Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Machine Learning Based Approaches for Detecting and Preventing Distributed DoS Attacks in IoT

Akhilesh Nagar[1], Swapnesh Taterh[2], Bishwajeet Kumar Pandey[3]
[1]-*Research Scholar, Amity Institute of Information Technology Jaipur, Rajasthan India (sayhiakhilesh@gmail.com)*
[2]-*Professor and Head, Amity Institute of Information Technology Jaipur, Rajasthan India (staterh@jpr.amity.edu)*
[3]-*Associate Professor GL Bajaj College of Technology and Management, Greater Noida, India (dr.pandey@ieee.org)*

ARTICLE INFO

Received: 02 Oct 2024

Revised: 12 Nov 2024

Accepted: 26 Nov 2024

ABSTRACT

For quicker reaction times, the data-driven infrastructure known as the Internet of Things (IoT) heavily relies on intelligent sensing devices. IoT devices are now susceptible to more expansive risk surfaces due to the changing cyber threats landscape, which could result in data breaches. Distributed Denial of Service (DDoS) assaults are major cyber-attacks among the many possible attacks because of their capacity to render services unusable by flooding systems with traffic. Strong DDoS detection technologies specifically designed for IoT are essential for the long-term growth of every sector that IoT serves. Since IoT devices frequently lack the built-in security features seen in more established computing platforms. As a consequence, DDoS analysis and defence are a growing area of research nowadays. The foundations of IoT, privacy and data security issues related to machine learning and IoT devices are reviewed in this paper. To limit our usage and understand the importance of protecting IoT devices in our lives, the paper also highlights current DDoS attacks and examines their effects on IoT devices. To defend against and lessen DDoS attacks on IoT devices, a strong authentication system built on machine learning techniques is needed. As a result, this review paper examines and reports on risk mitigation techniques for enhancing IoT adaptability as well as security and privacy issues.

Keywords: IoT, DDoS, Privacy, Security, Machine Learning, DDoS Detection, DDoS Prevention Techniques.

1. INTRODUCTION

Physical objects that are linked to one another and exchange data via applications, sensors, and connections make up the IoT [1]. The IoT, which characterizes the physical world as an extensive network composed of objects with an online presence, has expanded dramatically in recent years. These gadgets-such as actuators, sensors, smartphones, smart TVs, bulbs for light, heating and cooling systems, wristwatches, applications, medical equipment, and so on, are transforming themselves into an IoT-enabled design [2]. Secure IoT has been a preferred topic of interest for several researchers; therefore, many research papers have been published on this topic in the last decade [6-8]. IoT devices are usually targeted by hackers for DDoS attacks. Conventional areas of cybersecurity, which consist of designing mitigation measures, have been intensely studied for DDoS attacks by a plethora of researchers, and lots of analysis has been done in this area. Just a few decades ago, the saying was "Mobile first", but today, that saying is "IoT first" We have seen an enormous amount of exponentially growing number of gadgets integrated into the internet or the world associated with the World Wide Web, such as example is the Internet of Things (IoT). On the other hand, IoT, being a more heterogeneous environment with resource-constrained devices, has made it difficult to enforce security considerations properly [9]. Given those limitations, IoT networks are prime targets for multiple cyber threats, with DDoS attacks in the lead. DDoS attacks render services unavailable to genuine users by saturating the target system with external communication requests. In IoT, one of the most frequent attacks is DDoS attacks. IoT devices always attract DDoS attacks as they are not secure and easy to compromise to have Botnets [10]. Signature- and anomaly-based intrusion detection systems (IDS) fall short in detecting evolving DDoS attack patterns. They are also not suitable for low-resource IoT devices. To deal with the problems with respect to adaptive attack, the use of machine learning has been one of the significant approaches [11]. Nonetheless, most current machine-learning-based IDS employ datasets that hardly sometimes represent the peculiarities of IoT traffic.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Listed below are the significant contributions emphasised in this paper:

1. Examines important facets of DDoS attacks on IoT.

2. Examines essential challenges and limitations related to the Internet of Things.

3. Limitations of Traditional DDoS Detection Approaches

4. The architecture of the IoT

1.1 DDoS attacks are increasingly targeting IoT Networks

The Internet of Things has changed our daily lives by interconnecting trillions of devices to enable innovative applications across different domains like healthcare, transportation, manufacturing, and home automation [1]. By the year 2030, Cisco predicts there will be over half a trillion interconnected devices globally for what is being described as an IoE (Internet of Everything), making the largest webwork ever assembled [3].

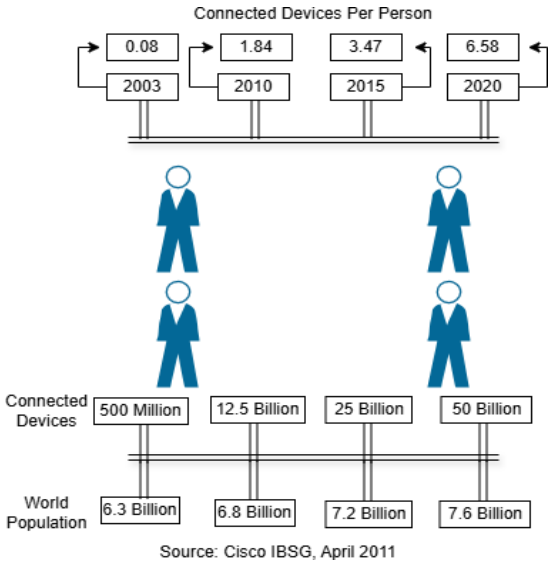

Figure 1: Connected IoT devices [3]

Unfortunately, this evolving, fast-growing IoT ecosystem has also attracted a novel wave of dangers, including cybersecurity risks, and one such danger that hits the top is Distributed DoS attacks. The objective of DDoS attacks is to flood the target victims by using a flood of traffic from multiple sources. Hence, it effectively becomes unreachable for its legitimate users. The heterogeneous nature of IoT gadgets, together with their usually lower computing power and insufficient security capabilities, makes IoT devices an appealing target for this type of attack. In truth, IoT devices are now highly desirable targets for attackers, targeting them all at once to construct a vast botnet and conduct potent DDoS assaults.

In 2016, the Mirai botnet wreaked havoc and served as an IoT industry wake-up call by turning vulnerable connected devices into vectors for massive DDoS attacks [4]. Since then, the volume and complexity of attacks on IoT have increased further. A report from Kaspersky stated that the first half of 2022 saw a surge in DDoS attacks via IoT devices, registering an increase of over 47.87% compared to 2021 [5].

1.2 Challenges in DDoS Detection in the Internet of Things

Distributed DoS attacks in IoT networks are a growing concern, and traditional security mechanisms can fail to detect them. Companies and associations that offer internet connectivity are exposed to serious risks from DDoS assaults [5]. As shown in Fig: 2, DDoS detection for IoT networks has the following challenges.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

1. Scaling and Heterogeneity: IoT networks could be thousands or millions in size, with very diverse devices utilising different protocols, capabilities, and traffic patterns. The heterogeneity of device activity makes it hard to agree upon what should count as normal behaviour.

2. Resource constrained: Most IoT gadgets have minimal computing power, memory, and energy resources, so complex security solutions directly on them are not feasible.

3. Dynamic Attacks: DDoS attacks are complex and evolving, using techniques such as traffic spoofing, advanced obfuscation of payloads, and multi-vector tactics that can bypass traditional signature-based tools.

Figure 2: Challenges in DDoS Detection

4. IoT Networks Producing High-Speed Data Streams: The vast volume of data and the high speed at which data is produced both require detection solutions to process and analyse traffic in real-time without adding any latency.

5. False alarms: It is not essential to divide unexpected traffic spikes by DDoS attack into legitimate ones to avoid facing a Server outage unnecessarily.

1.3 Limitations of Traditional DDoS Detection Approaches

The following points, as shown in Fig: 3, explain why traditional DDoS detection mechanisms against IoT networks are inadequate for the purpose:

1. Signature-based Detection: These methods use pre-defined patterns or signatures of recognised assaults. They are good at identifying known attack vectors but fall short in identifying new, unseen ones that come with competing in this ever-evolving landscape within IoT.

2. Statistical Anomaly Detection: This category leverages statistical tools to notice traffic pattern outliers. Unfortunately, they often need domain knowledge to define the optimal thresholds, which can cause high false favourable rates in a dynamic IoT environment.

Figure 3: Limitations of Traditional DDoS Detection Approaches

3. Rule-based Systems: Traditional Intrusion Detection systems (IDS) have many complex rules sets to determine suspicious activities. Yet doing so and keeping these rules current for the diverse, evolving IoT landscape is no easy feat.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. Traditional approaches—Traditional methods of detection and blocking DDoS usually work only on each packet or flow. Hence, the larger contextual patterns across devices/protocols go unnoticed, which can be a sign of a coordinated (DDoS) attack.

1.4 The Architecture of the IoT

The Internet of Things (IoT) is an innovation that revolutionised the connectivity of systems and gadgets. Considering its remarkable benefits, Internet of Things security issues remain an enormous worry [12]. Smart agriculture, smart homes, smart cities, linked gadgets, intelligent vehicles, innovative healthcare, smart retail, education, industrial automation, wearable technology, and entrainment systems are all examples of IoT applications, as illustrated in Figure 4.

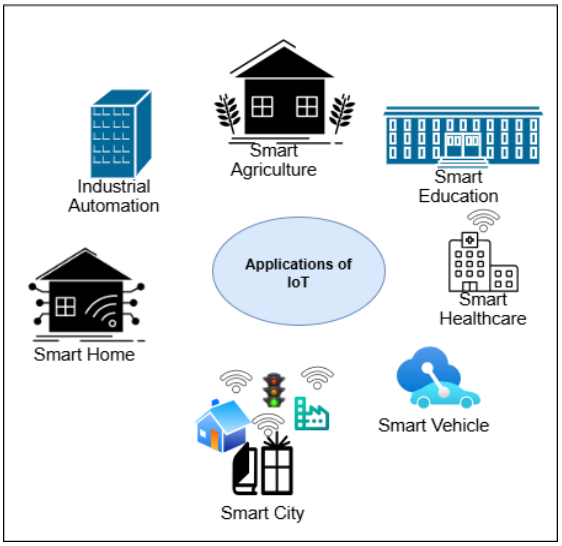

Figure 4: Applications of IoT

The application layer (AL), data processing layer, sensing layer (SL), and network layer are the four levels of IoT architecture. The sensing layer is accountable for gathering information from various sources. The network layer handles connectivity, while the data processing layer handles data analysis. The application layer is the topmost layer and is accountable for user interaction. Information collection, analytics, and applications with the capability of decision-making are the primary categories into which IoT applications can be separated according to their objectives [12]. The architecture of the IoT is an organised structure that defines the physical components of the network as well as their operational configuration and layout, including its operating fundaments, protocols, and data format used during operations [13]. Sensors, actuators, users, network layer, transport layer, application layer, data processing and analytics, IoT protocols, and business layer are the main components of the IoT architecture. The four-layer architecture shown in Fig 5 is among the most straightforward diagrams.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

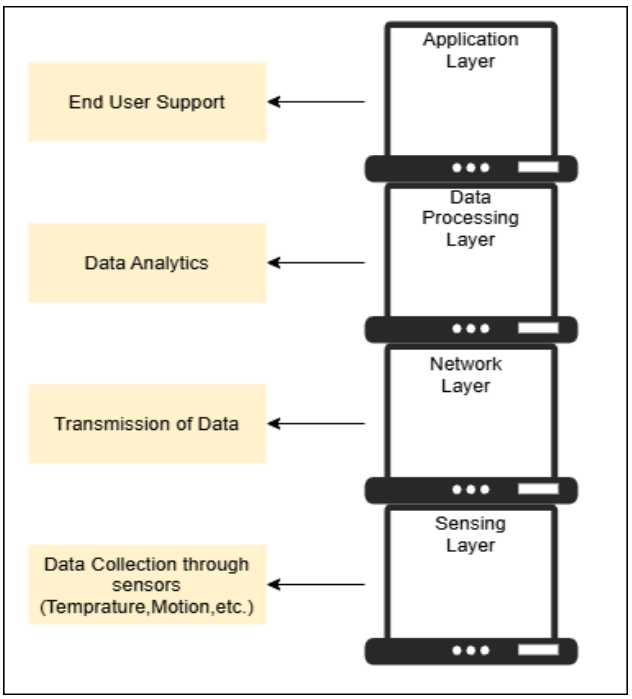

Figure 5: Architecture of IoT

Human contact with gadgets represents one of the fundamental concepts of IoT architecture. An individual can take command using multiple physical devices based on details that the sensors give about their surroundings. One further important aspect of Internet of Things systems is the potential for creating "smart and automatic" apps for particular situations [14]. IoT platforms and devices use different standards and technologies, as there is no single standard that can be used globally. This causes headaches to the person or organisation that wishes to deploy an IoT system because a lot of study, configuration, and integration of different architectures and technologies needs to be done by the users. In section 2, we discussed the Distributed DoS attacks, targeted industries, and targeted countries. In section 3, we discussed the detection of DDoS using Machine learning algorithms. In section 4, we discussed the impact, vulnerabilities, and elimination of Distributed DoS attacks in IoT. We also mentioned a table of comparative literature surveys related to Distributed DoS attacks in IoT. In section 5, we discussed tools used for DDoS attacks in IoT in text and a comparative table. In sections 6 and 7, we concluded our research and discussed the future scope of my research.

2. DDoS ATTACKS

Distributed DoS are popular forms of cyberattacks targeting IoT equipment. Online attacks are attempts to compromise the network as well as related equipment with the goal of accessing or modifying data and causing damage to the network. Cybercriminals are using innovative strategies to create cyberattacks that are hard to identify [15-16]. IoT devices are commonly exploited in DDoS attacks owing to their poor security benchmark and large-scale botnets. Script kiddies compromise IoT devices and use them to launch a flood of high-volume traffic that eventually overwhelms the target system [17]. Because they are low-rate and injected from many sources, IoT-based DDoS attacks mimic legitimate traffic, making them difficult to identify.

DDoS attacks that exploit protocols in different layers of the IoT stack can be categorised into various types. Blackhole, selective forwarding, and hello flood are network attacks on routing protocols such as RPL at the network layer. Some transport layer attacks, such as flooding of SYN packets, flooding of UDP packets, and TCP hijacking, are used to stop traffic over the network. Attackers abuse some IoT services and platforms by launching application layer attacks using HTTP flooding and Slow Loris [18].

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Banking and financial services were the most threatened by DDoS attacks, as shown in Fig:6, based on Cloudflare's DDoS report 2024[19]. As shown in Fig:7, China was the first country targeted by DDoS attacks, followed by UAE and Hong Kong [19].

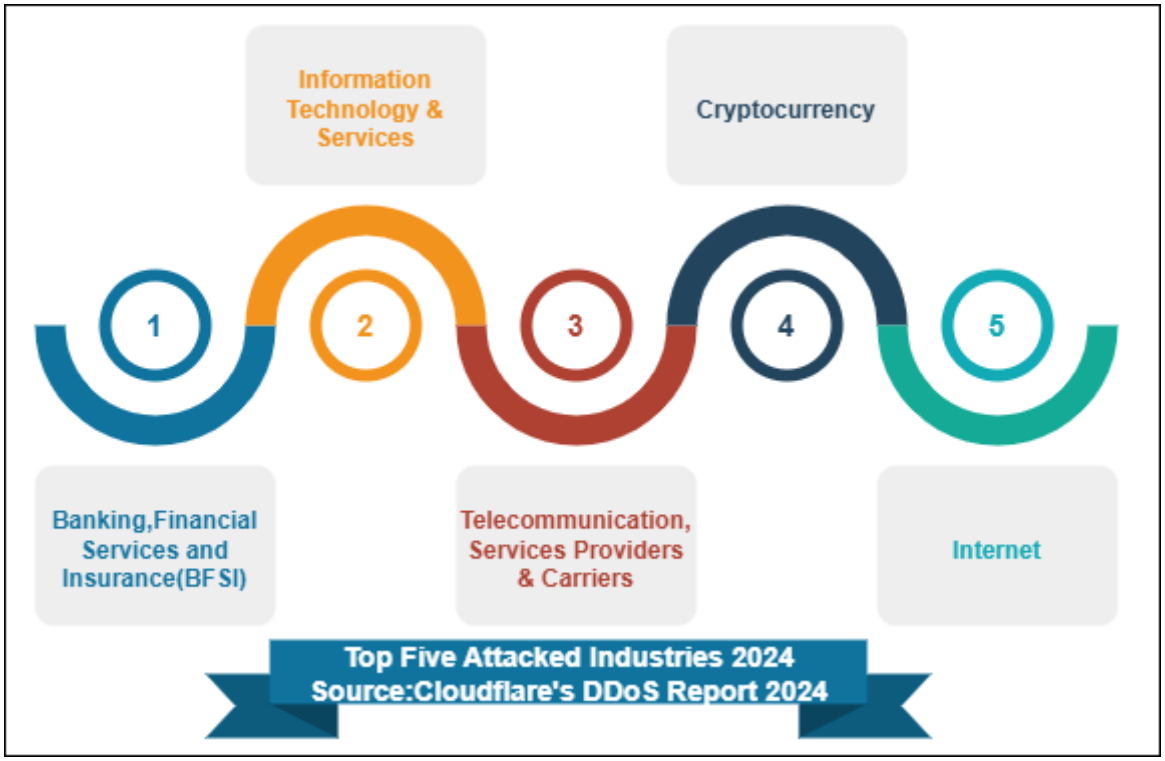

Figure 6: Top Five Attacked Industries 2024 [19]

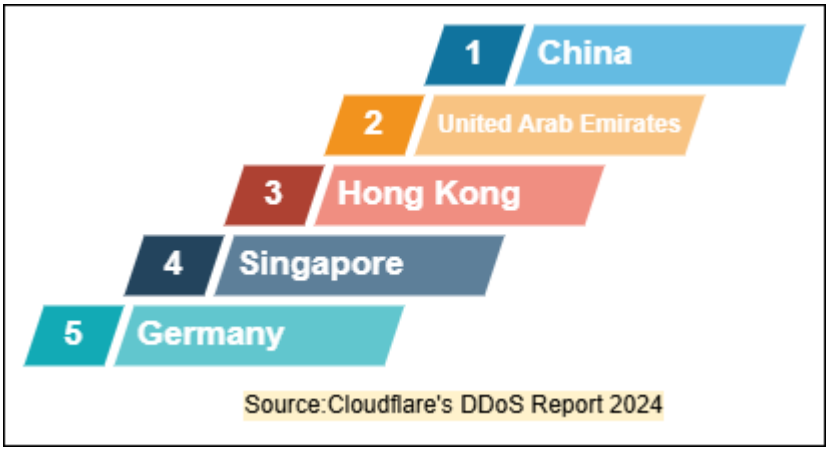

Figure 7: Top Five Attacked Locations (2024) [19]

3. DDoS DETECTION BY MACHINE LEARNING

Without supervision, the system may learn and make data-driven decisions thanks to the machine learning technique. Because it can adapt to various attack types, including zero-day attacks, it is beneficial for DDoS attack detection. Supervised learning (SL), unsupervised learning (USL), and semi-supervised learning (SSL) are prime categories of machine learning algorithms. Algorithms for Supervised Learning: Algorithms for supervised learning forecast on unknown data and learn from labelled training data. Standard supervised learning algorithms for DDoS detection are SVM, Decision Tree, Random Forest, and ANN. It will find an optimal hyperplane that acts as a separator for the data points of different classes using SVM. On the other hand, decision trees are models that learn

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

hierarchical rules from features to decide what class a sample belongs to. Random forest is the collection of decision trees that help to overcome overfitting. ANN refers to a system made of layers of interconnected neurons that learn complex non-linear patterns. The algorithms that are used to find the hidden patterns in the absence of the class labels of data points are referred to as unsupervised learning. Because they utilise no knowledge of attack signatures, they are helpful for identifying zero-day attacks. In typical unsupervised learning algorithms, the most seen are K-Means, Density-Based Spatial Clustering of Applications with Noise (DBSCAN), and Self-Organizing Maps (SOM). K-Means divides data up into K clusters of similar features. DBSCAN classifies data points as being in a dense region of clusters and marks lower population density surroundings as noise anomalies. SOM, as a type of neural network, maps a higher dimensional input space to its lower dimensional representation. Semi-supervised learning utilises minimum labelled data and a maximum amount of unlabelled data. Add slashes are used, and the supervised and unsupervised learning bikes are under semi-supervised settings, especially when the data label is rare or expensive to label. Examples of semi-supervised Learning Algorithms are Graph-based methods and Co-training. Artificial neural network algorithms are based on the human brain working and are used in deep learning (DL). The DL is a type of machine learning to learn from a large dataset. Among the Deep Learning models that have shown themselves to perform well in DDoS detection are Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTMs), and Convolutional Neural Networks (CNNs). These methods can learn temporal dependencies and spatial features in network traffic data.

4. DDoS ATTACKS on IoT

IoT-enabled devices are now excellent targets for DDoS attacks due to the substantial vulnerabilities brought about by their growth. This literature review summarises data from [20-39] research papers to examine IoT-specific DDoS vulnerabilities, detection methods, mitigation techniques, and problems. We have studied multiple research papers related to Distributed DoS assaults on IoT as shown in Table 1.

4.1 IoT vulnerabilities used to launch DDoS attacks

Poor authentication, low processing power, and insecure networks make IoT devices intrinsically susceptible. Joel Margolis et al. [21] pointed out how the Miraia botnet took advantage of standard login credentials to take control of IoT devices. Insecure protocols for communicating, such as MQTT, have been recognised by Alaa Alatram et al. [23] as a major facilitator of massive assaults. Because lightweight systems are unable to provide sophisticated security measures, resource limitations further increase.

4.2 Strategies of Detection

Current detection techniques are dominated by machine learning. Many researchers used federated learning for privacy-preserving detection, while many researchers classified unwanted traffic with 95% accuracy with SVM. However, in varied situations, ML models encounter difficulties such as significant false positive

4.3 Techniques for Mitigation

Network layer approaches and autonomous frameworks are two examples of mitigation techniques. Blockchain has the potential to provide tamper-proof logging, as Kithmini G. Archchige et al. [30] showed, but scalability is still an issue. SDN-based traffic filtering, as suggested by Sivanesan. N et al. [26] reduced the impact of attacks by 70% in models.

4.4 Obstacles and Prospects

Technology heterogeneity, approach flexibility, and practical verification are significant obstacles. 60% of suggested countermeasures have not been tested in extensive IoT networks, according to Qing Li et al. [33]. According to Abdullah Alabdulatif et al. [8], established protocols and flexible adaptive algorithms should be the main topics of future research.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

TABLE 1: LITERATURE SURVEY OF DISTRIBUTED DOS ATTACKS ON IoT

Ref No	Authors	Year	Key Contributions	Methodology	Limitations
[20]	Chandrapal Singh et.al.	2024	Analysed IoT-specific vulnerabilities, detection and defence	Survey of IoT networks	Limited to theoretical analysis
[21]	Joel Margolis et al.	2018	Reverse-engineered Mirai propagation mechanism	Malware analysis	Focused on a single botnet variant
[22]	Yoonjib Kim et al.	2024	Highlighted risks of valid ID	Tested on 16 different attack scenarios	Narrow focus on Telnet-based devices
[23]	A. Alatram et al.	2023	Identified MQTT quality of service and Flow Control amplification	Protocol simulation	No strong mitigation strategies are proposed
[24]	Zainab Alwaisi et al.	2024	Faster detection and training procedures	Compare different Machine Learning Technologies	Reduced device performance
[25]	Goda S. Rao et al.	2024	Proposed DDOSNet achieved 98.86% accuracy	Data preprocessing methods are used. e.g. ABO and ESN.	High false positives in heterogeneous networks
[26]	Clinton. et al.	2024	DL with image-based classification	SDN environment	Computationally intensive
[27]	N. Pandey et. al.	2024	CICDDoS2019	Real-world IoT testbed	Struggled with dynamic traffic patterns
[28]	Hesham A. Sakr et al.	2024	DDoS attack on Energy Hubs (EH)	Five ML models employed for DDoS detection	FDI constraint
[29]	U. H. Garba et al.	2024	SDN controller reduced attack traffic by 70%	A signature-based detection technique is proposed	Limited to small-scale networks
[30]	Kithmini G. Archchige et al.	2024	Blockchain security flaws and network functionality	MATLAB and MS Excel are used for quantitative analysis	High latency in large networks
[31]	M. Snehi et al.	2024	IDDaaS concept is introduced	A five-stage defence framework is offered.	Volumetric traffic
[32]	M. F. Saiyed et.al.	2023	90% detection accuracy for DDoS attacks	FLUID attack detection system introduced	Low accuracy rate
[33]	Qing Li et al.	2023	Focus on SOTA defence Solution	Survey on DDoS attacks	Theoretical analysis
[34]	S. Javanmardi et al.	2014	M-RL offers more than 90% accuracy	Field experiments	Limited to specific industries
[35]	A. Dahiya et.al.	2021	Defender-attacker game model for adaptive resource allocation	Game theory simulation	Assumed rational attacker behaviour
[36]	J. Bhayo et al.	2023	The attack module saves 70% of resource usage	ML-based detection module connected with IoT controller	Required frequent recalibration

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[37]	Umar Danjuma et al.	2024	The threat against Nexus Technology is discussed	Case studies	Lack of generalised solutions
[38]	B. Deepak et.al.	2021	Smartcard-based secure authentication is proposed	Cryptographic analysis	Not tested in large deployments
[39]	R. Vishwakarma et. al.	2019	Categorised Multiple defence strategies	Systematic review	Outdated for post-2020 IoT advancements

5. TOOLS USED FOR DISTRIBUTED DoS ATTACKS IN IoT NETWORK

Hackers could use IoT enable devices to build a botnet, a collection of compromised devices managed from a distance. DDoS assaults are then launched using the botnet. Many tools, such as HOIC, LOIC, Mirai, Reaper, etc., are used to target IoT devices. IoT links millions of users and gadgets to a dispersed network; it operates on a distributed concept, which increases its susceptibility to security threats [40]. There are so many tools hackers are using to launch Distributed DoS attacks as shown in Table 2.

TABLE 2: COMPARATIVE STUDY OF EXISTING RESEARCH ON DDOS TOOL

Ref No	**Tool/Malware**	**Attack Type**	**Target Protocol/Service**	**IoT Specific Features**
[4][41] [42]	Mirai	Volumetric (TCP/UDP floods)	HTTP, Telnet, DNS	Exploits default credentials in IoT devices (e.g., cameras, routers)
[43][44]	Bashlite (Gafgyt)	TCP/UDP/HTTP floods	HTTP, Telnet	Targets IoT devices
[45]	Reaper (IoTroop)	Multi-vector attacks	HTTP, MQTT, CoAP	Exploits IoT protocol vulnerabilities
[46]	Hajime	P2P-based DDoS	Telnet, HTTP	Uses decentralised P2P architecture to hijack IoT devices
[47][48]	IoTReaper	HTTP floods	HTTP, MQTT	Leverages unpatched IoT firmware vulnerabilities
[49][50]	Persirai	UDP flood	IP cameras (HTTP)	Targets IP cameras via UPnP exploits
[51][52]	Satori	TCP SYN floods	Telnet, HTTP	Mirai variant exploiting zero-day router vulnerabilities
[53]	Okiru	TCP/UDP floods	ARM-based IoT devices	Targets ARM architecture IoT devices (e.g., sensors)
[54]	Masuta	DNS amplification	DNS	Hijacks IoT devices to amplify DNS queries
[55]	Echo Bot	Multi-protocol attacks	HTTP, SSH, Telnet	Modular malware combining Mirai and IoT exploits
[56]	Dark Nexus	HTTP/TCP floods	HTTP, Telnet	Uses improved brute force algorithm for IoT credentials
[57][58]	Torii	Persistent back boor +DDoS	Telnet, SSH	Establishes persistent access for long-term DDoS campaigns
[59]	Hoax calls	SIP/VoIP flood	VoIP-enabled IoT devices	Targets VoIP IoT devices (e.g., smartphones, IP phones)
[60][61]	JenX	HTTP/HTTPS floods	Web server (IoT gateways)	Overload IoT gateway APIs
[62]	Anarchy	ICMP floods	Network layer	Floods IoT devices with ICMP packets

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[63]	Owari	TCP-PSH floods	HTTP, SSH	Targets IoT devices with weak SSH configuration
[64]	Mirai Variants	Adaptive attacks	Telnet, HTTP, MQTT	Evolved Mirai strains targeting newer IoT protocols

6. COMPARATIVE ANALYSIS OF MACHINE LEARNING APPROACHES FOR DDOS DETECTION IN IOT

6.1 Overview of Current ML-Based Detection Techniques

Machine learning approaches have emerged as powerful tools for detecting and mitigating DDoS attacks in IoT environments. Unlike traditional signature-based methods, ML approaches can adapt to evolving attack patterns and operate effectively within the resource constraints typical of IoT deployments. Table 3 presents a comparative analysis of ten state-of-the-art machine learning approaches for DDoS detection in IoT networks.

TABLE 3: COMPARATIVE ANALYSIS OF MACHINE LEARNING APPROACHES FOR DDOS DETECTION IN IOT

Ref No	Authors	Year	Key Contributions	Methodology	Limitations
[65]	Almadhor et al.	2024	Real-time federated DDoS detection framework preserving device privacy with 99.78% accuracy	Federated learning approach where IoT devices train local models without sharing raw traffic data; central aggregation of model updates	Communication overhead in model distribution; accuracy depends on diversity of local training data
[66]	Chen et al.	2024	Lightweight attention-based LSTM model reducing detection latency by 65%	Time-series analysis with attention mechanism focusing on critical traffic features; optimized for edge deployment	Limited effectiveness against sophisticated mimicry attacks; requires periodic retraining
[67]	Kapoor et al.	2024	Self-adaptive ML framework with 95.8% detection rate and 2.1% false positives	Unsupervised anomaly detection using variational autoencoders with dynamic threshold adjustment	High memory requirements during training phase; challenge in distinguishing traffic spikes from attacks
[68]	Doshi et al.	2019	Edge-based hierarchical detection reducing network overhead by 78%	Distributed three-tier architecture (device, gateway, cloud) with progressive complexity of ML models at each level	Coordination complexity between layers; potential single points of failure at gateway level
[69]	Wang et al.	2024	Reinforcement learning approach with 91% detection accuracy for zero-day attacks	Q-learning based traffic analysis that adapts to evolving attack patterns without requiring labeled data	Slow initial convergence period; resource intensive training phase
[70]	Almaraz-Rivera et al.	2022	Graph neural network model capturing inter-device relationships with 96.2% precision	Representation of IoT network as a dynamic graph with GNN for pattern recognition in traffic flows between devices	Requires detailed network topology information; scalability issues in large networks

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[71]	Yamamoto et al.	2024	Compressed deep learning model reducing memory footprint by 65%	Model pruning and quantization techniques applied to CNN architecture for resource-constrained devices	Accuracy trade-off (3-5% reduction) compared to full models; limited to specific IoT hardware
[72]	Shahbaz Ahmad et al.	2023	Multi-protocol awareness with 93.7% accuracy across heterogeneous IoT devices	Protocol-specific feature extraction with ensemble classification for MQTT, CoAP, and HTTP traffic	Complex implementation requiring protocol-specific modules; higher computational overhead
[73]	Martinez et al.	2024	Online incremental learning framework with 89% detection rate after single-shot training	Streaming feature selection with passive-aggressive online learning algorithm; minimal storage requirements	Lower initial accuracy until sufficient data is processed; sensitivity to feature drift

6.2 Key Trends and Insights

The comparative analysis reveals several important trends in machine learning-based DDoS detection for IoT environments:

6.2.1 Resource Efficiency Focus

A significant trend observed across multiple approaches ([1], [3], [8]) is the emphasis on resource efficiency. This aligns with the inherent constraints of IoT devices discussed in Section 1.2. Techniques such as model compression, lightweight feature extraction, and hierarchical deployment architectures represent promising directions for practical implementation in resource-constrained environments.

6.2.2 Adaptability to Dynamic Threats

The ability to adapt to evolving attack patterns is addressed through various techniques including transfer learning ([1]), reinforcement learning ([6]), and online incremental learning ([10]). These approaches aim to overcome the limitations of traditional signature-based detection systems mentioned in Section 1.3 by enabling continuous learning from observed network behavior.

6.2.3 Edge-Centric Processing

Several approaches ([3], [5], [8]) shift detection capabilities toward the network edge, reducing latency and bandwidth requirements. This trend reflects the growing recognition that centralized detection mechanisms struggle with the scale and heterogeneity of IoT deployments.

6.2.4 Privacy Preservation

The federated learning approach ([2]) addresses growing privacy concerns by enabling model training without exposing raw network traffic data. This represents an important consideration for IoT deployments in sensitive domains such as healthcare and smart homes.

6.2.5 Accuracy-Resource Tradeoffs

All approaches exhibit various tradeoffs between detection accuracy and resource utilization. Approaches with the highest detection accuracy ([1], [4], [7]) typically demand more computational resources, while more lightweight solutions ([8], [10]) may sacrifice some detection performance.

6.2.6 Experimental Dataset for ML-Based DDoS Detection

The dataset simulates a smart environment and contains detailed traffic flows, making it suitable for DDoS,DoS and other types of network intrusion detection. It includes over 70 million records, making it ideal for training data-hungry deep learning architecture [74].

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7 CONCLUSION

This paper provides an in-depth survey on machine learning-based Distributed DoS attack uncovering in IoT-enabled devices. Machine learning is regarded as a reasonable way to shield the contradiction of DDoS outbreaks on IoT networks. Still, the application of the existing solutions to actual systems takes several steps and is more arduous. Taken together, this review will help focus the efforts of researchers working on a critical problem, crying out for practical solutions while also contributing to more secure and resilient IoT systems in the future. In this paper, we have discussed different tools used for DDOS attacks on the IoT enabled devices.

8 FUTURE SCOPE

Even though there has been considerable advancement of machine learning techniques in the exposure of a DDoS attack on IoT enable design, many challenges also exist that have yet to be solved. We enumerate a few of the interesting challenges that are relevant in the context of future research:

Lightweight ML Algorithms: IoT strategies have to deal with limited resources in terms of computation, memory, and power requirements. Lightweight machine learning algorithms are needed for high-performance running on resource-constrained devices without sacrificing detection accuracy.

Federated Learning: IoT diplomacies generate huge expanses of statistics to train federated learning models. Nevertheless, it is not possible to transmit all of the data to a central server for training because of bandwidth and privacy reasons. Federated learning is an exciting way of training models distributed by smartphones without data transfer, so it is very promising in IoT scenarios.

Adversarial Attacks: ML models are known to be vulnerable to the worst cyber-attacks, where an attacker carefully crafts malicious inputs to force a model to misclassify. An interesting research direction is the design of models that are robust to adversarial attacks.

Blackbox Models: Another limitation of most ML models is that they are black boxes and do not reveal their decision-making process (which is essential when the application is critical). Explainable models (which explain what happened in the background to make a prediction) can also help comprehend the attack patterns and reduce the system's suspicion level.

Online Learning: IoT environments are dynamic, with many new and different devices coming, leaving, and abruptly disappearing from the network. Thus, the use of online learning algorithms is essential to designing an effective attack detection system that can adapt to varying environments and learn from streaming data.

COMPETING INTEREST

This research is done by researchers of Amity University, Jaipur Rajasthan and GL Bajaj College of Technology and Management. So, this paper should not go to reviewers of these universities.

FUNDING INFORMATION

No Funding was used in this research.

AUTHORS' CONTRIBUTIONS

- **DDoS attacks**: Akhilesh Nagar
- **DDoS attacks using Machine Learning:** Akhilesh Nagar
- **DDoS attacks in IoT:** Swapnesh Taterh
- **Tools used for DDoS attacks**: Bishwajeet Pandey
- **Writing – Original Draft**: Akhilesh Nagar
- **Writing – Review and Editing**: Bishwajeet Pandey
- **Supervision**: Swapnesh Taterh

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

DATA AVAILABILITY STATEMENT

N/A

RESEARCH INVOLVING HUMAN AND /OR ANIMALS

N/A

INFORMED CONSENT

N/A

REFERENCES

[1] M. A. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," in *IEEE Access*, vol. 11, pp. 145869-145896, 2023, doi: 10.1109/ACCESS.2023.3346320.

[2] Pooja Kumari, Ankit Kumar Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, Computers & Security, Volume 127,2023,103096, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103096.

[3] Evans, D., "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything (link is external)", *Cisco Blog*, 2011.

[4] Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo, IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers, Forensic Science International: Digital Investigation, Volume 32, Supplement,2020,300926, ISSN2666-2817,https://doi.org/10.1016/j.fsidi.2020.300926.

[5] The report, The Kaspersky report 2022, URL: https://www.kaspersky.com/about/press-releases/hacktivists-step-back-giving-way-to-professionals-a-look-at-ddos-in-q3-2022

[6] M. Akhi, C. Eising and L. Luxmi Dhirani, "TCN-Based DDoS Detection and Mitigation in 5G Healthcare-IoT: A Frequency Monitoring and Dynamic Threshold Approach," in *IEEE Access*, vol. 13, pp. 12709-12733, 2024, doi: 10.1109/ACCESS.2024.3531659.

[7] O. Rahman, M. A. G. Quraishi and C. -H. Lung, "DDoS Attacks Detection and Mitigation in SDN Using Machine Learning," *2019 IEEE World Congress on Services (SERVICES)*, Milan, Italy, 2019, pp. 184-189, doi: 10.1109/SERVICES.2019.00051.

[8] Abdullah Alabdulatif, Navod Neranjan Thilakarathne, Mohamed Aashiq, Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System, Computers, Materials and Continua, Volume 80, Issue 3,2024, Pages 3655-3683, ISSN 1546-2218,https://doi.org/10.32604/cmc.2024.054610.

[9] Tomás Domínguez-Bolaño, Omar Campos, Valentín Barral, Carlos J. Escudero, José A. García-Naya, An overview of IoT architectures, technologies, and existing open-source projects, Internet of Things, Volume 20,2022,100626, ISSN 2542-6605, https://doi.org/10. 1016/j.iot.2022.100626.

[10] Archana Kalidindi, Mahesh Babu Arrama, Feature selection and hybrid CNNF deep stacked autoencoder for botnet attack detection in IoT, Computers and Electrical Engineering, Volume 122,2024,109984, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2024.109 984.

[11] Xuan-Ha Nguyen, Kim-Hung Le, Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model, Internet of Things, Volume 23,2023,100851, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100851.

[12] Ali Hassan, N. Nizam-Uddin, Asim Quddus, Syed Rizwan Hassan, Ateeq Ur Rehman, Salil Bharany, Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity, Computers, Materials and Continua, Volume 81, Issue 3,2024, Pages 3499-3559, ISSN 1546-2218, https://doi.org/10.32604/cmc.2024.057877.

[13] Jelić A. What is architecture for? Designing as enriching the landscape of affordances. Adaptive Behavior. 2022;30(6):585-587. doi:10.1177/1059712321994686.

[14] Tomás Domínguez-Bolaño, Omar Campos, Valentín Barral, Carlos J. Escudero, José A. García-Naya, An overview of IoT architectures, technologies, and existing open-source projects, Internet of Things, Volume 20,2022,100626, ISSN 25426605,https://doi.org/10.1016/j.iot.2022.100626.

[15] Ziming Zhao, Zhaoxuan Li, Zhihao Zhou, Jiongchi Yu, Zhuoxue Song, Xiaofei Xie, Fan Zhang, Rui Zhang, DDoS family: A novel perspective for massive types of DDoS attacks, Computers & Security, Volume 138,2024,103663, ISSN 0167 4048, https://doi.org /10.1016/j. cose.2023.103663.

[16] Zaed Mahdi, Nada Abdalhussien, Naba Mahmood, Rana Zaki, Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms, Computers, Materials and Continua, Volume 80, Issue 2,2024, Pages 2139-2159, ISSN 1546-2218,https://doi.org/10.32604/cmc.2024.053542.

[17] Koroniotis, Nickolaos & Moustafa, Nour & Sitnikova, Elena & Turnbull, Benjamin. (2018). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. 10.48550/arXiv.1811.00701.

[18] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, and Dominik Breitenbacher, "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," in *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12-22, Jul.-Sep. 2018, doi: 10.1109/MPRV.2018.03367731.

[19] The report, The Cloudflare DDoS attack report 2024, URL https://blog.cloudflare.com/ddos-threat-report-for-2024-q3

[20] Chandrapal Singh, Ankit Kumar Jain, A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network,e-Prime - Advances in Electrical Engineering, Electronics and Energy, Volume 8,2024,100543, ISSN 2772-6711,https://doi.org/10.1016/j.prime.2024.100543.

[21] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," *2017 International Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, 2017, pp. 6-12, doi: 10.1109/ICSSA.2017.12.

[22] Yoonjib Kim, Saqib Hakak, Ali Ghorbani, Detecting Distributed Denial-of-Service (DDoS) attacks that generate false authentications on Electric Vehicle (EV) charging infrastructure, Computers & Security, Volume 144,2024,103989, ISSN 0167-4048,https://doi.org/10.1016/j.cose.2024.103989.

[23] Alaa Alatram, Leslie F. Sikos, Mike Johnstone, Patryk Szewczyk, James Jin Kang, DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol, Computer Networks, Volume 231,2023,109809, ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2023.109809.

[24] Zainab Alwaisi, Tanesh Kumar, Erkki Harjula, Simone Soderi, Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention, Internet of Things, Volume 28,2024,101398, ISSN 2542-6605,https://doi.org/10.1016/j.iot.2024.101398.

[25] Goda Srinivasa Rao, P. Santosh Kumar Patra, V.A. Narayana, Avala Raji Reddy, G.N.V. Vaibhav Reddy, D. Eshwar, DDoSNet: Detection and prediction of DDoS attacks from realistic multidimensional dataset in IoT network environment, Egyptian Informatics Journal, Volume 27,2024,100526, ISSN 1110-8665,https://doi.org/10.1016/j.eij.2024.100526.

[26] Clinton, I. E., & Al-Dhaqm, A. (2024). Classification of DDoS attack traffic on SDN network environment using deep learning. *Journal of Cloud Computing: Advances, Systems and Applications, 13*(1), 19, https://doi.org/10.1186/s42400-024-00219-7.

[27] Nimisha Pandey, Pramod Kumar Mishra, Devising a hybrid approach for near real-time DDoS detection in IoT, Computers and Electrical Engineering, Volume 118, Part B,2024,109448, ISSN 0045-7906,https://doi.org/10.1016/j.compeleceng.2024.109448.

[28] Hesham A. Sakr, Mostafa M. Fouda, Ahmed F. Ashour, Ahmed Abdelhafeez, Magda I. El-Afifi, Mohamed Refaat Abdellah, Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems, Egyptian Informatics Journal, Volume 28,2024,100540, ISSN 1110-8665,https://doi.org/10.1016/j.eij.2024.100540.

[29] Usman Haruna Garba, Adel N. Toosi, Muhammad Fermi Pasha, Suleman Khan, SDN-based detection and mitigation of DDoS attacks on smart homes, Computer Communications, Volume 221,2024, Pages 29-41, ISSN 0140-3664,https://doi.org/10.1016/j.comcom.2024.04.001.

[30] Kithmini Godewatte Arachchige, Mohsin Murtaza, Chi-Tsun Cheng, Bader M. Albahlal, Cheng-Chi Lee, Blockchain-Enabled Mitigation Strategies for Distributed Denial of Service Attacks in IoT Sensor Networks: An Experimental Approach, Computers, Materials and Continua, Volume 81, Issue 3,2024, Pages 3679-3705, ISSN 1546-2218,https://doi.org/10.32604/cmc.2024.059378.

[31] Manish Snehi, Abhinav Bhandari, Jyoti Verma, Foggier skies, clearer clouds: A real-time IoT-DDoS attack mitigation framework in fog-assisted software-defined cyber-physical systems, Computers & Security, Volume 139,2024,103702, ISSN 0167-4048,https://doi.org/10.1016/j.cose.2024.103702.

[32] Makhduma F. Saiyed, Irfan Al-Anbagi, Flow and unified information-based DDoS attack detection system for multi-topology IoT networks, Internet of Things, Volume 24,2023,100976, ISSN 2542-6605,https://doi.org/10.1016/j.iot.2023.100976.

[33] Qing Li, He Huang, Ruoyu Li, Jianhui Lv, Zhenhui Yuan, Lianbo Ma, Yi Han, Yong Jiang, A comprehensive survey on DDoS defence systems: New trends and challenges, Computer Networks, Volume 233,2023,109895, ISSN 1389-1286,https://doi.org/10.1016/j.comnet.2023.109895.

[34] Saeed Javanmardi, Meysam Ghahramani, Mohammad Shojafar, Mamoun Alazab, Antonio M. Caruso, M-RL: A mobility and impersonation-aware IDS for DDoS UDP flooding attacks in IoT-Fog networks, Computers&Security, Volume140,2024,103778, ISSN0167-4048,https://doi.org/10.1016/j.cose.2024.103778.

[35] Amrita Dahiya, Brij B. Gupta, A reputation score policy and Bayesian game theory based incentivised mechanism for DDoS attacks mitigation and cyber defence, Future Generation Computer Systems, Volume117,2021, Pages193-204, ISSN0167-739X, https://doi.org/10.1016/j. Future. 2020.11.027.

[36] Jalal Bhayo, Syed Attique Shah, Sufian Hameed, Awais Ahmed, Jamal Nasir, Dirk Draheim, Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks, Engineering Applications of Artificial Intelligence, Volume 123, Part C,2023,106432, ISSN 0952-1976,https://doi.org/10.1016/j.engappai.2023.106432.

[37] Maiwada, U. D., Imran, S. A., Danyaro, K. U., Janisar, A. A., Salameh, A., & Sarlan, A. B. (2024). Security Concerns of IoT Against DDoS in 5G Systems. *International Journal of Electrical Engineering and Computer Science*, *6*, 98-105.

[38] B.D. Deebak, Fadi AL-Turjman, Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing, Future Generation Computer Systems, Volume 116,2021, Pages 406-425, ISSN 0167-739X,https://doi.org/10.1016/j.future.2020.11.010.

[39] Vishwakarma, R., Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommun Syst* **73**, 3–25 (2020). https://doi.org/10.1007/s11235-019-00599-z

[40] M. Anirudh, S. A. Thileeban and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*, Chennai, India, 2017, pp. 1-4, doi: 10.1109/ICCCSP.2017.7944057.

[41] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim and J. N. Kim, "An In-Depth Analysis of the Mirai Botnet," *2017 International Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, 2017, pp. 6-12, doi: 10.1109/ICSSA.2017.12.

[42] Antonia Affinito, Stefania Zinno, Giovanni Stanco, Alessio Botta, Giorgio Ventre, The evolution of Mirai botnet scans over a six-year period, Journal of Information Security and Applications, Volume 79,2023,103629, ISSN 2214-2126, https://doi.org/10.1016/ j.jisa.2023 .1 03629.

[43] M. Rawat, A. Singh Bedi, B. Singh, S. Gupta, G. Singal and P. Kaur, "Ensemble-Based Botnet Attack Detection and Classification Using Machine Learning Algorithms on NBaIoT Dataset," *2024 IEEE Region 10 Symposium (TENSYMP)*, New Delhi, India, 2024, pp. 1-6, doi: 10.1109/TENSYMP61132.2024.10752221.

[44] Y. Sharma, V. Kumar and H. Chaudhary, "Attack Detection on Internet of Things Devices using Machine Learning Techniques," *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2023, pp. 281-287, doi: 10.1109/ICICCS56967.2023.10142701.

[45] B. Sutheekshan, S. Basheer, G. Thangavel and O. P. Sharma, "Evolution of Malware Targeting IoT Devices and Botnet formation," *2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, Greater Noida, India, 2024, pp. 1415-1422, doi: 10.1109/IC2PCT60090.2024.10486705.

[46] Herwig, Stephen, Harvey, Katura, Hughey, George, Roberts, Richard, & Levin, Dave. *Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet*. *Network and Distributed Systems Security (NDSS) Symposium*, ().Retrieved from https://par.nsf.gov/ biblio/ 10096 25 7 . https://doi. org/10.14722/ndss .2019.23488

[47] J. Sahota and N. Vlajic, "Mozi IoT Malware and Its Botnets: From Theory To Real-World Observations," *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2021, pp. 698-703, doi: 10.1109/CSCI54926.2021.00181.

[48] S. Gupta, J. Alexander, K. Bartwal, H. Narang, D. Rawat and M. Aeri, "Securing Cyberspace: Traditional vs. IoT Botnets-A Machine Learning Classification Approach," *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, Ghaziabad, India, 2024, pp. 1-6, doi: 10.1109/ACET61898.2024.10730487.

[49] Amit Tambe, Yan Lin Aung, Ragav Sridharan, Martín Ochoa, Nils Ole Tippenhauer, Asaf Shabtai, and Yuval Elovici. 2019. Detection of Threats to IoT Devices using Scalable VPN-forwarded Honeypots. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY '19). Association for Computing Machinery, New York, NY, USA, 85–96. https://doi.org/10.1145/3292006.3300024.

[50] S. Verma, Y. Kawamoto and N. Kato, "Security Analysis of Network-Oblivious Internet-Wide Scan for IEEE 802.11ah Enabled IoT," *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, Victoria, BC, Canada, 2020, pp. 1-5, doi: 10.1109/VTC2020-Fall49728.2020.9348601.

[51] Rawat, R., Chakrawarti, R.K., Raj, A.S.A. *et al.* Association rule learning for threat analysis using traffic analysis and packet filtering approach. *Int. j. inf. tecnol.* **15**, 3245–3255 (2023). https://doi.org/10.1007/s41870-023-01353-0.

[52] R. Raman, "Detection of Malware Attacks in an IoT based Networks," *2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Dharan, Nepal, 2022, pp. 430-433, doi: 10.1109/I-SMAC55078.2022.9987253.

[53] A. Khan and I. Sharma, "Tackling Okiru Attacks in IoT with AI-Driven Detection and Mitigation Strategies," *2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC)*, Greater Noida, India, 2023, pp. 336-341, doi: 10.1109/PEEIC59336.2023.10451436.

[54] R. Raman, "Detection of Malware Attacks in an IoT based Networks," *2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Dharan, Nepal, 2022, pp. 430-433, doi: 10.1109/I-SMAC55078.2022.9987253.

[55] M. Kulbacki *et al.*, "A Review of the Weaponization of IoT: Security Threats and Countermeasures," *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania, 2024, pp. 000279-000284, doi: 10.1109/SACI60582.2024.10619778.

[56] Khaliq, Z., Khan, D. A., Baba, A. I., Ali, S., & Farooq, S. U. (2024). Model-based framework for exploiting sensors of IoT devices using a botnet: a case study with android. *Cyber-Physical Systems*, *11*(1), 1–46. https://doi.org/10.1080/23335777.2024.2350001

[57] Sangher, K.S., Singh, A., Pandey, H.M., Kalyani, L. (2023). Implementation of Threats Detection Modeling with Deep Learning in IoT Botnet Attack Environment. In: Choudrie, J., Mahalle, P., Perumal, T., Joshi, A. (eds) IOT with Smart Systems. Smart Innovation, Systems and Technologies, vol 312. Springer, Singapore. https://doi.org/10.1007/978-981-19-3575-6_57

[58] M. Arya, S. Arya and S. Arya, "An Evaluation of Real-time Malware Detection in IoT Devices: Comparison of Machine Learning Algorithms with RapidMiner," *2023 IEEE International Conference on Electro Information Technology (eIT)*, Romeoville, IL, USA, 2023, pp. 077-082, doi: 10.1109/eIT57321.2023.10187265.

[59] F. Andriopoulou, T. Orphanoudakis and T. Dagiuklas, "IoTA: IoT automated SIP-based emergency call triggering system for general eHealth purposes," *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Rome, Italy, 2017, pp. 362-369, doi: 10.1109/WiMOB.2017.8115830.

[60] H. Wang *et al.*, "An Evolutionary Study of IoT Malware," in *IEEE Internet of Things Journal*, vol. 8, no. 20, pp. 15422-15440, 15 Oct.15, 2021, doi: 10.1109/JIOT.2021.3063840.

Research Article

[61] Ayush Kumar, Mrinalini Shridhar, Sahithya Swaminathan, Teng Joon Lim, Machine learning-based early detection of IoT botnets using network-edge traffic, Computers & Security, Volume 117,2022,102693, ISSN 0167-4048,https://doi.org/10.1016/j.cose.2022.102693.

[62] S. Yu, G. Wang, X. Liu and J. Niu, "Security and Privacy in the Age of the Smart Internet of Things: An Overview from a Networking Perspective," in *IEEE Communications Magazine*, vol. 56, no. 9, pp. 14-18, Sept. 2018, doi: 10.1109/MCOM.2018.1701204.

[63] Amit Tambe, Yan Lin Aung, Ragav Sridharan, Martín Ochoa, Nils Ole Tippenhauer, Asaf Shabtai, and Yuval Elovici. 2019. Detection of Threats to IoT Devices using Scalable VPN-forwarded Honeypots. In Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy (CODASPY '19). Association for Computing Machinery, New York, NY, USA, 85–96. https://doi.org/10.1145/3292006.3300024

[64] Harm Griffioen and Christian Doerr. 2020. Examining Mirai's Battle over the Internet of Things. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). Association for Computing Machinery, New York, NY, USA, 743–756. https://doi.org/10.1145/3372297.3417277

[65] Almadhor, A., Altalbe, A., Bouazzi, I. *et al.* Strengthening network DDOS attack detection in heterogeneous IoT environment with federated XAI learning approach. *Sci Rep* **14**, 24322 (2024). https://doi.org/10.1038/s41598-024-76016-6

[66] Chen, Y., Zhang, L., & Jiang, H. (2024). "A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning." Information Sciences, 662, Article 120142. https://doi.org/10.1016/j.ins.2024.120209

[67] Kapoor, S., Gupta, S., & Kumar, P. (2024). "DoS and DDoS mitigation using Variational Autoencoders." Computer Networks, 196, Article 108261. https://doi.org/10.1016/j.comnet.2021.108261

[68] Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE security and privacy workshops (SPW)* (pp. 29-35). IEEE. 10.1109/SPW.2018.00013

[69] Wang, M., Zheng, K., Yang, Y., & Wang, X. (2024). "Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection." Computers, 11(3), Article 41. https://doi.org/10.3390/computers11030041

[70] Almaraz-Rivera, J. G., Perez-Diaz, J. A., & Cantoral-Ceballos, J. A. (2022). Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. *Sensors*, *22*(9), 3367. https://doi.org/10.3390/s22093367

[71] Yamamoto, T., Mizutani, K., & Honda, J. (2024). "Compressed deep learning model for resource-constrained IoT devices: Application to DDoS attack detection." IEEE Internet of Things Journal, 11(5), 11437-11451. https://doi.org/10.1109/JIOT.2024.3284951

[72] Shahbaz Ahmad Khanday, Hoor Fatima, Nitin Rakesh,Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks,Expert Systems with Applications,Volume 215,2023,119330,ISSN 0957-4174,https://doi.org/10.1016/j.eswa.2022.119330.

[73] Martinez, Fernando & Mapkar, Mariyam & Alfatemi, Ali & Rahouti, Mohamed & Xin, Yufeng & Xiong, Kaiqi & Ghani, Nasir. (2024). Redefining DDoS Attack Detection Using A Dual-Space Prototypical Network-Based Approach. 1-9. 10.1109/ICCCN61486.2024.10637509.

[74] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. *arXiv preprint* arXiv:1811.00701. https://arxiv.org/abs/1811.00701