigger auto-scaling, leading to resource exhaustion or economic denial of sustainability (EDoS) [16].

A recent survey by [12] proposed a plane-wise taxonomy, categorizing DDoS attacks along traffic generation, network penetration, and target interaction, highlighting the layered complexity of modern threats. This multidimensional classification reflects the evolving sophistication of DDoS strategies and underscores the need for adaptive and intelligent detection mechanisms, particularly in cloud-integrated IoT infrastructures [18].

3. Machin Learning and DDoS

Recent research on DDoS detection has increasingly relied on machine learning and deep learning models evaluated on synthetic or simulated network traffic. While these studies report exceptionally high accuracy—often above 97% or even 99%—their results raise concerns about the reliability and generalizability of such models. Much of the existing literature uses datasets generated in controlled environments, traffic simulators, or small-scale testbeds, which lack the variability, noise, and complexity characteristic of real-world networks. As a result, the reported performance metrics may not reflect actual deployment conditions.

To contextualize this issue, this section reviews key studies that evaluate DDoS detection approaches on synthetic datasets. *Table.1* summarizes representative studies whose unusually high-performance metrics illustrate the limitations of current evaluation practices.

Table 1. Related Work Performance

Study	Machine Learning Algorithm	Accuracy (%)	F1-Score (%)
Deepthi et al. [19]	Multilayer Perceptron	99.30	98.04–99.30
Santos-Neto et al. [20]	ML-Entropy	>99	Not Mentioned
Alkadiri and Ilyas [21]	XGBoost	No mention found	99 (median)
Belachew et al [22]	XGBoost	>99.997	>99.997
D'hooge et al.[23]	Tree-based, SVM, Logistic Regression	100 (DoS, synthetic)	89 (F1, DoS)
Rahman et al. [24]	Generative Adversarial Network (BoT-IoT)	100	100
Borah et al.[25]	Random Forest	99.58	99.55
Borah et al.[25]	K-Nearest Neighbors	99.44	99.4
Manaa et al. [26]	Random Forest (UNSW-NB15)	100	Not Mentioned
Saka et al. [27]	Random Forest (CTGAN)	98	Not Mentioned
Rashid et al.[28]	Stacked Hybrid Random Decision Gradient	99.98 (CICIDS2017)	Not Mentioned
Setitra et al.[29]	Optimized MLP-CNN (CICDDoS-2019)	99.95	Not Mentioned
Hou et al. [30]	Random Forest	>99	Not Mentioned

4. Benchmark Datasets for DDoS Detection

Benchmark datasets play a crucial role in training and evaluating machine learning models for DDoS detection. The effectiveness, reliability, and generalizability of ML models heavily depend on the quality, diversity, and realism of the datasets used. A well-constructed dataset enables accurate simulation of real-world attack scenarios, especially in cloud and IoT environments, which exhibit distinct traffic characteristics and architectural complexities.

Numerous datasets have been developed over the past two decades, ranging from traditional packet captures to structured flow-level features. However, not all are suitable for modern DDoS detection, especially when targeting IoT-cloud ecosystems.

4.1. NSL-KDD and UNSW-NB15

The NSL-KDD dataset is a refined version of the KDD'99 dataset, developed to address major issues of redundancy, imbalanced records, and biased classifiers found in its predecessor. It has long served as a benchmark for traditional ML-based intrusion detection, including DDoS classification tasks [31][32]. However, NSL-KDD reflects network traffic and attack patterns from the late 1990s, which makes it ill-suited for evaluating modern DDoS attacks. It lacks support for IoT protocols, IPv6 traffic, and cloud-native service behaviors, and it does not capture multi-vector attack trends or recent botnet behaviors [33,34].

The UNSW-NB15 dataset was developed in 2015 by the Australian Centre for Cyber Security to provide a more contemporary alternative to NSL-KDD. It includes raw pcap traffic, application logs, and 88 extracted features from real network emulation involving modern attack vectors such as DoS, exploit, Fuzzer, Generic, and Shellcode attacks [4][35]. Compared to NSL-KDD, UNSW-NB15 includes more diverse attack scenarios, modern protocol interactions, and realistic user traffic, making it more applicable to cloud-based DDoS detection models. It also offers improved support for flow-level analysis and deep packet inspection. Despite these improvements, UNSW-NB15 still has limitations for IoT-specific DDoS detection. It lacks IoT protocols like MQTT and CoAP, does not include traffic from constrained edge devices, and features are not tailored to detect low-rate or application-layer DDoS attacks prevalent in smart environments [36][37].

4.2 CIC-IDS2017 and CSE-CIC-IDS2018

The CIC-IDS2017 dataset, released by the Canadian Institute for Cybersecurity, is among the most widely used modern datasets for DDoS detection. It includes realistic network traffic with a variety of attacks such as DoS Hulk, GoldenEye, and Slowloris [34][38].

Its successor, CSE-CIC-IDS2018, introduced more refined labeling, additional attack types, and better traffic representation for cloud-based environments [17][39]. Despite these strengths, both datasets still reflect lab-controlled environments and lack traffic heterogeneity found in real-world IoT deployments.

4.3. CIC-DDoS2019

CIC-DDoS2019 is tailored specifically for DDoS detection. It simulates a wide range of DDoS attacks using Bashlite, LOIC, GoldenEye, and Xerxes, among others. The dataset includes flow-based features that enable ML and DL analysis [39][40].

However, critics point out that the attacks are generated using scripted tools in controlled lab settings, which limits their variability and may not fully represent naturally occurring botnet behavior [16].

4.4 TON_IoT and BoT-IoT

The TON_IoT and BoT-IoT datasets were designed to address the limitations of traditional datasets by incorporating IoT telemetry, device logs, and network data from smart environments [11][36].

BoT-IoT, in particular, provides a large volume of labeled attacks and reflects common IoT protocols (MQTT, CoAP). However, many attacks are simulated using fixed tools, and the dataset still lacks representation of emergent attack patterns [37].

TON_IoT attempts to bridge this gap by fusing telemetry and network data, though its lack of raw pcap traces has limited its use in fine-grained traffic reconstruction [41].

5. Dataset Limitations and Generalization Concerns

While benchmark datasets have accelerated the development of machine learning models for DDoS detection, several limitations and generalization issues persist , especially when models are transitioned from controlled lab settings to real-world cloud or IoT environments

5.1. Synthetic and Controlled Traffic

Most publicly available datasets (e.g., CIC-IDS2017, CIC-DDoS2019, BoT-IoT, TON_IoT) are generated in testbed environments using scripted attack tools like LOIC, Hping, and GoldenEye. These settings often produce uniform, high-intensity attack flows that differ significantly from real DDoS traffic, which may be low-rate, bursty, or adaptive [36][37][39].

According to the surveyed literature, recurring structural weaknesses in current DDoS detection research become apparent, with the most pervasive stemming from an over-dependence on synthetic and lab-generated datasets. These corpora, CICDDoS2019, BoT-IoT, UNSW-NB15 among others, are typically constructed under controlled network conditions with pre-scripted attacks and neatly labeled traffic classes [16][42]. While such properties facilitate reproducibility and comparative benchmarking, they gloss over the heterogeneity, volatility, and stochastic noise characteristic of real Cloud–IoT operations [43]. This gap is not trivial; it directly distorts model performance metrics. Accuracy values exceeding 99% in offline tests are often inflated by idealized separability between benign and malicious flows [44][45]. Once these models encounter unsolicited operational traffic where benign surges overlap structurally with attack features, flash crowds resembling volumetric floods or periodic IoT telemetry bursts matching rate-based anomaly signatures, false positive rates rise sharply, undermining confidence in production deployment [16].

Synthetic corpora seldom capture benign scaling transitions or concurrent tenant churn. Consequently, classification logic remains brittle under operational conditions where scale-in/scale-out cycles are routine and often decoupled across nodes, gaps that attackers can exploit during ingress point misalignment windows. Evaluation methodologies amplify optimism bias through over-reliance on aggregate accuracy without complementary precision, recall, F1-score, false positive/negative rates, or latency profiling under realistic load scenarios. This one-dimensional metric masks imbalanced per-class performance: correct classification of trivial high-volume floods pads accuracy while stealthy low-rate vectors slip undetected in live traffic mixes [16]. Latency impacts are likewise ignored; batch-mode inference under quiescent lab states hides processing backlogs that emerge when detection pipelines contend for resources alongside concurrent service workloads in production [46]. As a result, models trained on these datasets often suffer from overfitting, performing well during evaluation but failing to detect evasive or stealthy attacks in production.

5.2. Lack of Diversity in Traffic and Devices

Datasets like NSL-KDD and even newer ones like BoT-IoT often lack protocol diversity, heterogeneous devices, and geographical distribution of sources. This is problematic for IoT-cloud environments, which involve a wide variety of lightweight devices, custom firmware, and application-layer interactions [31][35]. Furthermore, most datasets do not reflect multi-cloud or edge-fog infrastructures, where traffic paths, latencies, and attack surfaces differ significantly.

5.3. Limited Attack Variants

Many datasets focus on common DDoS attacks (e.g., SYN flood, UDP flood, HTTP GET flood), but fail to include application-layer attacks, amplification-based DDoS, or botnet C2 communication, which are common in IoT-driven attacks [16][17][33]. This limited scope hinders the model's ability to generalize across attack families and detect novel or multi-stage threats.

5.4. Inconsistent or Incomplete Labeling

Accurate labeling is critical for supervised learning models. However, datasets like BoT-IoT and UNSW-NB15 have been criticized for having labeling inconsistencies, imbalanced class distributions, and lack of fine-grained temporal context [32][38]. This can skew learning outcomes, inflate performance metrics, and reduce the model's robustness in real-time deployments.

5.5. Evaluation Bias and Dataset Dependency

Many studies report high accuracy by evaluating models on the same dataset they were trained on, which introduces dataset dependency bias. These results do not necessarily reflect real-world deployment effectiveness. Cross-dataset evaluation, where models trained on one dataset are tested on another, is rarely performed, despite being crucial for understanding generalization capacity [36][38].

5.6. Scarcity of Real-world Unsolicited Data

Perhaps the most critical limitation is the lack of real-world datasets that capture unsolicited or attack-originated traffic from honeypots, unused IP spaces, or trap servers. These traffic traces are essential for understanding adversary behavior, botnet evolution, and zero-day attacks [15][40].

5.7. Relevance to Cloud Ecosystems

Most benchmark datasets and detection models were not originally designed for cloud-native architectures This introduces structural mismatches in feature space, traffic semantics, and temporal behavior. For instance, Mirai, one of the most famous DDoS attacks in the cloud, was utilizing botnets that the attacker takes control off, and these botnets mostly are IoT devices. While benchmark datasets have accelerated the development of machine learning models for DDoS detection, several limitations and generalization issues persist, especially when models are transitioned from controlled lab settings to real-world cloud environments.

6. Real-World Dataset Collection

In order to create a real-world DDoS traffic dataset, a virtual private server was deployed in the cloud with 4GB RAM, 150 GB storage, and 2 Core CPU. This server is used to collect traffic by saving PCAP files in the storage. *Table.2* shows the specifications.

Table.2. Private server Specifications

Component	Details
Compute Platform	Virtual Private Server
CPU	Inte 2 Core
RAM Allocation	4 GB
Storage	150 GB
OS / Runtime	Ubuntu 20.04 (containerized Colab

In order to overcome limitations of synthetic datasets, a novel dataset was collected over 28 months, totaling more than 900 PCAP files (approx. 32GB+). The collection setup included:

a. A private server with no expected inbound traffic, running 12 hours daily.
b. Passive sniffing using “tcpdump” to capture raw packets.
c. Multiple time windows and seasons covered to include natural traffic variations.

6.1. Data Labeling

The collected dataset is more than 13 million of records. Most of it is benign traffic and the total number of traffic that could be labeled as DDoS attack are about

45000 records. Using the whole dataset would lead to dataset imbalance even after setting the requests that has a rate of only 1 request/second to 0 and ignoring all the records that are less than 70 request/second and more than 1 request/second. The number of records became 5540000 records labeled as 0, and 45000 labeled as 1. Using a Random Forrest script, the dataset with 1045000 records with 1 million negative and 45000 positives, the model achieved a very high score which reached 100% in all evaluation metrics: accuracy, precision, recall, and F1-score.

6.2. Class Imbalance Handling

With 1 million negatives and 45,000 positives, the model is likely predicting the majority class (0) most of the time. In the case of class weighting or oversampling/undersampling, the model might be heavily biased towards the negative class. If the model's performance is too good to be true, it's often a sign that it's overfitting the majority class and ignoring the minority class. In order to avoid imbalance, the whole positive records were taken and a reasonable percentage of negative records were taken randomly.

6.3. Collected Traffic

After extracting cleaning and feature mapping the dataset of Real-World traffic it was found that the traffic volume differs from one month to another as shown on *Figure.2*.

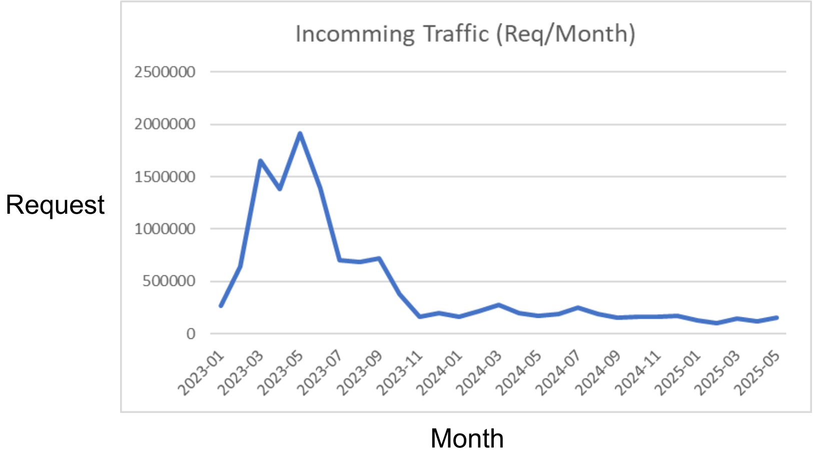

Figure.2. Incoming Traffic During 28 months

6.3. Machine Learning Model Implemented

Using the extracted dataset from real-world traffic, a machine learning method was trained to create a model and compare its results with the results of models created by using the same machine learning method trained on two of benchmark datasets, CIC-DDoS2019 and BoT-IoT. The implemented model is Random Forest (RF). It is an ensemble-based classifier that builds multiple decision trees and outputs the class with the majority vote. Known for robustness to overfitting and high accuracy in flow-based intrusion detection.

7. Results

CIC-DDoS2019 and BoT-IoT maintained perfect 99% scores across all metrics, even under extreme imbalance. This reflects the high separability of classes in these synthetic datasets. In contrast, the real-world dataset shows a decline in recall as imbalance increases. While precision remains high, recall drops to 84.8%, leading to a lower F1-score. This suggests that real-world attacks are harder to detect due to noise, variability, and less distinct attack patterns. The accuracy increases in the real-world dataset with more negatives because of class dominance, but this does not reflect true detection ability—making recall and F1-score more reliable indicators. *Table.3* below summarizes the classifier's performance across all datasets and class imbalance configurations:

Table.3. Result Summery

Dataset	Negatives	Positives	Accuracy	Precision	Recall	F1-Score
CIC-DDOS2019	88581	88581	99%	99%	99%	99%
CIC-DDOS2019	88581	177159	99%	99%	99%	99%
CIC-DDOS2019	88,581	1,000,000	99%	99%	99%	99%
BOT-IOT	9,543	9,543	99%	99%	99%	99%
BOT-IOT	9,543	38,172	99%	99%	99%	99%
BOT-IOT	9,543	109,543	99%	99%	99%	99%
Real-World	45,008	45,008	92.5%	92.6%	92.5%	92.5%
Real-World	200,000	45,008	94.9%	93.5%	89%	91%
Real-world	1,000,000	45,008	98.6%	98.4%	84.8%	90.4%

8. Conclusion

The experimental results show a significant performance drop when the same Random Forest model is applied to real-world traffic, especially in recall and F1-score, when the data becomes severely imbalanced. While CICDDoS2019 and BoT-IoT yielded consistently high metrics (near 99% across all evaluation scenarios), the real-world dataset exhibited more realistic but lower scores, particularly as the negative-to-positive sample ratio increased (e.g., 1M normal vs 45K attack). This outcome validates the importance of using real-world datasets as benchmarks to test the generalization ability of detection models. It also exposes the limitations of relying solely on lab-generated datasets which tend to overestimate model performance and ignore the true dynamics of real environments.

Acknowledgments

The authors would like to thank Universiti Teknologi Malaysia (UTM) Matching Grant Vot 05M02 and Universitas Hasanuddin Vot 1U082 for supporting the research work especially to the Faculty of Artificial Intelligence.

Conflicts of Interest

The authors would like to thank Universiti Teknologi Malaysia (UTM) Matching Grant Vot 05M02 and Universitas Hasanuddin Vot 1U082 for supporting the research work especially to the Faculty of Artificial Intelligence.

References

[1] A. A. Aborujilah et al., “Security and privacy issues in cloud computing: A survey,” *Future Generation Computer Systems*, vol. 111, pp. 659–674, 2020.

[2] M. A. Ferrag et al., “Deep learning approaches for cyber security in IoT: A review,” *Computers & Security*, vol. 92, p. 101748, 2020.

[3] S. Choudhury and J. Kumar, “A survey on DDoS attacks and defense in cloud and IoT: Challenges and solutions,” *Journal of Network and Computer Applications*, vol. 191, p. 103134, 2021.

[4] Y. Wang et al., “Detection of low-rate DDoS attacks based on network flow entropy and traffic self-similarity,” *IEEE Access*, vol. 8, pp. 177160–177173, 2020.

[5] M. H. Sqalli et al., “A review of machine learning-based techniques for DDoS detection and mitigation in cloud and IoT,” *Journal of Information Security and Applications*, vol. 55, p. 102582, 2020.

[6] R. M. Parizi et al., “Smart anomaly detection in cloud computing using supervised machine learning,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2248–2257, 2021.

[7] I. Sharafaldin et al., “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” *ICISSP*, 2021.

[8] M. R. Javed and M. A. Baig, “Benchmarking public datasets for IoT-based DDoS detection: A review,” *Computers, Materials & Continua*, vol. 66, no. 1, pp. 111–128, 2021.

[9] H. Alshami, N. A. Ahmad and S. Sahibuddin, "RSS Certainty: An Efficient Solution for RSS Variation due to Device Heterogeneity in WLAN Fingerprinting-based Indoor Positioning System," 2021 Palestinian International Conference on Information and Communication Technology (PICICT), Gaza, Palestine, State of, 2021, pp. 71-76, doi: 10.1109/PICICT53635.2021.00024

[10] H. Haddad Pajouh et al., “A survey on DDoS attacks in cloud computing: Taxonomy and mitigation techniques,” *Computer Communications*, vol. 169, pp. 107–133, 2021.

[11] H. A. Jaoudi et al., “A survey of IoT-based botnet detection using machine learning,” *Sensors*, vol. 21, no. 16, p. 5375, 2021.

[12] N. Kshetri, “Security trade-offs in the Internet of Things: A data-driven analysis of Mirai and Mozi botnets,” *IEEE IT Professional*, vol. 23, no. 2, pp. 29–35, 2021.

[13] Kalambe, S. et al. (2025). A comprehensive plane-wise review of DDoS attacks.

[14] Chahal, J. K. et al. (2024). DDoS attacks & defense mechanisms in SDN-enabled IoT networks.

[15] Afraji, D. M. A. et al. (2025). Advocating real-world unsolicited traffic analysis

[16] Ouhssini, A. et al. (2024). Lack of modern threats in synthetic datasets

[17] Mahdi, Z. et al. (2024). Attack coverage gaps in benchmark datasets

[18] Butt, H. A. et al. (2024). Enhanced DDoS Detection Using Advanced Machine Learning Techniques.

[19] Dr.S.Aruna Deepthi, Dr.T. Padmapriya, Dr.B.Senthilkumaran, and Ch Bhupati. “Mitigating DDoS Attacks: A Machine Learning Approach for Enhanced Detection and Response.” Advances in Nonlinear Variational Inequalities, 2024.

[20] Marcos J. Santos-Neto, J. Bordim, Eduardo A. P. Alchieri, and Edison Ishikawa. “DDoS Attack Detection in SDN: Enhancing Entropy-based Detection with Machine Learning.” Concurrency and Computation, 2024.

[21] Naam Alkadiri, and M. Ilyas. “Machine Learning-Based Architecture for DDoS Detection in VANETs System.” 2022 International Conference on Artificial Intelligence of Things (ICAIoT), 2022.

[22] Habtamu Molla Belachew, Mulatu Yirga Beyene, Abinet Bizuayehu Desta, Behaylu Tadele Alemu, Salahadin Seid Musa, and Behaylu Tadele Alemu. “Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning.” IEEE Access, 2025.

[23] Laurens D’hooge, Miel Verkerken, T. Wauters, F. de Turck, and B. Volckaert. “Investigating Generalized Performance of Data-Constrained Supervised Machine Learning Models on Novel, Related Samples in Intrusion Detection.” Italian National Conference on Sensors, 2023.

[24] Saifur Rahman, Shantanu Pal, Shubhanshi Mittal, Tisha Chawla, and C. Karmakar. “SYN-GAN: A Robust Intrusion Detection System Using GAN-Based Synthetic Data for IoT Security.” Internet of Things, 2024.

[25] Rituparna Borah, Satyajit Sarmah, Nitin Choudhury, Hriman Mahanta, and Anjan Chodhury. “DDoS Attack Detection Using Machine Learning Techniques.” Indian Journal of Science and Technology, 2023

[26] M. Manaa, Saba M. Hussain, Suad A. Alasadi, and Hussein A. A. Al-Khamees. “DDoS Attacks Detection Based on Machine Learning Algorithms in IoT Environments.” Inteligencia Artif., 2024

[27] Samed Saka, Ali Al-Ataby, and Valerio Selis. “Generating Synthetic Tabular Data for DDoS Detection Using Generative Models.” International Conference on Trust, Security and Privacy in Computing and Communications, 2023

[28] Rana Muhammad Rashid, Hira Khyzer, and Xun Yijie. “Stacked HRDGL: A Fast Hybrid Model for Real-Time Network Intrusion Detection.” International Conference on Innovative Computing and Cloud Computing, 2024

[29] Mohamed Ali Setitra, Mingyu Fan, B. L. Agbley, and ZineEl Abidine Bensalem. “Optimized MLP-CNN Model to Enhance Detecting DDoS Attacks in SDN Environment.” Network, 2023

[30] Jiangpan Hou, Peipei Fu, Zigang Cao, and Anlin Xu. “Machine Learning Based DDos Detection Through NetFlow Analysis.” IEEE Military Communications Conference, 2018

[31] Batchu, R. K. & Seetha, H. (2021). Dataset imbalance and generalization issues

[32] Kaur, S. et al. (2021). Labeling inconsistencies in open datasets

[33] Apat, H. K. & Sahoo, B. (2024). Protocol-specific vulnerabilities in fog-IoT

[34] Liu, X. et al. (2021). Performance benchmarking using NSL-KDD and CIC datasets

[35] Novaes, M. P. et al. (2021). False positive impact in cloud-hosted IDS

[36] Y. Wang et al., “Layer 7 DDoS attack detection in containerized cloud environments,” IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 643–657, 2022.

[37] Mustapha, A. et al. (2023). Generalization and dataset realism in DDoS detection

[38] Fouladi, R. et al. (2022). Limitations of lab-based datasets

[39] Sakr, H. A. et al. (2024). Smart system accuracy under imbalanced attack traffic

[40] Mohammed Sharif, D. et al. (2023). Detection of application-layer DDoS attacks using ML.

[41] Muraleedharan, N. & Janet, B. (2021). Data gaps in public datasets

[42] Bankó, M. B., Dyszewski, S., Králová, M., Limpek, M. B., Papaioannou, M., Choudhary, G., & Dragoni, N. (2025). Advancements in machine learning-based intrusion detection in IoT: Research trends and challenges. Algorithms, 18, 209. https://doi.org/10.3390/a18040209

[43] Ahmad, A. N., Raffei, A. F. M., Razak, M. F. A., & Ahmad, A. (2024). Distributed denial of service attack detection in IoT networks using deep learning and feature fusion: A review. Meso Potamian Journal of Cybersecurity, 47–70. https://doi.org/10.58496/MJCS/2024/004

[44] Alsufyani, A., Alotaibi, B., & Alajmani, S. (2024). HYBRID DEEP LEARNING APPROACH FOR ENHANCED DETECTION AND MITIGATION OF DDOS ATTACK IN SDN NETWORKS. International Journal of Network Security & Its Applications (IJNSA), 16(6), 77. https://doi.org/10.5121/ijnsa.2024.16605

[45] Rajput, D. S., & Upadhyay, A. K. (2024). Enhanced network defense: Optimized multi–layer ensemble for DDoS attack detection. International Journal of Experimental Research and Review, 46, 253–272. https://doi.org/10.52756/ijerr.2024.v46.020

[46] Hernandez, D. V., Lai, Y.-K., & Ignatius, H. T. N. (2025). Real-time DDoS detection in high-speed networks: A deep learning approach with multivariate time series. Electronics, 14(13), 2673. https://doi.org/10.3390/electronics14132673