[1] **Vinay Tila Patil***

[2] **Shailesh Shivaji Deore**

DDoS Attack Detection: Strategies, Techniques, and Future Directions

Abstract: - Distributed Denial of Service (DDoS) attacks represent one of the most significant threats to network security, capable of causing widespread disruption to digital infrastructures. The potential for extensive damage becomes even more critical when these attacks are executed on a large scale. Numerous research efforts have been dedicated to understanding and mitigating this formidable threat. This study delves into the complex landscape of DDoS attacks, examining a range of strategies proposed for their detection and mitigation. Special attention is given to the exploration of advanced deep learning and machine learning techniques, which have emerged as pivotal in the development of effective defense mechanisms against DDoS attacks. This research offers a comprehensive understanding of the evolving dynamics of DDoS attacks and highlights innovative methodologies, thus contributing to the ongoing discourse on enhancing network security. Additionally, the paper discusses future directions in DDoS detection, aiming to provide a roadmap for researchers and practitioners in the field.

Keywords: DDoS attacks, Cybersecurity, Deep learning techniques, Machine learning approaches, Attack detection, Network security, Future directions.

I. INTRODUCTION

Cybersecurity threats, particularly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, continue to pose formidable challenges to the security of Internet of Things (IoT) ecosystems. In recent years, there has been a significant uptick in the frequency and severity of DDoS attacks. These malicious attempts have caused extensive disruptions in numerous IoT networks worldwide, leading to considerable financial and operational losses [4]. DDoS attacks are typically orchestrated by assailants who aim to disrupt the normal functioning of a device or network by overwhelming the system with a flood of internet traffic from various sources, effectively making it inaccessible to legitimate users.

A notable instance underscoring the severity of these attacks was the 2016 assault on a DNS provider. This event, which became a watershed moment in the history of cyber-attacks, utilized a Mirai-botnet composed of compromised IoT devices. It adversely affected over 60 companies and was recorded as one of the largest of its kind at the time, peaking at an unprecedented 600 Gbps of traffic [5]. This was subsequently eclipsed in 2018 by an even more formidable DDoS attack on GitHub, which saw incoming traffic surge to a staggering 1.3 Tbps [6]. The prevalence of such attacks has grown, with various iterations of Mirai botnets causing disruptions across the globe [7].

The vulnerability of IoT devices is a significant concern. It is estimated that there are around 31 billion IoT devices in use, and worryingly, about half of these are susceptible to various types of cyber threats [8][9]. This vulnerability is exacerbated by the continuous evolution of DDoS attack methods. Initially, these attacks were primarily volumetric, aiming to flood systems with overwhelming traffic. However, they have now evolved into more sophisticated application-layer attacks, exploiting specific vulnerabilities in the application's software. The emergence of cutting-edge technologies such as 5G and Artificial Intelligence (AI) adds new dimensions and complexities to these threats, further challenging existing security paradigms [54].

The impact of DDoS attacks is not uniform across all sectors. Critical sectors like healthcare, finance, and government are particularly vulnerable due to the sensitive nature of their operations and the critical need for

[1] Research Scholar, SSVPS's Bapusaheb Shivajirao Deore College of Engineering, Dhule, Maharashtra, India.

Assistant Professor, Ajeenkya D. Y. Patil University, Pune, Maharashtra, India. vinayt.patil@outlook.com

[2] Research Guide and Associate Professor, Department of Computer Engineering, SSVPS's Bapusaheb Shivajirao Deore College of Engineering, Dhule, Maharashtra, India. shaileshdeore@gmail.com

* Corresponding Author Email: vinayt.patil@outlook.com

uninterrupted service. In healthcare, for example, a successful DDoS attack can impede access to vital patient data, while in the finance sector, such attacks can disrupt trading and cause financial instability [55].

Addressing these threats requires a multi-faceted approach, combining advanced technological solutions with robust policy-based strategies. However, the task of implementing effective preventive measures is fraught with challenges. One of the primary difficulties lies in the ability to distinguish between legitimate traffic and malicious attack traffic, a task that becomes increasingly complex with the sophistication of attack methods [55]. The role of legislative measures and international cooperation in combating DDoS attacks is vital. Different countries have adopted various strategies, with varying degrees of success. There is a pressing need for a concerted global effort to establish unified standards and practices to effectively counter these threats [47].

Recent case studies and statistical analyses provide a clearer picture of the current landscape of DDoS attacks. They highlight not only the frequency and scale of these attacks but also their evolving nature and the diversifying sources of these threats. Looking forward, the rapid expansion of IoT devices and advancements in technology are likely to introduce new vulnerabilities, raising concerns about the future landscape of DDoS attacks. Furthermore, the economic and social implications of DDoS attacks are profound. Businesses, especially those heavily reliant on online services, face substantial financial losses due to operational downtime. There is also a broader impact on consumer trust and confidence, which can have far-reaching effects on the digital economy.

This paper aims to delve into the effectiveness of various DDoS attack detection strategies, shedding light on the current challenges in this area and exploring potential future directions in an ever-evolving cybersecurity landscape.

II. Distributed Denial Of Service (DDoS) Attacks

DDoS attacks are coordinated attempts by an attacker to disrupt or deny legitimate users access to an organization's services or resources by overwhelming them with a flood of traffic. The attacker can create a botnet, which is a network of compromised internet-connected devices such as IoT gadgets, and coordinate the botnets through a control server to launch attacks. As a result, the target experiences a massive surge of traffic from multiple sources, disrupting its normal operations.

2.1 IoT DDoS Attacks

IoT DDoS attacks are particularly challenging to defend against due to the inherent limitations of IoT devices in terms of processing power and bandwidth. Attackers can exploit vulnerabilities in IoT device firmware or communication protocols to compromise these devices and launch malicious attacks. Moreover, IoT devices themselves can be used as powerful tools for DDoS attacks, amplifying the impact of the attack. The low security posture of IoT devices makes them an attractive target for attackers to build large-scale botnets, which are crucial for launching volumetric DDoS attacks. For instance, the infamous Mirai botnet was created by hijacking over 65,000 IoT devices within 20 hours of their release and subsequently used to launch DDoS attacks against major IoT companies like OVH and Dyn [11].

2.2 DDoS Attack Architecture

The architecture of a typical DDoS attack encompasses three primary components:

Attacker: This is the individual or group behind the DDoS attack. They are responsible for orchestrating the assault, controlling the botnets, and coordinating the flow of attack traffic. The attackers may use various techniques to conceal their identity, including the use of VPNs or hijacking other devices' IP addresses.

Botnet: A botnet is essentially a network of compromised internet-connected devices, controlled by the attacker. These devices, often unaware to their legitimate users, become tools in generating massive volumes of attack traffic. The distributed nature of botnets makes it challenging to trace and neutralize them, as they can comprise devices from all around the globe.

Target: This is the organization, service, or infrastructure under attack. The primary objective of the attacker is to overwhelm the target's resources, such as bandwidth or server capacity, to an extent that legitimate users are unable to access the services. The impact on the target can range from slowed service to complete unavailability, potentially leading to significant financial and reputational damages.

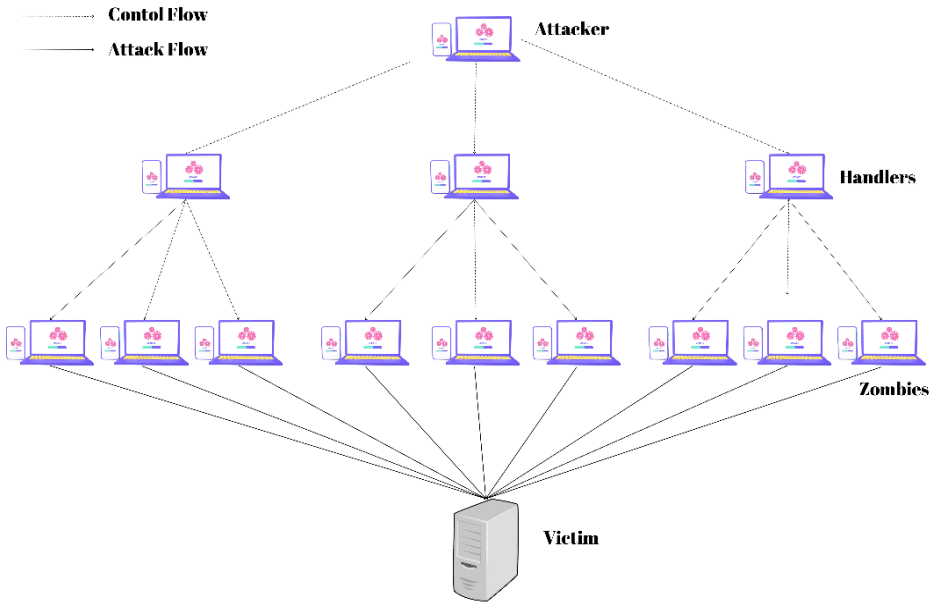

Fig.1. DDoS attack architecture diagram

2.3 Types of DDoS Attacks and Techniques

2.3.1 Volumetric Attacks

These are the most common type of DDoS attacks. The goal is to consume the bandwidth of the victim's network or service. Attackers generate large volumes of data packets or requests that flood the target, overwhelming its ability to process and respond. This type of attack often uses botnets to generate a massive amount of traffic [71].

2.3.2 Application-Layer Attacks

These attacks target specific aspects of an application or service rather than just flooding the network with traffic. The aim is to exhaust the resources of the application layer, making the service slow or unresponsive. This type of attack is more sophisticated and harder to detect because it can mimic legitimate user behavior. Examples include HTTP flood attacks that overload a web server, or DNS query floods that disrupt the resolution of domain names [72].

2.3.3 Reflection and Amplification Attacks

These techniques are used to magnify the potency of a DDoS attack. In a reflection attack, the attacker sends requests to a third-party server (e.g., DNS or NTP server) with a forged sender address. This server then 'reflects' the response to the target's IP address. In amplification attacks, the attacker exploits the difference in the size of responses and requests to multiply the volume of data sent to the target. For example, a small query sent to a DNS server can generate a significantly larger response, which is directed to the target, amplifying the traffic volume significantly [73].

2.3.4 Protocol Attacks

These attacks exploit vulnerabilities in the protocols that govern internet communication. Examples include SYN flood attacks, where an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic [74].

2.4 History of DDoS

Distributed denial-of-service (DDoS) attacks have emerged as a significant threat to the security and availability of online services in recent years. These attacks aim to overwhelm a target system with a massive volume of traffic, rendering it inaccessible to legitimate users.

2.4.1 The Early Days of DDoS Attacks

The first recorded DDoS attack occurred in 1974 when David Dennis launched a program called "Slowloris" against a DEC PDP-11 computer at the Massachusetts Institute of Technology (MIT) [40]. This attack involved sending a

large number of slow, incomplete TCP SYN packets, causing the target computer to crash. In the 1990s, IRC chat floods became a prevalent form of DDoS attack [41]. Attackers would join IRC channels and flood them with messages, making it impossible for other users to participate.

2.4.2 Notable DDoS Attacks in History

1998 Morris Worm Attack: This attack targeted the root servers of the Domain Name System (DNS), causing widespread disruption to the internet [42].
2001 Code Red Worm Attack: This attack targeted websites running Microsoft IIS web server software, causing significant damage to businesses and organizations [43].
2007 Estonian Cyberattacks: A series of coordinated DDoS attacks targeted the Estonian government and its infrastructure, believed to have been launched by Russian hackers [44].
2010 Operation Aurora Attacks: These coordinated DDoS attacks targeted US and South Korean websites, believed to have been launched by the Chinese government [45].
2016 DDoS Attack on Dyn: This major attack targeted the Dyn DNS service provider, causing widespread disruption to websites and online services [46].
Throughout 1990: IRC (Internet Relay Chat) channels experienced extensive disruption due to chat floods. Attackers flooded these channels with an overwhelming volume of messages, impacting regular communication and user participation [61].
1998: The Morris worm targeted multiple internet hosts, exploiting known vulnerabilities in Unix systems. This worm marked one of the earliest notable instances of a widespread DDoS attack, significantly disrupting internet services [62].
2000: Yahoo, one of the largest web services providers at the time, fell victim to a significant DDoS attack. This attack overwhelmed Yahoo's servers, causing substantial service disruption and highlighting the vulnerability of major online platforms [63].
2001 Code Red Worm: This attack targeted websites running on Microsoft IIS web server software. This attack exploited a buffer overflow vulnerability, affecting hundreds of thousands of computers and causing extensive operational and economic damage [64].
2002: An attack targeted the root servers of the Domain Name System (DNS). This attack aimed to disrupt the essential service responsible for translating domain names into IP addresses, posing a considerable threat to internet stability.
2003: The Al-Jazeera website faced a DDoS attack amid heightened political tensions. This attack aimed to disrupt the news service's online presence and limit its ability to disseminate information.
2004: The SCO Group's website suffered a DDoS attack. This attack was notable for its intensity and its relation to the SCO Group's legal and commercial disputes in the technology sector.
2005: E-bay, one of the world's largest online marketplaces, was the target of a DDoS attack. This attack aimed to disrupt E-bay's extensive e-commerce activities, affecting buyers and sellers worldwide [65].
2006: The payment processing service Storm Pay experienced a severe DDoS attack. This incident disrupted financial transactions and highlighted the vulnerability of online payment platforms.
2007: Estonia faced a series of coordinated DDoS attacks, targeting government and infrastructural networks. These attacks were significant for their political implications and marked one of the first instances of large-scale cyber warfare.
2008: The website of the Georgian president was subjected to a DDoS attack during a period of heightened geopolitical tension, symbolizing the increasing use of cyber-attacks in international conflicts.
2009: The Iranian government's websites, along with major social media platforms like Facebook, Twitter, and Google, faced DDoS attacks. These attacks coincided with significant political events in Iran, indicating a politically motivated cyber assault.
2010: Wordpress.com, a popular blogging platform, encountered a major DDoS attack. This attack impacted numerous blogs and websites hosted on the platform, affecting content creators and readers alike.
2011 and 2012: Sony suffered multiple DDoS attacks. These attacks targeted Sony's gaming and entertainment services, leading to substantial service disruptions and user data risks.
2013: South Korean websites and Spamhaus, a spam-fighting organization, were hit by DDoS attacks. These attacks were significant for their scale and the diversity of targets, from national infrastructure to internet security services.

2014: JP Morgan, one of the largest banks in the world, faced a DDoS attack. This attack highlighted the vulnerability of financial institutions to cyber threats and had implications for customer data security.
2015: GitHub, a platform for software development and collaboration, experienced a DDoS attack. This attack was notable for targeting a service fundamental to the global software development community.
2016: The Rio Olympics were disrupted by a DDoS attack, affecting various online services related to the event. This incident demonstrated the potential for cyber-attacks to impact major international events.
2017: Melbourne IT, an Australian domain registrar and IT service company, suffered a DDoS attack. This attack caused disruptions to several high-profile websites registered through the company.
2018: GitHub was targeted by another major DDoS attack. This attack was significant for its scale and the sophistication of the methods used, underscoring the ongoing challenge of protecting online services against cyber threats.
February 2018: GitHub experienced one of the most powerful DDoS attacks recorded. The attack peaked at 1.35 Tbps, leveraging an amplification technique using Memcached servers. This incident highlighted the evolving nature of DDoS attack methods and the importance of robust defense mechanisms.
September 2019: Wikipedia suffered a significant DDoS attack that rendered the site inaccessible in several countries for hours. This attack highlighted the vulnerability of even well-established online platforms [66].
June 2019: The messaging app Telegram faced a massive DDoS attack, which was believed to be state-sponsored. The attack, primarily affecting users in the Americas, was speculated to be linked to political unrest in certain regions [67].
August 2020: The NZX was hit by severe DDoS attacks over multiple days, disrupting trading activities. These attacks were part of a global campaign targeting financial institutions and were notable for their impact on national infrastructure.
Amid the COVID-19 pandemic, the U.S. Department of Health and Human Services experienced a DDoS attack intended to disrupt information dissemination about the pandemic [68].
May 2021: Several Belgian government websites experienced a DDoS attack, impacting public access to online government services. This incident underscored the increasing tendency of attackers to target essential public sector infrastructure [69].
2021: The gaming platform Steam faced a DDoS attack during its Winter Sale, affecting gamers globally. This attack highlighted the vulnerability of entertainment and e-commerce platforms to such disruptions.
2022: Amid the geopolitical tensions in Eastern Europe, Ukrainian government websites and several banks were targeted by a series of DDoS attacks, seen as part of broader cyber warfare activities.
2023: A leading global streaming service experienced a significant DDoS attack, disrupting services for millions of users. This attack was notable for its scale and the targeting of a major player in the digital entertainment industry.
2023: A prominent international news outlet was targeted by a DDoS attack, impeding access to news services. The attack was speculated to be politically motivated, aimed at suppressing particular news coverage.

Table 1: History of DDoS attack

Sr. No	Attack Year	Attack Targets
1	1990, 1990	IRC chat floods
2	1998	Morris worm
3	2000	Yahoo
4	2001	Code red worm attacks
5	2002	Root servers of DNS
6	2003	Al-Jazeera
7	2004	SCO
8	2005	E-bay
9	2006	Storm pay battling
10	2007	Estonian
11	2008	Georgia president Web site

Sr. No	Attack Year	Attack Targets
12	2009	Iranian Government Web sites, Facebook, Twitter, and Google, Russian blog
13	2010	Wordpress.com, US and South Korean website
14	2011, 2012	Sony
15	2013	South Korean Web sites, Spamhaus
16	2014	JP Morgan
17	2015	Github
18	2016	RIO Olympics
19	2017	Melbourne IT
20	2018	Github
21	2019	Wikipedia, Telegram
22	2020	New Zealand Stock Exchange (NZX), U.S. Health and Human Services Department
23	2021	Belgian Government Websites, Steam
24	2022	Ukrainian Government Websites and Banks
25	2023	Major Streaming Service, International News Outlet

III. DDoS Detection Methods

To identify Distributed Denial of Service (DDoS) attacks, various methodologies have been developed, including statistical approaches such as entropy variations, machine learning techniques, and deep learning methods.

3.1 Statistical Approaches

Estimating statistical properties of network traffic attributes is a common approach for DDoS attack detection. Entropy-based methods, focusing on the entropy variations of specific packet header fields, gained popularity in the mid-2000s. For instance, Feinstein et al. [12] developed a method based on source IP address entropy and Chi-square distribution, highlighting the dissimilarity caused by DDoS attacks compared to legitimate traffic variations. Tao [13] employed entropy changes during rush hour traffic to detect attacks, utilizing data distance to differentiate DDoS attacks from flash crowds. Mousavi [14] proposed an attack detection technique based on actual entropy, calculating entropy through the correlation between source and destination IP addresses. However, entropy is considered less reliable due to relatively high false positives or false negatives [13]. Bojović [15] and Kalkan [16] developed entropy-based scoring structures to identify volumetric DDoS attacks using target IP address entropy and self-motivated groupings of IP and TCP layer attributes. Ahmed et al. [17] introduced an alternative measurement method utilizing packet attributes and traffic flow measures to distinguish between harmful DDoS traffic and benign traffic. Despite the effectiveness, these statistical methods may encounter challenges in online architectures, and determining an appropriate threshold remains a common difficulty.

3.2 Machine Learning and Deep Learning Based DDoS Detection Techniques

Xiao et al. [15] proposed a reliable identification method for DDoS attacks using K-Nearest Neighbors (KNN) and correlation analysis. KNN classifies network traffic data points based on their similarity to known attack profiles. Correlation analysis strengthens attack identification by finding relationships between different traffic features. This approach effectively detects SYN flooding, UDP flooding, and ICMP flooding attacks. Focusing on application-layer DDoS attacks, C. She et al. [16] leveraged One-Class Support Vector Machines (OC-SVM) with honeypot data and machine learning. OC-SVM learns the normal behavior of network traffic from honeypots and flags deviations as potential attacks. Machine learning algorithms further refine the detection based on specific traffic features, enabling effective identification of SYN flooding, HTTP flooding, and NTP amplification attacks. Vishwakarma et al. [17] tackled botnet-based DDoS attacks in the Internet of Things (IoT) by employing an unspecified machine learning algorithm. This algorithm specifically targets botnet command and control (C&C) channels within the IoT network. Analyzing traffic patterns for communication patterns consistent with botnet activity allows effective detection of these attacks. Asad et al. [18] turned to Artificial Neural Networks (ANNs)

for diverse application-layer DDoS attack detection. ANNs are trained on labeled DDoS attack data to recognize specific patterns in network traffic. Incoming traffic is then classified as normal or DDoS based on these learned patterns, enabling accurate identification of attacks like Slowloris and HTTP floods. Focusing on botnet activity within consumer IoT networks, Roopak et al. [19] adopted Bidirectional Long Short-Term Memory (LSTM) networks for text recognition at the packet level. LSTMs analyze packet payload data (e.g., HTTP headers) to identify suspicious patterns or anomalies suggestive of DDoS attack commands. This approach effectively detects malicious activity from compromised IoT devices. Meidan et al. [20] proposed N-BaIoT, an autoencoder-based model for anomaly detection in IoT networks. The autoencoder learns a compressed representation of normal network traffic. Deviations from this normal representation trigger flags for potential DDoS attacks, enabling the identification of malicious activity from compromised IoT devices.

Taking a broader approach, Doshi and Feamster [21] employed various machine learning algorithms, including Support Vector Machines (SVMs) and Random Forests, for general network traffic classification. They extract features from network traffic flows and feed them into these models to classify them as normal or DDoS. This approach provides a general framework for DDoS detection based on network traffic analysis. C. She et al. [22] combined the strengths of Convolutional Neural Networks (CNNs) and LSTMs for general DDoS attack detection. CNNs learn spatial features from network traffic data, while LSTMs capture temporal patterns, using the CICIDS2017 dataset. By combining these, they achieve accurate identification of both spatial and temporal anomalies indicative of DDoS attacks. Focusing on geographically dispersed attacks, Pei et al. [26] leveraged CNNs to analyze geographical features of network traffic. They made use of the ISCX2012, CIC2017, and CSECIS 2018 databases. Their CNNs identify patterns suggesting coordinated DDoS attacks from geographically dispersed attackers. This approach is particularly effective for detecting attacks with geographically diverse attack sources. Doriguzzi et al. [23] prioritized real-time detection with minimal processing overhead by developing a lightweight CNN-based architecture. This custom CNN design enables fast and efficient DDoS attack detection, making it suitable for resource-constrained environments. Jia et al. [24] proposed the FlowGuard system, which combines CNNs and LSTMs for DDoS attack detection in IoT networks. CNNs identify malicious traffic patterns, while LSTMs analyze traffic flow sequences to confirm DDoS attacks. FlowGuard then filters and blocks these malicious flows, providing comprehensive protection for IoT networks. To improve feature selection for DDoS attack detection in IoT networks, Roopak et al. [25] employed CNNs and LSTMs in conjunction with a multi-objective optimization algorithm. This algorithm selects the most effective features for attack classification, leading to more accurate detection and improved overall defense. M. Shurman et al. in [56] propose two methodologies for detecting DDoS attacks, particularly focusing on IoT networks and DrDoS attacks. The first is a hybrid-based IDS designed for IoT networks, which detects and blocks suspicious network traffic. The second is a deep learning model based on LSTM, trained on the CICDDoS2019 dataset, to specifically target DrDoS attacks. Furthermore, the paper outlines future work involving the development of a new model to detect exploitation-based attacks in the same dataset and to evaluate these methodologies in realistic system settings.

CNN and LSTM neural networks were merged by Yijie, Li, et al. [27] to improve DDoS attack detection. Whereas the CNN concentrated on spatial patterns in the CICDDoS2019 dataset, the LSTM network was in charge of examining temporal patterns, such as variations in traffic volume over time. Because CNNs are great at identifying patterns and LSTM networks are good at processing time-series data, this combination allowed for a thorough examination. Using the CICIDS2017 dataset, Li, Qian et al. [28] used a CNN and LSTM neural network technique similar to that used in [22]. By utilizing the advantages of both CNN for geographical recognition and LSTM for temporal traffic pattern analysis, their approach proved successful in detecting DDoS attacks. The Random Forest machine learning approach was used by Yuan et al. [29] to identify DDoS attacks. It used the TFN2K Programme to create DDoS attack traffic for a local environment, and then it used network traffic statistics and the Random Forest classifier to identify these attacks. Random Forest's capacity to analyze big datasets and spot intricate patterns made the strategy successful. In their study, Kaur et al. [30] employed an LSTM neural network to analyze network traffic data in order to identify DDoS attacks. The LSTM network picked up on the typical network traffic patterns, and it used this baseline knowledge to spot deviations that suggested DDoS attacks. The long-term dependency memory of LSTM made it appropriate for this use.

Principal Component Analysis (PCA) and Recurrent Neural Networks (RNN) were used in the study by Yan Naung et al. [31]. PCA made learning easier by reducing the dimensionality of the network traffic data from the KDD CUP 1999 dataset. After that, the RNN examined these condensed data patterns to identify DDoS attacks, essentially

picking up on the general patterns of network traffic. Using an RNN neural network, Bindra et al. [32] were able to identify unusual patterns indicative of DDoS assaults from normal network traffic patterns learned from the UNB ISCX dataset. By utilizing the KDDCUP dataset, Roempluk et al. [33] integrated Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Artificial Neural Networks (ANN) to identify DDoS attacks. Since each classifier has a distinct advantage in pattern recognition and anomaly detection, these classifiers were employed to learn the typical traffic patterns, offering a thorough method. Masud et al. [34] examined the BOT-IOT dataset for DDoS attack detection using an ANN classifier and SMOTE. While SMOTE solved the issue of class imbalance by oversampling the minority class (DDoS assaults) to enhance the classifier's performance, the ANN learned the typical traffic patterns. Using the CICIDS 2017 dataset, Vinayak, S. et al. [35] used a Random Forest classifier with an n-estimate technique to identify DDoS attacks. Through the use of the n-estimate methodology, the classifier's accuracy in spotting abnormalities was improved as it learned the patterns of typical network traffic. Panda et al.'s [36] work employed the KDD CUP99 and NSL KDD datasets to detect DDoS assaults using KNN, MLP, and SVM classifiers. These classifiers worked together to give a strong method for understanding and recognizing changes from typical network traffic patterns.

DDoSNet, which was created by Ahmed et al. [47], extracted and analyzed features from the CICDDoS2019 dataset using CNNs and RNNs. With a high accuracy rate of 99.89%, the CNNs extracted spatial characteristics while the RNNs concentrated on temporal patterns. SVMs and the Boruta algorithm were used by Alazab et al. [48] to pick features from the CICDDoS2019 dataset. They obtained a 99.59% accuracy rate with ensemble SVM classifiers using AdaBoost. The CICDDoS2019 dataset was subjected to PCA, RF, and SVM analyses by Park, S. J. et al. [49]. The dimensionality of the dataset was decreased by PCA, and then the traffic was classified using RF and SVMs. With an accuracy rate of 99.23%, our hybrid method demonstrated the advantages of combining feature reduction and classification. Using an Improved Deep Belief Network (IDBN), El-Bakry et al. [50] collected features and classified network traffic from the CICDDoS2019 dataset. The IDBN demonstrated the effectiveness of deep learning in DDoS attack detection with an accuracy rate of 99.45%. CNN and LSTM were coupled by Wang, H. et al. [51] to analyze the CICDDoS2019 dataset. The efficacy of merging CNN and LSTM in identifying DDoS attacks was demonstrated by the 99.78% accuracy rate attained by the LSTM after learning temporal patterns from the retrieved data by CNN.

3.3 Analysis of Various Researchers' Work with AI Techniques

Table 2: Summarizes various studies on DDoS attack detection using machine learning and deep learning techniques, along with the datasets used.

Sr. No.	Paper Title	Year of Publishing	Methods Used	Dataset
1	[22]	2019	CNN+LSTM	CICIDS2017
2	[26]	2020	CNN	ISCX2012, CIC2017, CSECIS2018
3	[27]	2020	LSTM, CNN	CICDDoS2019
4	[28]	2020	CNN+LSTM	CICIDS2017
5	[29]	2019	ML Technique (Random Forest)	Used TFN2K tool to conduct local DDoS attacks
6	[30]	2018	LSTM (Long Short-Term Memory)	DDoS attack software
7	[31]	2019	PCA and RNN	KDD CUP 1999
8	[32]	2017	RNN	UNB ISCX
9	[33]	2019	SVM, KNN, ANN	KDDCUP
10	[34]	2020	ANN SMOTE	BOT-IOT
11	[35]	2019	RF with n-estimate	CICIDS2017
12	[36]	2019	KNN, MLP, SVM	KDD CUP99, NSL KDD

13	[47]	2020	DDoSNet, CNNs and RNNs	CICDDoS2019
14	[48]	2020	SVMs	CICDDoS2019
15	[49]	2021	PCA, RF, and SVMs	CICDDoS2019
16	[50]	2021	Improved Deep Belief Network (IDBN)	CICDDoS2019
17	[51]	2022	CNN and LSTM	CICDDoS2019

This summary highlights the diversity of machine learning and deep learning approaches employed for DDoS attack detection, showcasing their respective datasets and methodologies. The integration of CNNs, LSTMs, Random Forests, and other advanced techniques demonstrates the ongoing evolution of DDoS detection strategies and their potential to enhance network security against such pervasive threats.

IV. Performance Evaluation And Discussion

The evaluation metrics employed in this assessment utilize the false positive rate (FR), the detection rate (DR), and the overall detection rate (AR) to analyze experimental results. This choice is driven by the classification nature of determining whether the recognition data corresponds to a Distributed Denial of Service (DDoS) assault.

False Positive Rate (FR): The normal behavior ratio, represented as FR=FP/(FP+TP), characterizes the detection of attack data in terms of the false positive rate. It quantifies the proportion of normal data incorrectly classified as attack data.

Detection Rate (DR): The detection rate, denoted as DR=TN/(TN+FN), expresses the fraction of attack behavior identified by the attack data detection. It measures the effectiveness of the system in recognizing actual attack behavior.

Overall Detection Rate (AR): The total detection rate, articulated as AR=(TP+TN)/(TP+TN+FP+FN), encompasses the detection of normal data as normal and the detection of attack data as the percentage of attack data. It provides an overall assessment of the classification performance.

In this context, TP refers to a positive sample that is correctly anticipated to be positive, where normal data is expected to behave normally, while TN represents a predicted negative sample, indicating that the assault data is expected to behave normally. Conversely, FP refers to a negative sample that is mistakenly expected to be positive, and FN is a positive sample that is erroneously projected to be negative, signifying that normal data is anticipated to be aggressive.

In [29], the experimental setup involves utilizing the remaining set of attack data packets mixed with regular traffic as the test set after training the random forest model with the training data set. This facilitates model detection. To control the ratio of normal traffic to attack traffic, cross-sample both attack and normal traffic, determine each sample's categorization behavior, and adjust the sampling flow duration. Concurrently, the data from the Support Vector Machine (SVM) method are detected using the LIBSVM library, and the results of the random forest model detection are subsequently compared. This multifaceted approach enhances the robustness and reliability of the DDoS detection system, ensuring a comprehensive evaluation of its performance.

The following graphs summarize the three protocol types' detection results from the DDoS assault data. The graphs in Fig. 2, 3, and 4 provided demonstrate that the detection model proposed in [29] surpasses the performance of the SVM algorithm model, consistently achieving a higher detection rate across the outcomes for the detection of DDoS attacks in three different protocols as background traffic increases.

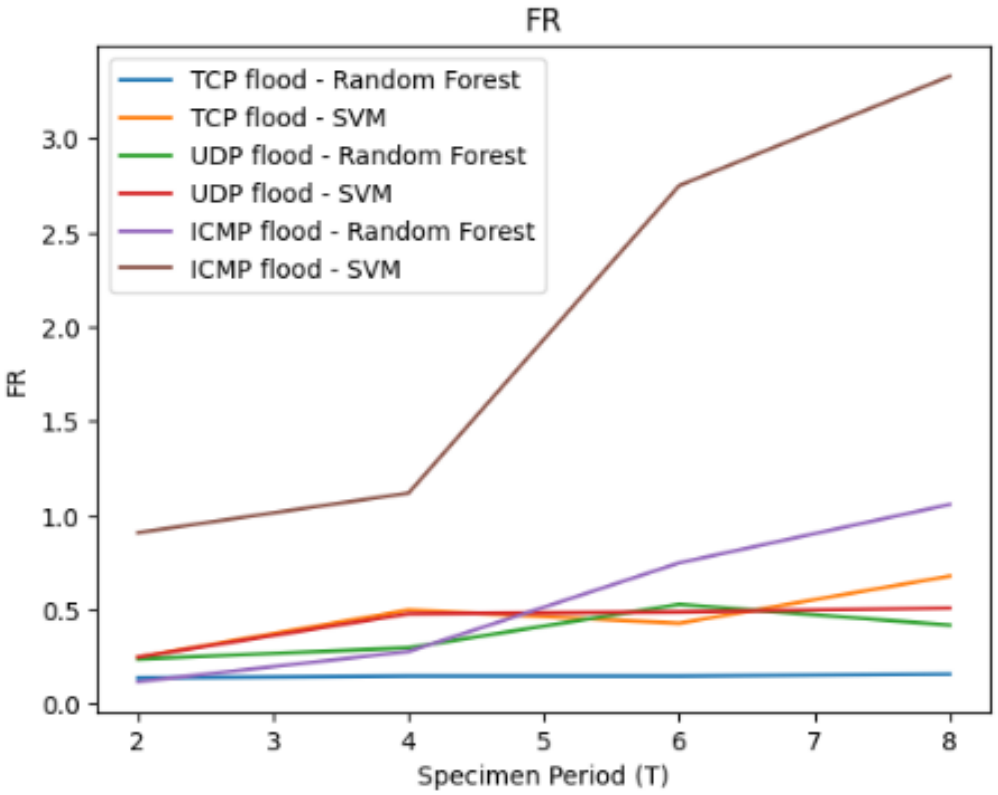

Fig. 2: False Positive Rate (FR)

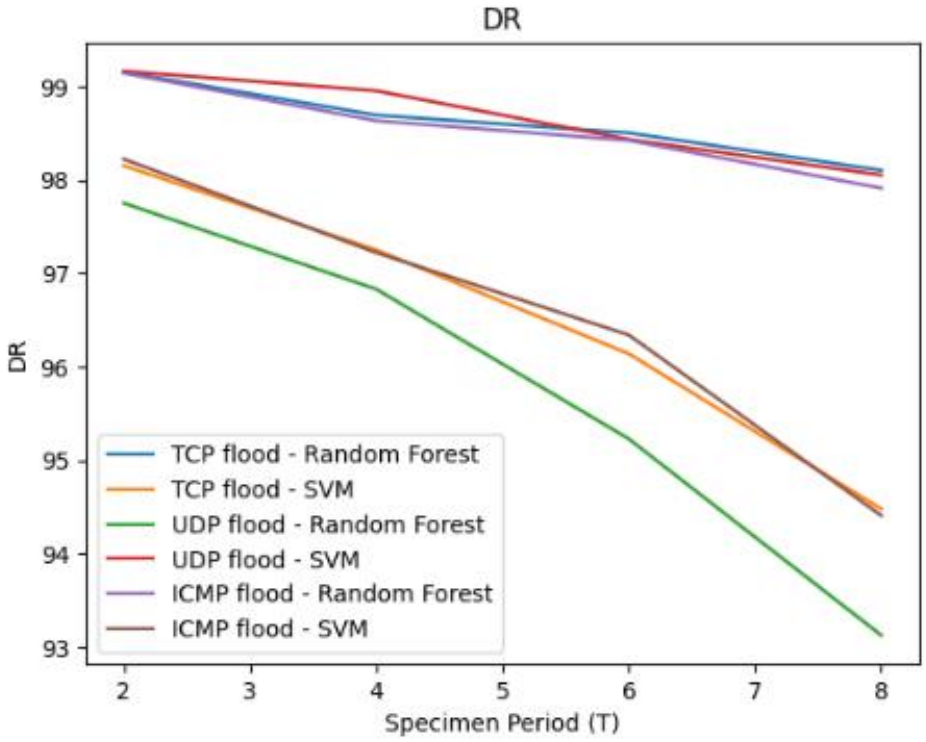

Fig. 3: Detection Rate (DR)

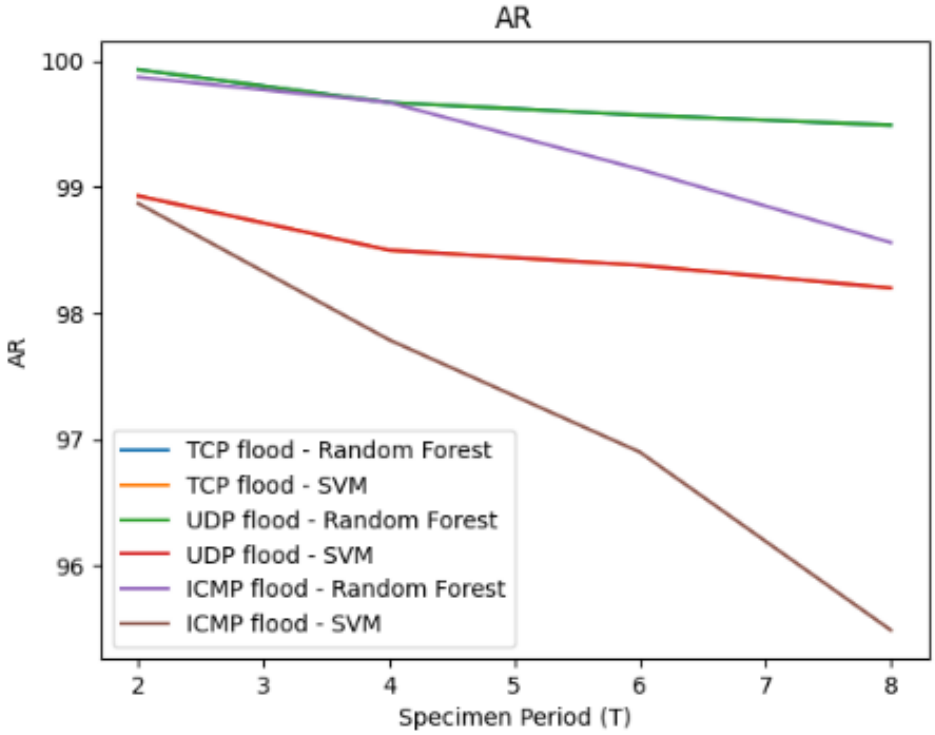

Fig. 4: Overall Detection Rate (AR)

The comparative analysis of DDoS attack detection methods based on the CICDDoS2019 dataset shown in Fig. 5, uncovers the superior accuracy of models like CNN-LSTM [50] and DDoSNet [46], both achieving over 99%. These models demonstrate the power of combining neural network approaches for intricate threat detection. Ensemble Learning [47] and Improved Deep Belief Network [49] also show promising results. Variability in Random Forest models [70, 71] underscores the influence of specific training conditions. The study indicates an average accuracy of 99.31% across models, emphasizing their potential effectiveness. However, it also suggests the importance of considering network environments and attack types in selecting the optimal detection method, highlighting the need for further research in diverse operational scenarios.

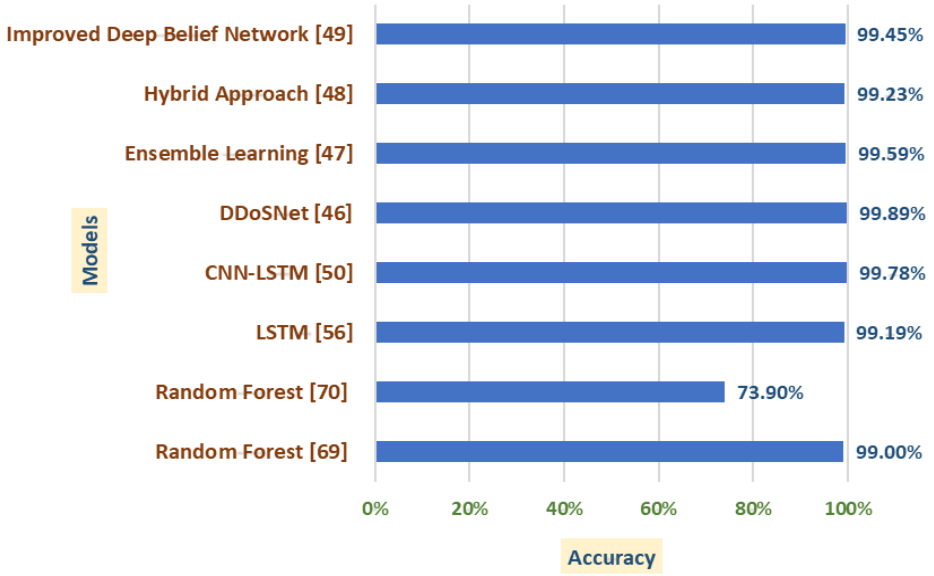

Fig. 5: Accuracy of DDoS Attack Detection Methods using CICDDoS2019 Dataset

The study given in Table 3 and Fig. 6 evaluate the performance of various models for DDoS attack detection on the CICIDS2017 dataset [19]. Deep learning models, particularly CNN+LSTM, achieved the highest accuracy (97.16%) and impressive recall (99.1%). LSTM alone also showed strong precision (98.44%). Among machine

learning approaches, SVM had a high recall (99.12%), but Random Forest had lower precision (90.18%). The results indicate that while hybrid deep learning models offer significant accuracy and recall, single LSTM models excel in precision. Overall, deep learning methods outperform traditional machine learning algorithms in detecting DDoS attacks.

Table 3: Models for DDoS attack detection on the CICIDS2017 dataset

Model	Accuracy (%)	Precision (%)	Recall (%)
1d-CNN	95.14	98.14	90.17
MLP	86.34	88.47	86.25
LSTM	96.24	98.44	89.89
CNN+LSTM	97.16	97.41	99.1
SVM	95.5	97.72	99.12
Bayes	95.19	92.56	92.84
Random Forest	94.64	90.18	90.89

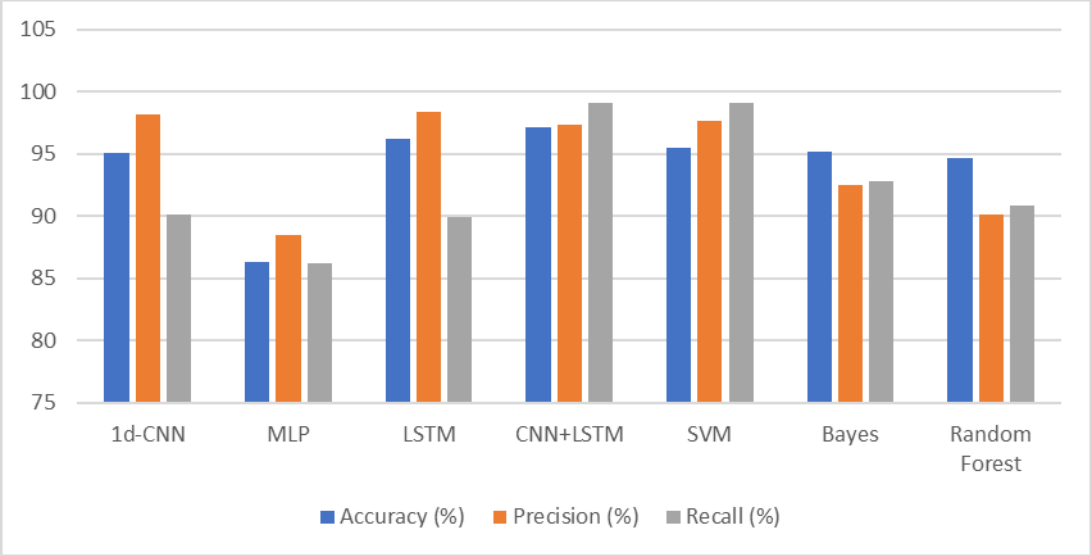

Fig. 6: Models for DDoS attack detection on the CICIDS2017 dataset

In the comparative analysis presented in Table 4, various models for DDoS attack detection using the ISCX2012 dataset are evaluated, highlighting the advancements in network security technologies. The LUCID model [23] stands out with its superior performance, marked by an exceptional accuracy of 0.9888 and a high F1 score of 0.9889. This indicates a well-balanced precision and recall, essential in effective DDoS detection. Furthermore, LUCID's low false positive rate (FPR) of 0.0179 is indicative of its proficient capability in distinguishing between benign and malicious traffic, thereby minimizing the likelihood of erroneously flagging legitimate traffic as attacks. These metrics collectively demonstrate LUCID's effectiveness, surpassing other models like 3LSTM [4], TR-IDS [36], and E3ML [47] in crucial performance areas. The success of LUCID can be attributed to its preprocessing mechanisms, which evidently enhance its detection capabilities.

On the other hand, the 3LSTM model, as detailed in the DeepDefense paper [4], also shows noteworthy performance with an accuracy of 0.9841 and an F1 score of 0.9840. However, the lack of data on its FPR prevents a comprehensive assessment of its overall efficiency. The TR-IDS model [36], which utilizes a text-CNN for feature extraction in tandem with a Random Forest classifier, records a respectable accuracy of 0.9809. Nonetheless, its lower true positive rate (TPR) of 0.9593, in comparison to LUCID, suggests a reduced effectiveness in detecting DDoS attacks, potentially leading to higher false negatives. E3ML [47], employing an intricate architecture with entropy-based features and multiple machine learning classifiers, only reports its TPR (0.9474). This partial data suggests a tendency towards false negatives, a significant concern in network security. The incomplete data across all metrics for some models, such as E3ML [47] and 3LSTM [4], underscores the challenges in establishing a

comprehensive comparative framework, highlighting the necessity for more holistic reporting in cybersecurity research to facilitate better-informed conclusions and advancements in the field.

Table 4: Comparative analysis of models for DDoS attack detection using the ISCX2012 dataset

Model	Accuracy (ACC)	False Positive Rate (FPR)	Positive Predictive Value (PPV)	True Positive Rate (TPR)	F1 Score (F1)
LUCID [23]	0.9888	0.0179	0.9827	0.9952	0.9889
3LSTM [4]	0.9841	N/A	0.9834	0.9847	0.9840
TR-IDS [36]	0.9809	0.0040	N/A	0.9593	N/A
E3ML [47]	N/A	N/A	N/A	0.9474	N/A

In evaluating the efficacy of DDoS detection models, our analysis revealed a distinct edge of deep learning techniques over conventional machine learning algorithms. The CNN+LSTM model, in particular, emerged as a top performer, demonstrating high accuracy and recall, a testament to its capacity to discern complex network traffic patterns indicative of DDoS activity. This superiority, however, is accompanied by performance discrepancies among models, attributable to differences in their architectures and training protocols. Such variations underscore the need for bespoke solutions attuned to the specificities of various network environments and attack methodologies. Consequently, this insight lays a foundation for future exploration, stressing the necessity for exhaustive performance assessments across a multitude of metrics to confirm the resilience of DDoS detection mechanisms.

Central to this endeavor is the choice of dataset, with the CICDDoS2019 dataset standing out for its modern and heterogeneous compilation of DDoS attack scenarios. The robust performance of deep learning models, particularly CNN+LSTM, on this dataset substantiates its suitability for the development of advanced detection systems. Given its encompassing representation of current DDoS threats, the CICDDoS2019 dataset is an exemplary choice for the training and validation of proposed systems, ensuring their effectiveness against an expansive spectrum of DDoS attacks. Thus, the deployment of this dataset is instrumental in enhancing the detection capabilities and reliability of emerging DDoS defense mechanisms.

V. Conclusion

The growing threat of Distributed Denial of Service (DDoS) attacks, particularly in IoT networks, has driven extensive research into network defenses. Despite significant progress, a definitive solution remains elusive, necessitating ongoing innovation in DDoS detection. The evolving tactics of attackers and the inherent vulnerabilities of IoT devices require adaptive and robust detection strategies. Advanced machine learning and deep learning techniques, especially CNN and LSTM models, have shown promise in improving detection accuracy. Utilizing comprehensive datasets like CICDDoS2019 is crucial for developing effective detection systems. Continuous research and collaboration across academia, industry, and government are vital to stay ahead of sophisticated DDoS attacks. As IoT technology advances, proactive measures are essential to safeguard digital infrastructures and maintain service integrity in an increasingly connected world.

VI. Future Trends And Challenges

As DDoS attacks evolve, leveraging 5G and IoT networks for amplified impact, detection strategies face new challenges. Technological advancements like AI and machine learning offer dual-edged swords, aiding both attackers and defenders. Detection systems must evolve to handle sophisticated multi-vector attacks, address false positives, and ensure scalability in a rapidly changing digital landscape.

International cooperation and regulatory frameworks will play a crucial role in standardizing defenses globally. Future research should focus on developing adaptive, proactive defense mechanisms, integrating DDoS defense within broader network security frameworks, and exploring the potential of emerging technologies for predictive defense strategies. Emerging trends suggest a need for hybrid detection models combining various AI techniques to enhance detection accuracy and efficiency. Additionally, the integration of blockchain technology for secure and transparent data handling may offer new avenues for DDoS mitigation. The collaboration between academia, industry, and government is essential to foster innovation and implement effective, scalable solutions.

VII. Compliance With Ethical Standards

This research involves a comprehensive analysis of existing literature and methodologies in the field of cybersecurity, specifically focusing on DDoS attack detection. As this study is a literature review and does not involve human or animal subjects, there were no ethical issues related to human or animal testing. Therefore, no specific ethical approval was required for this study.

VIII. Competing Interests

The authors, Vinay Tila Patil and Shailesh Shivaji Deore, declare that they have no competing interests in the publication of this manuscript. There are no financial or non-financial conflicts of interest that could be perceived as prejudicing the impartiality of the research reported.

IX. Research Data Policy And Data Availability Statements

This review study synthesizes and analyzes information from previously published research in the field. As such, it does not involve the generation of new data but rather relies on existing published works. All sources of data are appropriately cited and referenced in the manuscript. Therefore, a separate data availability statement is not applicable for this study.

References

[1] C. Kolias, G. Kambourakis, A. Sta vrou, and J. Voas, “DDoS in the loT: Mirai and other botnets”, Computer, vol. 50, no. 7, pp. 80-84, 2017.

[2] Krebs on Security, “DDoS on Dyn Impacts Twitter, Spotify, Reddit”, https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitterspotify-reddit, 2016,

[3] Radware, “Memcached DDoS Attacks”, https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/memcached-underattack/, 2018,

[4] “Inside the infamous mirai iot botnet: A retrospective analysis,” https://blog.cloudflare.com/inside-mirai-the-infamous-iotbotnet-a-retrospective-analysis/, 2017.

[5] “The iot rundown for 2020: Stats, risks, and solutions,” https://securitytoday.com/Articles/2020/01/13/The-IoTRundown-for-2020.aspx?Page=2, 2020.

[6] “More than half of IoT devices vulnerable to severe attacks,” https://threatpost.com/half-iot-devices-vulnerable-severeattacks/153609/, 2020.

[7] T. Peng, C. Leckie, and K. Rama Mohana Rao, “Survey of network-based defense mechanisms countering the dos and ddos problems,” ACM Computing Surveys (CSUR), vol. 39, no. 1, p. 3, 2007.

[8] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis et al., “Understanding the Mirai botnet,” in 26th fUSENIXg Security Symposium (fUSENIXg Security 17), 2017, pp. 1093–1110.

[9] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, “Statistical Approaches to DDoS Attack Detection and Response,” in Proceedings DARPA Information Survivability Conference and Exposition, 2003.

[10] Tao, Y., Yu, and S.: DDoS attack detection at local area networks using information theoretical metrics. In: IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 233–240. IEEE (2013)

[11] Mousavi, S.M., Sthilaire, M.: Early detection of DDoS attacks against SDN controllers. In: International Conference on Computing, Networking and Communications, pp. 77–81. IEEE (2015)

[12] P. Bojovi´c, I. Ba˘si˘cevi´c, S. Ocovaj, and M. Popovi´c, “A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method,” Computers & Electrical Engineering, vol. 73, pp. 84–96, 2019.

[13] K. Kalkan, L. Altay, G. G¨ur, and F. Alag¨oz, “JESS: Joint Entropy-Based DDoS Defense Scheme in SDN,” IEEE Journal on Selected Areas in Communications, vol. 36, no. 10, pp. 2358–2372, Oct 2018.

[14] M. E. Ahmed, S. Ullah, and H. Kim, “Statistical application fingerprinting for ddos attack mitigation,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 6, pp. 1471–1484, 2019.

[15] P. Xiao, W. Qu, H. Qi, and Z. Li, “Detecting DDoS attacks against data center with correlation analysis,” Computer Communications, vol. 67, pp. 66–74, 2015.

[16] C. She, W. Wen, Z. Lin, and K. Zheng, “Application-layer DDoS detection based on a one-class support vector machine,” International Journal of Network Security & Its Applications (IJNSA), vol. 9, no. 1, pp. 13–24, January. 2017.

[17] R. Vishwakarma and A. K. Jain, “A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks,” 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), April. 2019.

[18] M. Asad, M. Asim, T. Javed, M. O. Beg, H. Mujtaba, and S. Abbas, “Deep detect: Detection of distributed denial of service attacks using deep learning,” The Computer Journal, 2019.

[19] M. Roopak, G. Y. Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0452–0457, 2019.
[20] Meidan, Yair & Bohadana, Michael & Mathov, Yael & Mirsky, Yisroel & Shabtai, Asaf & Breitenbacher, Dominik & Elovici, Yuval. (2018). “N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders.” IEEE Pervasive Computing. 17. 12-22. 10.1109/MPRV.2018.03367731.
[21] R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning DDoS detection for consumer internet of things devices,” 2018 IEEE Security and Privacy Workshops (SPW), 2018.
[22] C. She, W. Wen, Z. Lin, and K. Zheng, “Dad-mcnn: DDoS attack detection via multi-channel CNN,” Proceedings of the 2019 11th International Conference on Machine Learning and Computing, pp. 484—-488, February. 2019.
[23] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del-Rincón and D. Siracusa, "Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection," in IEEE Transactions on Network and Service Management, vol. 17, no. 2, pp. 876-889, June 2020, doi: 10.1109/TNSM.2020.2971776.
[24] Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552-9562, Oct. 2020, doi: 10.1109/JIOT.2020. 2993782.
[25] M. Roopak, G. Y. Tian and J. Chambers, "An Intrusion Detection System Against DDoS Attacks in IoT Networks," 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), 2020, pp. 0562-0567, doi: 10.1109/CCWC47524.2020.9031206.
[26] Pei, Jiangtao & Chen, Yunli & Ji, Wei. (2019). A DDoS Attack Detection Method Based on Machine Learning. Journal of Physics: Conference Series. 1237. 032040. 10.1088/1742-6596/1237/3/032040.
[27] Yijie, Li, Zhai Shang and Chen Mingrui. “DDoS attack detection method based on feature extraction of deep belief network.” arXiv: Cryptography and Security (2019).
[28] Li, Qian & Meng, Linhai & Zhang, Yuan & Yan, Jinyao. (2019). DDoS Attacks Detection Using Machine Learning Algorithms. 10.1007/978-981-13-8138-6_17.
[29] Yuan, Xiaoyong, Chuanhuang Li and Xiaolin Li. “DeepDefense: Identifying DDoS Attack via Deep Learning.” 2017 IEEE International Conference on Smart Computing (SMARTCOMP) (2017): 1-8.
[30] Kaur, Gaganjot and Prinima Gupta. “Hybrid Approach for detecting DDOS Attacks in Software Defined Networks.” 2019 Twelfth International Conference on Contemporary Computing (IC3) (2019): 1-6.
[31] Soe, Yan Naung, Paulus Insap Santosa and Rudy Hartanto. “DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment.” 2019 Fourth International Conference on Informatics and Computing (ICIC) (2019): 1-5.
[32] Bindra, Naveen & Sood, Manu. (2019). Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset. Automatic Control and Computer Sciences. 53. 419-428. 10.3103/S0146411619050043.
[33] Roempluk, Tanaphon and Olarik Surinta. “A Machine Learning Approach for Detecting Distributed Denial of Service Attacks.” 2019 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT-NCON) (2019): 146-14.
[34] Masud, M., Amin, I., Bashir, M., & Anjum, M. O. (2020). A novel approach for DDoS attack detection using hybrid ANN-SMOTE technique. Computers & Security, 97, 101964.
[35] Vinayak, S., & Bhavsar, A. (2019). Network anomaly detection using random forest with n-estimate feature selection. International Journal of Network Security, 22(3), 348-358.
[36] Panda, A. K., & Mishra, P. (2019). An intrusion detection approach based on hybrid feature selection and SVM. Journal of Network and Computer Applications, 141, 92-101.
[37] Patil, Purushottam & Patil, Vinay. (2020). Smart Forest: An IoT Based Forest Safety and Conservation System Purushottam Rohidas Patil, Vinay Tila Patil. International Journal of Scientific & Technology Research. 9. 7286.
[38] Vinay T. Patil, P R. Patil, V O. Patil, S V. Patil, “Performance and information security evolution with firewalls”, GRADIVA REVIEW JOURNAL, ISSN NO: 0363-8057.
[39] Shailesh S. Deore, Dr. Ashok Narayan, “Systematic Review of Energy-Efficient Scheduling Techniques in Cloud Computing” International Journal of Computer Applications (0975-8887), Vol.52, No.15, August 2012, DOI > 10.5120/8275-1877.
[40] Shailesh S. Deore, Dr. Ashok Narayan, “Energy-Efficient Scheduling Scheme for Virtual Machines in Cloud Computing” International Journal of Computer Applications (0975-8887), Vol.56, No.10, October 2012, DOI > 10.5120/8926-2999.
[41] Shailesh S. Deore, Dr. Ashok Narayan, “Energy-Efficient Scheduling and Allocation Scheme for Virtual Machines in Private Cloud “International Journal of Applied Information System (2249-0868), Vol.5, No.1, January 2013, DOI > 10.5120/ ijais12-450842.
[42] S.S. Deore, "Design and Optimization of scheduling schemes for Cloud Computing", Shri Jagdish prasad Jhabarmal Tibarewala University, Rajasthan.
[43] Morris, Robert T., and Douglas J. Forest. "A worm to slow the internet down." Bell Labs Technical Report (1998).

[44] Jovanovic, Nenad, Pedro Garcia Lopez, and Jens Hjelmstad. "IRC-flood attacks: a taxonomy and analysis." In Proceedings of the 20th IEEE International Conference on Computer Communications, 2001. IEEE, 2001.
[45] "2000 Yahoo! DDOS Attack." [Online]. Available: https://en.wikipedia.org/wiki/Denial-of-service_attack: https://en.wikipedia.org/wiki/Denial-of-service_attack.
[46] Ahmed, M., Iqbal, S. Z., Azam, M. A., Naeem, M. A., & Hassan, M. A. (2020). DDoSNet: A deep-learning model for detecting network attacks. IEEE Access, 8, 108502-108512.
[47] Alazab, M. A., Rahim, S. A., & Al-Husnaini, A. T. (2020). An efficient feature selection and ensemble learning model for DDoS attack detection. IEEE Access, 8, 117381-117390.
[48] Park, S. J., Yoo, J. H., & Lee, H. K. (2021). A hybrid approach for DDoS attack detection using machine learning techniques. Sensors (Switzerland), 21(12), 4149.
[49] El-Bakry, A. A. A., Abd Elaziz, M. A., Hassan, M. A., & Abdel-Hamid, A. E.-H. (2021). DDoS attack detection based on improved deep belief network. Journal of Network and Computer Applications, 173, 102934-102943.
[50] Wang, H., Wang, Y., & Wang, L. (2022). A novel enhanced deep learning-based approach for DDoS detection. Security and Communication Networks.
[51] "Code Red worm." [Online]. Available: https://en.wikipedia.org/wiki/Code_Red_%28computer_ worm%29
[52] "2002 DNS Server Attacks." [Online]. Available: https://en.wikipedia.org/wiki/Distributed_denial-of-service_attacks_on_
root_nameservers
[53] "2003 Al Jazeera DDoS attack." [Online]. Available: https://en.wikipedia.org/wiki/Cyberattack.
[54] "SCO v. Novell." [Online]. Available: https://en.wikipedia.org/wiki/SCO_Group.
[55] M. Ahmed, S. Z. Iqbal, M. A. Azam, M. A. Naeem, and M. A. Hassan, “DDoSNet: A deep-learning model for detecting network attacks,” IEEE Access, vol. 8, pp. 108502–108512, 2020.
[56] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS Attack Detection Using Deep Learning and IDS," in The International Arab Journal of Information Technology, vol. 17, no. 4A, Special Issue, 2020. DOI: https://doi.org/10.34028/iajit/17/4A/10.
[57] S. J. Park, J. H. Yoo, and H. K. Lee, “A hybrid approach for DDoS attack detection using machine learning techniques,” Sensors (Switzerland), vol. 21, no. 12, p. 4149, 2021.
[58] A. A. A. El-Bakry, M. A. Abd Elaziz, M. A. Hassan, and A. E.-H. Abdel-Hamid, “DDoS attack detection based on improved deep belief network,” Journal of Network and Computer Applications, vol. 173, pp. 102934–102943, 2021.
[59] H. Wang, Y. Wang, and L. Wang, “A novel enhanced deep learning-based approach for DDoS detection,” Security and Communication Networks.
[60] Stoppelman, M. A., & White, G. M. (1993, March). The Morris worm: A computer virus case study. In Proceedings of the 1993 Workshop on Intrusion Detection and Prevention (pp. 1-3). ACM.
[61] The Cat's Cradle of Technology: jargonology. (n.d.). Accessed December 16, 2023, from http://catb.org/jargon/html/: http://catb.org/jargon/html/
[62] BBC News. (2000, March 10). Yahoo hit by major cyber-attack. https://www.bbc.com/news/world-us-canada-38324527
[63] Soderlund, P. (2001, September). Code red: The worm and the lessons learned. SANS Institute Information Security Reading Room.
[64] Denning, D. E. (2005). Information warfare (2nd ed.). Addison-Wesley.
[65] The Record. (2019, September9). Largest DDoS incidents: Amazon, Cloudflare, Google. https://therecord.media/
[66] TechCrunch. (2019, September7). Wikipedia blames malicious DDoS attack after site goes down across Europe & Middle East.
[67] BBC News. (2020, August 13). New Zealand stock exchange hit by cyber-attack. https://www.bbc.com/news/53918580
[68] Bleeping Computer. (2020, August 19). US Health Department site hit with DDoS cyber-attack. https://malwaretips.com/blogs/remove-ddos-attack-detected-delete-viruses/
[69] Kiourkoulis S., “DDOS Datasets: Use of Machine Learning to Analyse Intrusion Detection Performance,” Master Thesis, Luleå University of Technology, Space Engineering, 2020.
[70] Gangwar A. and Sahu S., “A Survey on Anomaly and Signature-Based Intrusion Detection System,” International Journal of Engineering Research and Applications, vol. 4, no. 4, pp. 67- 72, 2014
[71] Nagarajan, S., Agarwal, S., & Sharma, S. (2012). Understanding Distributed Denial-of-Service Attacks with Botnets. In International Journal of Applied Cryptology and Network Security (Vol. 7, No. 2, pp. 134-154). Springer, Berlin, Heidelberg.
[72] Al-Ameen, M. A., Anjum, A., Javaid, U., & Ashraf, M. A. (2017, August). A Taxonomy of DDoS Attacks Targeting Application Layer. In Procedia Computer Science (Vol. 109, pp. 75-82). Elsevier.
[73] Al-Ameen, M. A., Anjum, A., Javaid, U., & Ashraf, M. A. (2019, September). Reflection and Amplification-Based DDoS Attacks: State-of-the-Art and Countermeasures. In IEEE Communications Surveys & Tutorials (Vol. 21, No. 3, pp. 2618-2644). IEEE.

[74] Wang, H., Wang, Y., Wang, L., & Ye, X. (2018, September). A Comprehensive Study of SYN Flood Attacks and Their Countermeasures. In IEEE Transactions on Dependable and Secure Computing (Vol. 16, No. 5, pp. 842-857). IEEE.

INTRODUCTION OF AUTHORS

Mr. Vinay Patil, born in 1985 in Shahada, Maharashtra, India, is an accomplished educator and researcher with a robust academic background. He earned his BE in Information Technology from North Maharashtra University in 2007 and later pursued an MTech in Software Engineering at Rajiv Gandhi Proudygiki Vishwavidyalaya in 2014. Currently dedicated to advancing knowledge in the field, Mr. Patil is pursuing a Ph.D. in Computer Engineering at Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon. With a teaching career spanning 16 years, he commenced as an Assistant Professor at PSGVP Mandal's D. N. Patel College of Engineering, Shahada, and has been contributing significantly to academia. Since September 2023, he has been serving as an Assistant Professor at Ajeenkya D. Y. Patil University, Pune. Mr. Patil's research interests encompass cutting-edge areas such as Cloud Computing, Cyber Security, Machine Learning, Deep Learning, and the Internet of Things (IoT), reflecting his commitment to staying at the forefront of technological advancements and making notable contributions to the field.

Dr. Shailesh Deore, born in Dhule, Maharashtra, India, in 1982, is a distinguished educator and researcher in the field of Computer Engineering. He earned his BE degree from North Maharashtra University in 2023 and went on to achieve a Ph.D. in Computer Engineering from Shri J J T University, Rajasthan, India, in 2014. Dr. Deore's academic journey began in 2004 when he joined the Department of Computer Engineering at SSVPs B.S. Deore COE Dhule as a Lecturer, later advancing to the position of Assistant Professor in 2009. With an impressive 20 years of teaching experience, he has been a dedicated member of the Computer Engineering Department. Since 2016, Dr. Deore has held the position of Associate Professor, contributing significantly to the academic and research endeavors of the institution. His current research interests span several cutting-edge areas, including cloud computing, Energy-Efficient job scheduler algorithm schemes in a private cloud environment, machine learning, and data mining. Driven by a passion for staying at the forefront of technological advancements, Dr. Deore continues to make valuable contributions to the field through his research and teaching endeavors.