International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2025/39 Volume 12, Issue 4, July – August (2025)

SURVEY ARTICLE

# Lightweight and Intelligent DDoS Detection for IoT Networks: A Comprehensive Survey, Comparative Benchmark, and Research Roadmap

Thoyazan Sultan Algaradi
Department of Computers and Information Technology, University of Science and Technology (USTY), Sana'a, Yemen.
yaz.sul77@gmail.com

Received: 26 May 2025 / Revised: 07 August 2025 / Accepted: 17 August 2025 / Published: 30 August 2025

**Abstract – The integration of Internet of Things (IoT) technologies into critical systems has driven major advancements across industries. However, this integration has also introduced new avenues for security breaches, particularly Distributed Denial-of-Service (DDoS) attacks. These attacks are especially damaging in IoT environments due to the constrained processing power and limited defenses of many devices, which are often deployed without sufficient safeguards. This review sets out to explore and analyze the range of techniques proposed for detecting and mitigating DDoS attacks within IoT frameworks. Specifically, it organizes existing research into four primary categories: traditional detection methods, machine learning based techniques, deep learning models, and hybrid approaches that combine different strategies for enhanced performance. Using a methodology aligned with PRISMA guidelines, the study systematically filtered and reviewed 26 papers. Each paper was assessed according to its detection mechanism, dataset type, performance outcomes, and suitability for real world deployment. The findings highlight the increasing effectiveness of machine learning and deep learning methods. This is particularly evident when they are employed in hybrid configurations that improve detection rates and adaptability. Despite these advancements, several issues persist, such as the lack of standardized datasets and the challenge of deploying models on resource constrained devices. This review highlights these gaps and serves as a guide for researchers seeking to develop more practical and resilient IoT security solutions.**

**Index Terms – DDoS Attacks, IoT Security, Machine Learning, Deep Learning, Hybrid Detection Models, Lightweight Security Models.**

## 1. INTRODUCTION

The Internet of Things (IoT) has witnessed explosive growth in recent years, becoming an integral part of modern life. The number of deployed IoT devices worldwide now exceeds the global human population, with applications across smart homes, healthcare, industry, and agriculture [1]. For instance, smart sensors and devices in residential settings enhance comfort and quality of life through home automation and indoor environment monitoring. Remote sensing technologies also facilitate the surveillance of hard-to-reach areas. In the healthcare sector, IoT-enabled medical devices from wearable health monitors to remote patient monitoring systems have been instrumental in improving clinical outcomes and reducing human error in hospitals and home care [2]. Modern industries rely on IoT networks and sensors to optimize production lines and supply chains within the industry 4.0 paradigm [3]. Likewise, smart farming solutions leveraging IoT technologies are employed to monitor crops, optimize irrigation, and manage livestock more effectively. The widespread adoption of IoT across these sectors has drawn significant attention from investors, corporations, and academic researchers alike, owing to the technology's immense potential to drive efficiency and innovation in service delivery.

Despite its transformative benefits, IoT also introduces substantial security risks. The current state of cybersecurity in the IoT era has even been dubbed the "Internet of Vulnerabilities," reflecting the myriad of security loopholes arising from the rapid and often unregulated integration of devices [4]. One of the main difficulties arises from the fact that many IoT devices operate under strict resource limitations, often having minimal computational capabilities, restricted memory, and reduced energy availability. Some operating with mere kilobytes of RAM hindering their ability to support conventional cryptographic protocols and security mechanisms [5]. Additionally, many devices lack support for regular firmware updates or present significant barriers to secure patching, leaving known vulnerabilities unaddressed for extended periods. The lack of universal platform standards contributes to a fragmented ecosystem, complicating deployment of unified security solutions. Compounding the problem is the fact that most IoT devices are persistently connected to the internet and often operate without direct user supervision, making them continuously exposed to potential threats. These conditions make IoT devices highly attractive targets for attackers, who can exploit these weaknesses to

SURVEY ARTICLE

compromise and repurpose them for malicious ends. In many cases, the push by manufacturers to deliver low cost, innovative IoT products has come at the expense of robust security, resulting in widespread exposure to threats that jeopardize user privacy and the integrity of interconnected systems [6].

One of the most significant cybersecurity risks to IoT systems is the Distributed Denial of Service (DDoS) attack. This type of attack seeks to hinder the operation of a target service or network by saturating it with excessive unauthorized traffic, making it unavailable to genuine users [7]. These attacks exploit the under protected and resource limited nature of IoT devices, which can be hijacked in large numbers and incorporated into botnets. Once compromised, these devices can be orchestrated to launch massive, coordinated traffic floods against specific targets. A notable example that highlighted the seriousness of such threats was the Mirai malware outbreak in 2016. Mirai scanned the internet for vulnerable IoT devices such as IP cameras and DVRs still operating with default or weak passwords and succeeded in compromising hundreds of thousands of them. The attackers behind Mirai then used this vast network of compromised devices to initiate large scale DDoS campaigns. One of the most prominent incidents involved an attack on Dyn, a DNS service provider, which disrupted access to major websites including Twitter, Netflix, and Spotify for several hours [8]. Another high-profile target was Krebs on Security, a cybersecurity news site, which endured an attack peaking at around 623 Gbps unprecedented at the time. Some Mirai associated attacks later exceeded 1 Tbps in data throughput, underscoring the critical risk posed by the exploitation of insecure IoT devices. These events served as a wake-up call for the global technology community, revealing how IoT vulnerabilities could be weaponized to inflict widespread disruption across the internet.

Considering these issues, this research seeks to present an extensive and structured review of DDoS attacks aimed at IoT infrastructures, focusing particularly on detection and prevention methods. The analysis categorizes existing defensive approaches into several groups, such as traditional rule-oriented methods, network protocol-based solutions, machine learning (ML) approaches, deep learning (DL) models, and hybrid strategies that integrate multiple techniques. This classification outlines both the advantages and the constraints of each category. In addition, the study identifies existing research gaps in IoT security related to DDoS incidents and points out notable trends and recommendations for future investigations.

The primary objective of this review is to systematically survey and benchmark current DDoS detection approaches in IoT environments, identify their comparative strengths and weaknesses, and uncover unresolved challenges that researchers must address.

This paper contributes to the field by (1) providing a taxonomy of detection models based on learning strategies, (2) offering a comparative analysis of 26 selected studies, and (3) proposing a research roadmap outlining future directions.

Through this systematic review, a holistic perspective provided on the state of IoT security against DDoS attacks, aiming to guide researchers and practitioners in prioritizing future research efforts and in developing more robust and adaptive protection mechanisms for IoT ecosystems in the face of this escalating threat.

The remainder of this paper is organized as follows: Section 2 presents the review methodology. Section 3 outlines the theoretical background of DDoS attacks in IoT. Section 4 classifies and analyzes reviewed studies. Section 5 discusses challenges and future directions, and Section 6 concludes the paper.

## 2. METHODOLOGY

This study adopts a structured and systematic review methodology to analyze scholarly literature on Distributed Denial-of-Service (DDoS) attacks in Internet of Things (IoT) environments. The process encompasses the formulation of research questions, a detailed search strategy, strict inclusion/exclusion criteria, and a multi-phase study selection process to ensure comprehensiveness and academic rigor.

### 2.1. Research Questions

To guide the scope of the review, four key research questions were formulated:

- What techniques are currently employed to detect DDoS attacks in IoT environments?
- What prevention mechanisms are used to mitigate such attacks?
- What are the strengths and limitations of these approaches?
- What research trends and future directions are emerging in this domain?

These questions serve as the foundation for evaluating the effectiveness and evolution of defensive strategies within IoT ecosystems.

### 2.2. Search Strategy

An extensive literature search was performed across multiple academic databases, including IEEE Xplore, SpringerLink, ScienceDirect, ACM Digital Library, and Google Scholar. Search terms included combinations of keywords like "IoT", "DDoS", "attack detection", "prevention", "IoT security", and

SURVEY ARTICLE

"Botnet", utilizing logical operators (AND, OR) to refine results. This approach ensured relevant and wide-ranging coverage of literature related to DDoS defense in IoT contexts.

2.3. Inclusion and Exclusion Criteria

The following inclusion criteria were set to guarantee both the relevance and the quality of the selected studies:

- Publication date: 2015–2025.
- Language: English only.
- Topical relevance: Studies must focus specifically on DDoS in IoT.
- Peer-review status: Only peer-reviewed journals and conferences.
- Experimental validation: Preference for studies with empirical results.

Exclusion criteria included:

- Studies outside the date range or in non-English languages.
- Non-peer-reviewed sources (e.g., blogs, white papers).
- General IoT or DDoS research unrelated to IoT environments.
- Theoretical-only studies without implementation or evaluation.

These criteria ensured that only impactful, methodologically sound contributions were included.

2.4. Study Selection Process

Based on the PRISMA structured methodology guidelines, a multi-stage selection process was implemented to identify the final corpus of studies for analysis. The process unfolded as follows:

- Initial search: Preliminary queries yielded several hundred results, which were consolidated into a master list.
- Screening: Duplicates and clearly irrelevant entries (e.g., unrelated topics or non-English sources) were removed.
- Title and abstract review: Studies not explicitly focused on IoT-specific DDoS detection or prevention were excluded.
- Supplementary search: Reference lists of core studies were reviewed (snowballing) to identify additional relevant works.
- Full-text analysis: All remaining studies were read fully to confirm alignment with the research scope.
- Final classification: Studies were categorized by technique type (e.g., ML-based, rule-based, infrastructure-level) and security objective (detection vs. prevention).

This rigorous methodology resulted in the identification of a validated and representative set of literature that addresses various aspects of DDoS defense in IoT, providing a solid foundation for the analysis and synthesis presented in subsequent Sections.

## 3. THEORETICAL BACKGROUND

Distributed Denial of Service (DDoS) attacks are among the most prevalent and disruptive cyber threats, aiming to exhaust server or device resources to deny access to legitimate users [7].

In IoT environments, where resources are constrained and connectivity is constant, understanding DDoS attack types, IoT architecture, and detection challenges is vital [5][6].

3.1. Types of DDoS Attacks

DDoS attacks manifest in various forms, often distinguished by the targeted protocol layer and attack mechanism. Key types include:

- SYN Flood attacks take advantage of weaknesses in the TCP handshake sequence. In such attacks, numerous SYN packets with falsified IP addresses are sent, forcing the server to maintain incomplete connections for extended periods, which drains its connection resources [9].
- UDP Flood attacks work by transmitting a large number of UDP packets to arbitrary ports. When the targeted device tries to reply with ICMP “Destination Unreachable” notifications, it consumes processing capacity, which can ultimately cause service interruptions [10].
- ICMP Flood Attacks, also known as Smurf attacks, use spoofed broadcast addresses to send ICMP Echo requests. This leads to a reflection-based flood of ICMP replies, overwhelming the victim device, especially problematic for resource-limited IoT nodes [7].
- HTTP Flood Attacks operate at the application layer, issuing large volumes of HTTP GET or POST requests that mimic legitimate traffic. These attacks are effective at exhausting server-level resources without relying on high packet volumes [10].
- Slowloris Attacks exploit the server’s connection handling by opening numerous connections and keeping them alive through slow, partial HTTP header transmissions. This approach consumes the server's concurrent connection pool without generating high traffic volumes, making detection more difficult [11].

SURVEY ARTICLE

### 3.2. IoT Network Architecture

IoT ecosystems are composed of diverse, interconnected devices that collaboratively sense, process, and transmit data. The typical architecture follows a multi-tiered structure:

- The edge layer encompasses sensors and actuators communicating through short-range technologies (e.g., RFID, ZigBee, Wi-Fi, Bluetooth) to collect raw environmental or user data [1].
- The network layer serves as a bridge between edge devices and higher-level infrastructure. It comprises IoT gateways and routers, often supported by fog computing nodes that perform preprocessing to reduce cloud load [12].
- The application (cloud) layer is responsible for data aggregation, analysis, and storage. It supports intelligent decision-making, visualization, and remote monitoring in applications such as healthcare, smart homes, and industrial automation.

While this architecture enables scalable and flexible deployments, it significantly expands the attack surface. Persistent Internet connectivity and heterogeneous device configurations make IoT networks particularly susceptible to exploitation. Weakly secured endpoints may be hijacked and incorporated into botnets, amplifying the threat of large-scale DDoS attacks [5].

### 3.3. Challenges in Detecting Attacks within IoT Environments

Effective intrusion detection in IoT networks is hampered by several intrinsic factors:

- Resource Limitations: Many IoT devices operate with restricted computing capacity, memory, and power availability. Conventional intrusion detection systems are usually too demanding in terms of resources to run directly on these devices, making it necessary to adopt lightweight approaches that shift analytical tasks to more capable nodes [13].
- Protocol and Platform Heterogeneity: IoT deployments utilize a broad spectrum of communication protocols and operating systems (e.g., MQTT, CoAP, ZigBee, TCP/IP), creating challenges in establishing unified detection frameworks. Attackers may exploit protocol-specific vulnerabilities that bypass conventional monitoring tools [14].
- Massive Scale and Growth Dynamics: The scale of IoT networks can reach millions of nodes, posing challenges for real-time traffic monitoring and anomaly detection. The dynamic onboarding of new devices further complicates detection and tracking efforts. Scalable solutions must leverage big data analytics and distributed machine learning to process vast traffic volumes without degrading system performance [15].
- Irregular Firmware Updates: Many IoT devices lack mechanisms for timely firmware updates or remain unpatched due to vendor negligence or user inattention. These unpatched vulnerabilities persist in the network, making devices long-term targets for exploitation and botnet recruitment [5].
- Dynamic Network Topologies: IoT networks are inherently dynamic, with frequent changes in device connectivity, mobility, and traffic patterns. These fluctuations make it difficult to establish static baselines for normal behavior, increasing the likelihood of false positives or missed detections [16].
- Privacy Constraints: Many IoT applications deal with sensitive data such as health metrics or video surveillance. Centralized data collection for intrusion detection may conflict with privacy requirements. Thus, privacy-preserving methods - like local processing, secure multiparty computation, or federated learning - are essential to maintain security without violating confidentiality [4].

In summary, detecting DDoS attacks in IoT systems is a complex task due to the interplay of limited computational resources, diverse protocols, large-scale deployments, inconsistent security maintenance, dynamic behaviors, and privacy considerations. These constraints necessitate the development of lightweight, adaptive, and privacy-aware detection mechanisms tailored to the unique properties of IoT environments.

## 4. CLASSIFICATION AND ANALYSIS OF STUDY

In order to present a clear and organized review of existing work on DDoS detection in IoT environments, the selected studies have been grouped according to the fundamental techniques they employ. These groups comprise conventional detection strategies, machine learning-based approaches, deep learning methods, and hybrid systems that combine analytical models with technologies such as SDN or blockchain. Each category is examined independently, with attention given to its methodology, the datasets utilized, and the outcomes reported. This classification supports a comparative understanding of the literature and helps to uncover areas that remain underexplored.

### 4.1. Traditional DDoS Detection and Mitigation in IoT Networks

Traditional DDoS defenses for IoT lean on fixed heuristics, statistical thresholds, or rule driven traffic profiling tools that pre-date the recent surge in data-centric security. Although

SURVEY ARTICLE

lacking in adaptive intelligence, these methods remain attractive for their computational frugality and transparent operation on lightweight gateways. The Section revisits such conventional strategies, showing how careful feature selection, signature tuning, and protocol-level monitoring can still deliver credible protection in IoT networks.

Doshi et al. [17] present a robust IDS for detecting stealthy IoT-based DDoS attacks using the Online Discrepancy Test (ODIT), a non-parametric sequential anomaly detection method that requires no prior traffic distribution knowledge. It identifies persistent anomalies through kNN distances and cumulative statistics. Evaluations on the N-BaIoT dataset (real-world attacks on nine smart devices), a custom 15-device testbed, and simulations with 10 nodes monitoring 100 devices each show that ODIT outperforms deep autoencoders and information metrics, achieving 100% true positive rate with detection delays <0.2 seconds, false positives as low as 0.5–2%, and an AUC of 0.9825. ODIT handles dynamic environments, scales linearly, and enables instant identification and blocking of attacking nodes and devices, making it effective for real-time IoT defense.

Adat & Gupta [18] propose a lightweight and adaptive DDoS mitigation framework for IoT networks, operating at the border router to bypass IoT device limitations. The detection algorithm includes an analysis module filtering packets by IP, bitrate, and payload size, and a monitoring module classifying packets based on behavioral patterns to detect DoS or DDoS. Adaptive filtering uses blacklists and graylists, while extreme traffic is offloaded to a third-party EDoS server. Implemented in Contiki OS using the Cooja simulator with UDP clients and RPL-based topology, the system achieved up to 100% packet delivery at the border router and 86% at internal nodes, with fewer drops and lower complexity. Future enhancements may include lightweight authentication and dynamic defense for outbound threats.

Pandey and Mishra [19] introduce a hybrid DDoS detection model for IoT networks that combines entropy-based anomaly detection with signature-based methods, using conditional entropy to enhance accuracy. The two-stage process first calculates entropy to detect deviations from normal traffic, then applies conditional entropy to analyze relationships between features, improving anomaly detection and reducing false positives. Evaluated on datasets simulating normal and DDoS IoT traffic, the model demonstrated high detection accuracy, low false positive rates, and efficient detection time, outperforming existing methods. This hybrid framework effectively strengthens IoT network security against DDoS attacks.

Haripriya & Kulothungan [20] propose Secure-MQTT, a lightweight IDS using fuzzy logic to detect DoS attacks in MQTT-based IoT networks. It monitors features like Connection Message Ratio (CMR) and Connection Acknowledgment Message Ratio (CAMR), processed by a fuzzy inference engine with fuzzy rule interpolation to reduce computation and avoid large rule sets. Implemented in Contiki OS with COOJA, and tested on networks of 100–300 devices (10% attackers), Secure-MQTT achieved up to 91% precision, 90.9% recall, and low false positive rates (0.1–0.37), outperforming MQTT-S in accuracy and FPR. It also maintained high attack detection accuracy and stable communication, proving effective for constrained IoT environments.

Traditional DDoS detection approaches in IoT networks continue to demonstrate value through their low computational cost, simplicity, and suitability for constrained environments. Techniques such as statistical profiling, protocol-based monitoring, and fuzzy logic offer practical solutions for real-time detection and mitigation, especially at the edge or within resource-limited devices. However, these methods often rely on static thresholds, predefined rules, or manually crafted features, limiting their adaptability to dynamic traffic patterns and novel or evolving attack strategies. Moreover, their detection capabilities may degrade in complex or large-scale deployments without integration of adaptive intelligence. To remain effective in the face of modern threats, future iterations of these techniques must address scalability, automatic adaptation, and deeper contextual awareness without sacrificing efficiency.

### 4.2. Traditional Machine-Learning DDoS Detection in IoT Networks

Traditional machine learning methods, including well-known algorithms like decision trees, k-nearest neighbors (k-NN), support vector machines (SVM), and random forests, have shown strong capability in identifying DDoS attacks within IoT settings without the need for deep learning or hybrid models. Such techniques generally require less computational effort and are simpler to deploy on edge and gateway devices, which makes them suitable for delivering real-time protection in IoT networks with limited resources.

Bhunia & Gurusamy [21] propose “SoftThings,” an SDN-based hierarchical framework for detecting and mitigating attacks at the edge of IoT access networks. It deploys lightweight OpenFlow switches at each subscriber, grouped under local SDN controllers coordinated by a master controller. Attack detection is handled by a learning module within each cluster controller, training Support Vector Machines (linear and RBF kernels) on labeled traffic, which includes normal behavior and three emulated attacks: TCP SYN flooding, ICMP flooding, and multi-source DDoS, all generated in Mininet using POX. Features include flow and packet-level statistics such as request rates, failed authentications, source IPs, bandwidth usage, and time-of-day patterns. Three scenarios were tested: a single victim, a compromised source, and a two-bot DDoS attack. For TCP

SURVEY ARTICLE

flooding, the nonlinear SVM achieved 98% precision and 97% recall (linear: 94% / 92%), for ICMP flooding 97% / 96% (linear: 92% / 88%), and for DDoS 98% / 95% (linear: 94% / 93%). Link restoration after blocking or rate limiting took 2–3 seconds. The nonlinear SVM showed a false positive rate of about 2% or less. Overall, SoftThings demonstrates that ML-driven SDN can detect IoT flood attacks with up to 98% accuracy and mitigate them swiftly without burdening constrained devices.

Cvitić et al. [22] introduce a DDoS detection model for IoT traffic based on class affiliation of devices, leveraging the stable and uniform nature of MTC traffic. Devices are grouped into classes using features like send/receive ratio, with legitimate traffic profiles defined per class. The framework includes traffic collection, feature selection, class assignment via logistic regression, and anomaly detection using AdaBoost. Seven-day traffic data from a thermostat, vacuum cleaner, and camera confirmed temporal feature stability. Anomalies - deviations from class profiles - are flagged as potential DDoS activity. While prior ML models (KNN, SVM, ANN) achieved 91–99% accuracy, they lacked scalability; this model offers a scalable, adaptive approach suitable for zero-day DDoS detection without signature dependence.

Lawal et al. [23] propose a fog-based DDoS mitigation framework for IoT networks using an anomaly-based IDS with a k-NN classifier and a signature database for rapid detection. By offloading computation to fog nodes, the system supports real-time detection without straining IoT devices. Using the CICDDoS2019 dataset (241,173 instances, 23 features), and 10-fold cross-validation, k-NN achieved 99.99% accuracy, 100% precision, recall, and F1 score, with 0% false positives, outperforming DT (99.88%) and NB (95.55%). Euclidean and Manhattan distances yielded ≈99.99% accuracy, while Chebychev dropped to ≈79.75%. The results confirm k-NN's high accuracy and scalability for IoT DDoS defense.

Garba et al. [24] introduced a framework for real-time DDoS detection and mitigation in SDN-based smart home environments, employing machine learning models such as SVM, Logistic Regression, Decision Trees, and KNN, which were trained on both benign and malicious traffic patterns. These models run within the SDN controller for real-time detection, while SNORT (a signature-based IDS) protects the controller itself. Without SNORT, the controller failed quickly under attack, causing full packet loss. Among all models, Decision Tree achieved the highest accuracy at 99%, effectively identifying malicious traffic. The framework highlights the strength of combining ML and signature-based detection for securing smart home IoT networks.

Aslam et al. [25] proposed AMLSDM, an adaptive machine learning–driven framework designed to identify and counter DDoS attacks within SDN-enabled IoT systems. The architecture consists of three layers: the first integrates classifiers such as SVM, Naive Bayes, Random Forest, kNN, and Logistic Regression; the second employs Ensemble Voting (EV); and the third deploys the trained EV model for real-time traffic analysis. Tested on custom SDN-IoT topologies in Mininet with POX and Floodlight, and trained using tshark/sFlow-generated datasets, the model extracted five key features (e.g., RSIP, SDFP, RPFES). AMLSDM-EV achieved up to 99% accuracy, with high precision, recall, and F1-score, and lower false positives than individual classifiers and other methods like LEDEM and CONA. It also reduced DDoS traffic from 30–70 Mbps to 30–50 Kbps, restoring resources to legitimate users.

Islam et al. [26] propose a machine learning-based DDoS detection approach for IoT-enabled banking systems using a curated Banking Dataset. Three supervised models - SVM, RF, and KNN - were tested after preprocessing steps like null value removal, normalization, and K-means feature ranking. With a 70/30 train-test split, SVM achieved the highest accuracy (99.8%), surpassing KNN (98.74%) and RF (97.5%). It also recorded top precision (99.07%), recall (98.32%), and F1-score (98.5%). Confusion matrices confirmed SVM's robustness, and it showed the lowest time complexity, making it most efficient for real-time detection. Compared to prior ML/DL banking studies, the proposed SVM model demonstrated superior performance.

Mihoub et al. [27] present a novel detection and mitigation approach for DoS and DDoS attacks in IoT environments, featuring a two-part architecture: a detection module using a multi-class classifier enhanced with a "Looking-Back" mechanism, and a mitigation module. The mechanism analyzes historical traffic to better identify attack and packet types, enabling precise countermeasures. Evaluated on the Bot-IoT dataset, which includes both benign and malicious traffic, the system was preprocessed for ML training and testing. Results show that the "Looking-Back" mechanism improves detection accuracy and reduces false positives. The architecture supports tailored mitigation, enhancing IoT resilience against DoS/DDoS attacks through historical traffic analysis.

Doshi et al. [28] propose a lightweight ML framework for detecting DDoS attacks from consumer IoT devices by exploiting IoT-specific network behavior. The pipeline involves traffic collection, per-device feature extraction, and binary classification using stateless and stateful features like packet size, inter-packet interval, bandwidth, and protocol type. A controlled testbed with devices such as YI Home Camera and WeMo Smart Switch simulated TCP SYN, UDP, and HTTP GET floods (~1.5 mins each). The dataset comprised 491,855 packets (93.4% malicious, 6.6% benign). Among evaluated models - Random Forest, Decision Tree,

SURVEY ARTICLE

KNN, SVM, and Neural Networks - Random Forest and KNN achieved highest accuracy (0.999), precision (>0.998), and recall (>0.993). Neural networks also performed well despite limited data. Using both feature types improved F1 scores. The lightweight, protocol-agnostic design suits deployment on constrained devices like routers and smart gateways.

Above studies shown that traditional machine learning techniques have proven to be highly effective in detecting and mitigating DDoS attacks in IoT networks, particularly due to their low computational cost, ease of deployment, and adaptability to edge and fog environments. Approaches using SVM, k-NN, decision trees, logistic regression, and ensemble methods consistently achieved high accuracy, precision, and recall - often exceeding 98% - across diverse datasets and network architectures. These models also demonstrated strong real-time performance, especially when integrated with SDN or fog-based infrastructures. However, notable limitations remain. Many studies rely on simulated datasets or controlled testbeds, raising concerns about real-world generalization. Furthermore, the absence of deep contextual understanding or self-learning capabilities may reduce their effectiveness against sophisticated or evolving DDoS strategies, particularly zero-day attacks. Lastly, while ensemble methods enhance performance, they may introduce complexity that challenges the lightweight nature expected in constrained IoT devices. Future work should aim to strike a balance between efficiency, adaptability, and robustness in increasingly dynamic and heterogeneous IoT environments.

### 4.3. Deep Learning Techniques for IoT DDoS Detection

An increasing number of studies have concentrated on leveraging deep learning architectures to identify Distributed Denial-of-Service (DDoS) attacks within Internet of Things (IoT) networks. This Section reviews notable research that employs deep neural networks for intrusion detection, chosen for their strong methodology, clear experimental design, and use of publicly available benchmark datasets.

Popoola et al. [29] propose LAE-BLSTM, a hybrid deep learning framework for detecting botnet-based DDoS attacks in IoT networks. It integrates a Long Short-Term Memory Autoencoder (LAE) for reducing dimensionality with a Bidirectional LSTM (BLSTM) for classification. Using the BoT-IoT dataset (five classes: DDoS, DoS, reconnaissance, theft, normal), LAE reduced features from 37 to 6 and compressed data by 91.89%, outperforming PCE, XMP, and IFG by up to 27.03%. In binary classification, the Nadam optimizer achieved MCC = 95.80% and 100% accuracy with 0% false positives. For multi-class classification, MCC exceeded 98% for DDoS and DoS, with a mean MCC over 96%, outperforming SVM, RNN, FNN, and hybrid models like IFG-CSVM. LAE-BLSTM demonstrated strong generalization, minimal overfitting, and practical viability for real-world IoT intrusion detection.

Hnamte et al. [30] proposed a deep learning–driven framework aimed at identifying and countering DDoS attacks in SDN environments. It leverages the centralized architecture of SDN by incorporating a Deep Neural Network (DNN) into the controller for traffic inspection. The model underwent training and evaluation on the CICIDS2018 dataset. InSDN, and a Kaggle DDoS dataset, covering diverse attack types and normal traffic. The DNN effectively distinguished between benign and malicious flows by learning complex traffic patterns. Results showed high accuracy and low false positive rates, confirming real-time detection and mitigation capability. Integrating the DNN into the SDN controller enables adaptive analysis and rapid threat response, highlighting the potential of combining deep learning with SDN for efficient, evolving intrusion detection.

McDermott et al. [31] propose a deep learning-based detection framework using BLSTM networks to identify botnet-based DDoS attacks in IoT networks. The model analyzes packet-level data, converting the Info field into tokenized sequences via word embedding. A secure sandbox based on Mirai source code was used to launch real attacks (UDP, ACK, DNS, Mirai control) on infected IoT cameras. The dataset included millions of labeled packets covering normal and attack traffic. The BLSTM-RNN was trained and compared with a standard LSTM-RNN over 100 epochs using Adam optimizer and MAE loss. BLSTM showed superior performance in capturing bidirectional dependencies, achieving validation accuracies of 99.99% (Mirai), 98.58% (UDP), 98.48% (DNS), and 93.76% (ACK), with loss values from 0.0008 to 0.85. The model proved effective for complex, multi-vector DDoS detection at the packet level in IoT networks.

Meidan et al. [32] propose N-BaIoT, a network-based anomaly detection framework using deep autoencoders to detect IoT devices compromised by botnets like Mirai and BASHLITE. A separate autoencoder is trained per device on benign traffic, detecting anomalies via reconstruction errors. Each model processes 115 features across five-time windows (100 ms–1 min), capturing traffic behavior at MAC/IP/socket levels. Nine commercial devices were infected with both botnets and subjected to 10 attack types (e.g., UDP, TCP, SYN, DNS floods, spam). N-BaIoT achieved 100% TPR and a mean FPR of $0.007 \pm 0.01$, outperforming LOF, SVM, and Isolation Forest. Detection latency averaged $174 \pm 212$ ms. Using Keras, the models relied on reconstruction error and majority voting to reduce FPR. The framework proved scalable and effective for near-instant botnet detection in enterprise IoT networks.

Lee et al. [33] present a DDoS detection and prevention system for IoT networks using edge computing and 2D-CNNs. The system collects traffic and packet-level features from a Raspberry Pi-based IoT server under five scenarios:

SURVEY ARTICLE

normal, SYN, UDP, ICMP, and mixed floods. Two 2D-CNN models are trained - one on traffic statistics (CPU/memory usage, packet count) and another on packet features (interval, size, protocol) - using 25,000 traffic and 4.5 million packet samples over 200 iterations. The feature-based model achieved 99.8% accuracy, and the traffic-based model 99.5%. Real-world tests confirmed accurate detection across all attack types with average detection time under 8.72 seconds. The system reduced attack-induced throughput from 14.2 Mbps to 0.3 Mbps. Combining both CNNs (70% traffic, 30% feature) lowered false positives and ensured robustness, offering a high-accuracy, low-cost edge-based defense solution for IoT.

Doriguzzi-Corin et al. [34] introduced LUCID, an efficient CNN-driven DDoS detection framework created for operation in online settings with limited computational resources. It transforms network traffic into spatial matrices via custom time-windowing and packet-level preprocessing, eliminating the need for flow-level statistics. Trained on ISCX2012, CIC2017, and CSECIC2018 datasets, LUCID achieved F1 scores $> 0.994$, accuracy = 99.87%, FPR = 0.87%, and precision/recall $> 99.1\%$ on the composite UNB201X dataset. It outperformed deeper models like 3LSTM (1M+ parameters) using just 2241 parameters, processing 55,000 samples/sec on servers and 23,000 on Jetson TX2. Operating on only 1 GB RAM, it trained in under 2 hours on CPU-only hardware. LUCID remained robust under varied time and packet constraints, with kernel activation revealing it learned key attack indicators (e.g., “Highest Layer,” “IP Flags”), making it ideal for IoT and edge deployments.

Negera et al. [35] present a lightweight Hierarchical Convolutional Neural Network (HCNN) for botnet detection and classification using the Bot-IoT dataset. The model employs a 3-level classification: binary (normal vs. attack), 5-class, and 11-class, with each level building on the previous. It uses a CNN backbone with only 848 trainable parameters, and the hierarchical design adds 942, totaling 1790 parameters. With 72 million samples in the dataset, downsampling was used to address class imbalance. Evaluated with metrics like Accuracy, Precision, Recall, F1, MCC, and Cohen’s Kappa, the HCNN achieved 100% accuracy at levels 1 and 2, and 98% F1-score at level 3, surpassing non-hierarchical CNNs by 5%. MCC and Kappa were above 0.99 at all levels. The model classified each sample in 9.4 µs and had a total size of just 6.97 KB, enabling real-time IoT deployment. The study confirms HCNN’s ability to handle complex botnet class structures with high accuracy and minimal resource usage.

The studies reviewed at this Section have shown remarkable potential in detecting DDoS attacks within IoT networks, thanks to their ability to learn complex, high-dimensional patterns and generalize across diverse attack types. Models such as CNNs, BLSTMs, and deep autoencoders consistently achieved near-perfect accuracy, low false positive rates, and real-time performance, even under constrained environments like edge devices or SDN controllers. Furthermore, lightweight architectures like LUCID and HCNN proved that deep models can be optimized for resource-limited deployments without sacrificing detection accuracy. However, challenges remain. Many deep models require extensive training data and computational resources, which may not always be available in practical IoT scenarios. Additionally, while some frameworks address class imbalance or scalability, few offer comprehensive solutions for model interpretability or online adaptability to evolving threats. Future research should focus on balancing depth and efficiency, improving explainability, and enabling continuous learning to ensure robustness against zero-day and polymorphic attacks.

### 4.4. Hybrid DDoS Detection in IoT Networks

Hybrid approaches merge the pattern-recognition power of data-driven models with real-time control or defense mechanisms, yielding end-to-end, automated protection for resource-constrained IoT deployments. By coupling deep- or classical-learning detectors with SDN flow orchestration, GAN-based adversarial hardening, or cooperative decision logic, researchers aim to close the gap between high detection accuracy and immediate mitigation. Such integration is critical because IoT DDoS traffic often evolves faster than purely rule-based filters, yet any response must be lightweight enough for home gateways and edge devices. The following studies illustrate how this hybrid paradigm boosts both robustness and responsiveness, maintaining QoS while suppressing floods and stealth scans alike. Each work leverages a distinctive blend of learning architecture and network-aware actuator, demonstrating the practical gains of “sense-and-act” security pipelines in modern IoT environments.

Ravi & Shalinie [36] propose LEDEM, a learning-driven DDoS detection and mitigation system for wireless IoT attacks on servers, built on a decentralized SDN-cloud architecture. It employs a Semi-supervised Deep Extreme Learning Machine (SDELM) for accurate, efficient detection, with OpenFlow-based monitoring and classification at local controllers. For mitigation, static IoT devices use a VLAN-based approximation algorithm (fMS), while mobile devices use blacklisting with temporary rules. Evaluated on the UNB-ISCX dataset and a custom testbed (6 VLANs, 89,860 samples), LEDEM achieved 96.28% accuracy, surpassed Naive Bayes and deep belief networks, improved throughput by 21% during attacks, and reduced controller bandwidth via rule aggregation. The fMS strategy is mathematically proven as a 2-approximation algorithm, ensuring scalable, efficient DDoS mitigation for IoT.

**SURVEY ARTICLE**

Yan et al. [37] propose MLDMF, a Multi-Level DDoS Mitigation Framework for IIoT, structured across edge, fog, and cloud layers, with SDN at its core. At the edge, SDN-based IIoT gateways (SDNIGWs) handle access control, firmware checks, malware detection, and traffic filtering. The fog layer, via the IIoT Management Control Unit (IMCU), performs traffic analysis, DDoS detection, and redirection to honeypots. The cloud layer applies big data analytics and machine learning for detection and feedback. Simulations of Ping of Death and TCP SYN floods in Mininet showed SDN-based defense reduced response delay by up to 37%, keeping ping delays under 1 ms versus >3000 ms without defense. MLDMF effectively maintains service quality by distributing detection and mitigation, enabling fast edge responses and deep cloud analytics, enhancing IIoT resilience against DDoS.

Agbor et al. [38] propose a hybrid deep learning model combining CNNs, BiLSTM, and DNNs for detecting cybersecurity threats in IoT networks. Trained on IoT-23 and Edge-IIoTset datasets, which include attacks like DDoS, port scanning, Okiru, and injection, the model achieved 99.90% accuracy, precision, recall, and F1-score on IoT-23, and 100% accuracy with 99.99% F1-score on Edge-IIoTset in binary classification. For multi-class tasks, it reached 100% F1-score for most attacks and a minimum of 98.01% (OS fingerprinting), with average accuracy over 99.97%. To enable deployment on constrained devices, pruning and post-training quantization were applied, maintaining performance while reducing resource use. The architecture uses 1D CNNs for feature extraction, BiLSTM for temporal analysis, and DNNs for classification, with dropout, batch normalization, L2 regularization, and early stopping to prevent overfitting. The results confirm its high accuracy, efficiency, and real-time suitability for IoT intrusion detection.

Noor Ul Ain et al. [39] propose a hybrid deep learning model for DDoS detection in IoT networks, combining an Autoencoder for anomaly detection, LSTM for temporal sequence learning, and 1D CNN for spatial pattern recognition. Using the CICIoT2023 dataset (33 attack scenarios across 7 categories), the study applies preprocessing, reduces features from 46 to 37, and standardizes the data.

The hybrid model achieved 96.78% accuracy, 96% precision, recall, and F1-score, outperforming CNN (94.3%), LSTM (91.27%), and DNN (89.88%). It performed well on common attacks like UDP and ICMP floods but showed lower F1-scores on HTTP Flood (0.42) and SlowLoris (0.14). The Autoencoder effectively detected anomalies using a reconstruction error threshold at the 95th percentile. The model's hybrid design improved robustness and generalization, offering a scalable, adaptive solution for detecting DDoS in dynamic IoT environments.

Nguyen & Le [40] present a hybrid deep learning model for detecting unknown DoS/DDoS attacks in IoT networks by combining a soft-ordering CNN (SOCNN) with unsupervised anomaly detection methods, Local Outlier Factor (LOF) together with isolation-based nearest-neighbor ensembles (iNNE) were assessed using the BoT-IoT, CIC-IDS-2017, and CIC-IDS-2018 datasets. The model obtained average F1-scores of 98.94%, 91.68%, and 96.07%, showing superior performance compared to other existing approaches. SOCNN extracts spatial traffic features, while LOF and iNNE detect anomalies without prior attack knowledge, enabling detection of novel threats. The model also resisted adversarial attacks like FGSM and CW, showing strong robustness. This hybrid approach combines supervised and unsupervised learning for enhanced detection of both known and unknown intrusions in IoT networks.

Javeed et al. [41] proposed a hybrid deep learning–based intrusion detection framework for IoT networks leveraging SDN, integrating Cu-DNNGRU and Cu-BLSTM to enable lightweight, real-time detection. The system was trained on the CICIDS2018 dataset (84,702 entries, 3 classes) and assessed using 10-fold cross-validation. It achieved 99.87% accuracy and precision, along with 99.96% recall and F1-score, surpassing the performance of Cu-GRULSTM and Cu-DNNLSTM baselines. It recorded an FPR of 0.0554%, FOR of 0.0129%, and testing latency of 18.9 ms. Additional results include MCC = 99.6%, TPR = 99.96%, and TNR = 99.43%, confirming its robustness and suitability for scalable, low-cost intrusion detection in resource-constrained IoT environments.

Qureshi et al. [42] present a hybrid deep learning model - CNN-LSTM-GRU - for detecting DDoS and DoS attacks in IoT networks. Combining CNN for spatial learning, LSTM for temporal memory, and GRU for efficiency, the model is tested on UNSW-NB15 and Bot-IoT datasets, with features grouped by protocol types and preprocessing steps like IP normalization and Z-score scaling. It achieved up to 98.45% accuracy, precision, recall, and F1-score, with the lowest FPR (2.4%), highest MCC (0.9427), TNR (97.59%), and AUC (0.951). It also processed 1000 samples in 300 µs, outperforming CNN-LSTM and CNN-BiLSTM, offering a scalable and accurate real-time IDS for IoT environments.

As observed, Hybrid approaches for DDoS detection in IoT networks have emerged as powerful solutions that combine the high accuracy of deep learning models with the dynamic responsiveness of network-based control mechanisms such as SDN and anomaly-based filtering. The reviewed studies demonstrate how blending CNNs, LSTMs, GRUs, Autoencoders, and other neural architectures with network layer logic enables not only precise detection of both known and novel attacks, but also immediate, context-aware mitigation.

**SURVEY ARTICLE**

This dual capability ensures high performance even in real-time and resource-constrained environments. However, some challenges persist. Many hybrid models still rely on complex multi-module architectures, which may increase implementation overhead, training time, or model interpretability issues. In addition, certain attack types such as low-rate or stealthy floods (e.g., SlowLoris) remain difficult to detect reliably. Future work should aim to streamline hybrid frameworks for easier deployment, enhance detection of subtle or obfuscated attacks, and integrate continuous learning to adapt to evolving threat landscapes.

### 4.5. Comprehensive Comparative Summary

In this Section, a comprehensive comparative summary provided for the previous mentioned DDoS detection techniques in IoT environments, that covering 26 peer-reviewed research studies. The comparison evaluates each study across multiple dimensions, including the proposed model or algorithm, the dataset(s) used, training and testing methodologies, detection performance metrics (such as accuracy, precision, recall, F1-score, and false positive rate), detection latency, and key contributions.

Table 1 A Comprehensive Comparative Summary of the Reviewed Papers

| Authors | Technique / Model | Category | Dataset Used | Training/ Testing Strategy | Performance Metrics | Detection Time / Latency | Main Contributions |
|---|---|---|---|---|---|---|---|
| Doshi et al.[17] | Online Discrepancy Test (non-parametric) | Traditional | N-BaIoT + IoT testbed | Sequential learning | TPR: 100%, FPR: 0.5–2%, AUC: 0.9825 | < 0.2 sec | Detects stealthy DDoS without prior traffic knowledge |
| Adat & Gupta[18] | Rule-based + temporal filtering | Traditional | Contiki OS + Cooja | Custom test network | PDR: 100% (router), 86% (internal) | Not specified | Lightweight and modular edge-layer defense |
| Pandey & Mishra[19] | Entropy + Signature | Traditional | Custom traffic datasets | 2-stage entropy pipeline | High accuracy, low FPR | Not specified | Handles flash crowds |
| Haripriya et al[20] | Fuzzy logic | Traditional | Contiki + COOJA | Simulated attacks on MQTT | Precision: 91%, Recall: 90.9%, FPR: 0.1–0.37 | Not specified | No need for pre-defined rule base |
| Bhunia & Gurusamy [21] | SVM (linear + RBF) | Machine Learning | Custom / Mininet | 3 Scenarios | Precision: 98%, Recall: 97% (TCP) | 2–3 sec | Edge-based SDN with real-time SVM detection |
| Cvitic et al.[22] | AdaBoost + Logistic Regression | Machine Learning | Real device traffic (7 days) | Manual device class profiling | Accuracy: 91–99% | Not specified | Time-stable features with per-class profiles |
| Lawal et al.[23] | kNN | Machine Learning | CICDDoS2019 | 10-fold CV | Accuracy: 99.99%, Precision: 100%, FPR: 0% | Not specified | Highly scalable and accurate with fog nodes |
| Garba et al.[24] | Decision Tree (best) | Machine Learning | Simulated + real SDN smart home | Multiple ML models compared | Accuracy: 99% | Not specified | DDoS ML detection inside SDN controller |
| Aslam et al.[25] | Ensemble Voting (SVM, NB, RF, etc.) | Machine Learning | Custom Mininet SDN + tshark | Flows: 5k to 30k | Accuracy: 99%, F1-score high, Low FPR | Reduced traffic to 30–50 Kbps | 3-layer adaptive ML |
| Islam et al.[26] | SVM, KNN, RF | Machine Learning | Custom banking dataset | 70/30 split | Accuracy: 99.8%, Precision: 99.07% | Not specified | Best precision among models |
| Mihoub et al.[27] | Multi-class + historic | Machine Learning | Bot-IoT | Preprocessed & balanced | Improved accuracy, reduced | Not specified | Uses past packets to refine detection |

**SURVEY ARTICLE**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | context | | | | FPR | | |
| Doshi et al.[28] | RF, KNN, NN | Machine Learning | 491,855 packets | Custom IoT testbed | Accuracy: 0.999, FPR: ~0% | Fast | Lightweight + protocol agnostic |
| Popoola et al.[29] | Autoencoder + BiLSTM | Deep Learning | BoT-IoT | Nadam optimizer | Accuracy: 100%, MCC: 95.80%, FPR: 0% | Fast | Low resource, robust to over/underfitting |
| Hnamte et al.[30] | DNN | Deep Learning | CICIDS2018, InSDN, Kaggle | Supervised learning | High accuracy, low FPR | Real-time | Integrates with SDN |
| McDermott et al.[31] | BLSTM | Deep Learning | Mirai sandbox | 100 epochs | Acc: 99.99% (Mirai), FPR low | Good | Performs well on multivector attacks |
| Meidan et al.[32] | Autoencoder (per-device) | Deep Learning | N-BaIoT | Reconstruction error | TPR: 100%, FPR: 0.007, Delay: 174ms | 0.174 sec | Device-specific detection |
| Lee et al.[33] | 2D-CNN (x2) | Deep Learning | Raspberry Pi IoT data | 5 scenarios | Acc: 99.8%, 99.5%; Detect time < 8.72s | < 8.72 sec | Low cost + robust |
| Doriguzzi-Corin et al.[34] | Lightweight CNN | Deep Learning | ISCX2012, CIC2017, CSE-CIC18 | Sliding window | Acc: 99.87%, FPR: 0.87% | 23K/s (Jetson) | Tiny: 2241 params |
| Negera et al.[35] | Hierarchical CNN | Deep Learning | Bot-IoT (72M rows) | Hierarchical 3-stage | F1: 98%, MCC > 0.99 | 9.4 µs/sample | Only 6.97 KB size |
| Ravi & Shalinie[36] | SDELM (semi-supervised) | Hybrid | UNB-ISCX + testbed | VLAN setup, 89,860 samples | Accuracy: 96.28%, Throughput +21% | Not specified | Blacklisting + VLAN mitigation |
| Yan et al.[37] | Multi-level SDN + ML | Hybrid | Mininet | Edge/Fog/Cloud setup | Latency ↓ 37%, Ping <1ms | Real-time with honeypots | Distributed mitigation across layers |
| Agbor et al.[38] | Hybrid CNN + BiLSTM + DNN | Hybrid | IoT-23, Edge-IIoTset | Binary & Multiclass | Acc: 99.9–100%, F1 > 99% | Low | Pruned for edge deployment |
| Noor Ul Ain et al.[39] | Autoencoder + LSTM + CNN | Hybrid | CICIoT2023 | Filtered 37 features | Acc: 96.78%, F1: 96%, Weak on SlowLoris | Not specified | Strong on common attacks |
| Nguyen & Le[40] | Supervised + Unsupervised | Hybrid | BoT-IoT, CICIDS17,18 | Hybrid anomaly learning | F1: 98.94%, 91.68%, 96.07% | Robust | Also resistant to adversarial attacks |
| Javeed et al.[41] | GRU + BLSTM | Hybrid | CICIDS2018 | 10-fold CV | Acc: 99.87%, F1: 99.96%, FPR: 0.0554% | 18.9 ms | SDN-based, real-time |
| Qureshi et al.[42] | CNN + LSTM + GRU | Hybrid | UNSW-NB15 + Bot-IoT | By protocol type | Acc: 98.45%, F1: 98.45%, FPR: 2.4% | 0.3 ms/sample | Competitive + explainable |

The comparative shown at Table.1. above serves as a consolidated reference for identifying the strengths, weaknesses, and real-world applicability of each method. It highlights trends such as the increasing dominance of deep and hybrid models in achieving high detection accuracy, as well as the trade-offs in latency and resource consumption. This systematic comparison is instrumental for researchers and practitioners aiming to select or improve suitable intrusion detection solutions tailored for diverse IoT deployment scenarios.

SURVEY ARTICLE

## 5. CHALLENGES AND FUTURE DIRECTIONS

As IoT ecosystems expand, defending against DDoS attacks in these settings remains complex. Below, shown for the main barriers hindering effective protection and propose areas where future studies can contribute.

### 5.1. Challenges

Despite advances in intrusion detection, three key Limited device resources can be summarized as following points:

Limited processing power: Many IoT devices function with restricted computing capabilities, memory, and battery life. This limitation makes it challenging to execute complex detection algorithms directly on such devices. Although delegating analysis to fog or edge nodes can partially mitigate this issue, it may introduce latency and raise concerns about data integrity and trust.

Lack of realistic datasets: Most publicly available intrusion datasets are derived from enterprise or campus networks rather than actual IoT environments. As a result, they often fail to represent the distinct traffic behaviors and attack profiles of real-world IoT systems. Additionally, many existing datasets suffer from class imbalance, prompting researchers to depend on synthetic or oversampled data that may not accurately represent real operational conditions.

Evolving attack strategies. IoT botnets and DDoS techniques continuously adapt, leveraging new malware variants and amplification methods. Static signatures or models trained on outdated data struggle to detect novel or zero-day attacks. The heterogeneity of IoT traffic and the speed at which adversaries innovate demand dynamic detection mechanisms that current benchmarks do not fully emulate.

Collectively, these issues illustrate why achieving both high accuracy and practical deployability on constrained hardware remains an open problem. The surveyed studies consistently call for better data, lighter algorithms, and adaptive defenses to bridge this gap.

### 5.2. Directions for Future Research

To overcome these limitations, the recommendations focusing on three complementary research paths:

Development of lightweight detectors. Future work should tailor algorithms to IoT hardware constraints, for example by employing TinyML, streamlined rule-based systems, or feature extraction techniques with minimal overhead. Strategies such as decision-tree pruning, incremental learning, and hardware-assisted acceleration (e.g., microcontroller DSPs) can reduce computational and energy costs while preserving detection performance.

Creation of standardized IoT benchmarks. The community must establish open, representative datasets that include diverse device types, realistic usage patterns, and multiple DDoS vectors. Regular updates and consistent evaluation frameworks - such as containerized testbeds will enable fair comparisons and ensure that proposed methods generalize beyond controlled environments.

Exploration of adaptive AI methods. Reinforcement learning and other advanced AI approaches offer the ability to adjust detection policies in real time, keeping pace with shifting attack landscapes. In addition, techniques like federated learning can enhance privacy, while generative models (e.g., GANs) and self-supervised learning can address data scarcity by producing realistic training samples.

By advancing lightweight detection, realistic benchmarking, and adaptive intelligence, future research can close the gap between laboratory achievements and field-deployable solutions. These steps are essential for strengthening IoT security and ensuring that detection systems remain effective as attack methods continue to evolve.

## 6. CONCLUSION

With the increasing integration of Internet of Things (IoT) devices into everyday life and critical infrastructures, ensuring their security has become a pressing concern. The inherent limitations of IoT devices - such as constrained computational power and minimal memory make them especially susceptible to Distributed Denial of Service (DDoS) attacks, which can cause widespread service disruption. This underscores the growing necessity for efficient and adaptive intrusion detection solutions. In this review, a various defense mechanisms explored, ranging from traditional signature-based techniques to more advanced machine learning and deep learning models. While conventional methods provide simplicity and clarity, they often fall short in identifying novel or evolving threats. On the other hand, machine learning algorithms especially models like support vector machines and decision trees have shown improved detection capabilities with moderate resource consumption, making them suitable for many IoT scenarios. Deep learning methods, such as convolutional and recurrent neural networks, have consistently demonstrated high accuracy and strong resistance to complex attack patterns, although they typically require higher computational resources. Recent advancements have focused on hybrid detection frameworks that combine multiple techniques such as federated learning, SDN integration, and optimization-based control to enhance both accuracy and scalability. Despite this progress, several challenges remain unresolved. A lack of publicly available and diversified datasets, the dynamic nature of attacks, and the diversity of IoT environments continue to complicate the development of universal detection strategies. Looking ahead, future research should emphasize designing lightweight yet intelligent detection models capable of adapting to changing threat landscapes. Efforts should also focus on ensuring

**SURVEY ARTICLE**

privacy preserving data analysis, enabling real-time response, and creating standardized evaluation protocols. Addressing these areas will be key to developing more effective and resilient security solutions for the evolving IoT ecosystem.

## REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.

[2] Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. IEEE access, 3, 678-708.

[3] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future generation computer systems, 82, 395-411.

[4] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer networks, 57(10), 2266-2279.

[5] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

[6] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84.

[7] Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 15(4), 2046-2069.

[8] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In 26th USENIX security symposium (USENIX Security 17) (pp. 1093-1110).

[9] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

[10] Kumar, K., & Behal, S. (2021, March). Distributed denial of service attack detection using deep learning approaches. In 2021 8th international conference on computing for sustainable global development (INDIACom) (pp. 491-495). IEEE.

[11] Zhang, C., Cai, Z., Chen, W., Luo, X., & Yin, J. (2012). Flow level detection and filtering of low-rate DDoS. Computer Networks, 56(15), 3417-3431.

[12] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[13] Alwaisi, Z., Kumar, T., Harjula, E., & Soderi, S. (2024). Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention. Internet of Things, 28, 101398.

[14] Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 4(2), 118-137.

[15] Liu, H., Ning, H., Mu, Q., Zheng, Y., Zeng, J., Yang, L. T., ... & Ma, J. (2019). A review of the smart world. Future generation computer systems, 96, 678-691.

[16] Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115.

[17] Doshi, K., Yilmaz, Y., & Uludag, S. (2021). Timely detection and mitigation of stealthy DDoS attacks via IoT networks. IEEE Transactions on Dependable and Secure Computing, 18(5), 2164-2176.

[18] Adat, V., & Gupta, B. B. (2017, April). A DDoS attack mitigation framework for internet of things. In 2017 international conference on communication and signal processing (ICCSP) (pp. 2036-2041). IEEE.

[19] Pandey, N., & Mishra, P. K. (2025). Conditional entropy-based hybrid DDoS detection model for IoT networks. Computers & Security, 150, 104199.

[20] Ap, H., & K, K. (2019). Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. EURASIP Journal on Wireless Communications and Networking, 2019(1), 90.

[21] Bhunia, S. S., & Gurusamy, M. (2017, November). Dynamic attack detection and mitigation in IoT using SDN. In 2017 27th International telecommunication networks and applications conference (ITNAC) (pp. 1-6). IEEE.

[22] Cvitić, I., Peraković, D., Periša, M., & Botica, M. (2021). Novel approach for detection of IoT generated DDoS traffic. Wireless Networks, 27(3), 1573-1586.

[23] Lawal, M. A., Shaikh, R. A., & Hassan, S. R. (2021). A DDoS attack mitigation framework for IoT networks using fog computing. Procedia Computer Science, 182, 13-20.

[24] Garba, U. H., Toosi, A. N., Pasha, M. F., & Khan, S. (2024). SDN-based detection and mitigation of DDoS attacks on smart homes. Computer Communications, 221, 29-41.

[25] Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., ... & Jilani, S. F. (2022). Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT. Sensors, 22(7), 2697.

[26] Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., ... & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability, 14(14), 8374.

[27] Mihoub, A., Fredj, O. B., Cheikhrouhou, O., Derhab, A., & Krichen, M. (2022). Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques. Computers & Electrical Engineering, 98, 107716.

[28] Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE Security and Privacy Workshops (SPW) (pp. 29-35). IEEE.

[29] Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2020). Hybrid deep learning for botnet attack detection in the internet-of-things networks. IEEE Internet of Things Journal, 8(6), 4944-4956.

[30] Hnamte, V., Najar, A. A., Nhung-Nguyen, H., Hussain, J., & Sugali, M. N. (2024). DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 138, 103661.

[31] McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018, July). Botnet detection in the internet of things using deep learning approaches. In 2018 international joint conference on neural networks (IJCNN) (pp. 1-8). IEEE.

[32] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-baiot—network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12-22.

[33] Lee, S. H., Shiue, Y. L., Cheng, C. H., Li, Y. H., & Huang, Y. F. (2022). Detection and prevention of DDoS attacks on the IoT. Applied Sciences, 12(23), 12407.

[34] Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J., & Siracusa, D. (2020). LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Transactions on Network and Service Management, 17(2), 876-889.

[35] Negera, W. G., Schwenker, F., Feyisa, D. W., Debelee, T. G., & Melaku, H. M. (2024). Hierarchical Classification of Botnet Using Lightweight CNN. Applied Sciences, 14(10), 3966.

[36] Ravi, N., & Shalinie, S. M. (2020). Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet of Things Journal, 7(4), 3559-3570.

[37] Yan, Q., Huang, W., Luo, X., Gong, Q., & Yu, F. R. (2018). A multi-level DDoS mitigation framework for the industrial Internet of Things. IEEE Communications Magazine, 56(2), 30-36.

[38] Agbor, B. A., Stephen, B. U. A., Asuquo, P., Luke, U. O., & Anaga, V. (2025). Hybrid CNN–BiLSTM–DNN Approach for Detecting Cybersecurity Threats in IoT Networks. Computers, 14(2), 58.

**SURVEY ARTICLE**

[39] Ain, N. U., Sardaraz, M., Tahir, M., Abo Elsoud, M. W., & Alourani, A. (2025). Securing IoT Networks Against DDoS Attacks: A Hybrid Deep Learning Approach. Sensors, 25(5), 1346.
[40] Nguyen, X. H., & Le, K. H. (2023). Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model. Internet of Things, 23, 100851.
[41] Javeed, D., Gao, T., Khan, M. T., & Ahmad, I. (2021). A hybrid deep learning-driven SDN enabled mechanism for secure communication in Internet of Things (IoT). Sensors, 21(14), 4884.
[42] Qureshi, S. S., He, J., Zhu, M. N., Qureshi, S., Ullah, F., Nazir, A., & Wajahat, A. (2024). A new deep learning paradigm for IoT security: expanding beyond traditional DDoS detection. International Journal of Network Security, 26(3), 349-360.

Authors

**Dr. Thoyazan Sultan Algaradi** is a Yemeni academic specializing in computer science. He currently serves as an Assistant Professor and faculty member in the Department of Computers and Information Technology at the Taiz Branch of the University of Science and Technology (USTY), under the main campus in Sana'a, Yemen, where he is also the Cybersecurity Program Coordinator. He earned his Ph.D. in Computer Science with a specialization in Big Data Security from the Department of Computer Science at Kakatiya University, Telangana, India, in September 2021. He obtained his Master's degree in Computer Networks from the School of Computer Sciences at Swami Ramanand Teerth Marathwada University (SRTM University), Maharashtra, India, between 2015 and 2017. Dr. Algaradi's research interests focus on information security, including cryptography, key management, big data security, Internet of Things (IoT), and network security in general. He is known for his dedication to academic and professional development and is considered one of the leading cybersecurity experts in Yemen, actively contributing to the training of qualified professionals in this critical field.

**How to cite this article:**

Thoyazan Sultan Algaradi, "Lightweight and Intelligent DDoS Detection for IoT Networks: A Comprehensive Survey, Comparative Benchmark, and Research Roadmap", International Journal of Computer Networks and Applications (IJCNA), 12(4), PP: 652-665, 2025, DOI: 10.22247/ijcna/2025/39.