







## Review Article

# Distributed Denial of Service Attack Detection in IoT Networks using Deep Learning and Feature Fusion: A Review

Abdulhafiz Nuhu Ahmad<sup>1</sup>, Anis Farihan Mat Raffei<sup>1,\*</sup>, Mohd Faizal Ab Razak<sup>1</sup>, Abubakar Ahmad<sup>2</sup>

<sup>1</sup>Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, 26600 Pekan, Pahang, Malaysia

<sup>2</sup>Faculty of Computing, Federal University Dutin-Ma, 5001 Dutsin-Ma, Katsina, Nigeria

## ARTICLE INFO

### Article History

Received 09 Feb 2024  
Accepted 03 April 2024  
Published 28 April 2024

### Keywords

Deep learning

IoT

DDoS

Feature fusion

IDS

Cybersecure threats



## ABSTRACT

The explosive growth of Internet of Things (IoT) devices has led to escalating threats from distributed denial of service (DDoS) attacks. Moreover, the scale and heterogeneity of IoT environments pose unique security challenges, and intelligent solutions tailored for the IoT are needed to defend critical infrastructure. The deep learning technique shows great promise because automatic feature learning capabilities are well suited for the complex and high-dimensional data of IoT systems. Additionally, feature fusion approaches have gained traction in enhancing the performance of deep learning models by combining complementary feature sets extracted from multiple data sources. This paper aims to provide a comprehensive literature review focused specifically on deep learning techniques and feature fusion for DDoS attack detection in IoT networks. Studies employing diverse deep learning models and feature fusion techniques are analysed, highlighting key trends and developments in this crucial domain. This review provides several significant contributions, including an overview of various types of DDoS attacks, a comparison of existing surveys, and a thorough examination of recent applications of deep learning and feature fusion for detecting DDoS attacks in IoT networks. Importantly, it highlights the current challenges and limitations of these deep learning techniques based on the literature surveyed. This review concludes by suggesting promising areas for further research to enhance deep learning security solutions, which are specifically tailored to safeguarding the fast-growing IoT infrastructure against DDoS attacks.

## 1. INTRODUCTION

The Internet of Things (IoT) has led to an explosion of interconnected smart devices and objects capable of collecting, exchanging, and processing data. By 2025, projections estimate that there will be more than 30 billion connected IoT devices globally [1]. This massive growth is driving major innovations by allowing for new levels of monitoring, control, optimization, and automation through technologies such as wearables, smart homes, autonomous vehicles, and sensor-enabled manufacturing. Fig. 1 illustrates the complex web of connections among various IoT devices and services. While this extensive connectivity facilitates data sharing and automation, it also introduces vulnerabilities that heighten security risks. A major emerging threat is distributed denial of service (DDoS) attacks, where multitudes of compromised devices are weaponized to overwhelm systems or services with traffic, disrupting availability [2]. DDoS attacks, such as the Mirai botnet attack on Twitter and Netflix in 2016, illustrate the destructive potential of insecure IoT networks [2][3]. IoT networks not only serve as potential attack vectors but are also susceptible targets for DDoS attacks [4]. This underscores the urgent need for robust security solutions tailored to the unique nature of IoT networks to defend against escalating DDoS attacks.

A major challenge in securing IoT systems stems from the inherent limitations of IoT devices. Many IoT devices have low computing power, memory, and battery life [5]. This hinders the implementation of comprehensive security features such as encryption, firewalls, and frequent software updates. Moreover, security, functionality, usability, and low cost are often secondary concerns for IoT device design [6]. The resulting vulnerabilities, such as default passwords, unencrypted traffic, and unpatched firmware, make IoT devices ripe targets for attackers [7]. Botnets exploit these weaknesses to infect millions of poorly secured IoT devices and recruit them into DDoS armies.

The decentralized nature of the IoT makes traditional security, such as firewalls, insufficient [8]. Intelligent, tailored solutions are needed to address the IoT's immense scale and diversity. Disruptions to critical infrastructure through DDoS attacks could be catastrophic, underscoring robust IoT security needs. According to Statista [9], as illustrated in Fig. 2, the pricing

\*Corresponding author. Email: [anisfarihan@ump.edu.my](mailto:anisfarihan@ump.edu.my)

for DDoS attacks shows how affordable these cyber threats are. The data show that DDoS attacks can be purchased for as little as \$200 for a 24-hour strike on a premium website. Higher intensity attacks run from \$450 for a week-long attack on an unprotected site to \$850 for a month-long barrage. Overall, the figure confirms the accessibility of DDoS and malware services. This affordability underscores the critical need for robust, adaptive security to safeguard IoT networks from attacks.

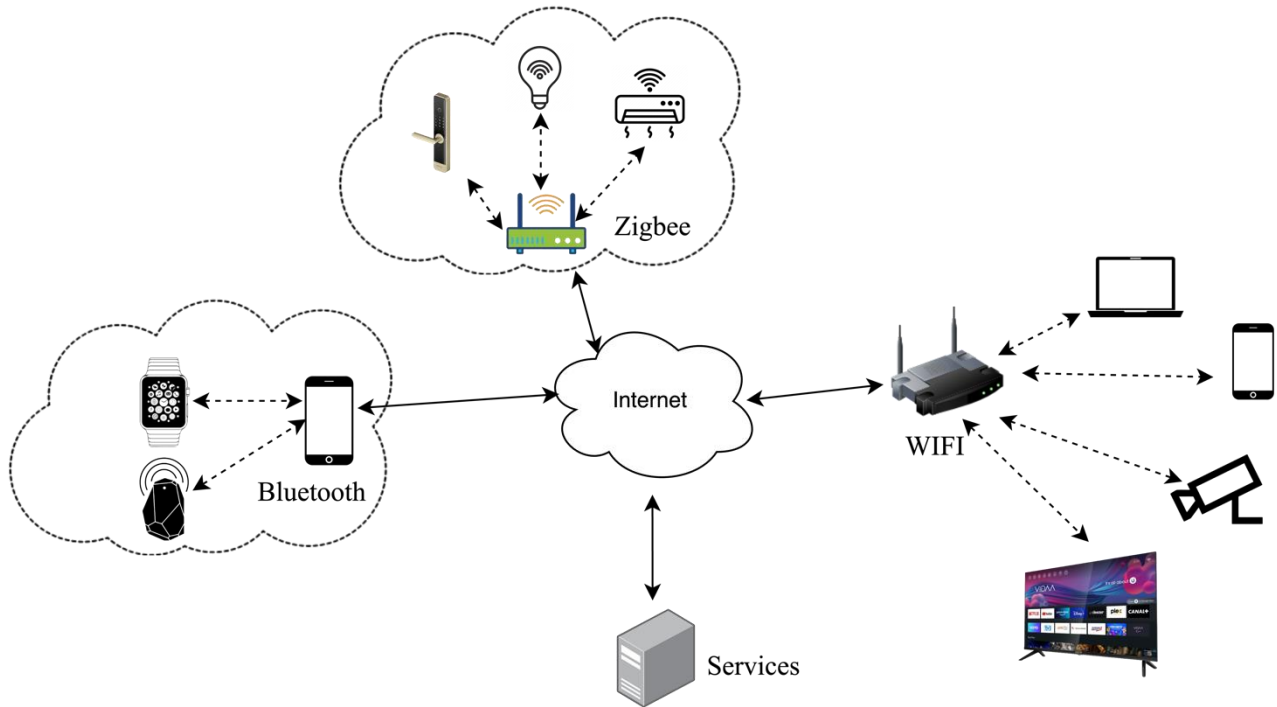


Fig. 1. Complex web of connections in IoT networks

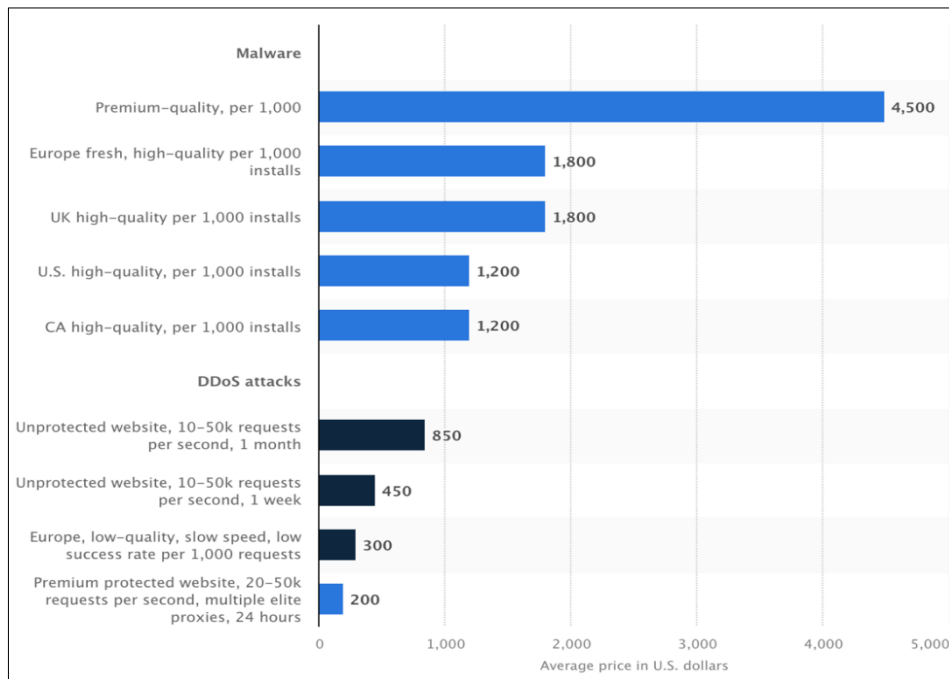


Fig. 2. Average price of malware and DDoS attack services for sale on the dark web as of March 2023 [9]

While intelligent security solutions are needed for the unique challenges of IoT environments, identifying optimal technologies tailored to the IoT remains an open research challenge. In recent years, deep learning (DL) has rapidly emerged as a transformative technology, achieving state-of-the-art results across domains as well as computer vision, natural language processing, and cybersecurity [10][11]. Compared to traditional machine learning, DL offers inherent advantages in automatically extracting complex features and patterns from high-dimensional data such as network traffic and system logs [12]. These characteristics make DL suitable for addressing the scale, dynamism, and heterogeneity of IoT ecosystems. Additionally, the integration of feature fusion techniques has gained momentum in improving the performance of DL models. This is achieved by combining complementary feature sets derived from multiple data sources [91]. The integration of feature fusion with DL has shown promising results in improving the accuracy and robustness of DDoS attack detection [92].

Consequently, applying DL and feature fusion specifically for IoT security represents an active emerging field, as researchers have investigated its potential to overcome the limitations of classical techniques. However, literature surveys lack comprehensive analysis dedicated to the pressing challenge of using DL and feature fusion to detect DDoS attacks in IoT networks. While valuable surveys have examined DL for general IoT security, most comprehensive analyses specifically focused on using DL and feature fusion for DDoS attack detection in IoT networks are lacking.

Therefore, this review provides a focused examination of applying DL and feature fusion to detect DDoS attacks that threaten IoT networks. This review offers insights into the various DL techniques and feature fusion approaches used for identifying DDoS attacks in IoT networks. Accordingly, the core contributions of the review include the following:

1. Examination and comparison of recent surveys addressing DL-based DDoS attack detection methods in IoT networks.
2. Comprehensive overview of different types of DDoS attacks.
3. Review and comparison of various DL techniques used for DDoS attack detection in IoT networks.
4. Review of recent applications of feature fusion for detecting DDoS attacks in IoT networks.
5. Identification of the challenges and limitations of current DL-based DDoS attack detection techniques based on the literature.
6. We suggest promising future research directions for advancing DL-based DDoS attack detection in IoT networks.

The paper is structured as follows: Section 2 examines previous work related to the current topic. Section 3 outlines the methodology employed for conducting a literature review on deep learning techniques for detecting DDoS attacks in IoT networks. Section 4 provides an overview of DDoS attacks, explaining their characteristics and impact. Section 5 reviews and synthesizes key trends and developments in the literature on deep learning techniques specifically designed for DDoS detection in IoT networks. Section 6 focuses on feature fusion techniques, which combine multiple features to enhance DDoS detection in IoT networks. Section 7 highlights the limitations of current approaches and discusses open challenges in this domain. Section 8 explores potential future research directions to improve the performance and effectiveness of deep learning-driven DDoS attack detection in IoT networks. Finally, Section 9 concludes the paper by summarizing the main findings and contributions.

## 2. RELATED WORK

Several prior survey papers have examined how DL can be applied to strengthen the security of IoT networks. However, many of these surveys do not investigate in-depth the specific use of DL for detecting DDoS attacks targeting IoT networks. While there is an extensive body of literature on DDoS attack detection techniques that could form the basis for developing effective DDoS prevention models for IoT networks, there appears to be a lack of surveys that comprehensively review feature fusion techniques aimed at enhancing the performance of DDoS attack detection systems specifically for IoT environments. Table I provides a comparative overview of related survey papers on this topic.

TABLE I. DEEP LEARNING TECHNIQUES FOR DDoS ATTACK DETECTION

Paper	Year	IoT	DL/ML	Feature fusion	Focus on DDoS detection
[93]	2024	Yes	DL	No	No
[94]	2024	Yes	ML/DL	No	Yes
[12]	2020	Yes	ML/DL	No	Partly
[13]	2021	Yes	DL	No	Partly
[11]	2021	Yes	DL	No	Partly
[14]	2023	No	DL	No	Yes
[15]	2022	Yes	ML/DL	No	Partly
[16]	2023	Yes	ML/DL	No	Partly
[17]	2022	Yes	ML/DL	No	Partly
[18]	2024	Yes	DL	No	Partly
[89]	2018	No	No	Yes	No
[90]	2019	Yes	No	Yes	No
<b>This paper</b>	2024	Yes	DL	Yes	Yes

Alsoufi et al. [13] conducted a survey presenting a taxonomy of DL approaches, evaluating model performance across diverse metrics and datasets. The authors explored seven DL methods used in IoT security, addressing key challenges. Moreover, the paper also offers an overview of DL and IoT intrusion detection while also suggesting avenues for future research.

Similarly, Aversano et al. [11] investigated DL approaches for IoT security, providing a structured taxonomy of the literature and shedding light on seven DL techniques. Another study [14] offered a systematic review of DL methods for detecting DDoS attacks, emphasizing methodologies, datasets, performance metrics, and research gaps. Importantly, this review diverges from the literature by not focusing on IoT networks, concentrating on DDoS detection within the broader context of network security.

In contrast, [18] explored various DL methods for IDS in IoT security. This paper analysed seven specific DL models, investigated their applications, and evaluated their performance using real-world traffic datasets (CSE-CIC-IDS2018 and Bot-IoT). The assessment examined models for both binary classification and multiclass classification. This comprehensive evaluation provided useful insights into how well these different DL methods perform across a range of scenarios relevant to securing IoT networks and systems.

Conversely, [12][15][16][17] provide comprehensive surveys of machine and DL methods for IoT security, contributing to the broader understanding of the field. However, our review provides a unique focus compared to previous surveys because we specifically concentrate on DL techniques for detecting DDoS attacks in IoT networks. DDoS attacks pose a critical threat to IoT networks, yet most prior surveys have taken a broad perspective on IoT security. This study provides a comprehensive analysis of the pressing issue of DDoS attack detection. It provides deeper insights into the DL methods for combatting DDoS attacks that compromise availability and service quality in increasingly essential IoT infrastructure.

While the above surveys focused primarily on deep learning techniques for IoT security and DDoS attack detection, a separate line of research has explored the potential of feature fusion approaches for enhancing intrusion detection performance. The study in [89] reviewed data fusion approaches in network intrusion detection systems. They proposed evaluation criteria to compare different fusion techniques and identified open challenges such as dealing with high-dimensional data and complex attacks. Their work highlighted the potential of fusion methods to improve detection accuracy by combining complementary feature sets. Similarly, [90] surveyed data fusion techniques for IoT applications across smart homes, grids, and transportation domains. They specified requirements for secure and private IoT data fusion and then evaluated existing approaches against those criteria. The emphasis was on multisource data integration while addressing privacy and security risks through potential solutions.

This paper specifically targeted surveys focused on DDoS attack detection in IoT networks to gain insights into the essential topics requiring coverage. However, it is noteworthy that many existing surveys tend to emphasize general IoT security rather than prioritizing the unique challenges associated with detecting DDoS attacks in IoT networks through DL models and feature fusion approaches. This paper argues that prioritizing the detection of DDoS attacks is crucial because of its significant impact on the internet.

### 3. METHODOLOGY

This paper follows a four-phase methodology: (1) search, (2) screening, (3) eligibility, and (4) analysis. Fig. 3 illustrates the methodology process flow of the various steps taken in the survey procedure.

#### 3.1 Search Phase

The first phase focused on searching for relevant papers using the Scopus database, selected specifically for its unparalleled coverage of over 76 million records spanning a wide range of disciplines [19][63]. Scopus provides access to an extensive collection of relevant technical and scientific studies. In contrast to the systematic review in [11], which searched multiple databases, this study focused exclusively on the Scopus database. A precisely constructed Boolean search query using relevant keywords and operators was used to locate relevant papers: "(DDoS AND detection AND IoT AND deep learning) OR (distributed denial of service AND detection AND internet of things)". Executing this search query resulted in an initial set of 455 papers for screening and further analysis.

#### 3.2 Screen Phase

In the screening phase, the titles and abstracts of the 455 retrieved papers were quickly scanned. Since only one database (Scopus) was searched, no duplicate removal step was necessary. After quick title and abstract screening, 235 potentially relevant papers were identified for further in-depth eligibility assessment.

### 3.3 Eligibility Phase

In the eligibility phase, the full texts of the 235 relevant papers were reviewed in depth to further filter the papers and thoroughly assess their suitability and quality for inclusion in the final analysis. The inclusion criteria stipulated that studies be peer-reviewed journal articles published between 2013 and 2023 and written in English. The date range was chosen to focus the review on current advancements in the research area. Moreover, the papers had to present original research examining the application of DL techniques to detect DDoS assaults in IoT networks. Several exclusion criteria were also applied to filter out papers that were not relevant to this review. Literature review papers were excluded because they specifically analysed original experimental studies. Papers not focused on IoT networks or not examining DDoS attacks in the field of IoT were excluded because of lack of relevance to the review. Additionally, papers that did not focus on DL techniques were also excluded. Furthermore, after applying all the criteria, the first directly relevant papers were published in 2020, indicating that DL for DDoS detection in the IoT is a relatively new but rapidly growing research subdomain. The rigorous application of the screening criteria resulted in the exclusion of 200 papers, leaving 35 high-quality papers that passed all aspects of the assessment for inclusion in the final in-depth analysis phase.

### 3.4 Analysis Phase

The final set of 35 eligible papers was analysed in depth to extract key technical details, assess the effectiveness of the techniques used, and synthesize findings across the studies. Specifically, the DL methods utilized, the performance of the models, limitations, and directions for future work were extracted, compared, and consolidated. This rigorous analysis phase helped in generating insights into the use of DL for DDoS detection in IoT networks.

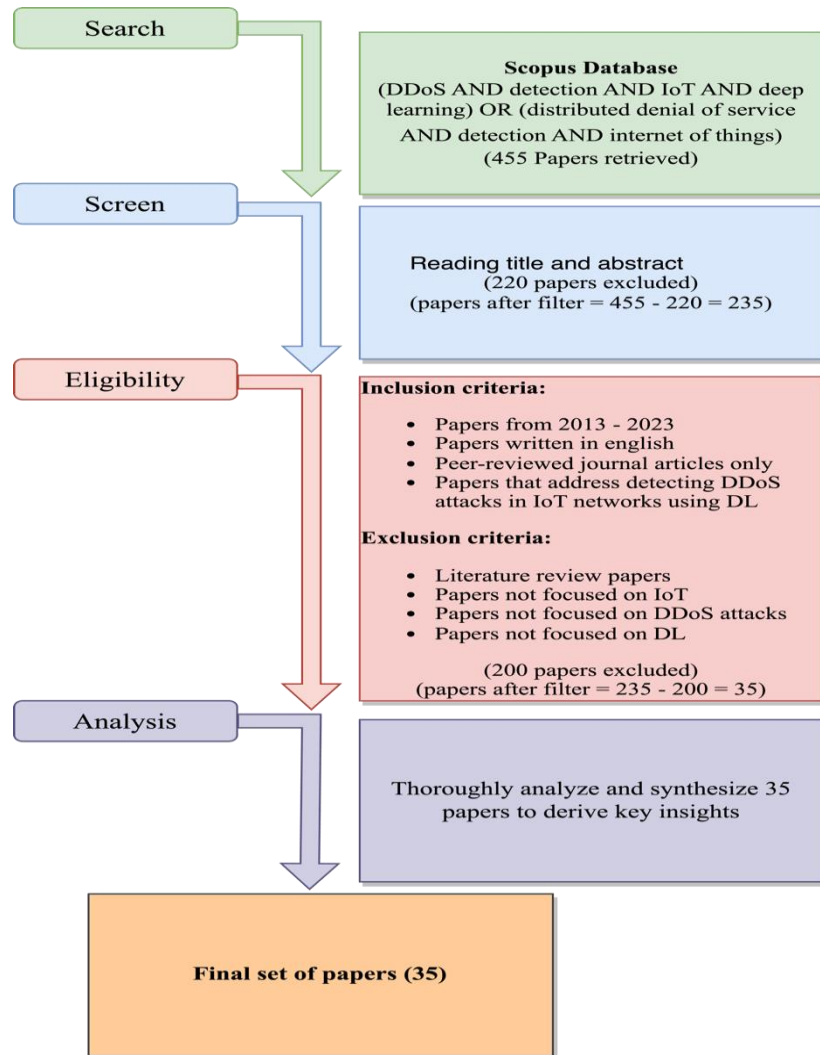


Fig. 3. Methodology process flow

## 4. OVERVIEW OF DDoS ATTACKS

This section provides an overview of DDoS attacks. In a DDoS attack, the victim is flooded with incoming traffic from various sources, making it challenging to halt the attack by blocking a single source [18][20]. Web servers, network infrastructure devices, and application servers are typical targets of DDoS attacks, with the key goal of overwhelming and crashing the target, causing a denial of service for authorized users [21]. The motives behind DDoS attacks include cyber vandalism, revenge, competition elimination, ideological belief, cyber warfare, and extortion [3][21]. With the proliferation of insecure network-connected devices in the expanding IoT landscape, DDoS attacks can now have crippling effects on organizations. Fig. 4 shows the types of DDoS attacks.

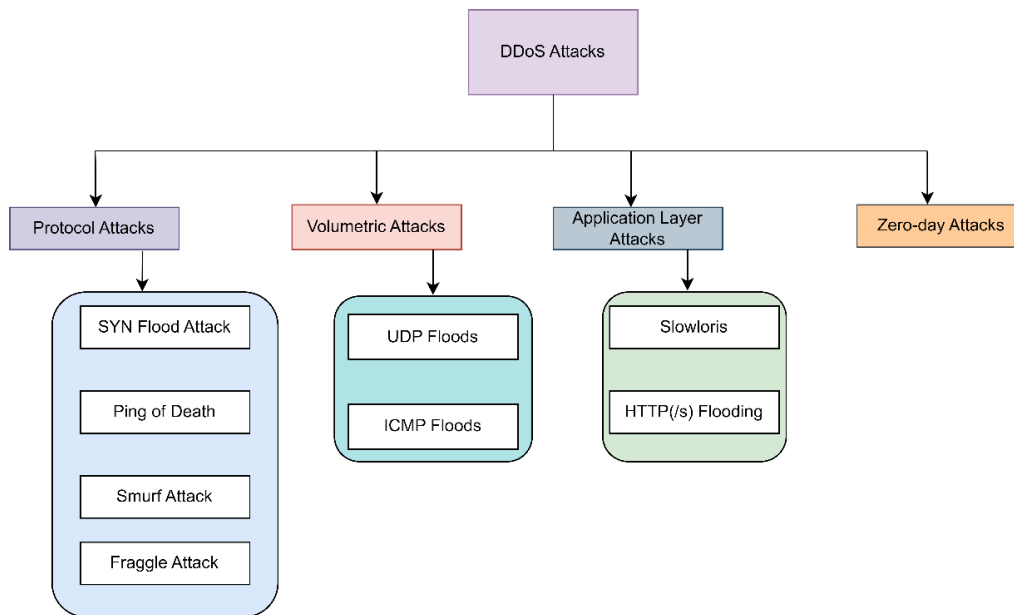


Fig. 4. Types of DDoS Attacks

### 4.1 Protocol Attacks

Protocol attack vectors attempt to consume excessive resources on the target by exploiting inherent weaknesses in communication protocols such as TCP, UDP, and ICMP [22]. They send specially crafted malicious packets that incur expensive processing costs for the victim for decoding and error handling. Some examples of protocol attacks include SYN flood, ping of death, smurfing, and fraggle attacks.

#### 1) SYN flood attack

The SYN flood is a type of attack that exploits vulnerabilities in the TCP three-way handshake process used to establish connections. Normally, a client initiates a TCP connection by sending an SYN packet to the server. The server responds with a SYN-ACK packet, and the client confirms with an ACK packet, completing the three-way handshake and establishing the connection. However, in an SYN flood attack, the attacker continuously bombards the target server with a stream of SYN packets from spoofed source IP addresses. The server, which is unaware of the spoofing, allocates resources and sends back SYN-ACK packets for each incoming SYN packet. However, since the source IP addresses are fake, the attacker never responds with the final ACK packets needed to complete the connections. As a result, the server's resources become increasingly consumed by an accumulation of half-open connections, eventually leading to resource exhaustion and an inability to accept legitimate connection requests [23].

#### 2) Ping of death attack

The ping of death attack involves sending malformed or oversized ping packets to the target. The ICMP protocol allows a maximum packet size of 65,535 bytes [24]. The attacker breaks this limit and sends "jumbo" pings that, when reassembled

on the target system, can reach millions of bytes. This causes the target system to freeze, crash, or reboot due to buffer overflows. Firing to process these large packets also consumes large amounts of CPU resources [22].

### 3) Smurf attack

In a Smurf attack, the attacker exploits the internet Control Message Protocol (ICMP), which is a fundamental protocol used to send echo requests, commonly known as "pings," across network segments. The attacker forges ICMP echo request packets, altering the source IP address to that of the victim. These packets are then sent to the broadcast address of a large network. This results in all the hosts on that network responding to the ICMP request and flooding the spoofed IP address (the victim) with echo response traffic [25]. The amplification effect of using broadcast addresses consumes significant bandwidth and overloads victim resources [26]. The scale of the attack traffic can overwhelm the victim's network capacity and exhaust computational resources such as CPU and memory as the victim attempts to process the influx of packets. Even if the victim's network does not go down entirely, the attack can severely degrade network performance and availability.

### 4) Fraggle attack

The Fraggle attack has the same concept as the Smurf attack, except it uses UDP instead of ICMP. The attacker sends large amounts of spoofed UDP traffic to the broadcast address of intermediate networks. This causes amplification flooding of the victim with UDP response traffic. The Fraggle attack is more potent than the Smurf attack because UDP networks are often much larger than ICMP networks [21][25].

## 4.2 Volumetric Attacks

Volumetric attacks aim to flood a target with an overwhelming amount of traffic that exceeds its available bandwidth capacity [26]. These attacks cause network congestion, slow down legitimate traffic and ultimately lead to denial of service when the infrastructure becomes overloaded. Some major types of volumetric attacks are UDP and ICMP floods.

### 1) UDP flood

A UDP flood attack involves sending a continuous massive volume of UDP packets to random ports on the victim system. The attacker spoofs the source IP address of the UDP packets to hide the source and make blocking difficult. When the target receives this flood of UDP packets, its network stack must determine which application is mapped to each destination port. However, since the ports are random, no application is listening to those ports [21]. However, the operating system still consumes resources to generate ICMP responses for unreachable ports and check port-to-application mappings. When the volume of malicious UDP packets sent by the attacker grows exponentially, it overwhelms the target system's capacity to process legitimate traffic, resulting in a denial of service conditions where the target becomes unresponsive to legitimate users and requests. [22].

### 2) ICMP flood

In an ICMP flood attack, the attacker spoofs multiple random source IP addresses and sends a high volume of ICMP echo request packets (pings) to the target. The target system allocates resources to confirm receipts and respond with ICMP echo reply packets for each incoming request. The attacker uses randomized spoofed source IP addresses so that the target cannot identify and block a single attack source [24]. This forces the target to respond to the flood of ping requests, consuming its available bandwidth and overwhelming the ICMP processing modules. The result is that the target is unable to handle valid ICMP and UDP traffic, thereby causing a denial of service [3].

## 4.3 Application Layer Attacks

Application layer DDoS attacks target web server resources, databases, APIs, and applications that run on the infrastructure [25]. They attempt to crash applications by depleting resources such as CPU, memory, sessions, and concurrency. Some major types of application layer attacks include the following:

### 1) Slowloris

Slowloris is a stealthy form of HTTP DDoS attack that opens multiple connections to the target web server and slowly sends partial HTTP requests to keep these connections open indefinitely. It does not rely on flooding the target with traffic but instead utilizes carefully crafted headers and minimal bandwidth to hold connections open as long as possible. By opening thousands of connections from multiple sources and dripping minimal traffic to maintain them, Slowloris can exhaust the concurrent connection limit of the target web server without sending significant volumes of data. The persistent

connections overwhelm the server's ability to respond to legitimate traffic without being detected by conventional rate-based DDoS protection [27].

## 2) HTTP flooding

HTTP flood attacks aim to overwhelm web servers and applications by saturating them with HTTP or HTTPS requests (depending on the protocol used). The most basic HTTP flood attack simply involves sending a very high volume of GET or POST requests to a web application in a short period. This deluge of requests exceeds the target's capacity to handle them, causing denial of service to legitimate users [20].

## 4.4 Zero-day Attacks

A zero-day DDoS attack utilizes an unknown vulnerability in systems and devices to rapidly infect them with malware and add them to a powerful botnet army. Attackers can therefore swiftly build an extremely large network of compromised devices under their control. They then use this massive botnet to overwhelm a target with junk traffic and take down its servers or online services through bandwidth overloading or resource exhaustion [3]. As the vulnerability is unknown when an attack occurs, the target has had zero days to patch systems or implement specific protections. Instead, defenders are forced to rely on general mitigation techniques such as traffic scrubbing and filtering [20].

## 5. DEEP LEARNING TECHNIQUES FOR DDoS DETECTION IN IoT NETWORKS

This section describes the DL techniques used for DDoS attack detection in IoT networks. It aims to perform a rigorous analysis of the diverse array of DL techniques that have recently emerged for detecting DDoS attacks in IoT networks. Many valuable studies proposing DL solutions for strengthening security in IoT networks remain outside the scope of current literature surveys on this crucial topic. More recent research has progressively applied DL architectures and techniques for DDoS detection in IoT networks. This study examines the latest research in this field by categorizing the works based on the DL models and approaches employed. Table II summarizes recent research on DL techniques for DDoS attack detection.

TABLE II. RECENT RESEARCH ON DL TECHNIQUES FOR DDOS ATTACK DETECTION

Ref	Year	Aim	Method	Dataset	Performance (Accuracy)	Limitations
[64]	2024	To develop a lightweight IDS framework which uses Modified Gated Recurrent Units (mGRU) stacked for the detection of DDoS attacks within healthcare applications and services that require timely responses.	Stacked Modified GRU (mGRU)	CIC-IoT2023	Binary classification: 98.10% Multiclass classification: 99.80%	The absence of a standard dataset for healthcare-related DDoS attacks means that the proposed IDS was tested on IoT datasets which do not accurately reflect the unique challenges of the healthcare domain.
				CIC-DDoS2019	Binary classification: 99.30% Multiclass classification: 99.60%	
[65]	2024	To propose a method called MRFM (Multidimensional Reconstruction and Function Mapping), designed for timely DDoS attack detection in IoT networks.	Multidimensional Reconstruction Encoder (MrE) with Function Mapping	CIC-DDoS2019	99.07%	The resource requirements of implementing MRFM, such as computational power and memory, have not been fully addressed.
				BOT-IoT	99.81%	
[83]	2024	To improve DDoS attack detection in IoT networks	Hybrid CNN and LSTM	CIC-IoT2023	Binary classification: 99.99% Multiclass classification: 99.96%	The study, while demonstrating promising results, does not fully address the trade-off between accuracy and efficiency, which could limit its immediate applicability in resource-constrained or time-sensitive environments.
				TON-IoT	Binary classification: 98.75%	
[28]	2023	To propose a robust DDoS attack detection technique for a secure IoT network using a piecewise Harris Hawks optimizer with a DL classifier (PHHO-ODLC).	PHHO-ODLC, ABiLSTM, and GWO	BOT-IoT	Binary classification: 99.20% Multiclass classification: 98.83%	The study only evaluated the method on BoT-IoT dataset without comparing it to other existing datasets. Thus, the findings cannot be



						generalized to other data samples.
[29]	2023	To introduce a novel technique for securing IoT networks by integrating dynamic counterbased methods into SDN architecture, alongside DL architectures.	dynamic counterbased approach and LSTM	CIC-DDoS2019	99.8%	There is a lack of IoT traffic in the CIC-DDoS2019 dataset.
[30]	2023	To propose an IDS based on a Conditional Tabular Generative Adversarial Network (CTGAN) for detecting DDoS and DoS attacks on IoT networks.	CTGAN	BOT-IoT	LSTM = 97.8% RNN = 69.3% GRU = 69.5%	The study only considered 2 types of attacks that use UDP and TCP protocols, which are the most common protocols used in these attacks. However, it did not explore other DDoS attacks that use other protocols for such attacks.
				Syntactic tabular dataset	LSTM = 99.4% RNN = 98.6% GRU = 98.1%	
[31]	2023	To make use of DL in detecting DDoS attacks in IoT environments.	CNN-BiLSTM	CIC-IDS2017	99.76%	The authors used a simulated dataset that does not necessarily reflect real-world IoT network traffic and DDoS attacks.
[32]	2023	To develop an advanced intrusion detection model capable of identifying various types of DDoS attacks through a hybrid deep learning methodology, aiming for high performance.	Hybrid (CNN, LSTM, Deep autoencoder, and DNN)	CIC-DDoS2019	80.75%	The proposed model is composed of several submodels and levels, which makes it complex and computationally intensive.
[33]	2023	To propose an edge heterogeneous IoT (HetIoT) IDS capable of detecting a range of DDoS attacks with learning techniques.	Hybrid CNN and LSTM	CIC-DDoS2019	F1-score = 100%	The disparity in how the data is distributed between the training and testing dataset can negatively impact the accuracy for certain classes or categories.
[34]	2023	To propose an efficient intelligent IDS for heterogeneous IoT using a CNN.	HetIoT-CNN IDS	CIC-DDoS 2019	Binary class = 99.75% Multiclass (8) = 99.95% Multiclass (13) = 99.99%	The method used in the study is based on a 1D-CNN model, which is simple and efficient. However, it does not fully account for the spatial dependencies present in network traffic features.
[35]	2023	To propose an intelligent, network-level IDS aimed at safeguarding IoT networks against DDoS attacks.	S-SL	BOT-IoT	99.96%	The substantial computational resources required to transform each network traffic flow into an image representation negatively impacts the efficiency and performance of the proposed solution.
				LATAM-DDoS-IoT	86.11%	
[36]	2023	To develop a new technique for DDoS attack detection in IoT network, this approach combines ensemble learning techniques with a snake optimizer algorithm.	DDAD-SOEL	BOT-IoT	99.76%	The study utilized deep learning models that demand substantial computational resources and memory, rendering them impractical and inefficient for deployment on IoT edge devices with constrained processing power and limited memory capacities.
[37]	2023	To propose a lightweight IDS for DDoS detection in IoT networks using ML classifiers.	ML and DL	BOT-IoT	ANN = 95% LSTM = 95%	The proposed method cannot identify new or unknown attacks.
				TON-IoT	ANN = 99% LSTM = 99%	
[4]	2023	To develop a resilient NIDS capable of accurately detecting previously unseen DoS and DDoS attacks in IoT networks,	SOCNN, LOF, and iNNE	CIC-IDS-2017	F1-score = 91.68%	Compared to supervised learning approaches, it exhibits a higher false positive, potentially
				CIC-IDS-2018	F1-score = 96.07%	

		while also providing defense against adversarial attacks.		BOT-IoT	F1-score = 98.94%	undermining its practical utility in real-world deployment scenarios.
[38]	2023	To propose an innovative approach for identifying DDoS attacks in IoT environments, leveraging an optimized Elman Recurrent Neural Network (ERNN) enhanced by Chaotic Bacterial Colony Optimization (CBCO).	CBCO - ERNN	BoT-IoT	99.02%	The study does not evaluate the scalability of the proposed method when dealing with large-scale and dynamic IoT networks with heterogeneous devices and protocols.
				CIC-IDS2017	98.49%	
				CIC-DDoS2019	98.29%	
				IoTID20	98.64%	
[39]	2023	To develop a new method for DDoS attack detection in the IoT environments using LSTM and BCO.	BCO-LSTM	BOT-IoT	98.75%	The BCO algorithm has a low convergence rate because it does a lot of random searches and inner iterations.
				CICIDS2017	95.38%	
[40]	2023	To develop a light and transparent decentralized IDS approach, called OPTIMIST, that can detect high and low DDoS attacks.	LSTM	Own generated	98.40%	The proposed IDS model requires sufficient memory and computation power to run on IoT devices.
[41]	2023	To develop a new DL-based method to detect DDoS attacks in smart farming systems.	Hybrid CNN and Bi-GRU	APA-DDoS	99.35%	The study did not conduct validations with different performance metrics to evaluate the effectiveness of the proposed IDS.
				ToN-IoT	99.71%	
[42]	2023	To propose an IDS incorporating DL model tailored for Agriculture 4.0	Hybrid CNN-LSTM	CIC-DDoS2019	100%	The dataset used does not reflect the real smart agricultural environment.
[43]	2023	To propose an efficient hybrid DNN model that combines a CNN and LSTM architecture for DDoS attack detection in Software-Defined IIoT networks.	Extreme Gradient Boosting with hybrid CNN & LSTM	CIC-DDoS2019	99.50%	The performance of the model on the dataset might not generalize to other network environments or attack scenarios not covered by the dataset.
[44]	2023	To enhance the security of Smart Grids by proposing a hybrid DL algorithm for detecting DDoS attacks.	Hybrid CNN and GRU	CIC-IDS2017	99.70%	The study's simulations are based on a benchmark dataset and do not account for the dynamic and unpredictable nature of actual cyberattack scenarios in operational Smart Grids.
[45]	2022	To develop a technique that employs blockchain and DL to safeguard the smart transport system from various cyberattacks.	Hybrid AE and MLP	CIC-DDoS2019	F1-score = 95% - 100%	The study did not analyse the scalability of the approach when dealing with large-scale and high-dimensional network data.
				CIC-IDS2017	F1-score = 94%	
				BOT-IoT	F1-score = 95%	
[46]	2022	To propose a Protocol Based Deep Intrusion Detection (PB-DID) architecture for detecting DoS and DDoS attacks in IoT networks using DL.	PB-DID	BOT-IoT, UNSW-NB15	96.3%	The study only used TCP and flow features from the datasets, which do not capture the complete network traffic and protocols prevalent in IoT networks.
[47]	2022	To propose a hybrid DL framework for DDoS attack detection in IoT-SDN network	MWOA-LSTM	NSL-KDD	98.37%	The study did not evaluate the robustness of the proposed method against adversarial attacks.
				CSE-CIC-IDS2018	99.84%	
				Own generated	99.48%	
[48]	2022	To introduce a novel approach for detecting botnet attacks, designed for fog computing environments, that leverages the programmable nature of SDN	Hybrid DNN and LSTM	N-BaIoT	99.98%	The study only focuses on bottleneck detection and does not address other security issues in IoT.
[49]	2022	To propose a novel algorithm named DALCNN to detect DDoS attacks in IoT using RNN and implementation of SDN using the OpenDayLight platform	DALCNN	NSL-KDD	99.98%	The study only considered a limited range of DDoS attacks, which affects the generalizability and validity of the results.
[50]	2022	To propose a hybrid algorithm that integrates a Sample Selected	SSRNN-ELM	NSL-KDD	99.2%	The employed dataset is obsolete and fails to capture

		Recurrent Neural Network (SSRNN) with an Extreme Learning Machine (ELM) for DDoS attack detection in IoT networks.				the contemporary and realistic attributes of IoT network traffic patterns and the evolving nature of DDoS attack vectors.
[51]	2022	To propose a deep intelligent DDoS attack detection scheme for fog-based IoT applications.	DI-ADS	DDoS-SDN	99.44%	The use of a single dataset in the study introduces challenges regarding the generalizability of the model.
[52]	2022	To propose a hybrid DL-based IDS for IoT networks using generative adversarial network (GAN) and binary particle swarm optimization (B-PSO)	HD_GAN	NSL-KDD	99.02%	The dataset used in the study has no IoT traffic included, therefore, restricting the model's capability to detect emerging IoT-based threats.
[53]	2022	To propose a method for detecting DoS and DDoS attacks in IoT networks using ML and DL algorithms.	SAD-IoT	Bot-IoT for training, and own generated for testing	DL (multiclass neural network) = 99.5% Stacked ML (KNN, NB, DT, RF) = 99.6%	The study did not evaluate the potential ramifications of adversarial attacks on the performance and robustness of the proposed SAD-IoT
[54]	2022	To propose a DL-based method to detect low-rate DDoS attacks for IoT network-based SDN.	LSTM	Edge-IIoTset	98.8%	While the employed dataset provides a comprehensive and realistic representation of IoT applications, it does not encompass all potential scenarios and variants of DDoS attacks that may target IoT networks.
[55]	2022	To design a model based on DL that can identify and prevent DDoS attacks on SIP-based multimedia transmission in mobile networks	Stacked autoencoder	Own generated	97.40%	The study only focuses on a few types of DDoS attacks.
[56]	2022	To propose an autonomous defense system that combines edge computing with a two-dimensional CNN to detect and prevent DDoS attacks on the IoT	2D CNN	Own generated	Packet traffic dataset = 99.5% Packet feature dataset = 99.8%	The dataset generated from the experimental network affects the generalization and robustness of the system.
[57]	2021	To create a hybrid DL framework for identifying replay and DDoS attacks within a smart city infrastructure.	Hybrid RBM and CNN	Environmental Smart river Smart soil	98.37% 98.13% 99.51%	The study used simulated cyber-attacks on a real smart city dataset, which does not necessarily reflect the actual behavior and impact of real attackers in a smart city environment
[58]	2021	To propose and evaluate three DL-based IDS for detecting DDoS attacks in Agriculture 4.0, which is the integration of advanced technologies into existing farm operations	CNN, DNN, and RNN	CIC-DDoS2019  TON-IoT	Binary classification: CNN = 99.95% DNN = 99.93% RNN = 99.94% Multiclass (7 class): RNN = 94.99% DNN = 94.91% CNN = 95.90% Multiclass (13 class): CNN = 95.12% DNN = 93.88% RNN = 94.88%  Multiclass CNN = 99.92% RNN = 98.94% DNN = 98.93%	The study only considered some types of DDoS attacks, while other types of DDoS attacks can affect the model.
[59]	2020	To develop an IDS for identifying attacks and anomalies in the IoT environment, using a DL-based method called the Deep Belief Network (DBN) algorithm	DBN	CIC-IDS2017	96.67%	The study relied on a single dataset. Additional datasets should be utilized to validate findings.

[60]	2020	The objective is to develop a security framework that can operate in near real-time within SDN environments. This framework aims to mitigate DDoS attacks launched from compromised internal devices, such as IoT devices that have been co-opted into botnets.	CNN	Own generated	99.9%	The study only tested the proposed system on a simulated environment with a limited number of hosts and DDoS attack types. Therefore, the results will not reflect the performance of the system in a real-world scenario.
				CIC-DDoS2019	95.4%	
[61]	2020	To propose methods to detect and prevent DoS and DDoS attacks in IoT networks.	LSTM	CIC-DDoS2019	99.19%	The study did not provide details on the implementation and deployment of the IDS and the DL models in a realistic IoT system, which limits the practicality of the proposed solutions.

As shown in Table II, numerous studies have effectively employed hybrid DL techniques, combining different methods to enhance DDoS attack detection in IoT networks. Elsaedy et al. [57] uniquely combined unsupervised restricted Boltzmann machines (RBMs) for generic traffic feature discovery and convolutional neural networks (CNNs) for temporal analytics to offer interpretable DDoS detection for smart city IoT assets. RBM density modelling trains robustly on small heterogeneous datasets for initial information distillation, thereby enabling CNN sequence learning. Evaluations of three distinct synthesized datasets of environment, river, and soil monitoring IoT networks infected with simulated DDoS attacks reported that the proposed method achieved a detection accuracy greater than 98%, outperforming standalone ML and DL approaches. The integrated approach hence demonstrates the value of hybrid tuning to match security assurance needs for diverse city infrastructures. The authors could further investigate the integration of feature fusion techniques within their hybrid framework, potentially combining features extracted by the RBM with additional domain-specific features to capture a more comprehensive representation of the IoT network behavior, which may lead to even higher detection accuracy.

Aswad et al. [31] proposed a hybrid DL architecture fusing a CNN for automatic spatial traffic data feature extraction with bidirectional LSTM networks with intrinsic sequence learning capabilities for enhanced attack pattern modelling. Tested for DDoS detection over the contemporary CICIDS2017 intrusion repository, the CNN-BiLSTM framework achieves 99.76% accuracy and 98.90% precision, surpassing standalone or ensemble alternatives of CNN, LSTM, and RNN architectures.

Additionally, Aldhyani & Alkahtani[42] introduced a hybrid DL intrusion detection framework that combines a CNN that automatically learns informative features from raw traffic data with LSTM recurrent networks that analyse temporal correlations in the extracted representations. Evaluated on the CICDDoS2019 benchmark containing diverse DDoS attacks on IoT networks, the CNN-LSTM model attained 100% detection accuracy across all threat types, outperforming state-of-the-art alternatives.

Furthermore, Diaba & Elmusrati[44] introduced a hybrid DL algorithm that pairs CNNs and gated recurrent units (GRUs) for real-time DDoS attack identification in a smart grid communication infrastructure. The GRU specializes in modelling longer-term sequential dependencies through gating mechanisms, while the CNN extracts spatial features. Validated over the CICIDS2017 dataset, the integrated CNN-GRU model achieves 99.70% accuracy, demonstrating hybrid tuning benefits for critical infrastructure protection against cyber threats.

Moreover, Liu et al. [45] integrated a DL-based anomaly detector combining autoencoders (AEs) for learning compressed threat traffic representations and multilayer perceptron networks (MLPs) for final attack classification. Evaluations using the CICIDS2017, CICDDoS2019, and BOT-IoT datasets prove 95-100% effectiveness across diverse DDoS attacks, affirming their applicability against evolving threats. Uniquely, blockchain mechanisms are also incorporated for secure and trustworthy anomaly data sharing with layered cyber-physical resilience. This underscores the pervasive need for multifaceted cybersecurity advancements that shield IoT networks.

Beyond hybrid techniques that combine multiple DL methods, extensive research has examined LSTM models for their exceptional capacity in sequential modelling and learning long-term dependencies prevalent in traffic classification [62]. Cherian & Varma [29] proposed an SDN framework for IoT networks that leverages a dynamic counterbased approach alongside LSTM architecture to detect and mitigate various DDoS attack types. The framework utilizes a dynamic counterbased mechanism to analyse network traffic and detects zero-day DDoS attacks based on abnormal counter values. This approach enables the detection of the latest DDoS variants and reduces the workload on the SDN controller. An LSTM model trained on the CICDDoS2019 dataset is utilized to enhance the detection capabilities. The LSTM model demonstrated over 99% detection accuracy across all attack types with minimal false positives. By combining counterbased filtering and the LSTM model, the framework provides superior detection efficiency and accuracy for securing IoT networks against different types of DDoS attacks.

Additionally, Alashhab et al. [54] developed a DL-based low-rate DDoS (LDDoS) attack detection technique employing an LSTM model for software-defined IoT networks. They implemented an experimental SDN-IoT testbed and simulated LDDoS attacks by generating legitimate OpenFlow protocol messages. A recurrent neural network (RNN) is utilized to classify network traffic as either malicious or benign. The LSTM model achieves a highly accurate LDDoS detection rate of 98.88% using the Edge-IoTset dataset containing recent cybersecurity attacks in IoT networks. The proposed methodology is shown to be highly effective for SDN-based IoT platforms to identify stealthy LDDoS attacks that avoid detection by traditional signature-based IDS.

Moreover, Ragab et al. [28] proposed a framework for DDoS attack detection in IoT networks by integrating feature selection, DL classifiers, and hyperparameter optimization. A piecewise chaotic Harris hawks optimization (PHHO) algorithm is used for selecting the most important features from the IoT traffic data. An attention-based bidirectional LSTM (ABiLSTM) architecture then leverages the sequential patterns in the filtered data to accurately categorize normal and attack traffic. Additionally, grey wolf optimization further tunes the ABiLSTM hyperparameters to improve the detection performance. Evaluation on the BOT-IoT dataset demonstrated accuracies of 99.20% and 98.83% for binary and multiclass classification, respectively. To further enhance the detection capabilities, the authors could explore feature fusion techniques, combining the selected features with additional relevant features from other data sources, potentially leading to even higher accuracy rates.

Alamer & Shadadi[39] developed a novel DDoS attack detection technique for IoT networks using LSTM and bacterial colony optimization (BCO) algorithms. LSTM is leveraged to learn long-term dependencies from network traffic data. BCO is a metaheuristic optimization strategy based on bacterial behavior. The integrated BCO-LSTM methodology uses BCO to optimize the architectural parameters of the LSTM model. The BoT-IoT and CICIDS2017 datasets containing different DDoS attack types were used for training and testing the model. The results demonstrate that BCO-LSTM achieves accuracies of 98.75% and 95.38% on the BOT-IoT and CICIDS2017 datasets, respectively. These results show that BCO-LSTM can effectively profile normal and abnormal traffic patterns in IoT networks. The incorporation of feature fusion techniques, such as combining features from multiple data sources or extracting higher-level features, could further improve the accuracy of the BCO-LSTM model.

While LSTM's sequential process shrinks for temporal pattern recognition, convolutional neural networks (CNNs) also garner significant attention because of their poor ability to automatically learn informative features from raw input data. Accordingly, Mahadik et al. [34] proposed an efficient and intelligent IDS leveraging a CNN for safeguarding heterogeneous Internet of Things (HetIoT) environments against various DDoS attack types. The proposed HetIoT-CNN IDS is evaluated on the CICDDoS2019 dataset containing DDoS attack traffic. Both binary and multiclass (8 and 13 attack categories) classifications are performed and compared to prior DL strategies. The results demonstrate that the proposed HetIoT-CNN IDS achieves significantly higher accuracy in identifying all classes of DDoS threats, reaching 99.75%, 99.95%, and 99.99% for the three classification tasks, respectively.

Nguyen & Kim-Hung [4] developed a robust network intrusion detection system (NIDS) for IoT networks that integrates a soft ordering convolutional neural network (SOCNN) architecture with outlier detection algorithms. The combined approach is evaluated using the BoT-IoT, CIC-IDS2017, and CIC-IDS2018 datasets, which contain different cyber attack scenarios and normal traffic. The results demonstrate that the SOCNN model in conjunction with isolation forest and influence function-based outlier detection can accurately identify DoS and DDoS attacks, including zero-day attack variants, attaining F1 scores greater than 98.94%, 91.68%, and 96.07% on the BoT-IoT, CIC-IDS2017 and CIC-IDS2018 datasets, respectively. However, the false alarm rates are higher than those of supervised classifiers, which is an area that needs improvement. One potential avenue for reducing false alarms and further enhancing detection performance is the application of feature fusion techniques, which could provide a more comprehensive representation of network traffic patterns.

Almaraz-Rivera et al. [35] introduced a novel self-supervised learning (S-SL) paradigm for network IDSs to protect IoT environments against DDoS attacks. Synthetic image representations of network traffic from the BOT-IoT and LATAM-DDoS-IoT datasets are generated. Without explicit attack labels, contrastive learning is employed on top of pretrained ImageNet weights to construct discriminative traffic embeddings in a completely unsupervised manner. Impressively, the S-SL approach achieves attack detection accuracy equivalent to or greater than that of supervised learning baselines, even with minimal labelled samples for fine-tuning. Specifically, accuracies of 99.96% and 86.11% are attained on the BOT-IoT and LATAM-DDoS-IoT datasets, respectively.

While CNN and LSTM models individually achieve formidable detection performance, assembling ensemble systems that aggregate multiple models can further boost accuracy and robustness. Accordingly, Aljebreen et al. [36] proposed a novel DDoS attack detection system named DDAD-SOEL that uses a snake optimization algorithm alongside an ensemble of DL architectures. The approach first selects the most relevant subset of features from the Bot-IoT dataset containing both benign and attack traffic using the snake optimization method. The filtered features are input to an ensemble of LSTM, bidirectional LSTM, and deep belief network models for efficient multiclass attack classification. Moreover, the Adadelta optimizer tunes

the neural network hyperparameters during the training process for enhanced detection. The evaluation demonstrated that the proposed DDAD-SOEL framework achieved a significantly improved accuracy of 99.76%.

Kumar et al. [53] proposed a novel method called SAD-IoT that utilizes both machine learning and DL algorithms to accurately detect DoS and DDoS attacks in IoT networks. The authors use the Bot-IoT dataset from the UNSW Canberra Cyber for training their models and generate their dataset with a 20-device testbed for testing purposes. Through extensive experimentation with various machine learning and deep neural network architectures, the authors determined that the stacking ensemble method with logistic regression achieves the highest accuracy of 99.61% among ML models, while a deep neural network with ReLU activation provides the highest accuracy of 99.52% for DL models in identifying DoS/DDoS attacks. The authors provide useful insights into the most relevant features and activation functions to consider for effective attack detection.

The studies reviewed in this section employ various datasets to evaluate the performance of their proposed DL techniques for DDoS attack detection in IoT networks. Table III provides an overview of available datasets on DL techniques for DDoS attack detection. The most commonly used datasets include the CIC-DDoS2019, Bot-IoT, and CIC-IDS2017 datasets, which provide a diverse range of network traffic data and attack scenarios.

TABLE III. AVAILABLE DATASETS ON DL TECHNIQUES FOR DDOS ATTACK DETECTION

Ref	Dataset	Description of the dataset	Size of the dataset (# of records)	Link of the dataset	Is it legally collected dataset?	Public/Private
[66]	CIC-DDoS2019	The Dataset was developed by the Canadian Institute for Cybersecurity (CIC). It contains real-world data representing both normal, benign network traffic as well as traffic from actual DDoS cyber-attacks. The dataset was specifically designed to capture DDoS attacks by using the CICFlowMeter tool developed by CIC. It introduces two new types of DDoS attack categories that were modelled - reflection-based attacks and exploitation-based attacks.	50,006,249	<a href="https://www.unb.ca/cic/datasets/ddos-2019.html">https://www.unb.ca/cic/datasets/ddos-2019.html</a>	Yes	Public
[67]	Bot-IoT	Researchers at the Cyber Range Lab of the University of New South Wales in Canberra curated a dataset comprising network traffic data, with some data representing normal, legitimate activities and other data representing various types of malicious attacks. This traffic data was simulated to mimic the network behavior of Internet of Things (IoT) devices operating within a smart home environment. The dataset captured malicious attack traffic such as keylogging, unauthorized data exfiltration, reconnaissance scans of operating systems and services, as well as denial of service (DoS) and distributed denial of service (DDoS) attacks. A notable characteristic of this dataset is its imbalanced nature, where the number of benign traffic samples is relatively small compared to the significantly larger volume of records representing malicious traffic.	73,370,443	<a href="https://research.unsw.edu.au/projects/bot-iot-dataset">https://research.unsw.edu.au/projects/bot-iot-dataset</a>	Yes	Public
[68]	CIC-IoT2023	The dataset is a collection of network traffic data from 105 diverse IoT devices, focusing on various attack scenarios in real-world IoT environments. This dataset captures a wide range of attacks that occur in real-world IoT networks. It comprises 47 features that describe both benign traffic and seven distinct categories of attacks: DDoS, DoS, Reconnaissance, Web-based attacks, Brute Force attacks, Spoofing, and Mirai. By providing a comprehensive set of features and a variety of attack types, the CIC-IoT2023 dataset enables researchers to develop and evaluate intrusion detection systems that can effectively identify and mitigate threats in contemporary IoT environments.	46,686,579	<a href="https://www.unb.ca/cic/datasets/iotdataset-2023.html">https://www.unb.ca/cic/datasets/iotdataset-2023.html</a>	Yes	Public
[69]	CIC-IDS2017	The dataset was created by the CIC, featuring various attack scenarios along with real user-generated background traffic. It includes attacks such as DoS, DDoS, Web Attack, Botnet, and Brute Force SSH. CICFlowMeter was used to extract 80 different network flow features.	2,827,876	<a href="https://www.unb.ca/cic/datasets/ids-2017.html">https://www.unb.ca/cic/datasets/ids-2017.html</a>	Yes	Public
[70]	UNSW-NB15	A dataset developed by the Australian Centre for Cyber Security captures a mix of real normal behaviors and	2,540,044	<a href="https://research.unsw.edu.au/projects">https://research.unsw.edu.au/projects</a>	Yes	Public

		synthetically generated modern cyber-attacks. It consists of 2,218,761 benign and 321,283 malicious records, including nine different attack types, and contains 49 features.		/unsw-nb15-dataset		
[71]	NSL-KDD	The NSL-KDD dataset, created in 2009 by the CIC, addresses limitations of the KDD CUP 99 dataset by eliminating duplicate and unbalanced data. However, the dataset is old and lacks recent attack types and packet-level information.	148,517	<a href="https://www.unb.ca/cic/datasets/nsl.html">https://www.unb.ca/cic/datasets/nsl.html</a>	Yes	Public
[72]	ToN-IoT	A dataset developed by UNSW Canberra IoT Labs combines data from various sources within an IIoT system. It identifies many attacks, including DDoS, and consists of 44 features grouped into four service-profile-based categories.	22,339,021	<a href="https://research.unsw.edu.au/projects/toniot-datasets">https://research.unsw.edu.au/projects/toniot-datasets</a>	Yes	Public
[73]	Edge-IIoTset	The dataset aims to support research on intrusion detection systems, particularly in evaluating the performance of federated deep learning and centralized approaches. It covers a wide range of IoT and IIoT-specific attacks, including DDoS attacks. The dataset has a nearly even split between benign and malicious instances. Each record is characterized by a rich set of 1176 features, providing a comprehensive view of the network traffic for effective intrusion detection.	20,780,120	<a href="https://ieeedataport.org/documents/edge-iiotset-new-comprehensive-realistic-cyber-security-dataset-iiot-and-iiot-applications#files">https://ieeedataport.org/documents/edge-iiotset-new-comprehensive-realistic-cyber-security-dataset-iiot-and-iiot-applications#files</a>	Yes	Public
[74]	DDoS-SDN	The dataset, sourced from Mendeley Data, is characterized by 23 attributes. It focuses on three specific types of DDoS attacks: TCP Syn flood, UDP flood, and ICMP flood. By providing a diverse set of network features, the dataset enables the development and evaluation of intrusion detection systems specifically tailored for SDN environments.	104,345	<a href="https://data.mendeley.com/datasets/jxpfjc64kr/1">https://data.mendeley.com/datasets/jxpfjc64kr/1</a>	Yes	Public
[75]	N-BaIoT	The dataset, released by the UCI Center of Machine Learning and Intelligent Systems in 2018, comprises real network traffic data collected from nine commercial Internet of Things (IoT) devices. To provide a realistic representation of IoT botnet attacks, the devices were intentionally infected with two notorious and destructive IoT botnets, Mirai and BASHLITE. The dataset is presented in CSV format and includes 115 statistical features derived from the captured traffic data. These features capture characteristics across ten different classes of attacks targeting IoT systems and devices. By incorporating real-world traffic from compromised IoT devices under the control of powerful botnets like Mirai and BASHLITE, this dataset aims to serve as a valuable resource for developing and evaluating security solutions tailored to the unique threats faced by IoT networks.	7,062,606	<a href="https://archive.ics.uci.edu/dataset/442/detection+of+iiot+botnet+attacks+n+baioot">https://archive.ics.uci.edu/dataset/442/detection+of+iiot+botnet+attacks+n+baioot</a>	Yes	Public
[76]	CSE-CIC-IDS2018	The dataset was developed due to the result of a joint effort by the Communications Security Establishment (CSE) and the CIC to create a benchmark for evaluating IDS. Carefully designed to simulate a wide range of real-world cyber threats and attacks within complex network environments, the dataset was collected over a period of ten days. It consists of 80 features and represents fifteen different attack types, such as brute force attacks on FTP and SSH, various DoS and DDoS attacks, SQL injection, infiltration, and bot activity.	16,233,002	<a href="https://www.unb.ca/cic/datasets/ids-2018.html">https://www.unb.ca/cic/datasets/ids-2018.html</a>	Yes	Public
[77]	APA DDoS-Attack	The dataset consists of data samples categorized into three distinct types: DDos-PSH-ACK, Benign, and DDos-ACK. This dataset is designed to represent various DDoS attack scenarios, with a primary focus on ACK and PUSH-ACK DDoS attacks. By providing a diverse set of DDoS attack samples alongside benign traffic, the APA-DDoS dataset enables researchers to develop and evaluate intrusion detection systems specifically tailored to detect and mitigate these types of DDoS attacks in real-world network environments.	151,201	<a href="https://www.kaggle.com/datasets/yashwanthkumbam/apa-ddos-dataset">https://www.kaggle.com/datasets/yashwanthkumbam/apa-ddos-dataset</a>	Yes	Public
[78]	IoTID20	The dataset is one of the few publicly available resources for IoT intrusion detection research, offering a realistic representation of modern IoT network communication patterns. It includes 80 network features and categorizes	625,783	<a href="https://sites.google.com/view/iiot-network-intrusion-dataset">https://sites.google.com/view/iiot-network-intrusion-dataset</a>	Yes	Public

		data into normal and anomaly classes. The anomaly category encompasses four attack types: DoS (Syn flooding), Mirai (Brute force, HTTP, and UDP flooding), MITM, and Scan (Host port and port OS).				
[79]	LATAM-DDoS-IoT	The dataset is the product of a joint effort involving Aligo, Universidad de Antioquia, and Tecnológico de Monterrey. It was generated using a specialized testbed environment explicitly designed to study Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The testbed incorporated both physical Internet of Things (IoT) devices as well as real users interacting with live services on a production network. During the data collection process, four physical IoT devices and one simulated IoT device were subjected to DDoS attack scenarios. The resulting dataset encompasses 20 distinct features, providing a comprehensive set of attributes tailored for analysing and detecting DDoS attacks targeting IoT environments.	49,666,991	<a href="https://iee-dataport.org/documents/latam-ddos-iot-dataset">https://iee-dataport.org/documents/latam-ddos-iot-dataset</a>	Yes	Public

## 6. FEATURE FUSION TECHNIQUES FOR DDoS DETECTION IN IOT NETWORKS

This section presents a comprehensive analysis of the recent feature fusion techniques proposed for detecting DDoS attacks in IoT networks. Despite the growing research on feature fusion solutions for IoT security, many significant studies remain unexamined in literature reviews. This study bridges this gap by categorizing and examining the latest research based on the employed feature fusion techniques and approaches. Table IV summarizes the utilization of data fusion techniques in DDoS attack detection in IoT networks. By combining features from multiple data sources, these techniques create a more comprehensive feature representation, enhancing the accuracy and robustness of detection models.

TABLE IV. UTILIZATION OF DATA FUSION TECHNIQUES IN DDoS ATTACK DETECTION IN IOT NETWORKS

Ref	Source data	Fusion type	Fusion techniques	Categorization of the fusion data sources	Data types of fusion	Solved challenges	Level of fusion
[80]	ToN-IoT dataset and CIC-DDoS2019 dataset	Feature-level fusion	Feature fusion using relational algebra to merge datasets	Network traffic data from IoT and IIoT devices	HTTP activity, Connection activity, DNS activity, Statistical activity, SSL activity,, TCP and UDP-based attack features	Improving the detection accuracy of ARP poisoning, SSL-based attacks, and DNS flood (DDoS) attacks by combining relevant features from multiple datasets	Feature-level fusion
[81]	NSL-KDD dataset and KDD CUP 99 dataset	Data-level fusion	N/A	Network traffic data	Network traffic data from NSL-KDD and KDD CUP 99 datasets	Improving the accuracy of intrusion detection in wireless sensor networks by using fused data.	Data-level fusion
[82]	Network traffic data and Power profiling data	Data-level fusion	Combining Power Profiling and Network Traffic data using Central Limit theorem	IoT edge device (IoT-ED) power consumption data and Network traffic data between IoT-ED and IoT gateway device (IoT-GD)	Power consumption values Number of messages per unit of time	Detecting multiple types of hardware Trojan-based attacks, including DoS attacks, in IoT-ED without requiring design time intervention	Centralized fusion at the coordinator level
[84]	NSL-KDD dataset	Multiview feature fusion	Concatenation of features extracted from knowledge graphs and statistical analysis	Features extracted by knowledge graph based on semantic relationships and Features extracted by statistical analysis based	Semantic data from knowledge graphs and Numerical/statistical data from network traffic analysis	Improving the accuracy and robustness of intrusion detection in IoT networks by combining semantic and statistical features	Feature-level fusion



				on numerical calculations and power-law distribution			
[85]	KDD CUP 99, NSL-KDD, and UNSW-NB15	Multisource data fusion	Word Embedding (WE) for mapping physical network features into feature space vectors	Network traffic data	Heterogeneous IoT data includes raw data collected by sensors, and the network sequences contain various data fields.	Difficulties in heterogeneous data preprocessing and fusion for traditional machine learning-based IDS.	Feature-level fusion
[86]	SDN-IoT	Feature-level fusion	Concatenation of features extracted from hidden layers of recurrent deep learning models (RNN, LSTM, and GRU)	Features extracted from network traffic data using recurrent deep learning models	Features extracted from network traffic data, representing various types of network attacks, including DDoS attacks	Improving the performance of network attack detection and classification by fusing features extracted from different recurrent deep learning models	Feature-level fusion
[87]	Network logs, Raw packet captures, Snort IDS logs, and power sensor readings	Multisource and multidomain fusion	Time-synchronized merge of data from multiple sources and Feature extraction and fusion of cyber and physical features.	Cyber data sources (network logs, packet captures), Physical data sources (power system measurements from DNP3 traffic)	Network traffic data and Power system measurements	Improvement in detection capabilities, handling feature explosion, data inconsistencies.	Data-level fusion
[88]	WUSTL-EHMS-2020 dataset and ICU dataset	Data-level fusion	Contractive Deep Autoencoder (CDAE) with differential privacy. The CDAE is used to correlate and fuse the data from different sources and reduce the data dimensions	Network traffic, sensor readings, and device logs.	Correlating and fusing data from different sources	Efficiently fusing and correlating heterogeneous IoMT data from multiple sources for effective attack detection	Feature-level fusion

As illustrated in Table IV, numerous studies have explored diverse feature fusion techniques for detecting distributed denial of service (DDoS) attacks in IoT networks. A prominent approach is data-level fusion, in which datasets from multiple sources are amalgamated to create a larger and more heterogeneous training dataset. For example, the study by Adnan Khan et al. [81] proposed a data fusion-based machine learning architecture that integrates the NSL-KDD and KDD CUP 99 datasets. Although not exclusively focused on DDoS attacks, the proposed real-time deep extreme learning machine (RTS-DELM) model demonstrates enhanced detection performance for various types of attacks in wireless sensor networks (WSNs). Notably, the RTS-DELM model achieves superior accuracy compared to other benchmark approaches, underscoring the efficacy of data fusion in augmenting the performance of intrusion detection systems, a technique that can be extended to DDoS attack detection in IoT networks.

Additionally, the research conducted by Mohammed et al. [82] addresses the challenge of hardware Trojan attacks in IoT edge devices through the implementation of a data fusion technique. The authors amalgamate network traffic (NT) and power profiling (PP) data via centralized fusion at the coordinator level, enabling the detection of various attack types, including DoS attacks. The proposed methodology exhibits high accuracy in identifying attacks while preserving privacy by retaining data at the local level, thereby demonstrating the efficacy of data fusion in enhancing security and privacy measures for IoT edge devices.

Feature-level fusion is another widely explored type of fusion in which features from different data sources or domains are combined to create a more informative and comprehensive feature set. Mohammed et al. [80] employed feature-level fusion to combine features from the CICDDoS2019 and ToN\_IoT datasets. The authors utilize relational algebra to merge the datasets, aiming to improve the detection of various attacks in IIoT networks. This includes DNS flooding, which is a type of DDoS attack. The proposed federated learning-based approach allows distributed IIoT nodes to collaboratively train a global model while preserving data privacy, demonstrating the benefits of feature fusion in enhancing the accuracy and robustness of DDoS attack detection.

Sahu et al. [87] explored the use of multisource and multidomain data fusion in the context of DDoS attack detection. The authors merged data from multiple sources, including network logs, raw packet captures with DNP3 traffic, and Snort IDS logs, to create a comprehensive feature set for detecting cyberattacks, including DoS attacks, in power systems. This approach addresses challenges such as handling data inconsistencies and reducing the explosion of the cyber-physical state space. This highlights the importance of multidomain data fusion in enhancing the accuracy of cyberattack detection.

Similarly, Chen et al. [85] proposed a novel approach that leverages word embedding and deep transfer learning to address the challenges of intrusion detection in heterogeneous IoT networks. The authors introduce a sample-based transfer learning method that fuses data from different source domains (the NSL-KDD, KDD CUP 99, and UNSW-NB15 datasets) by treating network sequences as sentences and applying natural language processing techniques. This approach allows for the integration of data from multiple sources without the need for extensive data preprocessing. Additionally, they employ a feature-based transfer learning method that utilizes word embedding coefficients to map the mathematical and logical features of heterogeneous network sequences into a shared feature space. This technique enables the fusion of features from different source domains, enhancing the system's ability to detect attacks across various IoT environments.

In summary, feature fusion has demonstrated promising results in enhancing the performance of DDoS attack detection systems in IoT networks. By leveraging and combining different data sources, feature sets, or models, these techniques create a more comprehensive and robust representation of the data, enabling more accurate and reliable detection of DDoS attacks in IoT networks.

## 7. CHALLENGES AND LIMITATIONS

While the studies covered in this review paper propose innovative techniques for detecting DDoS attacks in IoT networks, they also face some common challenges and limitations.

The use of public datasets for evaluating intrusion detection models in IoT networks is limited. Most were created using simulated traffic in laboratory settings. These methods lack vital protocol-specific features. They exhibit significant class imbalance. They have redundant attributes. They cover only a fraction of known attacks and provide no visibility to zero-day attacks. As such, the generalizability, efficiency, and robustness of models tuned on these datasets are questionable. These datasets are unable to accurately represent the complexity and diversity of modern real-world IoT traffic and threat models. Therefore, evaluating models on more recent, comprehensive, and balanced datasets representing complex real-world environments is a persistent challenge.

Additionally, complex hybrid DL models such as LSTM-autoencoders, CNN-RNNs, and ensemble architectures have shown promising detection capabilities, and their computational complexity makes deployment challenging for resource-constrained IoT devices. The memory, energy, and latency costs of running multiple interconnected neural network components on embedded IoT hardware can be prohibitive. As such, an open research gap exists in designing optimized shallow models that balance detection performance with feasibility for edge devices. Simplified models to retain predictive capacity while reducing the number of parameters and layers warrant further exploration.

Furthermore, most studies demonstrate model effectiveness through offline testing on datasets. However, while invaluable for initial development, offline datasets have significant limitations that must be addressed for real-world deployment. Specifically, offline data lack the diversity, scale, and noise of live production environments. Models tested solely on offline data will likely overestimate performance when faced with real-world attacks of varying intensity and patterns. Additionally, offline data reflect past behaviours and may fail to generalize to new, evolved attack types. More critically, controlled offline tests ignore many crucial real-world performance factors. There are no constraints on computational demand, system resilience, or heterogeneous hardware. Without rigorous live testing, models risk failure when transitioning from ideal offline settings to complex, dynamic production networks. These limitations clearly show the necessity of real-world testbeds to validate model effectiveness. Live testing is more likely to reveal performance gaps that are not exposed in offline testing by capturing real-world constraints that are absent in offline datasets. Thorough real-world validation will provide invaluable feedback to optimize models for reliable, efficient performance under noisy, constrained conditions.

Adversarial attacks designed explicitly to fail machine learning models are accounted for by few studies in detecting DDoS attacks in IoT networks. While DL has shown success in detecting known attacks, evaluating its robustness to deliberately engineered inputs and perturbations is lacking. Testing against evasion, poisoning, spoofing, encrypted payloads, and noise injection can reveal blind spots. Zero-day attacks using generative models can craft adversarial samples misclassified by detection models.

An additional challenge arises with feature fusion techniques that combine multiple feature sets for improved detection performance. Determining the optimal set of features and fusion methods is challenging because different features may exhibit varying degrees of relevance, redundancy, and noise across diverse IoT environments. Inappropriate feature selection

or fusion can degrade model performance. Extensive empirical analysis is required to identify robust feature combinations that are generalizable across IoT deployment scenarios. Furthermore, fusing heterogeneous feature sources increases computational overhead, which may impact real-time detection capabilities on resource-constrained devices.

DL models show promise for detecting DDoS attacks in IoT networks but require more evaluation on realistic, balanced datasets. While complex DL architectures demonstrate good detection capabilities, simplified models warrant research to enable feasibility on resource-constrained edge devices. Additional real-world testing is needed, as most studies evaluate models offline. Further work should prioritize model optimization, robustness against adversarial attacks, and addressing practical deployment challenges around overhead, false positives/negatives, reliability, and effective utilization of feature fusion techniques. Overall, DL has shown potential but needs more research into real-world effectiveness, model efficiency, adversarial robustness, and optimal multimodal feature combination to maximize DDoS attack detection in IoT networks.

## 8. FUTURE WORK AND RESEARCH DIRECTIONS

Although the literature has made good progress, there are several promising areas of future work to advance DDoS detection in IoT networks. Evaluating model performance on more recent and diverse datasets covering different IoT protocols, realistic benign and attack traffic distributions, and the latest DDoS variants will strengthen the generalizability of these techniques. Many studies rely on dated public datasets that fail to reflect current IoT environments and threats. Testing systems against modern benchmark datasets that capture the breadth of protocols, normal traffic patterns, and emerging attacks seen in real-world networks will provide a much better assessment of generalizable accuracy.

Designing optimized DL models that offer high detection accuracy while being lightweight enough for resource-constrained edge devices will increase the usability of these techniques for real-world IoT infrastructure. As many detection models leverage complex, multiarchitecture designs, their computational overhead makes deployment challenging on memory- and power-limited IoT endpoints. The development of innovative yet simplified model architectures tailored to edge hardware capabilities can thus enable localized on-device inference, which is critical for scalable threat visibility.

Testing detection methods by integrating them into operational IoT testbeds instead of just using offline datasets can reveal practical challenges and accuracy metrics closer to real-world environments. While offline dataset analysis provides a convenient method for initial model evaluations, those controlled settings differ vastly in terms of the sheer diversity and unpredictability of live production networks. Hence, real-world testing can serve as a litmus test, revealing additional factors impacting performance, false alarms, and evasion issues and guiding further improvement.

Enhancing model robustness against adversarial attacks through techniques such as adversarial retraining and ensemble modelling will improve resilience against evolving DDoS threats. The current literature overlooks evaluation under adversarial conditions. However, model manipulation attacks pose serious practical concerns. Prioritizing adversarial threat detection via robust training processes and ensemble approaches combining multiple model inferences could significantly expand protection against both current and zero-day DDoS attacks.

Another promising research direction is investigating self-supervised learning techniques to reduce the reliance on large, labelled datasets, which are expensive and time consuming to construct. Collecting and manually labelling massive amounts of IoT traffic data across diverse protocols and attacks poses a practical challenge, making adoption difficult. Self-supervised approaches that exploit structure within the data itself to automatically generate labels and learn useful representations could provide a pathway for more accessible and scalable model development.

An additional promising research direction is investigating optimal feature fusion techniques that combine complementary feature sets for enhanced detection performance. Determining the ideal set of features and fusion method across diverse IoT environments is nontrivial due to varying relevance, redundancy, and noise levels. Extensive empirical analysis is needed to identify robust multimodal feature combinations that are generalizable to different deployment scenarios. Furthermore, fusing heterogeneous features increases computational requirements, so lightweight fusion approaches suitable for resource-constrained devices warrant exploration.

In summary, advancing research in the above directions can help overcome the limitations of current DDoS detection techniques for IoT networks and enable more robust, adaptive, and practical solutions suited for production environments. Optimizing feature fusion strategies, model architectures for edge deployments, robustness against adversarial attacks, self-supervised learning, and evaluations on diverse real-world datasets are key areas of focus. This remains an active and crucial area of cybersecurity research to strengthen the IoT infrastructure against persistent DDoS risks.

## 9. CONCLUSION

In conclusion, this comprehensive review highlights the potential of deep learning methodologies and feature fusion techniques in detecting DDoS attacks within IoT networks. While these approaches show promise, their real-world application necessitates extensive research focused on enhancing generalization, developing resource-efficient algorithms, and strengthening detection methods against evolving threats. Feature fusion has demonstrated significant potential for improving the accuracy and robustness of DDoS attack detection by combining complementary features from multiple data sources. However, further research is needed to identify optimal feature fusion strategies that can effectively handle the heterogeneity and complexity of IoT data while remaining computationally efficient. Addressing these research limitations is crucial for deploying intelligent and robust security mechanisms in IoT networks, ensuring the security and reliability of these interconnected systems through cutting-edge deep learning and feature fusion approaches. As the IoT continues to penetrate every aspect of our lives, advancing research at the intersection of these domains is paramount to build a robust foundation for the IoT-driven future, where the benefits of widespread connectivity are utilized while mitigating the risks posed by malicious actors.

### Conflicts of interest

The authors declare no conflicts of interest.

### Funding

The authors would like to thank the Universiti Malaysia Pahang Al-Sultan Abdullah for financial support under Internal Research grant RDU220384 and the Postgraduate Research Grant Scheme PGRS2303103.

### Acknowledgements

The authors would like to thank the Universiti Malaysia Pahang Al-Sultan Abdullah for financial support under Internal Research grant RDU220384.

## References

- [1] L. S. Vailshery, "Internet of Things (IoT) and non-IoT active device Connections worldwide from 2010 to 2025," *Statista*. 2020. [Online]. Available: <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/#:~:text=The total installed base of,that are expected in 2021.>
- [2] K.-H. Le, M.-H. Nguyen, T.-D. Tran, and N.-D. Tran, "IMIDS: An Intelligent Intrusion Detection System against Cyber Threats in IoT," *Electronics (Basel)*, vol. 11, no. 4, p. 524, 2022, doi: 10.3390/electronics11040524.
- [3] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *ComputSecur*, vol. 127, p. 103096, 2023, doi: 10.1016/J.COSE.2023.103096.
- [4] X.-H. Nguyen and K.-H. Le, "Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model," *Internet of Things*, vol. 23, p. 100851, Oct. 2023, doi: 10.1016/j.iot.2023.100851.
- [5] Y. Zhao and A. Kuerban, "MDABP: A Novel Approach to Detect Cross-Architecture IoT Malware Based on PaaS," *Sensors*, vol. 23, no. 6, p. 3060, 2023, doi: 10.3390/s23063060.
- [6] G. Polat et al., "Security Issues in IoT: Challenges and Countermeasures," *ISACA*. 2019. [Online]. Available: <https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures>
- [7] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," *Internet of Things*, vol. 14, p. 100365, 2021, doi: 10.1016/j.iot.2021.100365.
- [8] C. Liang et al., "Intrusion Detection System for the Internet of Things Based on Blockchain and Multi-Agent Systems," *Electronics (Basel)*, vol. 9, no. 7, p. 1120, 2020, doi: 10.3390/electronics9071120.
- [9] Statista Research Department, "Selling price of malware and DDoS attack services on the darknet 2023," *Statista*. 2023. [Online]. Available: <https://www.statista.com/statistics/1350155/selling-price-malware-ddos-attacks-dark-web/>
- [10] S. Tsimenidis, T. Lagkas, and K. Rantos, "Deep Learning in IoT Intrusion Detection," *Journal of Network and Systems Management*, vol. 30, no. 1, pp. 1–40, Jan. 2022, doi: 10.1007/S10922-021-09621-9/FIGURES/13.
- [11] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, "A systematic review on Deep Learning approaches for IoT security," *Comput Sci Rev*, vol. 40, p. 100389, May 2021, doi: 10.1016/J.COSREV.2021.100389.

- [12] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1646–1685, Jul. 2020, doi: 10.1109/COMST.2020.2988293.
- [13] M. A. Alsoufi et al., "Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review," *Applied Sciences*, vol. 11, no. 18, p. 8383, Sep. 2021, doi: 10.3390/app11188383.
- [14] M. Mittal, K. Kumar, and S. Behal, "Deep learning approaches for detecting DDoS attacks: a systematic review," *Soft comput.*, vol. 27, no. 18, pp. 13039–13075, Sep. 2022, doi: 10.1007/s00500-021-06608-1.
- [15] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects," *Electronics (Basel)*, vol. 11, no. 9, p. 1502, May 2022, doi: 10.3390/electronics11091502.
- [16] A. Alotaibi and A. Barnawi, "Securing massive IoT in 6G: Recent solutions, architectures, future directions," *Internet of Things*, vol. 22, p. 100715, Jul. 2023, doi: 10.1016/j.iot.2023.100715.
- [17] S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," *Security and Communication Networks*, vol. 2022, pp. 1–41, Aug. 2022, doi: 10.1155/2022/8951961.
- [18] A. Aldhaheer, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in IoT networks: A review," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 110–128, 2024, doi: 10.1016/j.iotcps.2023.09.003.
- [19] A. Firdaus, M. F. A. Razak, A. Feizollah, I. A. T. Hashem, M. Hazim, and N. B. Anuar, "The rise of 'blockchain': bibliometric analysis of blockchain study," *Scientometrics*, vol. 120, no. 3, pp. 1289–1331, Sep. 2019, doi: 10.1007/s11192-019-03170-4.
- [20] A. Cheema, M. Tariq, A. Hafiz, M. M. Khan, F. Ahmad, and M. Anwar, "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review," *Security and Communication Networks*, vol. 2022, pp. 1–15, May 2022, doi: 10.1155/2022/8379532.
- [21] M. M. Salim, S. Rathore, and J. H. Park, "Distributed denial of service attacks and its defenses in IoT: a survey," *J Supercomput.*, vol. 76, no. 7, pp. 5320–5363, Jul. 2020, doi: 10.1007/s11227-019-02945-z.
- [22] M. Najafimehr, S. Zarifzadeh, and S. Mostafavi, "DDoS attacks and machine-learning-based detection methods: A survey and taxonomy," *Engineering Reports*, May 2023, doi: 10.1002/eng2.12697.
- [23] F. S. Dantas Silva, E. Silva, E. P. Neto, M. Lemos, A. J. Venancio Neto, and F. Esposito, "A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios," *Sensors*, vol. 20, no. 11, p. 3078, May 2020, doi: 10.3390/s20113078.
- [24] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, "Distributed Denial of Service (DDoS) Mitigation Using Blockchain—A Comprehensive Insight," *Symmetry (Basel)*, vol. 13, no. 2, p. 227, Jan. 2021, doi: 10.3390/sym13020227.
- [25] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Comput Sci Rev*, vol. 39, p. 100332, Feb. 2021, doi: 10.1016/j.cosrev.2020.100332.
- [26] R. M. A. Haseeb-ur-rehman et al., "High-Speed Network DDoS Attack Detection: A Survey," *Sensors*, vol. 23, no. 15, p. 6850, Aug. 2023, doi: 10.3390/s23156850.
- [27] S. Karnani and H. K. Shakya, "Mitigation strategies for distributed denial of service (DDoS) in SDN: A survey and taxonomy," *Information Security Journal: A Global Perspective*, vol. 32, no. 6, pp. 444–468, Nov. 2023, doi: 10.1080/19393555.2022.2111004.
- [28] M. Ragab, S. M. Alshammari, L. A. Maghrabi, D. Alsalman, T. Althaqafi, and A. A.-M. AL-Ghamdi, "Robust DDoS Attack Detection Using Piecewise Harris Hawks Optimizer with Deep Learning for a Secure Internet of Things Environment," *Mathematics*, vol. 11, no. 21, p. 4448, Oct. 2023, doi: 10.3390/math11214448.
- [29] M. Cherian and S. L. Varma, "Secure SDN-IoT Framework for DDoS Attack Detection Using Deep Learning and Counter Based Approach," *Journal of Network and Systems Management*, vol. 31, no. 3, 2023, doi: 10.1007/s10922-023-09749-w.
- [30] B. A. Alabsi, M. Anbar, and S. D. A. Rihan, "Conditional Tabular Generative Adversarial Based Intrusion Detection System for Detecting Ddos and Dos Attacks on the Internet of Things Networks," *Sensors*, vol. 23, no. 12, 2023, doi: 10.3390/s23125644.
- [31] F. M. Aswad, A. M. S. Ahmed, N. A. M. Alhammedi, B. A. Khalaf, and S. A. Mostafa, "Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks," *Journal of Intelligent Systems*, vol. 32, no. 1, 2023, doi: 10.1515/jisys-2022-0155.
- [32] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," *IEEE Access*, vol. 11, pp. 119862–119875, 2023, doi: 10.1109/ACCESS.2023.3327620.
- [33] S. S. Mahadik, P. M. Pawar, and R. Muthalagu, "Edge-HetIoT defense against DDoS attack using learning techniques," *Comput Secur.*, vol. 132, 2023, doi: 10.1016/j.cose.2023.103347.

- [34] S. Mahadik, P. M. Pawar, and R. Muthalagu, “Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT),” *Journal of Network and Systems Management*, vol. 31, no. 1, 2023, doi: 10.1007/s10922-022-09697-x.
- [35] J. G. Almaraz-Rivera, J. A. Cantoral-Ceballos, and J. F. Botero, “Enhancing IoT Network Security: Unveiling the Power of Self-Supervised Learning against DDoS Attacks,” *Sensors*, vol. 23, no. 21, p. 8701, Oct. 2023, doi: 10.3390/s23218701.
- [36] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama, and M. A. Hamza, “Enhancing DDoS Attack Detection Using Snake Optimizer With Ensemble Learning on Internet of Things Environment,” *IEEE Access*, vol. 11, pp. 104745–104753, 2023, doi: 10.1109/ACCESS.2023.3318316.
- [37] S. A. Khanday, H. Fatima, and N. Rakesh, “Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks,” *Expert Syst Appl*, vol. 215, 2023, doi: 10.1016/j.eswa.2022.119330.
- [38] M. I. T. Hussan, G. V. Reddy, P. T. Anitha, A. Kanagaraj, and P. Naresh, “DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization,” *Cluster Comput*, Nov. 2023, doi: 10.1007/s10586-023-04187-4.
- [39] L. Alamer and E. Shadadi, “DDoS Attack Detection using Long-short Term Memory with Bacterial Colony Optimization on IoT Environment,” *Journal of Internet Services and Information Security*, vol. 13, no. 1, pp. 44–53, 2023, doi: 10.58346/JISIS.2023.I1.005.
- [40] P. Bhale, D. R. Chowdhury, S. Biswas, and S. Nandi, “OPTIMIST: Lightweight and Transparent IDS With Optimum Placement Strategy to Mitigate Mixed-Rate DDoS Attacks in IoT Networks,” *IEEE Internet Things J*, vol. 10, no. 10, pp. 8357–8370, May 2023, doi: 10.1109/JIOT.2023.3234530.
- [41] K. Kethineni and G. Pradeepini, “Intrusion detection in internet of things-based smart farming using hybrid deep learning framework,” *Cluster Comput*, 2023, doi: 10.1007/s10586-023-04052-4.
- [42] T. H. H. Aldhyani and H. Alkahtani, “Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model,” *Mathematics*, vol. 11, no. 1, 2023, doi: 10.3390/math11010233.
- [43] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, “An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IoT Networks,” *IEEE Internet Things J*, vol. 10, no. 10, pp. 8491–8504, May 2023, doi: 10.1109/JIOT.2022.3196942.
- [44] S. Y. Diaba and M. Elmusrati, “Proposed algorithm for smart grid DDoS detection based on deep learning,” *Neural Networks*, vol. 159, pp. 175–184, 2023, doi: 10.1016/j.neunet.2022.12.011.
- [45] T. Liu, F. Sabrina, J. Jang-Jaccard, W. Xu, and Y. Wei, “Artificial intelligence-enabled ddos detection for blockchain-based smart transport systems,” *Sensors*, vol. 22, no. 1, 2022, doi: 10.3390/s22010032.
- [46] M. Zeeshan et al., “Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets,” *IEEE Access*, vol. 10, pp. 2269–2283, 2022, doi: 10.1109/ACCESS.2021.3137201.
- [47] M. M. Fadel, S. M. El-Ghamrawy, A. M. T. Ali-Eldin, M. K. Hassan, and A. I. El-Desoky, “The proposed hybrid deep learning intrusion prediction IoT (HDLIP-IoT) framework,” *PLoS One*, vol. 17, no. 7 July, 2022, doi: 10.1371/journal.pone.0271436.
- [48] F. Sattari, A. H. Farooqi, Z. Qadir, B. Raza, H. Nazari, and M. Almutiry, “A Hybrid Deep Learning Approach for Bottleneck Detection in IoT,” *IEEE Access*, vol. 10, pp. 77039–77053, 2022, doi: 10.1109/ACCESS.2022.3188635.
- [49] O. Yousuf and R. N. Mir, “DDoS attack detection in Internet of Things using recurrent neural network,” *Computers and Electrical Engineering*, vol. 101, 2022, doi: 10.1016/j.compeleceng.2022.108034.
- [50] S. Hariprasad, T. Deepa, and N. Bharathiraja, “Detection of DDoS Attack in IoT Networks Using Sample Selected RNN-ELM,” *Intelligent Automation and Soft Computing*, vol. 34, no. 3, pp. 1425–1440, 2022, doi: 10.32604/iasc.2022.022856.
- [51] S. P. K. Gudla, S. K. Bhoi, S. R. Nayak, and A. Verma, “DI-ADS: A Deep Intelligent Distributed Denial of Service Attack Detection Scheme for Fog-Based IoT Applications,” *Math ProblEng*, vol. 2022, 2022, doi: 10.1155/2022/3747302.
- [52] S. Balaji and S. Sankaranarayanan, “Hybrid Deep-Generative Adversarial Network Based Intrusion Detection Model for Internet of Things Using Binary Particle Swarm Optimization,” *International Journal of Electrical and Electronics Research*, vol. 10, no. 4, pp. 948–953, 2022, doi: 10.37391/ijeer.100432.
- [53] P. Kumar, H. Bagga, B. S. Netam, and V. Uduthalapally, “SAD-IoT: Security Analysis of DDoS Attacks in IoT Networks,” *Wirel Pers Commun*, vol. 122, no. 1, pp. 87–108, 2022, doi: 10.1007/s11277-021-08890-6.
- [54] A. A. Alashhab, M. S. M. Zahid, A. Muneer, and M. Abdulkahi, “Low-rate DDoS attack Detection using Deep Learning for SDN-enabled IoT Networks,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 11, pp. 371–377, 2022, doi: 10.14569/IJACSA.2022.0131141.
- [55] N. Mahajan, A. Chauhan, H. Kumar, S. Kaushal, and A. K. Sangaiah, “A Deep Learning Approach to Detection and Mitigation of Distributed Denial of Service Attacks in High Availability Intelligent Transport Systems,” *Mobile Networks and Applications*, vol. 27, no. 4, pp. 1423–1443, 2022, doi: 10.1007/s11036-022-01973-z.
- [56] S.-H. Lee, Y.-L. Shiue, C.-H. Cheng, Y.-H. Li, and Y.-F. Huang, “Detection and Prevention of DDoS Attacks on the IoT,” *Applied Sciences (Switzerland)*, vol. 12, no. 23, 2022, doi: 10.3390/app122312407.

- [57] A. A. Elsaedy, A. Jamalipour, and K. S. Munasinghe, “A Hybrid Deep Learning Approach for Replay and DDoS Attack Detection in a Smart City,” *IEEE Access*, vol. 9, pp. 154864–154875, 2021, doi: 10.1109/ACCESS.2021.3128701.
- [58] M. A. Ferrag, L. Shu, H. Djallel, and K.-K. R. Choo, “Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0,” *Electronics (Switzerland)*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111257.
- [59] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan, and R. Patan, “Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network,” *IEEE Access*, vol. 8, pp. 77396–77404, 2020, doi: 10.1109/ACCESS.2020.2986013.
- [60] M. V. O. de Assis, L. F. Carvalho, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proença Jr, “Near real-time security system applied to SDN environments in IoT networks using convolutional neural network,” *Computers and Electrical Engineering*, vol. 86, 2020, doi: 10.1016/j.compeleceng.2020.106738.
- [61] M. Shurman, R. Khrais, and A. Yateem, “DoS and DDoS attack detection using deep learning and IDS,” *International Arab Journal of Information Technology*, vol. 17, no. 4A Special, pp. 655–661, 2020, doi: 10.34028/iajit/17/4A/10.
- [62] K. N. K. Thapa and N. Duraipandian, “Malicious Traffic classification Using Long Short-Term Memory (LSTM) Model,” *Wirel Pers Commun*, vol. 119, no. 3, pp. 2707–2724, Aug. 2021, doi: 10.1007/s11277-021-08359-6.
- [63] N. Bakhmat, O. Kolosova, O. Demchenko, I. Ivashchenko, and V. Strelchuk, “Application of International Scientometric Database in the Process of Training Competitive Research and Teaching Staff: Opportunities of Web of Science (WOS), Scopus, Google Scholar,” *J Theor Appl Inf Technol*, vol. 15, no. 13, 2022, [Online]. Available: [www.jatit.org](http://www.jatit.org)
- [64] A. D. Aguru and S. B. Erukala, “A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning,” *Information Sciences*, vol. 662, p. 120209, Mar. 2024, doi: <https://doi.org/10.1016/j.ins.2024.120209>.
- [65] L. Xie et al., “MRFM: A Timely Detection Method for DDoS Attacks in IoT with Multidimensional Reconstruction and Function Mapping,” *Computer standards & interfaces*, vol. 89, pp. 103829–103829, Apr. 2024, doi: <https://doi.org/10.1016/j.csi.2023.103829>.
- [66] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” 2019 International Carnahan Conference on Security Technology (ICCST), Oct. 2019, doi: <https://doi.org/10.1109/ccst.2019.8888419>.
- [67] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset,” *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019, doi: <https://doi.org/10.1016/j.future.2019.05.041>.
- [68] C. Pinto, Sajjad Dadkhah, R. Ferreira, Alireza Zohourian, R. Lu, and A. A. Ghorbani, “CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment,” *Sensors*, vol. 23, no. 13, pp. 5941–5941, Jun. 2023, doi: <https://doi.org/10.3390/s23135941>.
- [69] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, vol. 1, 2018, doi: <https://doi.org/10.5220/0006639801080116>.
- [70] N. Moustafa and J. Slay, “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set),” *IEEE Xplore*, Nov. 01, 2015, doi: <https://doi.org/10.1109/MilCIS.2015.7348942>.
- [71] M. Tavallae, E. Bagheri, W. Lu, and A. A. Ghorbani, “A detailed analysis of the KDD CUP 99 data set,” *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Jul. 2009, doi: <https://doi.org/10.1109/cisda.2009.5356528>.
- [72] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, “TON\_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-driven Intrusion Detection Systems,” *IEEE Access*, vol. 8, pp. 165130 - 165150, 2020, doi: <https://doi.org/10.1109/access.2020.3022862>.
- [73] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, “Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning,” *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: <https://doi.org/10.1109/access.2022.3165809>.
- [74] N. Ahuja, G. Singal, and D. Mukhopadhyay, “DDoS attack SDN Dataset,” *Mendeley Data*, vol. 1, Sep. 2020, doi: <https://doi.org/10.17632/jxpfjc64kr.1>.
- [75] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici, “N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders,” *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, Jul. 2018, doi: <https://doi.org/10.1109/mprv.2018.03367731>.
- [76] Canadian Institute for Cybersecurity, “CSE-CIC-IDS2018 on AWS: A collaborative project between the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC),” <https://www.unb.ca/cic/datasets/ids-2018.html> (accessed Mar. 23, 2024).

- [77] Y. R. KUMBAM, “APA-DDoS Dataset,” <https://www.kaggle.com/datasets/yashwanthkumbam/apaddos-dataset> (accessed Mar. 28, 2024).
- [78] I. Ullah and Q. H. Mahmoud, “A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks,” *Advances in Artificial Intelligence*, vol. 12109, pp. 508–520, 2020, doi: [https://doi.org/10.1007/978-3-030-47358-7\\_52](https://doi.org/10.1007/978-3-030-47358-7_52).
- [79] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, J. F. Botero, and L. A. Trejo, “Toward the Protection of IoT Networks: Introducing the LATAM-DDoS-IoT Dataset,” *IEEE Access*, vol. 10, pp. 106909–106920, 2022, doi: <https://doi.org/10.1109/access.2022.3211513>.
- [80] M. M. Salim, A. E. Azzaoui, X. Deng, and J. H. Park, “FL-CTIF: A federated learning based CTI framework based on information fusion for secure IIoT,” *Information Fusion*, vol. 102, pp. 102074–102074, Feb. 2024, doi: <https://doi.org/10.1016/j.inffus.2023.102074>.
- [81] M. Adnan Khan, T. M. Ghazal, S.-W. Lee, and A. Rehman, “Data Fusion-Based Machine Learning Architecture for Intrusion Detection,” *Computers, Materials & Continua*, vol. 70, no. 2, pp. 3399–3413, 2022, doi: <https://doi.org/10.32604/cmc.2022.020173>.
- [82] H. Mohammed, S. R. Hasan, and F. Awwad, “Fusion-On-Field Security and Privacy Preservation for IoT Edge Devices: Concurrent Defense Against Multiple Types of Hardware Trojan Attacks,” *IEEE Access*, vol. 8, pp. 36847–36862, 2020, doi: <https://doi.org/10.1109/access.2020.2975016>.
- [83] S. Yaras and M. Dener, “IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm,” *Electronics*, vol. 13, no. 6, Mar. 2024, doi: <https://doi.org/10.3390/electronics13061053>.
- [84] X. Yang, G. Peng, D. Zhang, and Y. Lv, “An Enhanced Intrusion Detection System for IoT Networks Based on Deep Learning and Knowledge Graph,” *Security and Communication Networks*, vol. 2022, Apr. 2022, doi: <https://doi.org/10.1155/2022/4748528>.
- [85] D. Chen, F. Zhang, and X. Zhang, “Heterogeneous IoT Intrusion Detection Based on Fusion Word Embedding Deep Transfer Learning,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 8, pp. 9183–9193, Aug. 2023, doi: <https://doi.org/10.1109/tii.2022.3227640>.
- [86] V. Ravi, R. Chaganti, and M. Alazab, “Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system,” *Computers and Electrical Engineering*, vol. 102, p. 108156, Sep. 2022, doi: <https://doi.org/10.1016/j.compeleceng.2022.108156>.
- [87] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Daviz, A. Goulart, and S. Zonouz, “Multi-Source Multi-Domain Data Fusion for Cyberattack Detection in Power Systems,” *IEEE Access*, vol. 9, pp. 119118–119138, 2021, doi: <https://doi.org/10.1109/access.2021.3106873>.
- [88] M. Al-Hawawreh and M. S. Hossain, “A privacy-aware framework for detecting cyber attacks on internet of medical things systems using data fusion and quantum deep learning,” *Information Fusion*, vol. 99, p. 101889, Nov. 2023, doi: <https://doi.org/10.1016/j.inffus.2023.101889>.
- [89] G. Li, Z. Yan, Y. Fu, and H. Chen, “Data Fusion for Network Intrusion Detection: A Review,” *Security and Communication Networks*, vol. 2018, pp. 1–16, 2018, doi: <https://doi.org/10.1155/2018/8210614>.
- [90] W. Ding, X. Jing, Z. Yan, and L. T. Yang, “A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion,” *Information Fusion*, vol. 51, pp. 129–144, Nov. 2019, doi: <https://doi.org/10.1016/j.inffus.2018.12.001>.
- [91] K.-H. Lin et al., “Fusion-Extracted Features by Deep Networks for Improved COVID-19 Classification with Chest X-ray Radiography,” *Healthcare*, vol. 11, no. 10, pp. 1367–1367, May 2023, doi: <https://doi.org/10.3390/healthcare11101367>.
- [92] W. Guo, H. Qiu, Z. Liu, J. Zhu, and Q. Wang, “GLD-Net: Deep Learning to Detect DDoS Attack via Topological and Traffic Feature Fusion,” *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–20, Aug. 2022, doi: <https://doi.org/10.1155/2022/4611331>.
- [93] H. Liao et al., “A Survey of Deep Learning Technologies for Intrusion Detection in Internet of Things,” *IEEE Access*, Jan. 2024, doi: <https://doi.org/10.1109/access.2023.3349287>.
- [94] B. Bala and S. Behal, “AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges,” *Computer science review*, vol. 52, May 2024, doi: <https://doi.org/10.1016/j.cosrev.2024.100631>.