
AI-Driven Next-Generation DDoS Mitigation in IoT: A Comprehensive Survey of Deep Learning and Large Language Models

Mosieur Rahaman¹, Nicko Cajes², Varsha Arya^{3,4,5},
Razaz Waheeb Attar⁶, Kwok Tai Chui⁷ and Brij B. Gupta^{8,9,10,11,*}

¹*Department of Computer Engineering, King Mongkut's University of Technology Thonburi, Bangkok, Thailand*

²*Northern Bukidnon State College, Manolo Fortich, Philippines*

³*Electronic Engineering and Computer Science, Hong Kong Metropolitan University, Hong Kong*

⁴*Center for Interdisciplinary Research, University of Petroleum and Energy Studies (UPES), Dehradun, India*

⁵*UCRD, Chandigarh University, Chandigarh, India*

⁶*Department of Management, College of Business Administration, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi*

⁷*Electronic Engineering and Computer Science, Hong Kong Metropolitan University, Hong Kong SAR, China*

⁸*Department of Computer Science and Information Engineering, Asia University, Taichung 413, Taiwan*

⁹*Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan*

¹⁰*Symbiosis Centre for Information Technology (SCIT), Symbiosis International University, Pune, India*

¹¹*School of Cybersecurity, Korea University, Seoul, South Korea*

*E-mail: mosiurahaman@gmail.com; nickocajes@gmail.com;
varshaarya2108@gmail.com; Raattar@pnu.edu.sa; jktchui@hkmue.edu.hk;
gupta.brij@ieee.org*

**Corresponding Author*

Received 23 March 2026; Accepted 26 May 2026

Journal of Web Engineering, Vol. 25_7, 1215–1294.

doi: 10.13052/jwe1540-9589.2571

© 2026 River Publishers

Abstract

The global Internet of Things (IoT) network has experienced unprecedented expansion, reaching 75.44 billion connected devices worldwide. Due to this rapid growth, the IoT ecosystem has become larger but also more vulnerable to various threats in cyberspace. As a result, this situation has accelerated the development of more complex cyberattacks, especially Distributed Denial of Service (DDoS) attacks, which can damage systems by overwhelming network traffic. This attack exploits the inherent vulnerabilities of IoT networks with limited resources, leading to significant service interruptions, monetary losses, and potentially the failure of vital infrastructures. As a result, this survey presents a new taxonomy of attack types, a thorough assessment of conventional and AI-driven detection techniques, and a comparison of advanced countermeasures. This survey aims to provide a comprehensive and systematic overview of DDoS attack detection, prevention, and mitigation approaches for the IoT. A major contribution of this work is the inclusion of blockchain-based security frameworks, federated learning, deep learning, machine learning, and quantum computing paradigms in its discussion for reducing DDoS attacks on the IoT. Furthermore, real-world case studies highlight the severe impact of such attacks on mission-critical domains, including smart cities, healthcare, and industrial control systems (ICSs). This survey provides a basis for cybersecurity researchers, security experts, and hobbyists, grounded in the understanding gained from previous research.

Keywords: IoT, deep learning, artificial intelligence, language model.

1 Introduction

The world continues to move towards development and progressive changes, where many aspects of life have changed compared to previous years. One of the primary reasons for this change is the technology. With its emergence, many useful devices were created, and one of them is the Internet of Things (IoT). IoT is a network of interconnected devices that generates and transfers data with the help of sensors. According to Statista, the number of IoT-connected devices installed worldwide has already reached 75.44 billion, which is an increase of approximately 13.5 billion compared to last year of only 62.12 billion [1]. The global growth of IoT devices in the span of 10 years is presented in Figure 1, showing the great increase in IoT-connected devices every year.

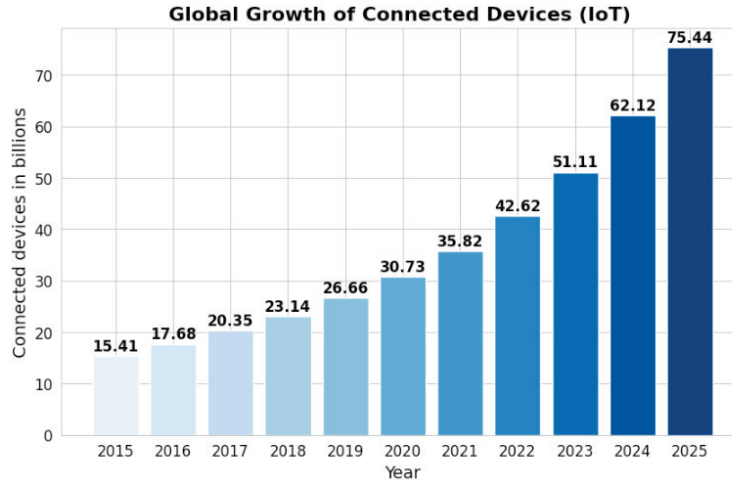


Figure 1 Growth of IoT connected devices from 2015 to 2025 according to statista.

1.1 Root Causes of DDoS Attacks

Due to its continuous development and widespread use in the present time, attackers have found great interest in exploiting these devices and carrying out attacks that have the potential to harm critical aspects of their targets. In this context, DDoS attacks have emerged as a top cyber threat [2, 3]. A DDoS attack is a type of cyber attack that primarily aims to exhaust the target server by sending floods of fraudulent traffic, resulting in slow response to legitimate users, eventually leading to a shutdown [4, 5]. To carry out this fraudulent activity, a coordinated attack is conducted through controlling the compromised networks [6]. A detailed attack mechanism has been presented in Figure 2.

1.2 Cause and Effects of DDoS in IoT Systems

The advancement of technology generally affects human beings. In its adaptation, positive and negative impacts are observed. Figure 3 presents the general benefits and the IoT-specific drawbacks related to the technology, which can lead to convenience or risks. Positive developments during its emergence include greater connectedness and easier access to information that was previously hard to acquire. With technology, connectedness has never been a problem. However, bad actors who play the role of villain are also advancing their methods with the help of technology, making their

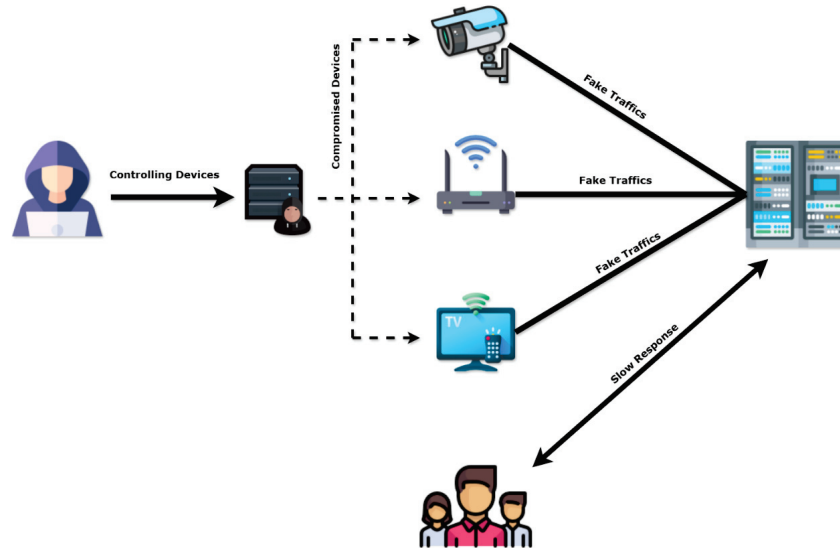


Figure 2 DDoS attack in mechanism.

attacks more sophisticated and harder to detect. In the field of IoT, this attack is not new; in fact, it has already dealt a significant blow. IoTs are characterized by inherent vulnerabilities that attackers exploit regularly, specifically their inadequate memory and CPU resources, which make them difficult to implement effective security mechanisms. Robust security mechanisms require substantial processing power to effectively secure data and privacy. By having it, IoT devices can handle essential management of users' sensitive data, authentication, service availability, and data management [7–9].

These weaknesses can serve as a basis for the attacker's attack and provide a solid foundation for their attack techniques. With effective exploitation, they will eventually hit the target organization, especially if the target is not well prepared for the attack. An infamous incident occurred in 2016: the Mirai botnet attack, carried out on a large scale. In the Mirai botnet attack, bots, which are a collection of compromised devices, were used to launch an attack on IoT devices in the form of DDoS. This is achieved through an auto-replication module that detects vulnerabilities on devices by scanning the entire internet [10]. By creating a strong bot network, the attack gained remote access to more than half a million IoT devices, which served as the foundation for creating variants of this attack. These bots have targeted major businesses like Domain Name System (DNS) and the French web hosting

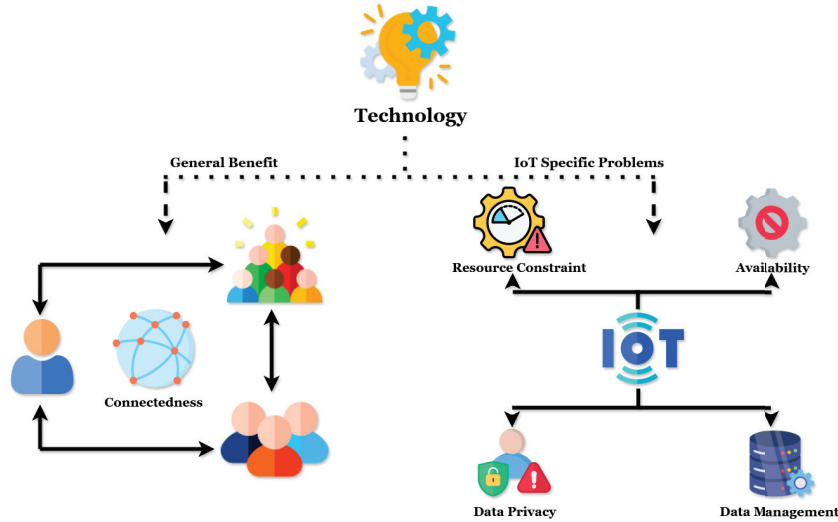


Figure 3 Positive and negative impact of technology (exclusively for IoT devices).

provider OVH, as well as people opposed to technological security. The attack has significantly impacted both the user and the owner, primarily by disrupting its services and preventing access [11].

1.3 Comparative Analysis of Past Surveys

Table 1 presents the thorough review we conducted of existing survey studies on IoT-based DDoS attack detection and mitigation, which vary in comprehensiveness, methodology quality, and evaluation. Our contribution differs by employing a multivariate, hierarchical, and taxonomy-based framework that encompasses both traditional and modern DDoS detection, mitigation, and prevention approaches.

As shown in Table 1, our work provides a comprehensive, descriptive analysis of DDoS threats and their detection, prevention, and countermeasures in IoT environments. Thematic differentiation is evident in current works targeting specific categories: [12] focuses on detection techniques. [13] limits its application to Industrial Internet of Things (IIoT) security frameworks. DDoS countermeasure architectures are the focus of [14] and [15], and [15] in particular, which emphasizes machine learning models. [16] ventures into the most AI-oriented trends by researching DDoS attacks using blockchain.

Table 1 Comparative analysis of past surveys

Criteria	Ours	[12]	[13]	[14]	[15]	[16]
Comprehensive Scope	General coverage	Detection focus	Industrial IoT focus	DDoS defense systems	ML-based DDoS detection	Blockchain-based attack detection
Hierarchical Taxonomy	✓	✓	–	✓	✓	–
AI/ML/FL Detection	✓	✓	✓	✓	✓	✓
Comparative Analysis	✓	✓	✓	✓	✓	✓
Real-World Cases	✓	–	–	✓	–	–
Dataset Analysis	✓	–	✓	–	–	–
Lightweight Mechanisms	✓	–	–	–	–	✓
Privacy & Ethics	✓	✓	✓	✓	✓	✓
Emerging Trends	✓	✓	✓	–	–	✓
Blockchain-Based Security Frameworks	✓	–	✓	–	–	✓
Quantum Computing Paradigms	✓	–	–	–	–	–
Novel Contributions	✓	✓	✓	✓	✓	✓

1.3.1 Hierarchical Taxonomy of DDoS attacks

One key component of successful mitigation techniques is structural control over DDoS attack types. The multi-level classification framework in our survey, along with [12,14], and [15], provides a systematic characterization of attacks. [13] and [16] lack an organizational decomposition and are therefore not very analytically specific.

1.3.2 AI/ML-driven detection methodologies

Our work and the other research papers surveyed agree that AI/ML is important for improving DDoS detection frameworks. Recent trends in predictive security models are supported by techniques such as expert knowledge, reinforcement learning (RL), federated learning (FL), and deep learning (DL).

1.3.3 Comparative evaluation of defense strategies

One of its key contributions is the comparative analysis of several DDoS security approaches in our research, which simplifies comparative evaluation. This comparative evaluation, shared by all the articles reviewed, promotes a multi-faceted discussion of the effectiveness of mitigation.

1.3.4 Real-world use cases and deployment scenarios

When conducting cybersecurity research, it is crucial to validate data. To accommodate conceptual notions within realistic deployment contexts, our research includes real-world case studies. The absence of empirical validation in [12, 13, 15], and [16] significantly distinguishes our survey from theirs.

1.3.5 Dataset analysis

A thorough assessment of datasets is needed for data-driven approaches. Along with [13], our survey combines bias assessments, statistical assessments, and dataset taxonomies. Nevertheless, [12, 14, 15], and [16] miss this crucial aspect.

Lightweight Security Mechanisms, Privacy Preserving, and Ethical Consideration: Low-overhead security mechanisms and lightweight encryption protocols are common, especially with the inherent resource constraints of the Internet of Things. All publications considered here address the explanation between ethical compliance and security controls in light of the widespread adoption of privacy-preserving AI and secure multi-party computation (SMPC). Differential privacy, GDPR-compliant security models, and data sovereignty all rely heavily on research in IoT security.

1.3.6 Emerging threats and opportunities

By identifying novel threats and adaptable security designs, our study goes deeper than past surveys, tackling FL for decentralized attack detection, Quantum cryptography (QC) as a future adversarial mitigation model, and Anomaly detection based on blockchain technology for tamper-evident security intelligence. Although [12, 13], and [16] examine emerging trends, [14] and [15] offer no discussion and may be less significant in light of changing threat scenarios.

1.3.7 Novel contribution

These novel contributions are presented in our survey:

1. Categorization of attacks in IoT networks on the basis of a hierarchical and taxonomy-driven approach.
2. Methodological consistency is promoted through dataset-driven knowledge and existing benchmarks.
3. Highlighting security frameworks, which are a necessity for the limited resources of the IoT.

4. Our work is cutting-edge in IoT security, including discussions of advanced models such as federated and quantum learning.

1.4 Scope, Objectives, and Contributions of the Survey

This comprehensive survey aims to clearly discuss the effectiveness of existing DDoS attack detection, prevention, and mitigation in IoT environments, supported by an analysis of the DDoS attack taxonomy, techniques, and challenges. In this way, the information can be well organized, which can help in the overall clarity of the topic. By discussing relatable scenarios and use cases, providing a comparison table, and specifically highlighting the key parts of a DDoS attack for each actor, this survey will effectively explain the problem's causes and offer a solution. The rest of the paper will be structured sequentially as follows. In Section 2, the taxonomy of IoT-specific DDoS attacks will be explained. In this section, the root causes, types of attacks, and real-world use cases will be discussed. In Section 3, DDoS attack detection techniques will be covered, which include traditional, anomaly-based, FL, AL, DL, and QC. After that, discussions on mitigation strategies, including lightweight security protocols, edge and fog computing, blockchain, and artificial intelligence, will be presented in Section 4. In Section 5, a comprehensive discussion on the datasets, validation approaches, and metrics was conducted. Section 6 will discuss the challenges in IoT DDoS detection and mitigation, and Section 7 will outline the privacy and ethical issues in IoT security. Section 8 will discuss the development lifecycle of IoT. Section 9 will discuss real-life use cases and applications. Finally, Section 10 concludes the paper. The overall flow of the survey paper is presented in Figure 4.

1.5 Methodology

This comprehensive survey has been conducted with careful consideration for effective discussion and understanding by the reader. In this regard, understanding the methods used in this research has also been an important consideration for an in-depth understanding of the study's scope. In this section, we will discuss the research questions that have guided this paper, the criteria for selecting relevant literature, the queries used to search the database, and the inclusion and exclusion criteria considered. With this systematic approach, this survey will not only demonstrate its robustness but also its practical importance.

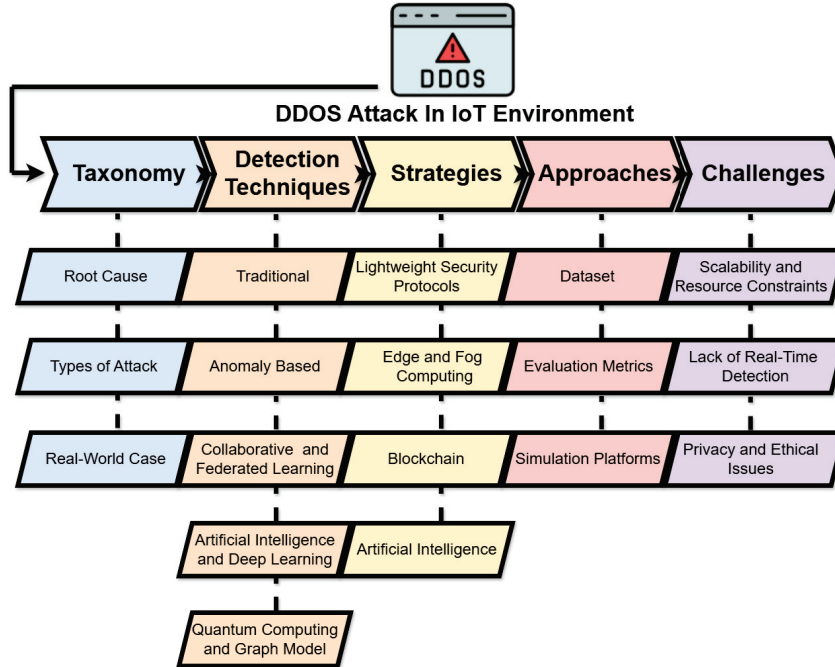


Figure 4 Comprehensive survey flow.

To have an effective discussion and comprehensive flow, the following research questions have served as the basis for this survey:

1. What type of DDoS attack is frequently used in IoT environments?
2. What modern and traditional detection techniques are currently employed to detect IoT-based DDoS attacks? Does this include AI-driven defense, Machine Learning (ML), DL, FL, and QC?
3. How effective are advanced mitigation strategies, such as blockchain-based systems, in addressing DDoS attacks in IoT environments?
4. What are the existing development challenges and opportunities in deploying a lightweight security mechanism in an IoT environment?
5. What drives the evolution of DDoS attacks, and what are the opportunities that await in handling the emerging DDoS threats in the IoT environment?

To have an accurate and clear understanding of the topics discussed in the paper, the selection criteria for this survey include studies that primarily focus on DDoS attacks in IoT environments, including research articles, conference

papers, and technical reports. Specifically, the published papers used in the comparative analysis table were published in the last five years, and to obtain specific information on some of the discussion and definitions, a few of those have been published in the last 10 years. In addition, published papers that present empirical evaluations of detection and mitigation techniques are included, along with those that discuss the challenges and some future opportunities in IoT DDoS security. Papers excluded from the selections are those that focus on general cybersecurity threats and do not discuss DDoS specifically, do not provide empirical results or case studies, or are not related to our topic.

To ensure we can meet our aim in this paper, we have used several databases to collect relevant literature. These databases included ScienceDirect, ResearchGate, Google Scholar, Scopus, and SpringerLink. In finding the relevant papers, some of the keywords that we have used in querying are “DDoS attack in IoT,” “Machine Learning in IoT,” “Challenges in DDoS detection in IoT,” “DDoS attack mitigation strategies in IoT,” and many more, along with the Boolean operators such as OR and AND.

By effectively utilizing this method, we can develop a comprehensive survey that provides an in-depth understanding of this dynamically evolving cyber threat. Figure 5 presents the overall method in developing our comprehensive survey.

2 Taxonomy of IoT-Specific DDoS Attacks

DDoS attacks can be carried out in many ways. Generally, knowing what this attack does and how it is carried out can be valuable, especially in today’s digital era. To effectively prevent becoming a victim of this attack, diving deep into its types and understanding its real-world use cases can also be a good way to understand it better. In this chapter, we will comprehensively classify the root causes of IoT DDoS vulnerabilities, types of DDoS attacks targeting IoT networks, and real-world cases and impacts.

2.1 Root Causes of IoT DDoS Vulnerabilities

Instances of DDoS attacks in IoT environments have been constantly growing. Incidents that happen like this become more crucial and need to be addressed. However, the effectiveness of mitigation strategies can be challenging due to inherent vulnerabilities in IoT devices. Vulnerabilities like weak credentials, lack of security standards, resource constraints, and

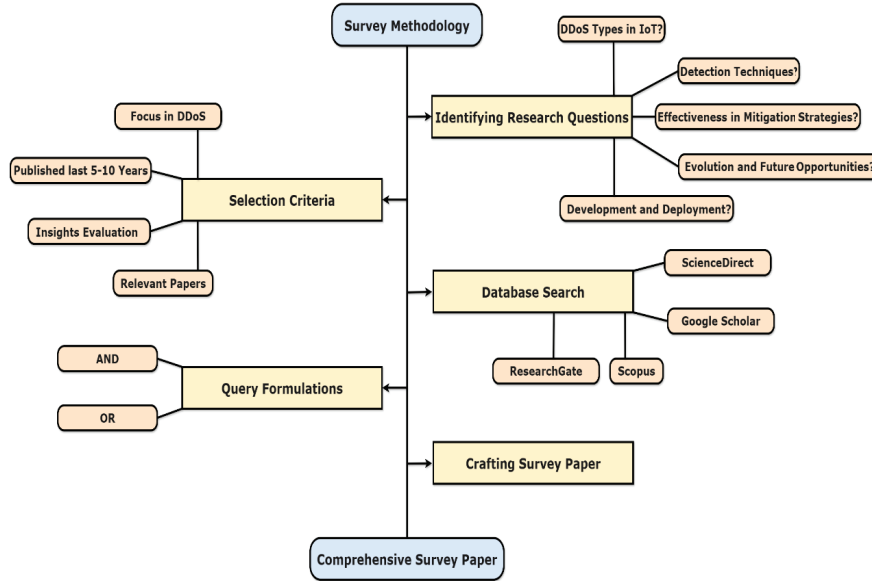


Figure 5 Survey methodology flowchart.

network-related challenges are the most commonly exploited by attackers. Figure 6 presents the overall workflow by which DDoS attackers can exploit these weaknesses, showing the mechanisms for creating IoT devices, acquiring users, and exploiting them.

2.1.1 Weak credentials

Cybersecurity problems cannot be experienced if there are no flaws or weaknesses in the implementation of technologies. Diving deep into the root cause, we can see that the main problem is humans. One effective counter-measure against it is implementing strong credentials, such as usernames and passwords. According to the study by [17], the majority of malware targeting IoT devices attacks those with weak passwords and ID credentials, as well as those whose Secure Shell (SSH) and Telnet authentication services are accessible over the World Wide Web. This study has highlighted the importance of applying strong credentials to avoid being scanned by this type of attack. It has been suggested that changing the username and password, or ID combos, during login could be an effective precaution to prevent malware or hackers from infiltrating these electronic devices. It is also advised that the default configuration should already be sufficient upon

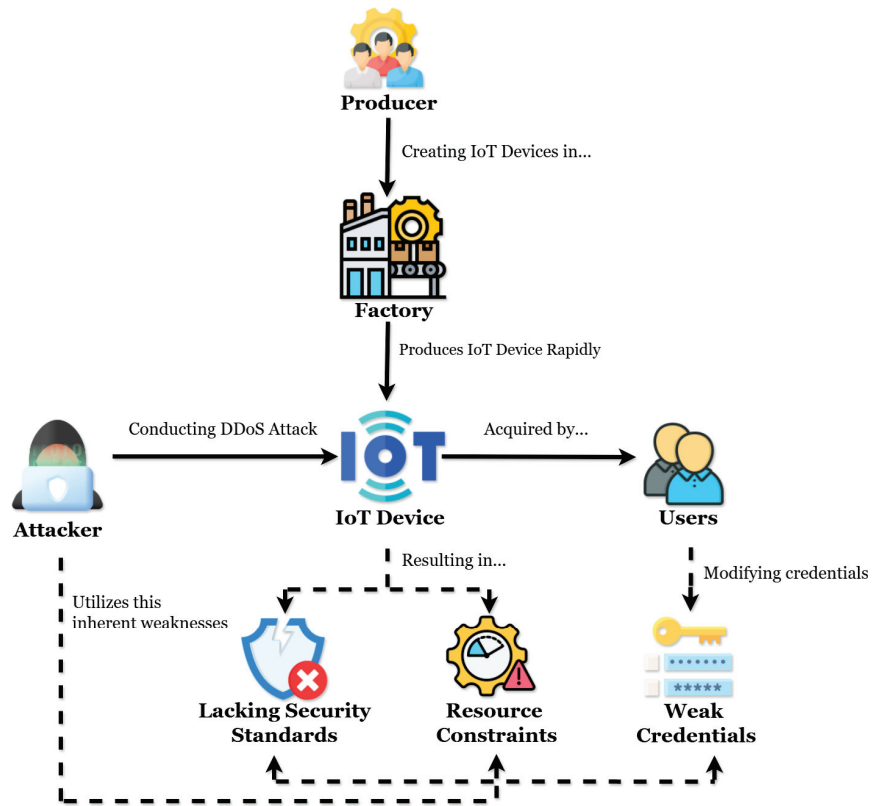


Figure 6 Root causes of DDoS attack.

delivery, and that modifications to credentials by consumers could lead to their exploitation [17].

2.1.2 Lack of security standards

The safety of IoT networks and devices has been steadily declining due to the lack of effective regulations, standards, and governance. This has created a wide range of privacy-related challenges that have caused the industry to fall victim to uncontrolled IoT development. Another reason for poor security [18].

2.1.3 Resource constraints

These challenges have been encountered with a few low-cost computer devices, including limited processing power, limited bandwidth, and

constrained storage space [19]. These characteristics first transform the hacked device into a bot. It has been shown that Mirai significantly affects resource usage on IoT edge devices: when they're overloaded with TCP and User Datagram Protocol(UDP) packets, their CPU, Ethernet, and SD usage significantly rise, while their internal memory utilization decreases [20].

2.1.4 Network-related challenges

Authentication, provisioning, configuration, monitoring, routing, and device software management are among the capabilities enabled by IoT network management [21]. DDoS attacks are among the primary concerns for administrators when dealing with network-related problems, as they can lead to unavailability and production downtime, resulting in financial losses [22].

2.2 Types of DDoS Attacks Targeting IoT Networks

The attack mechanisms of DDoS attackers can take many forms and employ different approaches. Each of these methods has two common goal: to cease operations or deny services. There are three common types of DDoS attacks targeting IoT networks: volume-based, protocol-based, and application-layer. The general differentiation of these attacks is shown in Figure 7, which highlights how attackers can successfully target their victims using each method.

2.2.1 Volume-based attacks

This kind of attack uses a lot of false traffic to use up the server's network bandwidth [23, 24]. Because of its straightforward nature and general applicability, this attack is more likely to appear than other attack types [25]. The following are examples of a volume-based attack

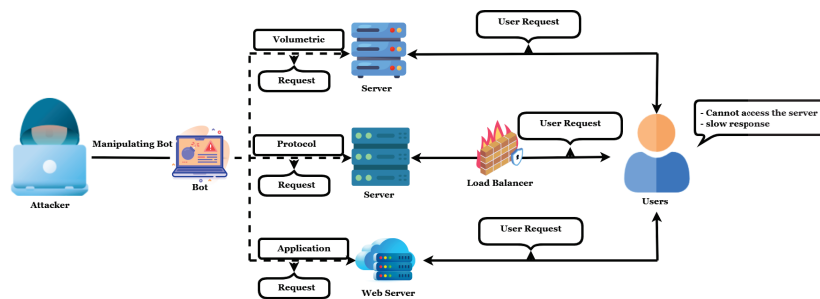


Figure 7 Different types of DDoS attacks targeting IoT networks.

2.2.2 UDP flooding

This attack is not new to IoT. The fundamental idea behind a UDP flood is the thought that the attacker would use a large amount of traffic to overload the targeted server [26]. In addition to consuming a significant portion of the targeted server's resources and network traffic, this type of attack also paralyzes the entire network [27].

2.2.3 ICMP flood

Although network administrators frequently use this method to troubleshoot reports, a person can now exploit this protocol to attack a target by sending a large number of messages [28].

2.2.4 DNS amplification attack

A DNS amplification attack involves a hacker using publicly available, globally accessible iterative resolvers to overwhelm a victim's computer with massive DNS response traffic, ultimately resulting in a DDoS attack against the target [29].

2.2.5 Protocol-based attacks

Unlike volumetric attacks, this attack targets server resources rather than bandwidth. Additionally, it targets intermediary devices, such as load balancers and firewalls, that sit between the computer and the website or server [30]. The following are the types of protocol-based attacks.

2.2.6 SYN flood

This attack, recognized as a component of the growing threat within the DDoS perspective, uses the popular TCP protocol, particularly the 3-way handshake flooding using SYN packets, to go after end hosts like victims, draining their storage and processing resources and causing them to lose their ability to respond to genuine requests [31].

2.2.7 ACK flooding

This kind of DDoS attack overloads its victim's system by sending out many ACK packets. ACK packets, which acknowledge receipt of data packets from the sender, are a standard component of TCP's data transfer procedure [32].

2.2.8 HTTP GET/POST flood

The objective of an HTTP GET/POST flood attack is to compromise the internet server and the website's application. The HTTP GET or POST

method is used by the end user to submit a request to the designated website server. In order to completely take over the targeted server and use up most of its computational resources, an attacker uses a network of bots to execute a big GET (image or scripts) or POST (file or forms) request, blocking genuine requests from getting through and resulting in a flooding assault [33].

2.2.9 Application layer attacks

Application protocols are crucial because they serve as the foundation for communication between services and apps that operate on various IoT devices [34]. Prior to computer security, application attacks were what made security susceptible. Attackers can create systems that may compromise IoT devices, alter data, and disable functionality by using Trojan horses, worms, viruses, spyware, and malicious scripts [35]. The following are the types of application-layer attacks.

2.2.10 Slowloris attack

A famous cybersecurity expert, Robert Hansen, created this attack initially. Slowloris uses insufficient resources as a key tactic, unlike conventional DDoS attacks, which rely on excessive bandwidth usage. By often transmitting useless HTTP requests, it creates several low-rate interactions with the destination server and keeps them available [36].

2.2.11 HTTP-based botnet attack

Some of the increasingly common and dangerous malware that appear in cyberattacks nowadays are botnets. Due to the considerable difficulty of blocking port 80, which is utilized for webpage communication and possesses an elevated percentage of regular traffic, attacks via website services, which are commonly utilized on the World Wide Web as a means of transmission of instructions, have been the most significant feature of HTTP-based botnets [37].

2.2.12 Session hijacking attack

Theft or alteration of sensitive data during a session-based communication channel is a threat known as session hijacking [38]. According to [39], this type of attack is among the top five threats to the crucial elements.

To further provide readers with a deep understanding of the occurrence and severity of cyber threats today, the relationship between the depth of

an incident and the damage it may cause must be considered. Volumetric attacks, such as UDP and ICMP flooding, have the highest relative frequency because they are easy to execute with botnets without requiring a complex script. Despite being prevalent, the severity can usually be mitigated through traffic scrubbing and rate limiting, except when traffic exceeds the network's bandwidth capacity.

On the other hand, protocol-based attacks such as SYN floods are relatively infrequent but severe, compared to the basic volumetric attack. This is because it directly targets the system resources, such as connection tables of firewalls and load balancers. The most dangerous among them is application-layer attacks; though they occur infrequently, they are the most severe. This type of attack uses small traffic volumes but precision-targets the server's critical functions, making it hard to detect amid real user traffic, and can result in complete service paralysis for a long period of time.

2.3 Real-World Use Cases

2.3.1 Mirai botnet attack

Internet access in the US and Europe was disrupted by numerous DDoS attacks in 2016, caused by the Mirai botnet. These attacks target IoT devices, including routers, cameras, and Digital Video Recorders (DVRs), that use default or weak credentials, and infect them with malware, creating a network of compromised devices [40].

2.3.2 KrebsOnSecurity DDoS attack

The KrebsOnSecurity website was targeted by a DDoS attack in 2016 that sent over 600 gigabits of traffic per second [20].

2.3.3 IoT-based DDoS attack on OVH

The Mirai botnet launched a particularly intense attack against OVH, a French hosting service provider, around September 2016, forcing the company offline for many hours [6].

2.3.4 IoT reaper botnet

Malicious software Reaper, commonly referred to as IoTroop, was created around 2017 primarily by a group of information researchers, and it gained improved capabilities. Unlike the Mirai botnet, it can quickly compromise an IoT device. Since the whole system is quickly overthrown, this attack has a variety of consequences [41].

2.3.5 Satori botnet

Satori is an altered version of the Mirai botnet, using the Realtek software development kit (SDK) rather than the telnet scanner module to gain remote access to Huawei routers and other devices by exploiting weaknesses in those devices [42]. About 280,000 IoT devices that were compromised by the botnet, as well as another 220,000 devices, were thought to be at risk [43].

2.3.6 DDoS attack on smart city

The increasing frequency of cyberattacks on smart cities is an existential risk to the progress achieved through the field of technology. Because smart cities depend largely on computer-driven, sophisticated digital networks to deliver many city services and systems, they have become more prone to cyberattacks, regardless of the target [44].

These attacks have caused significant problems for their targets and have prompted them to take notice. Due to these instances, many published studies have already examined how these attacks operate in IoT environments. Table 2 presents a comparative analysis of the different types of attacks, their impacts, and mechanisms.

A comparative taxonomy of attacks specific to the IoT, with descriptions of their effect vectors, operational concepts, and exploitation mechanisms, is presented in Table 2. While consuming computer resources, violating protocol compliance, and disrupting services, network-layer harmful campaigns such as UDP Flooding, ICMP Flood, DNS Amplification, SYN Flood, and ACK Flooding exploit volumetric Denial-of-Service (DoS) and DDoS mechanisms. Application-layer attacks such as HTTP GET/POST flooding, Slowloris, and HTTP-based botnets exploit request flooding and session persistence to coordinate the delivery of high-bandwidth payloads on demand, consuming bandwidth and causing system slowness. Session hijacking also facilitates easy illegal session persistence, and bypassing normal authentication processes creates attack vectors for attacker privilege escalation. Threat vectors, improved intrusion detection systems (IDSs), dynamic rate-limiting systems, and secure cryptographic exchanges must be implemented to keep pace with future IoT threat models.

3 DDoS Attack Detection Techniques

As technology grows day by day, the way things are done is becoming more convenient. Methods for attacking and detecting cyber threats have also changed as a result. The old style of cyber threat detection, such as DDoS

Table 2 Impacts, targets, and mechanisms of different DDoS attack types

Attack Type	Target	Impact	Mechanism	References
UDP Flooding	IoT and embedded devices	Consume more energy than their regular usage	Exploiting compromised IoT devices and making them bots to launch an attack	[45]
	Edge resources / Fog gateways	Sabotages fog gateways and bypasses traditional techniques of filtering data	Flooding edge nodes with a spoofed USP packets.	[46]
	Wireless sensor networks (WSN)	Network resource unavailability and high resource consumption	Flooding WSNs with UDP packets	[47,48]
ICMP Flood	IoT resource constrained device	Disrupts the device functionality of IoT Device	Sending a massive number of ICMP-echo requests	[49]
	IoT devices/IoT Networks	Hijacked devices used for flooding leading to DDoS	Flooding requests with the use of the hijacked devices	[50]
	Network services	Service disruption	Sending massive volumes of ICMP packets	[51]
DNS Amplification	DNS Servers and IoT Devices	Extensive service disruptions for both IoT and DNS infrastructures	Sending spoofed IP address to open DNS resolvers	[52]
	Public DNS servers	Degradation of DNS availability	Attackers sends small DNS queries with spoofed source IPs	[53]
	DNS servers	Network congestion and service disruption	Send spoofed DNS 'ANY' queries to domain names returning with large responses	[54]
SYN Flood	IoT devices within smart environment	Overwhelm IoT devices resulting in denial of service and disruptions of operations	Sending a large number of TCP SYN and consuming the device resources preventing connections from being established	[55]
	Internet of Medical Things	Disruption of services and security risks	Malicious nodes performing TCP SYN flooding to overwhelm resources	[56]
	Internet Service Provider networks	Disrupts the availability of network	Attack floods the network with SYN requests to exhaust server resources	[57]

(Continued)

Table 2 Continued

Attack Type	Target	Impact	Mechanism	References
ACK Flooding	IoT Servers and Devices within the networks	Degrading the performance and completely shutting down the server	Sending high volume of ACK packets to the targets, resulting in an overwhelmed processing capacity and network bandwidth	[58]
HTTP GET/POST Flood	Home IoT Devices	Depleting the IoT device resources, power, and bandwidth	Sending high volume of HTTP GET or POST requests to target IoT devices	[59]
	Cloud computing environments	Overwhelming the server resulting in DDoS	Flooding servers with a large volume of HTTP-GET request	[60]
	Web servers/IoT devices	Degrades the performance of servers	Flooding web services with massive HTTP request using zombie hosts	[61]
HTTP-Based Botnet	Home IoT Devices	Overwhelming these devices by sending a high volume of HTTP requests	Sending high volume of HTTP GET or POST requests to target IoT devices	[62]
Slowloris	IoT Device utilizing SSH and FTP protocols	Increase the power consumption of the target device	Causing too large computational demands compared to the minimal resources used by the attacker	[63]
	Web servers/IoT networks	Paralysis of servers through exhausting them	Sending many slow, incomplete HTTP requests to keep the connection open	[64]
	IoT networks	Exhaustion of resources	Sending slow-rate HTTP requests	[65]
Session Hijacking	IoT Devices utilizing traditional authentication protocols	Leads to unauthorized control and data breaches in IoT systems	Taking advantage of the physical access to IoT devices, intercepting it and manipulating authentication sessions	[66]
	TCP/IP layers	Unauthorized access to user sessions	Taking control of active sessions made by the user through stealing session cookies	[67]
	Web applications in IoT systems	Unauthorized control of user sessions	Hackers taking over between user and server, effectively impersonating legitimate user	[68]

attacks, is no longer fully utilized due to its limitations. This has led to the use of advanced security measures that leverage artificial intelligence, which has been seen as one of the bright spots in addressing this problem. However, despite the introduced effectiveness of these detection systems, they also have their own challenges, which we will discuss in this section. Table 3 presents a brief summary of existing DDoS attack detection approaches, including their advantages and disadvantages. This is to better understand what needs to be considered when discussing or implementing these in the future.

3.1 Traditional Approaches

Traditional attack detection was based on statistical analysis; these approaches are well known as rule-based, where they only react to specific rule sets in the program's backend. This approach is very good at detecting known attacks, but it will struggle to detect new variants of cyberattacks.

Signature-based: This detection technique relies on known patterns or characteristics of DDoS attacks. Techniques that utilize these usually employ IDS and intrusion prevention systems, which detect attacks by analyzing network traffic and looking for patterns that match the recorded network traffic labeled as attack characteristics in the database [69]. This method is very effective at identifying known attacks; however, signature-based detection struggles to detect new and zero-day attacks, making it less adaptive to attackers' evolving attack techniques [70].

Threshold-based detection: This detection technique relies on defining acceptable and unacceptable limits for IoT traffic at devices and networks. An attack can be identified when traffic exceeds a predefined threshold, triggering an alert indicating a potential attack [71]. This technique is both simple and computationally efficient; however, it lacks the flexibility to adapt to dynamically changing network conditions [72]. Some attackers may bypass this technique by performing a low-rate or slow-drip DDoS attack that doesn't exceed the threshold [73].

Rule-based: This type of detection technique uses predefined rules and a policy-driven mechanism to effectively detect and respond to DDoS attacks [74]. Well-known techniques such as firewalls, access control lists (ACLs), and packet filtering fall under this category. Rule-based detection techniques can be done by creating some specific rules in order to block suspicious traffic; however, even with the effectiveness of this technique in identifying DDoS attacks, one of its challenges is that it will need to have regular updates and annual tuning for new types of DDoS attacks, making it almost unachievable, especially in large-scale IoT environments [75].

Blacklist and Whitelist: The blacklisting technique is another method that maintains a list of IP addresses or websites known to be malicious or involved in attacks. By doing this, when this technique encounters a specific IP address or website on the maintained list, it will block it. On the other hand, there is the whitelist, which is the opposite of a blacklist. A whitelist is a maintained list of IP addresses or websites that are allowed. When an unknown address or website is detected, it will be blocked [76].

3.2 Anomaly-Based Detection

By collecting common traffic patterns over a predefined period and establishing a foundational description, the anomaly-based detection technique successfully identifies and detects zero-day and other unidentified attacks. Each newly introduced trend that falls beyond the foundation's area is considered an anomaly, which may indicate an attack is underway.

Statistical Analysis: A common approach for identifying anomaly-based DDoS attacks in IoT environments, it effectively distinguishes between normal and abnormal traffic patterns. With the help of continuous monitoring of specific metrics to quickly identify cyber threats [77]. However, when using this approach, there is a high risk of false positives, as normal attack patterns can be mistakenly identified as attacks due to IoT's dynamic and heterogeneous nature [78].

Machine Learning (ML): ML-based anomaly detection has gained significant attention in cybersecurity over the past few years, as it improves accuracy and reduces false-positive rates in DDoS defense mechanisms [79]. ML has two types: supervised and unsupervised learning. In supervised learning, models are trained on labeled datasets containing normal and attack traffic, enabling them to identify incoming traffic with high accuracy. The second one is unsupervised learning. In this type of learning, the model will be trained with unlabeled data. The model will identify normal traffic and attack traffic by detecting differences, such as outliers, and flagging them as potential attacks [79].

3.3 Collaborative and FL

FL can be well-suited for detecting DDoS attacks in an IoT environment, as it enables IoT devices to train in a decentralized manner, process data, and share new insights with a central server [80]. With this technique, privacy and scalability can be enhanced, effectively reducing the need for large-scale data transmission, a common issue in IoT networks due to resource

constraints [81]. Additionally, this technique will help detect DDoS attacks in IoT environments by leveraging its accuracy without exposing users' sensitive data [81].

Collaborative learning involves one or more nodes of IoT devices that dynamically share information about how well the network's behavior is [82]. With this technique, anomalies in IoT behavior can be quickly detected, as multiple IoT nodes can communicate and monitor traffic. By using a consensus mechanism, this technique will ensure a coordinated response whenever a DDoS attack is detected, effectively reducing the likelihood that an attacker will successfully exploit the weaknesses of individual nodes [82].

Using the mentioned detection technique, multiple businesses can collaborate to improve DDoS detection and classification across multiple edge nodes while preserving their confidential information [83].

3.4 AI and Deep Learning Techniques

This type of DDoS detection approach uses AI techniques to effectively detect DDoS attacks. This approach is effective and can compensate for the limitations of traditional security approaches.

Supervised DL models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), will be trained on large datasets containing both normal and attack traffic. With this, these models can provide more accurate detection and recognition of complex attack patterns and extract hidden features from each flow of traffic in the data. This is a powerful aid in detecting DDoS attacks, as it can analyze sequential traffic over time [71].

In addition, there are unsupervised learning approaches. These approaches have included autoencoders and Generative Adversarial Networks (GANs) to effectively identify unknown or zero-day attacks. In this context, autoencoders will learn from the normal distribution of network traffic and flag deviations, while GANs will generate synthetic datasets of attacks to improve the model's robustness in detecting DDoS attacks [84,85].

Another implementation of AI techniques has already been applied to automatically adapt and respond to DDoS threats: RL. In this technique, effective adjustments to mitigation strategies based on real-time attack patterns can be made in IoT security systems, greatly reducing damage and improving IoT network performance [86].

3.5 Quantum Computing and Graph Models

Advanced detection models, such as quantum computing and graph models, have emerged as approaches that are impenetrable, as numerous methodologies become outdated. It appears essential to switch to a quantum-based approach because it provides sophisticated encryption techniques that improve online protection against evolving cyber threats and leverages quantum mechanics, making it extremely secure and extremely difficult for hackers to penetrate undetected [87].

Quantum computing leverages the principles of quantum mechanics, including superposition and entanglement, to efficiently execute multiple computations at high speed [88]. Algorithms that employ this, such as Shor's algorithm, have great potential to rapidly analyze and detect DDoS attacks in IoT environments by identifying their attack patterns, which can be a computational constraint for traditional security systems [89]. Currently, quantum machine learning (QML) is being explored, aiming to make security systems for DDoS attack detection and mitigation more robust by effectively analyzing large volumes of network traffic generated by IoT devices [90]. However, it faces challenges at present, especially in implementation, due to limited available quantum hardware [91].

One of the great innovations in cybersecurity for effective DDoS attack detection is the graph-based model. Graph Neural Networks (GNNs) and graph-based anomaly detection approaches can effectively analyze network traffic as a graph, where IoT devices are represented as nodes and communication flows as edges [92]. By carefully analyzing anomalies in traffic flow structure, this approach can flag DDoS attacks that may be undetectable by traditional DDoS detection techniques.

3.6 LLMs for DDoS Attack Detection

Large Language Models (LLMs) have emerged as one of the most powerful tools for transforming DDoS detection through the integration of contextual understanding, understandable reasoning, and multimodal data handling. The recent advancements clearly showcase their abilities not only as passive detectors but also as active participants in cybersecurity defense. One example of this is the study by [47], which presents ShieldGPT, a robust framework that directly leverages LLMs to effectively mitigate DDoS attacks, bridging the gap between natural language processing and network traffic analysis.

Their system uses structured prompt engineering and a dual-template architecture to provide a clear interpretation of global and local traffic features, generate an understandable threat assessment, and propose context-specific mitigation actions. Compared to conventional black-box models, ShieldGPT addresses the challenge of complex interpretability, an important aspect of real-time defense compliance for sensitive information. A similar approach using LLM-based threat detection and prevention for IoT ecosystems has further supported the idea of practical integration of LLMs in real-world network scenarios. In their utilized framework, lightweight LLMs that were fine-tuned on domain-specific devices are being employed to have a high performance in anomaly detection across resource-constrained IoT devices, though their framework primarily focuses on the broader spectrum of IoT threats, their framework still effectively identifies significant early signs of volumetric and protocol-based DDoS attacks [46].

One important value of LLM-based systems is their capacity for explainability and adaptability. Techniques like SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME), when integrated into LLMs, can provide a comprehensive feature attribution and rationale generation for decisions made during the evaluation of DDoS threats. In the adaptive-end-to-end encryption IoT security framework [48], LLMs are coupled with explainable AI tools to translate complex detections into human-readable insights. This idea is very important for incident responders who deal with DDoS events. Moreover, the BARTPredict model developed by [50] underscores the predictive power of LLMs, leveraging transformer-based architectures to analyze temporal patterns in network traffic; their system can identify malicious behavior that may signal an attack before the payload is fully delivered. The anticipatory capability of their model is a major turning point, together with the reactive detection mechanism, adding to the papers that state the effective role of LLMs in cyber defense. Another noteworthy contribution is CyBERT [51], a featureless LLM-based system that achieves excellent performance in detecting vulnerabilities in IoT devices without handcrafted features. Its featureless design has simplified the integration of LLMs across diverse network infrastructures, enabling greater scalability and deployment feasibility.

The effectiveness of various detection approaches in the existing DDoS attack detection mechanisms is presented in Table 3. With a high detection accuracy approaching perfection, it highlights how well researchers have adapted to emerging technologies such as ML and DL, enabling their approach to detect even unknown security threats. However, common

Table 3 Advantages and disadvantages of DDoS attack detection approach

Approach	Advantages	Disadvantages
Traditional Detection	Simplicity [93–97] Low resource consumption [93–96] Real-time capability [93–95, 97] High accuracy for known attacks [93, 94] Already been established techniques [95, 96] Deterministic Results [96]	Inflexible [93] Difficulty in detecting unknown attacks [93, 96] High false positives [93–97] Issues in scalability [93–97] Maintenance overhead [93] Ineffective in detecting novel attacks [94] Lack of adaptability [94, 95, 97] Lack of context awareness [95, 97] Maintenance Overhead [96]
Anomaly-Based Detection	Detection of unknown attacks [98–100] Reduced the need of human intervention [98] Adaptability to the dynamic nature of IoT [98–100] Can monitor in a wide range network activities [99, 100]	High false positive rates [98–100] Establishing a normal behavior in the context of wide networks of IoT is challenging [98–100] Resource constraints [98–100]
Federated Learning	Privacy preservation [101–105] Reduced communication overhead [101–104] Real-time detection [101] Enhanced model stability [101] Improved aggregation methods [101] Scalability [102–104] Adaptability [102–104] Robustness against poisoning attacks [105] Comprehensive detection	Model performance degradation [101–105] Non-IID data distribution [101] Aggregation algorithm sensitivity [101–104] Data heterogeneity [102–105] Resource constraints [102, 105]
Quantum Computing	Enhanced threat detection [106] Improved machine learning algorithms [106] Real-time threat analysis [106] Simulation of complex systems [106] Enhanced computational power [107–109] Advance cryptographic techniques [107] Improved data analysis [107] Improved data handling [108, 109] Scalability [108, 109]	Hardware instability and fragility [106, 107, 109] High development costs [106, 107] Limited software ecosystem [106, 107] Security risk to current encryption [106, 109] Integration complexity [107, 109] Complex implementation [108] High resource requirements [108] Limited practical applications [108]

problems these security mechanisms have faced include constraints in IoT devices, as these techniques require substantial computational resources to be integrated. Combatting the increasing instances of DDoS attacks cannot still be completely feasible even with the presence of sophisticated detection approaches and, in the future, one of the focused things that is being done by the researchers is the development of a detection mechanism that doesn't need huge computational resources, which some of them are presented in Table 4.

4 DDoS Prevention and Mitigation Strategies

A DDoS Attack is a type of online threat with significant potential to inflict damage on the target. Prevention and mitigation strategies are more likely to be built to solve it. Even though this type of cyberattack is currently on the rise, techniques to address this problem have already been developed. In this section, we will discuss prevention and mitigation strategies to effectively counter the emerging, sophisticated threat of DDoS attacks in the IoT environment. These strategies have a single purpose: mitigating DDoS attacks in IoT environments. The comprehensive analysis of the succeeding strategies is presented in Table 4, along with a comparative analysis of existing DDoS prevention and mitigation strategies.

Lightweight Security Protocols for IoT Devices: Lightweight security protocols involve key management, authentication, and encryption. The lightweight encryption protocol outlines the data encryption algorithms, generalized encryption processes, and encryption operational methods. Many key pools have been made accessible to authorized users in key management, and every key is generated effectively via multiple methods, including the key store seed that the user and devices share. During authentication, the system administrator configures it using a secure method, such as a manual procedure, to ensure the device communicates its hidden identification to the network hub alongside all other devices that must connect to it [110].

Leveraging Edge and Fog Computing for Localized Defense: Cloud computing capabilities are extended closer to the network edge via fog computing, a decentralized architecture [111, 112]. A great deal of data can be processed locally by fog systems, which also run on-premises, are fully portable, and can be mounted on a variety of hardware, such as Internet of Things devices that need to analyze massive volumes of data rapidly. Numerous security measures related to data, virtualization, discrimination, networks, malware,

Table 4 Comparative analysis of different DDoS detection and prevention strategies

Mitigation Strategy	Technique Used	Computational Overhead	Scalability	Ref
Lightweight Security Protocol	Physical Unclonable Functions (PUF)	Minimal computational overhead	Adaptable to devices operating on diverse technologies	[116]
	Lightweight Intrusion Detection System, Novel Data Preprocessing Technique, ML and DL classifiers, SMOTE for handling imbalance	Target lightweight IDS suitable for IoT devices, which has minimal resources	Designed to IoT constrained devices, so scaling it to non-IoT constrained devices can be possible	[117]
	Distributed transparent IDS network, Optimally placed using a K-uniform hypergraph model	Optimal placement of IDS nodes, Transparent operation to avoid unnecessary processing, Use of offline training	Distributed architecture, Efficient placement strategy using graph-based optimization, capable of adapting to larger or more dynamic IoT networks	[118]
	Custom Preprocessing Pipeline, Class balancing, ML Classifiers, Binary and Multi-Class Classification	Compact and lightweight, low resource consumption, Fast training and inference	Built with the consideration of resource-limited IoT, Small to medium size IoT networks	[119]
	Stacked modified gated recurrent units for sequential data modeling, Two customized IDS models (BCE, MCE), Temporal feature preservation	Lightweight, lower time complexity, able to be deployed in mobile healthcare devices	Tailored for Healthcare IoT systems, Scalable to handle multi-vector DDoS attacks	[120]
Fog Computing	Adaptive Neuro-Fuzzy Interference System (ANFIS) and Software Defined Networking (SDN)	Tasks are distributed and minimize the load of individual devices	Can accommodate the growing number of IoT devices	[121]
	Anomaly-based intrusion detection using KNN algorithm, Signature-based detection using a database of known attacks	Offloaded to the fog layer reducing the burden of IoT devices, Lightweight approach	The utilization of fog computing implies that scalability is possible	[122]
	Randomness measurement, Fog computing to process data near the source	Low in IoT devices as processes are offloaded in the fog layer, KNN imposes moderate computational cost	Scalability is enhanced through fog computing by distributing load and centralized processing layers	[123]
	Fog computing anomaly detection architecture, Continuous Ranked Probability Score (CRPS) metric to support multi-variable inputs	–	Scalable design via fog nodes in a 3-tier architecture	[124]
	Two phase architecture (online and offline)	Optimized for low resource usage, Offline training avoids real-time computations, Lightweight encryption	Offline model training, Fog computing decentralization, Use of ensemble learning and lightweight algorithms	[125]

(Continued)

Table 4 Continued

Mitigation Strategy	Technique Used	Computational Overhead	Scalability	Ref
Blockchain	Blockchain Technology	Minimized the resource consumption and is suitable for deployment on resource-constrained devices	Can handle the growing amount of IoT devices and increasing volumes of threat data	[126]
	Ethereum Blockchain, Authentication Mechanism, IP tracing, Two-way message exchange	Minimal, Reduced I/O load, Lightweight processing	Moderately scalable with the help of decentralization	[127]
	Ethereum Blockchain, Authentication Mechanism, IP tracing, Two-way message exchange	Minimal, Reduced I/O load, Lightweight processing	Moderately scalable with the help of decentralization	[127]
	Software Defined Networking, Blockchain technology, Artificial Neural Networks	Computational and communication overhead	Improved scalability and fault tolerance, Blockchain provides security in a distributed manner, ANN is computationally	[128]
	Integration of ML model for detecting DDoS attacks, Use of blockchain framework to support ML models		Suitable for diverse IoT environment	[129]
	ML for detecting real-time DDoS attacks, Blockchain ledger to store the blacklisted IP addresses and timestamps securely and transparently	Efficient in inference overhead model using Random forest, Blockchain introduces additional overhead for processing transactions	Real-time ML detection scales well	[130]
AI-Driven	SDN with Adaptive ML	Can efficiently manage computational resources	Can adapt to changing sizes of the network and handle an increasing number of IoT devices	[131]
	DL Models (Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU))	Its computational complexity is moderate to high	Good scalability, Can generalize well to various DDoS attacks, Needs hardware acceleration for real-time performance	[132]
	ML and DL, Neural Network Based Intrusion Detection	Requires more training time, Inference is relatively efficient	Scaled with the use of distributed training	[133]
	AI for anomaly detection, ML for traffic analysis	Requires continuous processing of traffic data	Can be deployed across multiple nodes or edge devices, More scalable compared to traditional systems	[134]

and monitoring are enhanced by this broad range of functionality-driven applications [113].

Role of Blockchain Technology in Preventing IoT DDoS Attacks: Within an IoT context, blockchain can significantly reduce DDoS attacks. Security can begin with network-level protection, where blockchain technology is implemented at the internet service provider level, on a system that could

be remote from the hacker's or target's operational location. A different approach is to focus on the near-attack domain, given that the majority of the most recent DDoS botnets are constructed by assembling genuine IoT devices spread throughout the internet and targeting victims. Near-attack mitigation at the attacker's network is an efficient method for dealing with DDoS attacks because the traffic generated by the attack never spreads through the internet's network infrastructure. Another one is close to the victim's location; in that case, every DDoS service provider will need its own account in the permission blockchain to offer DDoS defense services. The person who was attacked can then search the blockchain to find the attacker's IP address and determine which trusted service provider IP address has authorization to provide DDoS mitigation services [114].

AI-Driven Adaptive Mitigation Systems: Several novel DDoS detection strategies have been recently implemented, including DL and AI-based approaches. As powerful computing equipment becomes more affordable and accessible, it is used extensively to anticipate and identify DDoS mitigation risks, serving as a supplemental protection mechanism against security threats, such as viruses and botnets [115].

Traditional filtering and rate-limiting methods remain effective against volumetric attacks due to their fast response time, but they have huge limitations in identifying sophisticated application-layer attacks. On the other hand, AI-driven detection systems are more effective at identifying patterns that manual configuration cannot, especially Zero-day and Low-and-Slow attacks, which are disguised as normal traffic. Nevertheless, the effectiveness of Moving Target Defense (MTD) technologies is considered High but Resource-Extensive, as they require constant network configuration changes, which can result in latency on IoT devices. While Blockchain-based solutions provide strong countermeasures for authentication and integrity, their effectiveness in preventing large volumes of real-time traffic is moderate due to scalability issues. In short, the most effective defense is a hybrid approach that combines fast filtering for bulk traffic with AI-based analysis for complex threats, ensuring high detection accuracy and a low false alarm rate.

As shown in Table 4, the mitigation strategies employed by various researchers are presented. Most of them have high detection accuracy, ranging from 90–100%, which is good for detecting DDoS attacks. As indicated in Table 4, techniques that use traditional ML and DL have achieved strong results. These are already given as approaches that utilize this; they have been extensively explored by researchers, making it well known as an effective countermeasure against it. However, given its effectiveness, it also presents

challenges, such as computational complexity and integration feasibility, which require expertise to implement successfully in an IoT network.

5 Validation Approaches and Metrics

The effectiveness of the developed model against cyberattacks is measured by its overall performance. To realize its full potential, the model must be trained on high-quality, trustworthy datasets. However, some of those high-quality datasets are not yet publicly available and can be accessed only by certain individuals for personal reasons. In this section, we will discuss the validation approaches and metrics used by the developer in their created defense model, including the challenges in IoT DDoS detection, strategies for evaluation metrics, simulation platforms and tools for real-world testing, and the limitations of existing approaches and proposed enhancements.

5.1 Datasets for IoT DDoS Detection

Datasets are crucial for developing an AI model to predict cyberattacks. This is one of the bases of its performance and effectiveness, as this is where the model will get data to train from. The following are the most common places where researchers used to access various types of datasets, including IoT traffic, for training and testing.

5.1.1 IoT-specific datasets

The prevention of botnet malware attacks **Ton-IoT Dataset**: ToN-IoT includes a range of databases collected across the entire IIoT system, including internet traffic associated with the IIoT system, records from Linux- and Windows-running systems, and sensor information from connected devices. Its diverse information was collected from a medium-sized IoT network and developed by the Cyber Range and UNSW Canberra IoT Labs, and is available in the ToN-IoT repository [135].

Bot-IoT Dataset: This dataset was created in the UNSW Canberra Cyber Center's Cyber Range Lab, which replicates an accurate networking scenario by combining botnet and regular traffic attacks, including DDoS distributed attacks that rely on TCP, UDP, and HTTP methods for collecting information such as the operating system fingerprints and service inspection, along with information-stealing techniques like keylogging [136].

CIC-IoT-2023: Among IoT datasets generated from actual IoT devices, CIC-IoT-2023 is the most extensive one. A total of 33 observed incidents are

documented in the collection, which includes data collected through 105 IoT devices. Interestingly, malevolent IoT devices attacking additional nodes in the IoT environment were the ones that initiated these incidents. Furthermore, certain attack types in CIC-IoT-2023 are not present in other IoT datasets, making it more novel [137].

MedBIoT: With 80 simulation devices and three genuine devices, the MedBIoT dataset aims to mimic an average-sized network. A switch, a lightbulb, a lock, and a fan appeared among the gadgets utilized. Three different kinds of botnets, namely Mirai, BASHLITE, and Torii, were introduced within the network. The purpose of this data collection is to provide information for the prevention of botnet malware attacks [138].

IoT-23: Three genuine IoT devices were used to produce the IoT-23 dataset. The three electronic gadgets were configured to simulate three safe instances and 20 distinct malicious instances. Every malicious instance, including Mirai, Gafgyt, Torii, and others, was subjected to a botnet (bot) attack. Both normal and malicious traffic characteristics were observed in this dataset [139].

As shown in Table 5, each dataset contains distinct attributes that reflect the current, dynamically evolving landscape of IoT security. While modern datasets like CICIoT2023 reflect evolving risk theories, older datasets like Bot-IoT and Ton-IoT provide a fundamental baseline for prior attack research. Whether it is the exploration of botnet development, adversarial malware strategies, or anomaly-based intrusion detection approaches, the

Table 5 Comparative analysis of different IoT specific datasets.

Year	Dataset	Attack Types	Source of Data	Reference
2019	Ton-IoT	DDoS, DoS, Ransomware, Password attacks, scanning, injection	Collected from telemetry datasets of IoT and IIoT sensors, operating system logs of Windows 7/10, Ubuntu 4/18, and network traffic captures	[140]
2018	Bot-IoT	DDoS, DoS, OS, Service Scan, Keylogging, and Data exfiltration	Network traffic from realistic IoT environments	[141]
2023	CIC_IoT_2023	DDoS, Dos, Web-Based, Brute Force, Spoofing, Mirai	Network traffic captures from an IoT topology of 105 devices	[142]
2020	MedBIoT	Mirai, Bashlite, and Tori	Network traffic that was captured from an IoT network comprising 83 devices	[143]
2020	IoT-23	Okiru, Tsunami, and Mirai Malwares	Network traffic that has been captured from IoT devices, including malicious and benign	[144]

careful selection of a dataset will greatly affect the scope and significance of the research. Future datasets may include different IoT environments with distinct attack routes and prioritize real-world attack simulation scenarios to further strengthen the security measures implemented, enabling the effective deployment of robust, advanced cybersecurity.

5.1.2 General network security datasets

CIC-DDoS-2019: In CICDDoS2019, some of the more recent and harmless DDoS attacks that mimic data in reality (PCAPs) are included. The network stream results analyzed using CICFlowMeter-V3 have been included as well, alongside the movements identified by their timestamps, destinations, and sources, in both IP addresses and ports, and the protocol, in CSV files [145].

CICIDS2017: CICIDS-2017 is a sizable, comprehensive dataset useful for evaluating experiments on online malicious incidents. The data collection was initially created at the University of New Brunswick's Faculty of Computer Science. The dataset mimics the actual world of data (PCAP) by including current, benign, frequent crimes. Alongside the tagged flows determined by timestamps and IP source, it also contains the findings of the internet traffic assessment performed using CICFlowMeter [146].

NSL-KDD: The NSL-KDD dataset is a synthetic dataset that mimics the web traffic an actual attack detection system encounters, with only the signs of its presence remaining. This dataset also includes logs of the web traffic that a basic IDS detected. Each entry in the data collection has 43 attributes, 41 of which relate to the traffic entry itself. The final two features comprise tags indicating whether the input is benign or a malicious attempt, and they measure the importance of that input [147].

CAIDA DDoS Attack: The CAIDA DDoS Attack dataset comprises approximately an hour of concealed traffic traces from a DDoS attack on August 4, 2007. It has an overall length of 5.3 gigabytes and is divided into 5-minute PCPA files from the 1-hour trail. The trails only contain malicious traffic sent to the person who was attacked and that person's replies to the assault. As far as viable, benign traffic was eliminated. The payload content was removed from every packet, and the trails in this set of data have been disguised using CryptoPAn, a prefix-preserving anonymity scheme with a single encryption key [148].

Regarding the practical evaluation of traffic, the CIC-DDoS2019 dataset (2019) in Table 6 provides a precise simulation of the latest DDoS attack vectors, such as NTP, DNS, MSSQL, NetBIOS, SNMP, SYN, and TFTP floods, based on an isolated experiment. The CICIDS2017 dataset (2017)

Table 6 Comparative analysis of general network security datasets.

Year	Dataset	Attack Types	Source of Data	Reference
2019	CIC-DDoS2019	NTP, DNS, MSSQL, NetBIOS, SNMP, SYN, and TFTP	Network traffic from testbed simulating real-world scenario	[149]
2017	CICIDS2017	Brute Force, Heartbleed, Botnet, DoS, DDoS, and Web Attacks	Captured network traffic from simulated environment with 25 users	[150]
2009	NSL-KDD	DDoS, Probe, R2L, U2R	Captured from simulated environment	[151]
2007	CAIDA DDoS Attack	DDoS attack traffic	Captured network traffic from real-world DDoS attack	[152]

goes beyond DDoS and includes brute-force, Heartbleed, botnet, DoS, and web-based attacks, recorded in a simulated shared context to aid in the study of intrusion identification. The NSL-KDD dataset (2009) is a better version of the KDD Cup 99. It includes DDoS, Probe, R2L, and U2R attacks along with multiple mitigation methods. It provides a basic but out-of-date standard for predictive systems.

Among the quite rare openly accessible datasets of actual DDoS traffic are the CAIDA DDoS Attack dataset (2007), which provides concrete insights into the mechanics of massive botnet-driven attacks. As seen in Table 5, CICIDS2017 provides a comprehensive attack taxonomy; NSL-KDD remains an outdated standard; CAIDA offers vital insight into actual DDoS practices for long-term anomalous identification; and CIC-DDoS2019 focuses on modern DDoS studies.

5.1.3 Open resources for IoT security datasets

Kaggle: Kaggle is an online platform where the data science and machine learning communities come together. It provides a place where data scientists, analysts, and ML enthusiasts can work on real-world problems, share knowledge, and participate in competitions. Kaggle hosts one of the largest public repositories of datasets, which are crucial for training models and conducting research. Users can find data on almost every topic, including IoT network traffic [153].

IEEE DataPort: The ability to reproduce research is supported by IEEE DataPort, which also enables users to maintain, exchange, and access research datasets, including DDoS datasets and datasets from different researchers. By entering their IEEE login information or registering for a

free IEEE DataPort account, users can access publicly available datasets and submit their personal datasets for research [154].

Zenodo: Zenodo is a multipurpose research database created to make it easier for researchers across all fields of study to share, preserve, and disseminate their findings. Zenodo, introduced by CERN in 2013, provides academics and organizations with an easy-to-use platform for uploading and archiving a variety of intellectual materials, such as applications and datasets [155].

5.2 Common Evaluation Metrics for Detection and Mitigation Strategies

Accuracy: This is a common evaluation metric for assessing a classification model's effectiveness, providing a brief overview of its predictive accuracy. This is determined by dividing the total number of input items by the number of accurate predictions [156].

Precision: The metric used to evaluate a classification model's ability to identify the positive class. It can be calculated by dividing the total number of accurate predictions for the positive class by the total number of times the model has predicted it as positive [157].

Recall: the model's metric that measures how accurately it predicts positive instances. It is like answering the question: among the total number of positive examples, how many were predicted by the model? Recall will indicate how well the model predicts positive instances [158].

F1-Score: The F1-score is an evaluation metric for classification models based on a dataset and is primarily used for binary classification systems, which assign a given example to either positivity or negativity [159].

False Positive Rate: The false positive rate is the metric used to measure the instances in which the model mistakenly predicts negative data as positive, and it ranges from 0 to 1. If the false positive rate is low, it indicates that the model is good at handling instances; it produces few false attack alarms, whereas a high rate indicates that the model produces many false alarms [160].

False Negative Rate: The false negative rate is the metric that shows how many instances the model predicted as negative in the dataset were actually positive; it has the same range and concept as the false negative rate, but with a different instance type [161].

Receiver Operating Characteristic (ROC) Curve & AUC Score: A graphic depiction of how well the model performed over all criteria is the ROC

curve, which is simply drawn with the calculation of true positive and false positive rates in every possible criterion. It will then indicate the graph of the true positive rate over the false positive rate. The AUC Score indicates the likelihood that the model will assign greater prominence to the positive instance than to the negative when presented with a random selection of both [162].

5.3 Simulation Platforms and Tools for Real-World Testing

5.3.1 Network simulation tools (for IoT network testing)

NS-2 (Network Simulator 2): A freely available event-driven simulation tool designed specifically for computer communication system studies. This operates as a single-event simulator for network studies and provides significant support for simulating multiple protocols, including TCP, FTP, UDP, HTTPS, and DSR. C++ and Object-oriented Tool Command Language (OTcl) are two of its main programming languages, and the system is largely based on Unix and supports both wired and wireless networks [163].

NS-3 (Network Simulator 3): A freely available network modeling platform that prioritizes realism over NS-2, which was built to compensate for NS-2's limitations. This platform includes various useful features and resources for scalability and cross-layer interoperability, which facilitate the ease of reading and parsing packet capture (PCPA) files [164].

OMNET++: Instead of offering simulation items for networks of computers, queueing theory, and several fields, the Objective Modular Network Testbed in C++ (OMNeT++) serves as an object-oriented dynamic simulation platform for testing protocols for communicating and various systems that are distributed. It utilizes a structure and stance that provide basic resources and equipment for creating models. In addition to supporting large-scale simulations and visualization tools that facilitate debugging and result interpretation, OMNeT++ allows researchers to build customized models tailored to a particular investigation [165].

Mininet: Mininet is used to prototype large networks using process-level virtualization, a simpler form of virtualization in which computer resources are distributed at the OS level. Mininet's original purpose was to enable users to quickly prototype large networks with limited resources. Mininet network topologies can be constructed in Python and deployed in a matter of seconds. Additionally, this capability makes it easier to share topologies among different researchers, who may then modify these to suit their own research requirements [166].

5.3.2 IoT-specific simulator (IoT device behavior and security)

Cooja: It was developed in Java and allows individuals to designate either large or small Contiki motes (sensor network nodes) for the network's deployment. Users can obtain important network data, including timeframes and mote outputs, upon completing the simulation. It is important to note that the template settings define motes in a particular way. The simulated situations focus more on network and hardware problems instead of on IoT instances or publish-subscribe relationships [167].

CupCarbon: It is compatible with automated execution of repetitive tasks and distributed algorithms for industrial applications. Educators may utilize this to illustrate important procedures and the workings of smart sensor systems. The researcher will also be able to evaluate its wireless structure, connectivity, protocols, operation, and other aspects with its assistance [168, 169].

5.3.3 Cloud-based testing environments (real-world IoT security testing)

AWS IoT Device Simulator: Through an easy-to-use graphical user interface (GUI), the Amazon Web Services IoT Device Simulator platform helps clients test, integrate devices, and enhance the functionality of their IoT backend applications. Eliminating the need for laborious script writing or the configuration and management of physical devices, this method enables the creation and simulation of numerous connected devices [170].

Google Cloud IoT Core: For managing IoT devices, it is a fully managed platform. Along with cloud-stored device metadata and the ability to transmit configuration information to devices from other GCP or external sources, it facilitates registration, authentication, and authorization [171].

5.3.4 Cybersecurity and attack simulation tools (testing DDoS scenarios)

Hping3: Hping3 is used by hackers to send packets to the target. Such packets have been created and faked and, when customized, they are exceedingly helpful to the attacker and powerful enough to be used for the purposes listed below: Path MTU identification and Firewalking. Utilizing various protocols, packet sizes, TOS (a type of service), and fragmentation, advanced port scanning, and Net Tests performance [172].

Metasploit: The Metasploit Framework is a tool for developing and exploiting vulnerabilities targeting specific devices. Fundamentally, this is a compilation of identified weaknesses and payloads designed to assist testers

in penetration testing and system testing, and to maintain a current database of potential attacks. The framework allows the individual who uses it to personally define particular goals and settings when conducting a strike and provides an outline based on recognized vulnerabilities [173].

5.3.5 AI/ML model testing framework (anomaly detection in IoT traffic)

TensorFlow: Another popular ML framework, created by Google and currently free, with Java and Python wrappers. Python was one of TensorFlow's recognized programming languages and is the language of choice for data science and ML. Interestingly, at the moment, TensorFlow is the sole ML library that adapts its manual to the user's degree of expertise [174].

PyTorch: Due to its ease of building and training neural networks, PyTorch has emerged as a widely used framework in academia. Its commercial population is also becoming increasingly prominent. It was created by Meta in 2016 and, since then, it has undergone numerous enhancements from both Meta and the sizable community that has grown around PyTorch [175].

Scikit-learn: a well-known Python ML library. Numerous NTA methods, including SVMs, decision trees, and random forests, are included in Scikit-learn. The particular objective and its application can influence which frameworks and algorithms are employed [176].

5.3.6 Real-world IoT security testbeds (for experimental validation)

FIT IoT-Lab: This testbed is a public IoT research facility. Across six locations in France, it offers over 2700 nodes. This provides complete ownership of 23 distinct IoT boards and a means to reserve several nodes for an investigation via the central REST API that runs the lab. For every accessible node, it employs a specially made hardware gateway to flash and configure it. The purpose of this gateway is to continuously monitor the Received Signal Strength Indicator (RSSI) power indicator, radio operation, and energy usage [177].

SmartSantander Testbed: Because of its expansive, accessible, and adaptable form, SmartSantander structure can federate alongside other research facilities both vertically and horizontally. It is meant to encourage the creation of new apps by a range of users, including those conducting realistic user acceptance testing and exploratory, sophisticated studies on IoT technology. Using a wide range of technologies, the initiative intends to install 20,000 sensors in the cities of Belgrade, Guildford, Lubeck, and Santander [178].

6 Challenges in IoT DDoS Detection and Mitigation

The environment in which IoT devices operate is now observable, expanding rapidly and, with many devices now connected, the potential for DDoS attacks is rising. However, they are unique in their inherent nature. Challenges with these devices can be classified into several areas, including scalability, real-time detection, data privacy, and more. In this section, we will discuss the challenges of implementing security measures against DDoS attacks, which most researchers encounter, and propose a solution to address this problem.

6.1 Scalability and Resource Constraints in IoT Devices

In the case of IoT devices, they usually execute their tasks in resource-constrained environments, indicating that, during operation, they have limitations in computational power, memory, and bandwidth [179]. These limitations have posed challenges, especially in detecting and mitigating DDoS attacks.

Device Limitations: Many IoT devices, particularly low-cost sensors and resource-constrained edge devices, lack the computational capabilities required to perform effective real-time detection of DDoS attacks [180], making the implementation of a robust security system difficult, which includes traffic filtering, anomaly detection, and behavior analysis.

Large-Scale Networks: The rapid development and adoption of IoT devices across diverse fields have enabled the formation of large-scale networks comprising millions of interconnected devices [181]. Considering this, detection and mitigation in large-scale IoT network environments can be expensive in terms of computational power and complexity [182]. The use of network monitoring tools can make it difficult to identify malicious activity across many devices [183].

Data Overload: With many interconnected devices generating data, the volume will overwhelm current defenses against cyberattacks, leading to high false-positive rates and significant delays in detecting attacks [184]. Because of this, the security system's ability to scale its traffic analysis, filter noise, and isolate suspicious network activity will become more critical.

Network Bandwidth: IoT devices usually operate over low-bandwidth networks, which can be exploited by DDoS attackers, leading to poor service performance or network congestion [185]. A strong defense mechanism against this should consider bandwidth limits, especially in areas where accessibility and reliability are critical, such as smart cities, healthcare, or industrial IoT [186].

Decentralized Nature: Implementing a robust security mechanism against DDoS attacks is challenging given the system's decentralized architecture [187]. Because IoT networks are decentralized, implementing robust safety measures against DDoS attacks may be more difficult [154]. Because of this, a coordinated defense mechanism will face challenges, as different IoT devices may have different configurations, making it impossible to identify and mitigate them uniformly [188, 189].

6.1.1 Real-world IoT security testbeds (for experimental validation)

FIT IoT-Lab: This testbed is a public IoT research facility. Across six locations in France, it offers over 2700 nodes. This provides complete ownership of 23 distinct IoT boards and a means to reserve several nodes for an investigation via the central REST API that runs the lab. For every accessible node, it employs a specially made hardware gateway to flash and configure it. The purpose of this gateway is to continuously monitor the RSSI power indicator, radio operation, and energy usage [177].

SmartSantander Testbed: Because of its expansive, accessible, and adaptable form, SmartSantander structure can federate alongside other research facilities both vertically and horizontally. It is meant to encourage the creation of new apps by a range of users, including those conducting realistic user acceptance testing and exploratory, sophisticated studies on IoT technology. Using a wide range of technologies, the initiative intends to install 20,000 sensors in the cities of Belgrade, Guildford, Lubeck, and Santander [178].

Many solutions have been proposed to address resource constraints and sustainability issues in IoT devices while maintaining sufficient security, as shown in Table 7. To mitigate hardware limitations, an effective Convolutional Neural Network (CNN) based intrusion detection system was proposed. Its 99.75% accuracy and lower computational demands make it well-suited for implementation across different connected devices, though additional research is needed to assess its timeliness of detection. However, its use of advanced neural networks can lead to high computational requirements, especially in resource-limited environments. An F1-score of 81% was achieved for detecting hidden DDoS attacks in large-scale IoT networks using a correlation-aware neural network. Despite variations in efficiency based on attack techniques, a lightweight time-based ML system that addressed excessive data and computational limitations achieved over 99.7% accuracy across most classification algorithms, successfully optimizing computational

Table 7 Comparative analysis of existing papers that tackle the scalability and resource constraints of IoT devices with their solutions

Challenge Studied	Proposed Solution	Computational Overhead	Scalability	Limitations	Ref
Device Limitations and Resource-constrained devices	Lightweight CNN-Based IDS	Reduced the complexity through fewer layers	Can operate on different IoT devices	The ability to perform real-time detection needs to be validated	[190]
	Distributed architecture-based solutions, Access management-based solutions, Traffic control-based solutions, Ethereum platform-based solutions	Computational overhead is a challenge due to limited resources	The introduction of blockchain on resource-constrained devices offers performance scalability	Resource constraints, Scalability, Latency, Complexity, Lack of unified solution	[191]
	Edge2Guard as a standalone and lightweight intrusion detection system	Specifically designed for low resource constraints devices	Device level independence, No network bottlenecks	Scope of detection, Model deployment scalability, Storage constraints, No network level defense	[192]
	Lightweight Intrusion Detection System	Designed to be lightweight, making it suitable for resource-constrained IoT devices	Adaptability across various network conditions, Training phase may require more computational resources	Imbalanced data, Generalizability, Resource constraints, Binary classification focus	[193]
	Optimally Placed, Transparent, Distributed IDS	Minimize at runtime due to offline training and optimal placement	High scalability due to distributed IDS design, transparent and optimal placement, and modular LSTM placement	Training complexity, No real-time adaptation, Lack of interpretability	[194]
Sophisticated DDoS attacks in large-scale IoT networks	Correlation-aware Neural Network	May require computational resources due to the utilization of advanced neural network	Depends on the deployment environment	Computational requirements may become a hurdle in resource constrained device	[195]
	Development of synthetic attack generator, Multi-label feed forward neural network to detect attack nodes	Low to moderate due to the utilization of simple feed-forward neural network, Suitable for centralized or cloud-based processing	High scalability potential, Design enables training models for large networks	No real attack data, Limited model complexity, Limited feature discussion	[196]

(Continued)

Table 7 Continued

Challenge Studied	Proposed Solution	Computational Overhead	Scalability	Limitations	Ref
	Creation of comprehensive IoT attack dataset which is intended to support the development and evaluation of IDS	Not applicable, The created dataset has the ability to support lightweight and complex models	Good scalability shown through the involvement of 105 devices and 33 types of attacks	No detection method, Fixed environment, Unknown diversity of IoT device, Static scenario	[197]
	Optimized Multiclass Intrusion Classifier	Efficient due to memory-optimized pipeline and chunk-based data handling, Offers substantial gains in processing efficiency	Can be deployed in real-world, large-scale IoT networks with the help of modular and memory-efficient architecture	Reduced accuracy on certain attack types, Framework complexity	[198]
	Federated Learning-based IDS	Avoids cloud centralization, Reduce inter device network traffic	High scalability as architecture can support large distributed environments, can be deployed across edge-to-cloud hierarchies	Complexity of federated architecture, Unsupervised detection tradeoffs, Security of FL	[199]
Data Overload and resource-constrained IoT device	ML lightweight time-driven framework	It can minimize the computational load in IoT devices	Suitable for large-scale IoT deployment	The efficiency may be based on the attack patterns	[200]
	Hybrid IDS combining Support Vector Machine, Convolutional Neural Network, and Gated Recurrent Unit	Lower prediction time compared to existing methods	Implicitly scalable as it is trained with large-scale network data, Can handle increased network traffic	Trained on a single dataset, Limited generalizability	[201]
	Power Management System	Scalable for smart homes	Only addresses energy-based attacks, Attack sophistication		[202]
	EffiGRU-GhostNet	Low resource consumption due to lightweight Ghostnet and dimensionality reduction with PCA-LLP, Designed for efficient operation in big data environments	Validated on multiple large-scale datasets, Suitable for real-time detection	Operational deployment	[203]

(Continued)

Table 7 Continued

Challenge Studied	Proposed Solution	Computational Overhead	Scalability	Limitations	Ref
Securing against unauthorized access and tampering of data	Blockchain-based security strategy	Utilizing efficient smart contract to minimize the computational load	It will depend on the deployment environment	Challenges may be faced depending on the IoT infrastructure	[204]
	Arbiter PUF-based Lightweight Security, Permission blockchain integration	Designed with lightweight cryptography, Lower overhead, Moderate computational cost	Collaborative and decentralized nature, Improved efficiency compared to public chains	Blockchain latency and storage overhead, PUF technology may introduce variability and error rates	[205]
	A hybrid AI-Blockchain security framework	Mentioned as a known challenge	Computational demands, Scalability concerns, Integration complexity, Interoperability		[206]
	IDS in IoT networks	IDS introduced a slight overhead	IDS must adapt to high device density and heterogeneous networks	Vague IDS implementation	[207]
	Chain of Things	High computational and energy cost	Utilizing smart contracts, Suitable for small to medium scale deployments	Consensus overhead, Smart contract risks, Storage bloat	[208]

costs while enabling massive IoT deployments. Furthermore, a lightweight security method based on host-based, off-device learning was 100% accurate and easy to deploy, requiring minimal resources. Despite its viability in the IoT network, a security approach based on Blockchain that uses effective smart contracts to minimize computational overhead achieved 95% detection in protecting IoT devices against malicious access and data manipulation. There are trade-offs among computational efficiency, installation feasibility, and attack resistance in constrained environments, while each method supports IoT security and scalability.

6.2 Real-Time Detection

The constantly changing, difficult-to-predict nature of DDoS techniques has highlighted the importance of developing real-time detection and adaptive response defense mechanisms. However, there are a number of factors that make this difficult to implement to effectively detect and mitigate DDoS attacks in real-time IoT networks, and these are the following:

Latency and Delay: Enabling real-time detection and mitigation of DDoS attacks requires low-latency systems to effectively identify malicious activity and enable rapid responses [209]. However, IoT devices often operate in environments where data transmission is delayed by long distances, slow data rates, or limited bandwidth, resulting in slower performance in identifying and responding to attacks.

Complex Attack Patterns: DDoS attacks may employ highly advanced, multi-vector strategies that evolve dynamically. As IoT environments contain various types of devices and protocols, detecting complex real-time attack patterns can be very difficult [210]. Many conventional defense mechanisms for detecting DDoS attacks, including signature-based security systems, don't handle the dynamically evolving attack techniques of DDoS attackers [211].

Detection vs Response Speed: Even if we assume the DDoS attack was detected in real time, the response could still not be fast enough to prevent the damage it can cause. This is because, to effectively mitigate an attack, the cooperation of multiple network elements, such as firewalls or gateways, and delays in network communication among them can render defense mechanisms against DDoS attacks ineffective [212].

Static Mitigation Strategies: The effective mitigation of DDoS attacks requires the ability to adapt to emerging threats, which in IoT environments can be difficult to implement an adaptive defense mechanism that can autonomously change in response to dynamic attack vectors. A static mitigation strategy is insufficient for handling new DDoS attack techniques, underscoring the need for a security system that can learn from incoming traffic patterns and adapt accordingly [213].

Resource Allocation: Implementing real-time detection and mitigation of DDoS attacks requires adequate resources, including memory and computational power. As many IoT devices operate in resource-constrained environments, they may struggle to handle these heavy processing requirements, posing challenges for implementing effective DDoS detection systems [214].

Table 8 presents a comparative analysis of state-of-the-art approaches to real-time, challenging problems in IoT environments, with special emphasis on resource efficiency and DDoS mitigation. Supported by a Temporal Convolutional Network (TCN)-based framework enhanced with frequency-domain monitoring and adaptive thresholding, the latency-constrained and computation-limited Healthcare IoT (H-IoT) system has been provided with a solution that achieves 99.99% accuracy on UDP traffic. However, the limited network topology and differences in attack strategies can still pose challenges. In the case of IoT data with complex multidimensional features

Table 8 Comparative analysis of existing studies tackling real-time challenges

Challenge Studied	Proposed Solution	Result	Contribution	Limitation	References
Low Latency Requirement of H-IoT, Limited Computational Resources of IoT	TCN-based model, Frequency Monitoring, Dynamic Thresholding	99.8% Message Queuing Telemetry Transport (MQTT), 99.99% (UDP)	Address DDoS attacks detection in 5G Healthcare IoT	Network configuration, attack pattern diversity	[215]
Complexity of Multi-Dimensional IoT Network Data	RNN + Autoencoders	98.98% Accuracy	Introduces novel mechanism in Detecting DDoS attacks	Need high quality training data, may not be suitable for resource constrained IoT devices	[216]
Limited Processing Power of IoT devices	SCN-based model	99.29% Accuracy	Introduces solution for DDoS detection of resource limited IoT devices	Depends on dataset quality, real-time deployment	[217]
Network congestion and resource allocation	Mixed Integer non-linear programming	Efficient resource allocation even with limited signal	Provided a reliable resource allocation in Internet of Battlefield Things (IoBT)	Environmental noise, hardware variations	[218]
Real-Time analysis and scalability	CNN+BiLSTM with Attention Mechanism	99.32% accuracy	Offered an efficient DDoS attack detection and mitigation in IoT	Computational overhead	[219]

and limited resource constraints, a hybrid RNN-Autoencoder model achieved an excellent accuracy of 98.98%. Table 8 clearly illustrates the trade-off between computational complexity and detection effectiveness across different dynamic IoT threat scenarios.

7 Privacy and Ethical Issues in IoT Security

One of the primary concerns in IoT systems is security. Because of this, an effective way to address these ethical issues has become increasingly important, especially for detecting and mitigating DDoS attacks. In this regard, the following are some privacy and ethical concerns that can be identified.

Data Privacy: Data privacy is a common issue. An IoT device executes an operation that gathers a large amount of data, including personal or sensitive

information such as location, health metrics, and environmental data [220]. The failure to monitor network traffic from IoT devices in a timely manner can silently violate the user's privacy rights, as it may involve the collection of sensitive data without the user's consent [221]. This highlights the importance of balancing the development of security systems to monitor network traffic for suspicious activity and to implement data privacy measures.

Surveillance and Consent: There are a few DDoS detection mechanisms, including deep packet inspection to analyze the content generated by communication among IoT devices [222], which heightens concerns about monitoring user behavior. This can be highly performed in smart homes or H-IoT environments. To inform users that their data is being used, transparent consent is needed to provide assurance [223].

Personal Data in DDoS Mitigation: In mitigation, many IoT networks involve identifying the source of suspicious network traffic and blocking it or separating it from specific devices [224]. This action may lead to the unplanned exposure of the user's personal data if the wrong devices are ever targeted. An effective mitigation technique for DDoS attacks should not unintentionally compromise user privacy [225].

Ethical Implications of Attack Attribution: Identifying the source of a malicious network in a DDoS attack can be difficult. In some cases, attackers may improperly use compromised IoT devices to turn them into bots [226]. Misattribution may lead to legitimate users being denied access to important services due to a mistake in treating them as malicious users, raising ethical challenges when attackers can successfully use IoT networks to disguise themselves and penetrate the network undetected [227].

Data Collection and Retention Policies: To make the DDoS security system more efficient, it should be trained on data patterns related to DDoS, attack signatures, and device behavior, in accordance with data privacy laws [228]. However, collecting that data may pose risks to user privacy if proper data retention policies are not in place. Implementing security systems that process minimal data is important, as this helps ensure that collected data is anonymized and encrypted to prevent unauthorized access [229].

Regulation and Legal Framework: IoT devices are influenced by a complex regulatory landscape, with various regions and countries implementing different data privacy laws. The implementation of robust security mechanisms against sophisticated cyberattacks, together with compliance with these regulatory laws, has become a challenge for researchers and developers in the cybersecurity field [230].

8 Development Lifecycle of IoT DDoS Security Systems

In developing an effective and robust security system for IoT DDoS attack detection, developers implement common phases that are important throughout the development lifecycle (Figure 8). Successful implementation of these steps helps ensure that detection, mitigation, and prevention are both reliable and scalable. These phases include several stages, starting with identifying the problem and ending with continuous monitoring of the model for improvement. Each phase of the development process is vital, as it influences how the model will perform.

Problem Identification & Analysis: The primary phase in the life cycle is the identification and analysis of the problem. This phase includes the careful understanding of what the unique vulnerabilities of IoT networks are, which include the things that we mentioned earlier, like the resource constraints, large attack surfaces, and the heterogeneity of IoT devices [231]. Researchers developing effective mitigation strategies in this field have carefully examined past DDoS events to identify attack vectors, including botnets, amplification, and protocol exploitation [232]. By studying real-world cases of DDoS attacks, researchers can identify the most common patterns and craft effective security requirements formulations. By clearly defining the problem scope, it will ensure that the following sequences proceed smoothly and that the focus remains on addressing the most vital challenges in IoT security.

System Design & Framework Development: After the successful identification and definition of the problem, the following phase would be the design and development of the framework. In this phase, defining the framework that would be utilized is involved [233]. One of the main focuses of this phase should be designing a scalable framework that can handle a large amount of network traffic while minimizing latency and computational overhead [234].

Data Collection & Dataset Creation: After the system design has been successfully implemented, the next step is to gather data and create a dataset, which is essential to developing an effective security solution. These datasets serve as the ML models' training ground; obtaining a large, high-quality dataset is essential for practical applications that require dependable predictions. The datasets can be collected from real-world IoT networks, simulated environments, and publicly available datasets [235]. One criterion for selecting it is that it must contain a diverse range of normal and attack network traffic to effectively improve the model's detection accuracy [236].

Technique Selection and Algorithm Development: With a carefully developed dataset, it can be used in the next phase, which is selecting a technique

and developing the algorithm. Usually, researchers examine various methods to be implemented, such as signature-based [237], anomaly-based [238], and hybrid methods that combine multiple techniques [239]. The use of ML and DL algorithms is growing, leveraging classifiers such as Support Vector Machine (SVM) [240], CNN [241], and Long Short-Term Memory (LSTM) [241].

Model Training and Evaluation: The model training analysis will come next. The preprocessed data will be used to properly train the ML and DL models, and they will be adjusted to further improve their performance. Most users employ cross-validation techniques to ensure the model generalizes well to unseen attack scenarios [242]. After identifying the model's performance. Benchmarking against existing security systems can also be used to assess the effectiveness of the developed security system.

Testing and Validation in Real-World Environments: Once the model is evaluated and delivers excellent results, it will be tested and validated in real-world environments. This can be done by deploying the developed security system in a simulated IoT environment to effectively evaluate its performance under realistic conditions [243]. This phase will include stressing the model through various attack scenarios, evaluating its false-positive and false-negative rates, and optimizing its detection parameters [244].

Deployment and Integration into IoT Networks: After successful validation, the system will be ready for deployment and integration into IoT networks [245]. In this phase, IoT devices will be embedded with the security mechanisms. The integration should have no flaws to ensure it is well compatible with the IoT network's existing architecture [246]. Most of the time, autonomous responses to cyber threats automatically trigger mitigation strategies when DDoS attacks occur, such as rate limiting or blacklisting.

Continuous Monitoring and Improvement: Even with a successful deployment of the security system, continuous monitoring and improvement should still be required [247]. One of the factors that led to this being implemented is the continuous evolution of cyber-attacks, which utilize various attack techniques; to cope with these techniques, this needs to be applied.

9 Real Life Use Case and Application

The continuous integration of IoT devices across different fields has greatly helped in automating manual tasks. However, this rapid integration has also

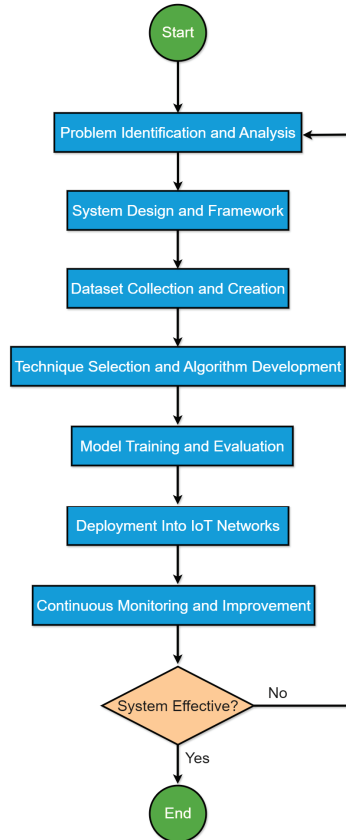


Figure 8 Development lifecycle of DDoS detection in IoT.

posed novel security challenges, especially in the context of DDoS attacks. In this section, we will explore real-world use cases where IoT is being applied and where IoT security is particularly critical.

9.1 DDoS in Smart Homes

In smart homes, various IoT devices are integrated, including CCTV, smart thermostats, and connected appliances, thereby greatly enhancing user convenience [248]. However, these devices are often vulnerable to cyber threats due to weak authentication mechanisms, outdated firmware, and limited security protocols, leading to issues when targeted by DDoS attacks, including malfunctioning devices, DoS attacks, and unauthorized user access [249].

One of the most well-known examples is the Mirai botnet, which penetrates vulnerable IoT devices and commences large-scale DDoS attacks. IoT devices in smart homes with weak credentials have been hijacked and used to generate a flood of network traffic, disrupting both home users and external services [250]. Smart home security solutions may use behavior-based anomaly detection or network segmentation to separate infected IoT devices from the main network, thereby preventing them from becoming victims of those attacks.

9.2 Industrial IoT (IIoT)

IIoT has been making a huge impact across sectors, including manufacturing, energy, and logistics, by enabling real-time monitoring and autonomous production. This network includes sensors, actuators, robotics, and an industrial control system (ICS) that must be reliable and available [251]. An instance of a successful DDoS attack in IIoT infrastructure may result in the cessation of operation, damage to equipment, and financial losses [252].

One of the famous attacks we can cite is the one targeting an energy grid, which disrupted communication among control systems and stationary power [253]. This attack has highlighted weaknesses in the IIoT environment, which can cause widespread disruption and serious consequences. Effective approaches to solving this problem include implementing IDS and AI-driven anomaly detection, which can detect and block malicious network traffic before it penetrates the network and causes damage [254].

9.3 Securing IoT in Healthcare Systems

The healthcare industry has also leveraged the emergence of IoT technology to improve patient care and streamline hospital operations. Heart monitors and connected medical imaging equipment are among the IoT devices they use, and they mostly rely on network connectivity to function effectively [255]. However, these devices also become a feasible target for cybercriminals aiming to disrupt healthcare services through DDoS attacks.

In 2020, a major DDoS attack targeted healthcare providers' IoT networks. This attack disrupted connected medical devices and monitoring systems, causing delays in important patient treatments [256]. Given that the patient's life is at stake, robust security in H-IoT systems is needed. This could be a combination of network segmentation and real-time monitoring. Currently, medical institutions are adopting zero-trust security to ensure that only authorized devices and users can access the network [257].

10 Conclusion

The need for sophisticated, adaptive, and resource-aware protection mechanisms is emphasized by the rising occurrence and scale of DDoS attacks in IoT networks. In order to outline the evolving attack vector profile and mitigation solutions, this survey has thoroughly examined the taxonomy of IoT-specific DDoS threats, reviewed detection techniques being employed, and reviewed preventative measures and mechanisms. This paper presents an integrative view of new and current security concepts by examining blockchain-based resilient mechanisms, FL architecture, ML based anomaly detection, and quantum-secured cryptography.

The survey's primary findings include the underlying security effectiveness and the computational overhead trade-off in resource-limited IoT environments. Computationally lightweight, conventional rule-based, and threshold-based detection mechanisms are not suitably adaptive to counter adversarial AI-driven DDoS attacks and zero-day exploits effectively. On the other hand, while DL-based detection models significantly enhance accuracy, they also require high computational resources, making them not directly applicable to large-scale IoT deployments without distributed intelligence or edge computing optimization. In addition, the rise of malicious AI requires robust, in-depth defense mechanisms that include real-time behavior analytics, federated anomaly detection, and threat intelligence sharing.

Another important aspect to consider is the growing convergence of decentralized, trustless frameworks such as blockchain and QC with IoT security. While blockchain-based DDoS protection ensures decentralized, tamper-evident traffic filtering, scalability and latency overhead issues are significant challenges. Similarly, while quantum computing is promising for post-quantum cryptographic security, its incorporation into IoT security mechanisms in practice is still in development. Quantum-enhanced anomaly detection models, lightweight cryptographic methods, and self-learning AI-based intrusion prevention systems should be the primary targets of future development.

Finally, given the security posture of IoT-based systems, the survey outcomes call for a transition away from conventional cybersecurity principles. To defend IoT networks from the emerging DDoS threat profile, cross-domain intelligence fusion, adaptive security design, and self-healing threat management will be required. The protection of networked systems of the future needs a diversified, possessive, and adaptive protection strategy. This is because the cyberattacks conducted today use AI and evasion techniques.

Acknowledgment

This research work is supported by National Science and Technology Council (NSTC), Taiwan Grant No. NSTC114-2221-E-468-015. Also, Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2026R343), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

References

- [1] J. M. Fernández-Batanero, M. Montenegro-Rueda, J. Fernández-Cerero, E. López Meneses, Adoption of the Internet of Things in higher education: opportunities and challenges, *Interactive Technology and Smart Education* 21 (2) (2024) 292–307. doi:10.1108/ITSE-01-2023-0025.
- [2] P. Chaudhary, A. K. Singh, B. B. Gupta, Dynamic multiphase DDoS attack identification and mitigation framework to secure SDN-based fog-empowered consumer IoT networks, *Computers and Electrical Engineering* 123 (2025) 110226. doi:10.1016/j.compeleceng.2025.110226.
- [3] B. Gupta, P. Chaudhary, X. Chang, N. Nadjah, Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers, *Computers & Electrical Engineering* 98 (2022) 107726. doi:10.1016/j.compeleceng.2022.107726.
- [4] A. Gaurav, B. B. Gupta, W. Alhalabi, A. Visvizi, Y. Asiri, A comprehensive survey on DDoS attacks on various intelligent systems and its defense techniques, *International Journal of Intelligent Systems* 37 (12) (2022) 11407–11431. doi:10.1002/int.23048DigitalObject Identifier(DOI).
- [5] M. Anupama, N. Gupta, B. Gupta, Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller, *Telecommunication systems* 77 (1) (2021) 47–62. doi:10.1007/s11235-020-00747-w.
- [6] M. Snehi, A. Bhandari, Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks, *Computer Science Review* 40 (2021) 100371. doi:10.1016/j.cosrev.2021.100371.
- [7] Y. Al-Hadhrani, F. K. Hussain, DDoS attacks in IoT networks: a comprehensive systematic literature review, *World Wide Web* 24 (3) (2021) 971–1001. doi:10.1007/s11280-020-00855-2.

- [8] H. C. Lau, G. T. Ho, K. Chu, W. Ho, C. K. Lee, Development of an intelligent quality management system using fuzzy association rules, *Expert Systems with Applications* 36 (2) (2009) 1801–1815. doi:10.1016/j.eswa.2007.12.066.
- [9] G. T. Ho, V. Tang, An Intelligent Decision Support Model for Sustainable Automated E-fulfillment Centers Through Fuzzy Association Rules Mining, in: 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), IEEE, 2024, pp. 1397–1401. doi:10.1109/IEEM62345.2024.10857246.
- [10] R. Maciel, J. Araujo, C. Melo, P. Pereira, J. Dantas, J. Mendonça, P. Maciel, Impact evaluation of DDoS attacks using IoT devices, in: 2021 IEEE International Systems Conference (SysCon), IEEE, 2021, pp. 1–8. doi:10.1109/SysCon48628.2021.9447145.
- [11] G. Kambourakis, C. Kolias, A. Stavrou, The mirai botnet and the iot zombie armies, in: MILCOM 2017-2017 IEEE military communications conference (MILCOM), IEEE, 2017, pp. 267–272. doi:10.1109/MILCOM.2017.8170867.
- [12] A. Pakmehr, A. Aßmuth, N. Taheri, A. Ghaffari, DDoS attack detection techniques in IoT networks: a survey, *Cluster Computing* 27 (10) (2024) 14637–14668. doi:10.1007/s10586-024-04662-6.
- [13] S. Chaudhary, P. K. Mishra, DDoS attacks in Industrial IoT: A survey, *Computer Networks* 236 (2023) 110015. doi:10.1016/j.comnet.2023.110015.
- [14] Q. Li, H. Huang, R. Li, J. Lv, Z. Yuan, L. Ma, Y. Han, Y. Jiang, A comprehensive survey on DDoS defense systems: New trends and challenges, *Computer Networks* 233 (2023) 109895. doi:10.1016/j.comnet.2023.109895.
- [15] A. A. Alahmadi, M. Aljabri, F. Alhaidari, D. J. Alharthi, G. E. Rayani, L. A. Marghalani, O. B. Alotaibi, S. A. Bajandouh, DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions, *Electronics* 12 (14) (2023) 3103. doi:10.3390/electronics12143103.
- [16] Z. A. Khan, A. S. Namin, A survey of DDoS attack detection techniques for IoT systems using Blockchain technology, *Electronics* 11 (23) (2022) 3892. doi:10.3390/electronics11233892.
- [17] K. Murakami, T. Kasama, D. Inoue, A large-scale investigation into the possibility of malware infection of IoT devices with weak credentials, *IEICE TRANSACTIONS on Information and Systems* 106 (9) (2023) 1316–1325. doi:10.1587/transinf.2022ICT0001.

- [18] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, R. Ande, IoT standardisation: Challenges, perspectives and solution, in: Proceedings of the 2nd international conference on future networks and distributed systems, 2018, pp. 1–9. doi:10.1145/3231053.3231103.
- [19] A. Imteaj, U. Thakker, S. Wang, J. Li, M. H. Amini, A survey on federated learning for resource-constrained IoT devices, *IEEE Internet of Things Journal* 9 (1) (2021) 1–24. doi:10.1109/JIOT.2021.3095077.
- [20] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, Y. Liu, The impact of dos attacks on resource-constrained iot devices: A study on the mirai attack, *arXiv preprint arXiv:2104.09041* (2021). doi:10.48550/arXiv.2104.09041.
- [21] M. Aboubakar, M. Kellil, P. Roux, A review of IoT network management: Current status and perspectives, *Journal of King Saud University-Computer and Information Sciences* 34 (7) (2022) 4163–4176. doi:10.1016/j.jksuci.2021.03.006.
- [22] S. Liebl, L. Lathrop, U. Raithel, A. Aßmuth, I. Ferguson, M. Söllner, Analyzing the attack surface and threats of industrial Internet of Things devices, *arXiv preprint arXiv:2405.16318* (2024). doi:10.48550/arXiv.2405.16318.
- [23] S. Datta, A. Bhattacharya, R. Rana, U. Venkanna, idam: A distributed mud framework for mitigation of volumetric attacks in IoT networks, in: 2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), IEEE, 2022, pp. 326–331. doi:10.1109/CSNDSP54353.2022.9908058.
- [24] J. Shroff, R. Walambe, S. K. Singh, K. Kotecha, Enhanced security against volumetric DDoS attacks using adversarial machine learning, *Wireless Communications and Mobile Computing* 2022 (1) (2022) 5757164. doi:10.1155/2022/5757164.
- [25] A. Ghosh, A. Pahade, R. Malviya, Adversarial Machine Learning Challenges in Modern Network Security Systems, in: 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG), IEEE, 2023, pp. 1–6. doi:10.1109/ICTBIG59752.2023.10456181.
- [26] N. Z. Bawany, J. A. Shamsi, K. Salah, DDoS attack detection and mitigation using SDN: methods, practices, and solutions, *Arabian Journal for Science and Engineering* 42 (2) (2017) 425–441. doi:10.1007/s13369-017-2414-5.
- [27] Z.-Y. Shen, M.-W. Su, Y.-Z. Cai, M.-H. Tasi, Mitigating SYN Flooding and UDP Flooding in P4-based SDN, in: 2021 22nd Asia-Pacific

- Network Operations and Management Symposium (APNOMS), IEEE, 2021, pp. 374–377. doi:10.23919/APNOMS52696.2021.9562660.
- [28] D. Stiawan, M. E. Suryani, M. Y. Idris, M. N. Aldalaien, N. Alsharif, R. Budiarto, et al., Ping flood attack pattern recognition using a K-means algorithm in an Internet of Things (IoT) network, *IEEE Access* 9 (2021) 116475–116484. doi:10.1109/ACCESS.2021.3105517.
- [29] S. Adiwal, B. Rajendran, S. D. Sudarsan, et al., Dns intrusion detection (did)—a snort-based solution to detect dns amplification and dns tunneling attacks, *Franklin Open* 2 (2023) 100010. doi:10.1016/j.fraope.2023.100010.
- [30] A. A. Alahmadi, M. Aljabri, F. Alhaidari, D. J. Alharthi, G. E. Rayani, L. A. Marghalani, O. B. Alotaibi, S. A. Bajandouh, DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions, *Electronics* 12 (14) (2023) 3103. doi:10.3390/electronics12143103.
- [31] M. Dimolianis, A. Pavlidis, V. Maglaris, SYN flood attack detection and mitigation using machine learning traffic classification and programmable data plane filtering, in: 2021 24th conference on innovation in clouds, internet and networks and workshops (ICIN), IEEE, 2021, pp. 126–133. doi:10.1109/ICIN51074.2021.9385540.
- [32] D. Tymoshchuk, O. Yasniy, M. Mytnyk, N. Zagorodna, V. Tymoshchuk, Detection and classification of DDoS flooding attacks by machine learning method, *arXiv preprint arXiv:2412.18990* (2024). doi:10.48550/arXiv.2412.18990.
- [33] T. R. Sree, S. M. S. Bhanu, HADM: detection of HTTP GET flooding attacks by using Analytical hierarchical process and Dempster–Shafer theory with MapReduce, *Security and Communication Networks* 9 (17) (2016) 4341–4357. doi:10.1002/sec.1611.
- [34] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, N. Bizon, State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions, *Sustainability* 13 (16) (2021) 9463. doi:10.3390/su13169463.
- [35] M. M. Ahemd, M. A. Shah, A. Wahid, IoT security: A layered approach for attacks & defenses, in: 2017 international conference on Communication Technologies (ComTech), IEEE, 2017, pp. 104–110. doi:10.1109/COMTECH.2017.8065757.
- [36] M. I. Ibrahim, M. Y. Darus, DDOS Attack Analysis on IoT Device for Smart Home Environment and A Proposed Detection Technique,

- JOIV: International Journal on Informatics Visualization 8 (4) (2024) 2104–2110. doi:10.62527/joiv.8.4.2175.
- [37] E. Alomari, S. Manickam, B. Gupta, P. Singh, M. Anbar, Design, deployment and use of HTTP-based botnet (HBB) testbed, in: 16th International Conference on Advanced Communication Technology, IEEE, 2014, pp. 1265–1269. doi:10.1109/ICACT.2014.6779162.
- [38] S. Darwish, I. Nouretdinov, S. D. Wolthusen, Towards composable threat assessment for medical IoT (MIoT), *Procedia computer science* 113 (2017) 627–632. doi:10.1016/j.procs.2017.08.314.
- [39] S. Zardari, N. Nisar, Z. Fatima, L. L. Dhirani, Iot-assets taxonomy, threats assessment and potential solutions, in: 2023 Global Conference on Wireless and Optical Technologies (GCWOT), IEEE, 2023, pp. 1–8. doi:10.1109/GCWOT57803.2023.10064657.
- [40] I. Ali, A. I. A. Ahmed, A. Almogren, M. A. Raza, S. A. Shah, A. Khan, A. Gani, Systematic literature review on IoT-based botnet attack, *IEEE access* 8 (2020) 212220–212232. doi:10.1109/ACCESS.2020.3039985.
- [41] P. Podder, M. Mondal, S. Bharati, P. K. Paul, Review on the security threats of internet of things, *arXiv preprint arXiv:2101.05614* (2021). doi:10.5120/ijca2020920548.
- [42] H. Jin, G. Jeon, H. W. A. Choi, S. Jeon, J. T. Seo, A threat modeling framework for IoT-Based botnet attacks, *Heliyon* 10 (20) (2024). doi:10.1016/j.heliyon.2024.e39192.
- [43] T. Trajanovski, N. Zhang, An automated and comprehensive framework for IoT botnet detection and analysis (IoT-BDA), *IEEE Access* 9 (2021) 124360–124383. doi:10.1109/ACCESS.2021.3110188.
- [44] M. M. Alshahrani, A secure and intelligent software-defined networking framework for future smart cities to prevent DDoS attack, *Applied Sciences* 13 (17) (2023) 9822. doi:10.3390/app13179822.
- [45] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, Y. Liu, The impact of dos attacks on resource-constrained IoT devices: A study on the mirai attack, *arXiv preprint arXiv:2104.09041* (2021). doi:10.48550/arXiv.2104.09041.
- [46] S. Javanmardi, M. Ghahramani, M. Shojafar, M. Alazab, A. M. Caruso, M-RL: A mobility and impersonation-aware IDS for DDoS UDP flooding attacks in IoT-Fog networks, *Computers & Security* 140 (2024) 103778. doi:10.1016/j.cose.2024.103778.
- [47] N. Chukkayapally, Detection of UDP flood attacks in wireless sensor networks by visualization on parallel coordinate plot (2021).

- [48] N. K. Singh, S. K. BJ, Detection and prevention of udp protocol exploiting and smurf attack in wsn using sequential probability ratio test algorithm, in: 2023 International Conference on Data Science and Network Security (ICDSNS), IEEE, 2023, pp. 1–6. doi:10.1109/ICDSNS58469.2023.10245010.
- [49] S. M. Zarei, R. Fotohi, Defense against flooding attacks using probabilistic thresholds in the internet of things ecosystem, *Security and Privacy* 4 (3) (2021) e152. doi:10.1002/spy2.152.
- [50] O. M. Almorabea, T. J. S. Khanzada, M. A. Aslam, F. A. Hendi, A. M. Almorabea, IoT network-based intrusion detection framework: a solution to process ping floods originating from embedded devices, *IEEE access* 11 (2023) 119118–119145. doi:10.1109/ACCESS.2023.3327061.
- [51] M. Roshani, M. Nobakht, Hybriddad: Detecting ddos flooding attack using machine learning with programmable switches, in: *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–11. doi:10.1145/3538969.3538991.
- [52] K. Mohit, DNS Amplification Attacks: Obsolete or Potent Threats?, *International Journal for Multidisciplinary Research* 6 (5) (2024) 1–12. doi:10.36948/ijfmr.2024.v06i05.27130.
- [53] J. Stanešić, Z. Morić, V. Dakić, M. Bašić, Prevention of DNS Amplification Attacks, *Annals of DAAAM & Proceedings* 34 (2023). doi:10.2507/34th.daaam.proceedings.012.
- [54] O. van der Toorn, J. Krupp, M. Jonker, R. van Rijswijk-Deij, C. Rossow, A. Sperotto, ANYway: measuring the amplification DDoS potential of domains, in: 2021 17th International Conference on Network and Service Management (CNSM), IEEE, 2021, pp. 500–508. doi:10.23919/CNSM52442.2021.9615596.
- [55] A. Berguiga, A. Harchay, An IoT-based intrusion detection system approach for TCP SYN attacks, *Computers, Materials, & Continua* 71 (2) (2022) 3839. doi:10.32604/cmc.2022.023399.
- [56] A. Berguiga, A. Harchay, An IoT-based intrusion detection system approach for TCP SYN attacks, *Computers, Materials, & Continua* 71 (2) (2022) 3839. doi:10.32604/cmc.2022.023399.
- [57] P. Bhutani, C. S. Dash, Deep Learning Approaches for SYN Flood Detection in Internet Service Providers Network, *International Journal of Innovative Research in Engineering & Management (IJIREM)* 11 (4) (2024) 86–94. doi:10.55524/ijirem.2024.11.4.11.

- [58] P. Kumari, A. K. Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, *Computers & Security* 127 (2023) 103096. doi:10.1016/j.cose.2023.103096.
- [59] L. Huraj, M. Šimon, T. Horák, Resistance of IoT sensors against DDoS attack in smart home environment, *Sensors* 20 (18) (2020) 5298. doi:10.3390/s20185298.
- [60] Z. R. Alashhab, M. Anbar, S. D. A. Rihan, B. A. Alabsi, K. Ateeq, Enhancing cloud computing analysis: A CCE-based HTTP-get log dataset, *Applied Sciences* 13 (16) (2023) 9086. doi:10.3390/app13169086.
- [61] H. Tang, Evaluation of HTTP DDOS cyber attack on web servers Apache and Nginx (2024).
- [62] F. Moldovan, P. Sătmărean, C. Opriș, An analysis of http attacks on home iot devices, in: 2020 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), IEEE, 2020, pp. 1–6. doi:10.1109/AQTR49680.2020.9129980.
- [63] N. Gavric, G. Bhandari, A. Shalaginov, Introducing the Slowloris E-DoS Attack: a Threat Arising From Vulnerabilities in the FTP and SSH Protocols, *Journal of Sensor and Actuator Networks* 15 (2) (2026) 34. doi:10.3390/jsan15020034.
- [64] D. Tymoshchuk, V. Yatskiv, Slowloris ddos detection and prevention in real-time, *Collection of scientific papers (August 16, 2024; Oxford, UK) (2024)* 171–176. doi:10.36074/logos-16.08.2024.036.
- [65] E. D. Ramirez-Martinez, J. A. Perez-Diaz, N. M. Yungaicela-Naula, P4-Assisted slowloris DDoS attack detection in IoT environments by using ML and DL, *Computer Networks* 267 (2025) 111364. doi:10.1016/j.comnet.2025.111364.
- [66] O. Alruwaili, F. M. Alotaibi, M. Tanveer, S. Chaoui, A. Armghan, PSFA-IoT: Physically secure authentication framework for the Internet of Things, *IEEE Access* 12 (2024) 78549–78561. doi:10.1109/ACCESS.2024.3407353.
- [67] M. B. Muzammil, M. Bilal, S. Ajmal, S. C. Shongwe, Y. Y. Ghadi, Unveiling vulnerabilities of web attacks considering man in the middle attack and session hijacking, *IEEE Access* 12 (2024) 6365–6375. doi:10.1109/ACCESS.2024.3350444.
- [68] S. Sarika, An approach to perceive session hijacking in IoT health care, in: *Information and Communication Technology for Competitive Strategies (ICTCS 2021) Intelligent Strategies for ICT*, Springer, 2022, pp. 525–533. doi:10.1007/978-981-19-0098-3_51.

- [69] P. Szynekiewicz, Signature-based detection of botnet DDoS attacks, in: *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*, Springer, 2022, pp. 120–135. doi:10.1007/978-3-031-04036-8_6.
- [70] M. Dimolianis, A. Pavlidis, V. Maglaris, Signature-based traffic classification and mitigation for DDoS attacks using programmable network data planes, *IEEE Access* 9 (2021) 113061–113076. doi:10.1109/ACCESS.2021.3104115.
- [71] M. Mittal, K. Kumar, S. Behal, Deep learning approaches for detecting DDoS attacks: A systematic review, *Soft computing* 27 (18) (2023) 13039–13075. doi:10.1007/s00500-021-06608-1.
- [72] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, A. Abdelmaboud, T. A. A. Abdullah, U. D. Maiwada, Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model, *IEEE access* 12 (2024) 51630–51649. doi:10.1109/ACCESS.2024.3384398.
- [73] S. Karnani, N. Agrawal, R. Kumar, A comprehensive survey on low-rate and high-rate DDoS defense approaches in SDN: taxonomy, research challenges, and opportunities, *Multimedia Tools and applications* 83 (12) (2024) 35253–35306. doi:10.32604/cmc.2021.016288.
- [74] A. Hussain, E. M. Tordera, X. Masip-Bruin, H. C. Leligou, Rule-based with machine learning IDS for DDoS attack detection in cyber-physical production systems (CPPS), *IEEE access* 12 (2024) 114894–114911. doi:10.1109/ACCESS.2024.3445261.
- [75] S. Taminana, D. L. Bhaskari, Dynamic Firewall Rule Building Engine for Hybrid Cloud, *International Journal on Recent and Innovation Trends in Computing and Communication* 11 (2023) 2626–2638. doi:10.17762/ijritcc.v11i9.9335.
- [76] Z. Shah, I. Ullah, H. Li, A. Levula, K. Khurshid, Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey, *Sensors* 22 (3) (2022) 1094. doi:10.3390/s22031094.
- [77] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, S. A. Bahaj, Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT), *Electronics* 11 (3) (2022) 494. doi:10.3390/electronics11030494.
- [78] M. M. Inuwa, R. Das, A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT

- networks, *Internet of Things* 26 (2024) 101162. doi:10.1016/j.iot.2024.101162.
- [79] H. Huang, P. Ye, M. Hu, J. Wu, A multi-point collaborative DDoS defense mechanism for IIoT environment, *Digital Communications and Networks* 9 (2) (2023) 590–601. doi:10.1016/j.dcan.2022.04.008.
- [80] Y. Alhasawi, S. Alghamdi, Federated learning for decentralized DDoS attack detection in IoT networks, *IEEE Access* 12 (2024) 42357–42368. doi:10.1109/ACCESS.2024.3378727.
- [81] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghan-tanha, G. Srivastava, Federated-learning-based anomaly detection for IoT security attacks, *IEEE Internet of Things Journal* 9 (4) (2021) 2545–2554. doi:10.1109/JIOT.2021.3077803.
- [82] Y. Feng, W. Zhang, S. Yin, H. Tang, Y. Xiang, Y. Zhang, A collaborative stealthy DDoS detection method based on reinforcement learning at the edge of Internet of Things, *IEEE Internet of Things Journal* 10 (20) (2023) 17934–17948. doi:10.1109/JIOT.2023.3279615.
- [83] E. C. P. Neto, S. Dadkhah, A. A. Ghorbani, Collaborative DDoS detection in distributed multi-tenant IoT using federated learning, in: *2022 19th annual international conference on privacy, security & trust (PST)*, IEEE, 2022, pp. 1–10. doi:10.1109/PST55820.2022.9851984.
- [84] R. Ahmad, I. Alsmadi, W. Alhamdani, L. Tawalbeh, Zero-day attack detection: a systematic literature review, *Artificial Intelligence Review* 56 (10) (2023) 10733–10811. doi:10.1007/s10462-023-10437-z.
- [85] M. Roopak, S. Parkinson, G. Y. Tian, Y. Ran, S. Khan, B. Chandrasekaran, An unsupervised approach for the detection of zero-day distributed denial of service attacks in Internet of Things networks, *IET Networks* 13 (5-6) (2024) 513–527. doi:10.1049/ntw2.12134.
- [86] N. Niknami, J. Wu, Deepidps: An adaptive drl-based intrusion detection and prevention system for SDN, in: *ICC 2024-IEEE International Conference on Communications*, IEEE, 2024, pp. 2040–2046. doi:10.1109/ICC51166.2024.10622849.
- [87] T. S. R. Team, Quantum Computing in Cyber security: The Next Frontier (2024). <https://thesiliconreview.com/2024/10/quantum-computing-in-cyber-security-the-next-frontier>
- [88] H. Alhakami, Enhancing IoT Security: Quantum-Level Resilience against Threats., *Computers, Materials & Continua* 78 (1) (2024). doi:10.32604/cmc.2023.043439.

- [89] A. Alomari, S. A. Kumar, Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions, *Internet of Things* 25 (2024) 101132. doi:10.1016/j.iot.2024.101132.
- [90] A. Alomari, S. A. Kumar, Deqsvc: Dimensionality reduction and encoding technique for quantum support vector classifier approach to detect DDoS attacks, *IEEE Access* 11 (2023) 110570–110581. doi:10.1109/ACCESS.2023.3322723.
- [91] M. Y. Küçükkara, F. Atban, C. Bayılmış, Quantum-Neural Network Model for Platform Independent Ddos Attack Classification in Cyber Security, *Advanced Quantum Technologies* 7 (10) (2024) 2400084. doi:10.1002/qute.202400084.
- [92] M.-L. Messai, H. Seba, Iot network attack detection: Leveraging graph learning for enhanced security, in: *Proceedings of the 18th international conference on availability, reliability and security*, 2023, pp. 1–7. doi:10.1145/3600160.3605053.
- [93] A. Pakmehr, A. Aßmuth, N. Taheri, A. Ghaffari, DDoS attack detection techniques in IoT networks: a survey, *Cluster Computing* 27 (10) (2024) 14637–14668. doi:10.1007/s10586-024-04662-6.
- [94] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, S. A. Bahaj, Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT), *Electronics* 11 (3) (2022) 494. doi:10.3390/electronics11030494.
- [95] A. A. Alahmadi, M. Aljabri, F. Alhaidari, D. J. Alharthi, G. E. Rayani, L. A. Marghalani, O. B. Alotaibi, S. A. Bajandouh, DDoS attack detection in IoT-based networks using machine learning models: a survey and research directions, *Electronics* 12 (14) (2023) 3103. doi:10.3390/electronics12143103.
- [96] A. Heidari, M. A. Jabraeil Jamali, Internet of Things intrusion detection systems: a comprehensive review and future directions, *Cluster Computing* 26 (6) (2023) 3753–3780. doi:10.1007/s10586-022-03776-z.
- [97] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, N. Dragoni, Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques, *Sensors* 24 (11) (2024) 3571. doi:10.3390/s24113571.
- [98] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed, M. Nasser, Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review, *Applied sciences* 11 (18) (2021) 8383. doi:10.3390/app11188383.

- [99] M. Bhavsar, K. Roy, J. Kelly, O. Olusola, Anomaly-based intrusion detection system for IoT application, *Discover Internet of things* 3 (1) (2023) 5. doi:10.1007/s43926-023-00034-5.
- [100] E. Altulaihan, M. A. Almaiah, A. Aljughaiman, Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms, *Sensors* 24 (2) (2024) 713. doi:10.3390/s24020713.
- [101] G. Shirvani, S. Ghasemshirazi, M. A. Alipour, Enhancing IoT security against DDoS attacks through federated learning, *arXiv preprint arXiv:2403.10968* (2024). doi:arXiv:2403.10968.
- [102] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, M. Elsharief, A federated learning-based approach for improving intrusion detection in industrial internet of things networks, *Network* 3 (1) (2023) 158–179. doi:10.3390/network3010008.
- [103] F. N. Al-Wesabi, H. A. Mengash, R. Marzouk, N. Alruwais, R. Allafi, R. Alabdan, M. Alharbi, D. Gupta, Pelican optimization algorithm with federated learning driven attack detection model in internet of things environment, *Future Generation Computer Systems* 148 (2023) 118–127. doi:10.1016/j.future.2023.05.029.
- [104] F. L. de Caldas Filho, S. C. M. Soares, E. Oroski, R. de Oliveira Albuquerque, R. Z. A. Da Mata, F. L. L. De Mendonça, R. T. de Sousa Júnior, Botnet detection and mitigation model for IoT networks using federated learning, *Sensors* 23 (14) (2023) 6305. doi:10.3390/s23146305.
- [105] Z. Yin, K. Li, H. Bi, Trusted multi-domain DDoS detection based on federated learning, *Sensors* 22 (20) (2022) 7753. doi:10.3390/s22207753.
- [106] D. Said, Quantum computing and machine learning for cybersecurity: Distributed denial of service (DDoS) attack detection on smart microgrid, *Energies* 16 (8) (2023) 3572. doi:10.3390/en16083572.
- [107] A. Alomari, S. A. Kumar, Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions, *Internet of Things* 25 (2024) 101132. doi:10.1016/j.iot.2024.101132.
- [108] G. Visalaxi, A. Muthukumaravel, IOT monitoring membrane computing based on quantum inspiration to enhance security in cloud network, *Measurement: Sensors* 27 (2023) 100755. doi:10.1016/j.measen.2023.100755.
- [109] D. Javeed, M. S. Saeed, I. Ahmad, M. Adil, P. Kumar, A. N. Islam, Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions, *Future*

- Generation Computer Systems 160 (2024) 577–597. doi:10.1016/j.future.2024.06.023.
- [110] X.-W. Wu, E.-H. Yang, J. Wang, Lightweight security protocols for the Internet of Things, in: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, 2017, pp. 1–7. doi:10.1109/PIMRC.2017.8292779.
- [111] N. Kaur, A systematic review on security aspects of fog computing environment: Challenges, solutions and future directions, Computer Science Review 54 (2024) 100688. doi:10.1016/j.cosrev.2024.100688.
- [112] K. Bhushan, B. B. Gupta, Security challenges in cloud computing: state-of-art, International Journal of Big Data Intelligence 4 (2) (2017) 81–107. doi:10.1504/IJBDI.2017.083116.
- [113] S. Khan, S. Parkinson, Y. Qin, Fog computing security: a review of current applications and security solutions, Journal of Cloud Computing 6 (1) (2017) 19. doi:10.1186/s13677-017-0090-3.
- [114] R. Chaganti, B. Bhushan, V. Ravi, The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions, arXiv preprint arXiv:2202.03617 (2022). doi:10.48550/arXiv.2202.03617.
- [115] S. Arora, P. Khare, S. Gupta, AI-driven DDoS mitigation at the edge: Leveraging machine learning for real-time threat detection and response, in: 2024 International Conference on Data Science and Network Security (ICDSNS), IEEE, 2024, pp. 1–7. doi:10.1109/ICDSNS.2024.10690930.
- [116] C. Gupta, G. Varshney, A lightweight and secure puf-based authentication and key-exchange protocol for iot devices, arXiv preprint arXiv:2311.04078 (2023). doi:10.48550/arXiv.2311.04078.
- [117] S. A. Khanday, H. Fatima, N. Rakesh, Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks, Expert Systems with Applications 215 (2023) 119330. doi:10.1016/j.eswa.2022.119330.
- [118] P. Bhale, D. R. Chowdhury, S. Biswas, S. Nandi, OPTIMIST: Lightweight and transparent IDS with optimum placement strategy to mitigate mixed-rate DDoS attacks in IoT networks, IEEE Internet of Things Journal 10 (10) (2023) 8357–8370. doi:10.1109/JIOT.2023.3234530.
- [119] S. Sadhwani, B. Manibalan, R. Muthalagu, P. Pawar, A lightweight model for DDoS attack detection using machine learning techniques, Applied Sciences 13 (17) (2023) 9937. doi:10.3390/app13179937.

- [120] A. D. Aguru, S. B. Erukala, A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning, *Information Sciences* 662 (2024) 120209. doi:10.1016/j.ins.2024.120209.
- [121] R. Bensaid, N. Labraoui, A. A. Abba Ari, L. Maglaras, H. Saidi, A. M. Abdu Lwahhab, S. Benfriha, Toward a Real-Time TCP SYN Flood DDoS Mitigation Using Adaptive Neuro-Fuzzy Classifier and SDN Assistance in Fog Computing, *Security and Communication Networks* 2024 (1) (2024) 6651584. doi:10.1155/2024/6651584.
- [122] M. A. Lawal, R. A. Shaikh, S. R. Hassan, A DDoS attack mitigation framework for IoT networks using fog computing, *Procedia Computer Science* 182 (2021) 13–20. doi:10.1016/j.procs.2021.02.003.
- [123] K. F. Hassan, M. E. Manaa, Detection and mitigation of DDoS attacks in internet of things using a fog computing hybrid approach, *Bulletin of Electrical Engineering and Informatics* 11 (3) (2022) 1604–1613. doi:10.11591/eei.v11i3.3643.
- [124] D. K. Sharma, T. Dhankhar, G. Agrawal, S. K. Singh, D. Gupta, J. Nebhen, I. Razzak, Anomaly detection framework to prevent DDoS attack in fog empowered IoT networks, *Ad Hoc Networks* 121 (2021) 102603. doi:10.1016/j.adhoc.2021.102603.
- [125] E. K. Kareem, M. E. Manaa, A Fog Computing-Based Machine Learning Framework for DDoS Attacks Detection: Balancing Offline and Real-Time Analysis for IoT Data., *International Journal of Safety & Security Engineering* 14 (6) (2024). doi:10.18280/ijss.140620.
- [126] A. Aguru, S. Erukala, OTI-IoT: A blockchain-based operational threat intelligence framework for multi-vector DDoS attacks, *ACM Transactions on Internet Technology* 24 (3) (2024) 1–31. doi:10.1145/3664287.
- [127] R. F. Ibrahim, Q. Abu Al-Haija, A. Ahmad, DDoS attack prevention for internet of thing devices using ethereum blockchain technology, *Sensors* 22 (18) (2022) 6806. doi:10.3390/s22186806.
- [128] R. Jmal, W. Ghabri, R. Guesmi, B. M. Alshammari, A. S. Alshammari, H. Alsaif, Distributed blockchain-SDN secure IoT system based on ANN to mitigate DDoS attacks, *Applied Sciences* 13 (8) (2023) 4953. doi:10.3390/app13084953.
- [129] A. I. El Sayed, M. Abdelaziz, M. Hussein, A. D. Elbayoumy, DDoS mitigation in IoT using machine learning and blockchain integration, *IEEE Networking Letters* 6 (2) (2024) 152–155. doi:10.1109/LNET.2024.3377355.

- [130] P. Kumari, A. K. Jain, A. Seth, Raghav, Leveraging blockchain and machine learning to counter DDoS attacks over IoT network, *Multi-media Tools and Applications* 84 (1) (2025) 317–341. doi:10.1007/s11042-024-18842-4.
- [131] M. Aslam, D. Ye, A. Tariq, M. Asad, M. Hanif, D. Ndzi, S. A. Chelloug, M. A. Elaziz, M. A. Al-Qaness, S. F. Jilani, Adaptive machine learning based distributed denial-of-services attacks detection and mitigation system for SDN-enabled IoT, *Sensors* 22 (7) (2022) 2697. doi:10.3390/s22072697.
- [132] S. Arora, P. Khare, S. Gupta, AI-driven DDoS mitigation at the edge: Leveraging machine learning for real-time threat detection and response, in: *2024 International Conference on Data Science and Network Security (ICDSNS)*, IEEE, 2024, pp. 1–7. doi:10.1109/ICDSNS62112.2024.10690930.
- [133] T. Nay, Enhancing iot security with ai-driven hybrid machine learning and neural network-based intrusion detection system, *Babylonian Journal of Artificial Intelligence* 2024 (2024) 158–167.
- [134] K. Kamarapu, K. R. K. Vucha, Adaptive AI Framework for Anomaly Detection and DDoS Mitigation in Distributed Systems, *Indian Journal of Computer Science and Technology: Fifth Dimension Research Publications* (2025) 23–31doi:10.59256/indjct.20250401005.
- [135] A. R. Gad, A. A. Nashat, T. M. Barkat, Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset, *IEEE access* 9 (2021) 142206–142217. doi:10.1109/ACCESS.2021.3120626.
- [136] S. Alosaimi, S. M. Almutairi, An intrusion detection system using BoT-IoT, *Applied Sciences* 13 (9) (2023) 5427. doi:10.3390/app13095427.
- [137] S.-M. Tseng, Y.-Q. Wang, Y.-C. Wang, Multi-class intrusion detection based on transformer for IoT networks using CIC-IoT-2023 dataset, *Future Internet* 16 (8) (2024) 284. doi:10.3390/fi16080284.
- [138] S. Haque, F. El-Moussa, N. Komninos, R. Muttukrishnan, A systematic review of data-driven attack detection trends in IoT, *Sensors* 23 (16) (2023) 7191. doi:10.3390/s23167191.
- [139] A. Parmisano, S. Garcia, E. MJ, IoT-23 Dataset: A labeled dataset of Malware-and Benign IoT Traffic. *StratosphereIPS*, Stratosphere IPS (2018).
- [140] N. Moustafa, M. Keshky, E. Debiez, H. Janicke, Federated TON_IoT Windows datasets for evaluating AI-based security applications, in:

- 2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom), IEEE, 2020, pp. 848–855. doi:10.1109/TrustCom50675.2020.00114.
- [141] N. Koroniotis, N. Moustafa, E. Sitnikova, J. Slay, Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques, in: International conference on mobile networks and management, Springer, 2017, pp. 30–44. doi:10.1007/978-3-319-90775-8_3.
- [142] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, A. A. Ghorbani, CICIOT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment, *Sensors* 23 (13) (2023) 5941. doi:10.3390/s23135941.
- [143] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, S. Nömm, Med-BIoT: Generation of an IoT botnet dataset in a medium-sized IoT network, in: ICISSP, 2020, pp. 207–218. doi:10.5220/0009187802070218.
- [144] S. Garcia, A. Parmisano, M. J. Erquiaga, IoT-23: A labeled dataset with malicious and benign IoT network traffic (2020). doi:10.5281/zenodo.4743746.
- [145] I. Sharafaldin, A. H. Lashkari, S. Hakak, A. A. Ghorbani, Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, in: 2019 international carnahhan conference on security technology (ICCST), IEEE, 2019, pp. 1–8. doi:10.1109/CCST.2019.8888419.
- [146] A. M. OYELAKIN, Overview and exploratory analyses of CICIDS2017 intrusion detection dataset, *Indonesian Journal of Data and Science* (2023).
- [147] G. Saporito, A Deeper Dive into the NSL-KDD Data Set (2025). <https://medium.com/data-science/a-deeper-dive-into-the-ns1-kdd-data-set-15c753364657>
- [148] CAIDA, The CAIDA “DDoS Attack 2007” Dataset (2007). https://www.caida.org/catalog/datasets/ddos-20070804_dataset/
- [149] M. C. P. Saheb, M. S. Yadav, S. Babu, J. J. Pujari, J. B. Maddala, A review of DDoS evaluation dataset: CICDDoS2019 dataset, in: International Conference on Energy Systems, Drives and Automations, Springer, 2021, pp. 389–397. doi:10.1007/978-981-99-3691-5_34.
- [150] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, et al., Toward generating a new intrusion detection dataset and intrusion traffic

- characterization, *ICISSp* 1 (2018) (2018) 108–116. <https://www.unb.ca/cic/datasets/ids-2017.html>.
- [151] M. Tavallaee, E. Bagheri, W. Lu, A. A. Ghorbani, A detailed analysis of the KDD CUP 99 data set, in: 2009 IEEE symposium on computational intelligence for security and defense applications, IEEE, 2009, pp. 1–6. doi:10.1109/CISDA.2009.5356528.
- [152] V. Shirsath, CAIDA UCSD DDoS 2007 Attack Dataset (2023). doi: 10.21227/dvp9-s124.
- [153] GeeksforGeeks, What is Kaggle? (2025). <https://www.geeksforgeeks.org/machine-learning/what-is-kaggle/>
- [154] I. DataPort, IEEE DataPort (2025). <https://www.ieee.org/communities/ieee-dataport>
- [155] O. at CERN, Open Infrastructure and Open Source Software: Zenodo (2025). <https://openscience.cern/node/448>
- [156] L. S. Easily, What is: Accuracy in Data Science and Statistics (2025). <https://statisticseasily.com/glossario/what-is-accuracy-in-data-science-and-statistics/>
- [157] EvidentlyAI, Accuracy vs. precision vs. recall in machine learning: what's the difference? (2025). <https://www.evidentlyai.com/classification-metrics/accuracy-precision-recall>
- [158] Ruman, Precision, Recall and F1 Explained [With 10 ML Use case] (2025). <https://rumn.medium.com/precision-recall-and-f1-explained-with-10-ml-use-case-6ef2fbe458e5>
- [159] T. Wood, F-Score (2025). <https://deepai.org/machine-learning-glossary-and-terms/f-score>
- [160] T. with Kolena, False Positive Rate (FPR) – Testing with Kolena (2025). <https://docs.kolena.com/metrics/fpr/>
- [161] R. Peters, Performance Metrics: False Negative Rate (2025). <https://www.roelpeters.be/glossary/false-negative-rate-machine-learning/>
- [162] G. for Developers, Classification: ROC and AUC (2025). <https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc>
- [163] T. Issariyakul, E. Hossain, Introduction to network simulator 2 (NS2), in: Introduction to network simulator NS2, Springer, 2008, pp. 1–18. doi:10.1007/978-0-387-71760-9_2.
- [164] J. Gomez, E. F. Kfoury, J. Crichigno, G. Srivastava, A survey on network simulators, emulators, and testbeds used for research and education, *Computer Networks* 237 (2023) 110054. doi:10.1016/j.comnet.2023.110054.

- [165] Admin, OMNeT++ Online Summit 2022 (2022). <https://omnetpp.org/articles/2022/11/06/summit.html>
- [166] D. Dholakiya, T. Kshirsagar, A. Nayak, Survey of mininet challenges, opportunities, and application in software-defined network (SDN), in: International Conference on Information and Communication Technology for Intelligent Systems, Springer, 2020, pp. 213–221. doi:10.1007/978-981-15-7062-9_21.
- [167] R. Almutairi, G. Bergami, G. Morgan, Advancements and challenges in IoT simulators: A comprehensive review, *Sensors* 24 (5) (2024) 1511. doi:10.3390/s24051511.
- [168] B. N. Rashid, K. H. Sharif, T. H. Shreef, A survey of simulation tools for modelling Internet of Thing, *Passer Journal of Basic and Applied Sciences* 4 (1) (2022) 37–44. doi:10.24271/psr.2022.313553.1105.
- [169] P. Elechi, S. M. Ekolama, E. Okowa, S. Kukuchuku, A review of emerging technologies in wireless communication systems, *Innovation and Emerging Technologies* 12 (2025) 2550005. doi:10.1142/S2737599425500057.
- [170] A. S. Library, IoT Device Simulator (2022). <https://aws.amazon.com/tw/solutions/implementations/iot-device-simulator/>
- [171] P. Vergadia, What is Cloud IoT Core? (2021). <https://cloud.google.com/blog/topics/developers-practitioners/what-cloud-iot-core>
- [172] M. M. Islam, S. Shahid, K. B. Awar, R. Khan, M. Sohail, Cyber-Security: Dos Attack Outcomes are Dangerous, *European Journal of Electrical Engineering and Computer Science* 5 (3) (2021) 54–59. doi:10.24018/ejece.2021.5.3.297.
- [173] C. Scherb, L. B. Heitz, F. Grimberg, H. Grieder, M. Maurer, A cyber attack simulation for teaching cybersecurity, *EPiC Series in Computing* 93 (2023) 129–140.
- [174] S. P. Thirimann, E. Y. Lemang, G. Antoniol, M. Nayebi, Current Trends in Tensorflow and the Future of MI Software Documentation: One Documentation Does Not Fit All, *SSRN* (2024).
- [175] J. Sawtell-Rickson, What Is PyTorch? (2025). <https://builtin.com/machine-learning/pytorch>
- [176] A. Dhakad, S. Singh, M. Moharir, A. K. AR, et al., Real time network traffic analysis using artificial intelligence, machine learning and deep learning: A review of methods, tools and applications, in: 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), IEEE, 2023, pp. 372–378. doi:10.1109/ICSSAS57918.2023.10331855.

- [177] P. Schwaiger, D. Simopoulos, A. Wolf, Automated IoT security testing with SecLab, in: NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, IEEE, 2022, pp. 1–6. doi:10.1109/NO MS54207.2022.9789797.
- [178] T. Zhang, C. Xue, J. Wang, Z. Yun, N. Lin, S. Han, A survey on industrial Internet of Things (IIoT) Testbeds for connectivity research, arXiv preprint arXiv:2404.17485 (2024). doi:10.48550/arXiv.2404.17485.
- [179] A. Imteaj, U. Thakker, S. Wang, J. Li, M. H. Amini, A survey on federated learning for resource-constrained IoT devices, IEEE Internet of Things Journal 9 (1) (2021) 1–24. doi:10.1109/JIOT.2021.3095077.
- [180] G. Kornaros, Hardware-assisted machine learning in resource-constrained IoT environments for security: review and future prospective, IEEE Access 10 (2022) 58603–58622. doi:10.1109/ACCESS.2022.3179047.
- [181] S. Kumar, A. kumar Keshri, An effective DDoS attack mitigation strategy for IoT using an optimization-based adaptive security model, Knowledge-Based Systems 299 (2024) 112052. doi:10.1016/j.knosys.2024.112052.
- [182] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, S. A. Bahaj, Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT), Electronics 11 (3) (2022) 494. doi:10.3390/electronics11030494.
- [183] P. Maniriho, A. N. Mahmood, M. J. M. Chowdhury, A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges, Future Generation Computer Systems 130 (2022) 1–18. doi:10.1016/j.future.2021.11.030.
- [184] M. Zahid, T. S. Bharati, Comprehensive Review of IoT Attack Detection Using Machine Learning and Deep Learning Techniques, in: 2024 Second International Conference on Advanced Computing & Communication Technologies (ICACCTech), IEEE, 2024, pp. 827–834. doi:10.1109/ICACCTech65084.2024.00136.
- [185] P. Kumari, A. K. Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, Computers & Security 127 (2023) 103096. doi:10.1016/j.cose.2023.103096.
- [186] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, U. U. Fayyaz, F. Shahzad, N. M. Garcia, E. Zdravevski, A framework for malicious traffic detection in IoT healthcare environment, Sensors 21 (9) (2021) 3025. doi:10.3390/s21093025.

- [187] Y. Alhasawi, S. Alghamdi, Federated learning for decentralized DDoS attack detection in IoT networks, *IEEE Access* 12 (2024) 42357–42368. doi:10.1109/ACCESS.2024.3378727.
- [188] N. V. Patil, C. Rama Krishna, K. Kumar, Distributed frameworks for detecting distributed denial of service attacks: a comprehensive review, challenges and future directions, *Concurrency and Computation: Practice and Experience* 33 (10) (2021) e6197. doi:10.1002/cpe.6197.
- [189] V. Tang, K. L. Choy, G. T. Ho, H. Y. Lam, Y. P. Tsang, An IoMT-based geriatric care management system for achieving smart health in nursing homes, *Industrial Management & Data Systems* 119 (8) (2019) 1819–1840. doi:10.1108/IMDS-01-2019-0024.
- [190] S. Mahadik, P. M. Pawar, R. Muthalagu, Efficient intelligent intrusion detection system for heterogeneous internet of things (HetIoT), *Journal of Network and Systems Management* 31 (1) (2023) 2.
- [191] Z. Shah, I. Ullah, H. Li, A. Levula, K. Khurshid, Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey, *Sensors* 22 (3) (2022) 1094. doi:10.3390/s22031094.
- [192] B. Sudharsan, D. Sundaram, P. Patel, J. G. Breslin, M. I. Ali, Edge2guard: Botnet attacks detecting offline models for resource-constrained iot devices, in: *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, IEEE, 2021, pp. 680–685. doi:10.1109/PerComWorkshops51409.2021.9431086.
- [193] S. A. Khanday, H. Fatima, N. Rakesh, Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks, *Expert Systems with Applications* 215 (2023) 119330. doi:10.1016/j.eswa.2022.119330.
- [194] P. Bhale, D. R. Chowdhury, S. Biswas, S. Nandi, OPTIMIST: Lightweight and transparent IDS with optimum placement strategy to mitigate mixed-rate DDoS attacks in IoT networks, *IEEE Internet of Things Journal* 10 (10) (2023) 8357–8370. doi:10.1109/JIOT.2023.3234530.
- [195] A. Hekmati, J. Zhang, T. Sarkar, N. Jethwa, E. Grippo, B. Krishnamachari, Correlation-aware neural networks for DDoS attack detection in IoT systems, *IEEE/ACM transactions on networking* 32 (5) (2024) 3929–3944. doi:10.1109/TNET.2024.3408675.

- [196] A. Hekmati, E. Grippo, B. Krishnamachari, Large-scale urban iot activity data for ddos attack emulation, in: *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, 2021, pp. 560–564. doi:10.1145/3485730.3493695.
- [197] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, A. A. Ghorbani, CICIOT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment, *Sensors* 23 (13) (2023) 5941. doi:10.3390/s23135941.
- [198] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, H. El Makhtoum, OMIC: A bagging-based ensemble learning framework for large-scale IoT intrusion detection, *Journal of Future Artificial Intelligence and Technologies* 1 (4) (2025) 401–416. doi:10.62411/faith.3048-3719-63.
- [199] X. Sáez-de Cámara, J. L. Flores, C. Arellano, A. Urbieto, U. Zurutuza, Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks, *Computers & Security* 131 (2023) 103299. doi:10.1016/j.cose.2023.103299.
- [200] N. Gavric, G. Prasad Bhandari, A. Shalaginov, Towards resource-efficient DDoS detection in IoT: leveraging feature engineering of system and network usage metrics, *Journal of Network and Systems Management* 32 (4) (2024) 69. doi:10.1007/s10922-024-09848-2.
- [201] I. Ahmad, Z. Wan, A. Ahmad, A big data analytics for DDOS attack detection using optimized ensemble framework in Internet of Things, *Internet of Things* 23 (2023) 100825. doi:10.1016/j.iot.2023.100825.
- [202] P. Bhardwaj, R. Mukesh, IoT Under Attack: Designing Techniques for Mitigating Energy-Oriented DDOS Attacks on Smart Home Networks, in: *NIELIT's International Conference on Communication, Electronics and Digital Technologies*, Springer, 2024, pp. 289–305. doi:10.1007/978-981-97-3601-0_21.
- [203] A. A. Alshdadi, A. A. Almazroi, N. Ayub, M. D. Lytras, E. Alsolami, F. S. Alsubaei, Big data-driven deep learning ensembler for DDoS attack detection, *Future Internet* 16 (12) (2024) 458. doi:10.3390/fi16120458.
- [204] I. I. Al Barazanchi, W. Hashim, Enhancing IoT device security through blockchain technology: A decentralized approach, *Shifra* 2023 (2023) 10–16. doi:10.70470/SHIFRA/2023/002.
- [205] E. S. Babu, B. SrinivasaRao, S. R. Nayak, A. Verma, F. Alqahtani, A. Tolba, A. Mukherjee, Blockchain-based Intrusion Detection System of IoT urban data with device authentication against DDoS attacks,

- Computers and Electrical Engineering 103 (2022) 108287. doi:10.1016/j.compeleceng.2022.108287.
- [206] N. Baksh, G. Wallace, AI and Blockchain Integration: Ensuring End-to-End Security for IoT Devices (2025).
- [207] R. Rahim, M. A. Chishti, M. M. Raheem, Improving the security of internet of things (iot) using intrusion detection system (ids), in: 2024 21st Learning and Technology Conference (L&T), IEEE, 2024, pp. 290–295. doi:10.1109/LT60077.2024.10469668.
- [208] E. Halim, M. Reda, Y. Maher, M. Younan, Chain of things (CoT): A Blockchain-based framework for Securing internet of things applications, *Journal of Computing and Communication* 4 (1) (2025) 1–18. doi:10.21608/jocc.2025.411109.
- [209] N. V. Patil, C. Rama Krishna, K. Kumar, Distributed frameworks for detecting distributed denial of service attacks: a comprehensive review, challenges and future directions, *Concurrency and Computation: Practice and Experience* 33 (10) (2021) e6197. doi:10.1002/cpe.6197.
- [210] M. Z. Hasan, Z. Mohd Hanapi, Efficient and secured mechanisms for data link in IoT WSNs: A literature review, *Electronics* 12 (2) (2023) 458. doi:10.3390/electronics12020458.
- [211] N. Mishra, S. Pandya, Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review, *IEEE Access* 9 (2021) 59353–59377. doi:10.1109/ACCESS.2021.3073408.
- [212] K. B. Adedeji, A. M. Abu-Mahfouz, A. M. Kurien, DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges, *Journal of Sensor and Actuator Networks* 12 (4) (2023) 51. doi:10.3390/jsan12040051.
- [213] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, A. Abdelmaboud, T. A. A. Abdullah, U. D. Maiwada, Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model, *IEEE access* 12 (2024) 51630–51649. doi:10.1109/ACCESS.2024.3384398.
- [214] S. Hashemi, M. Zarei, Internet of Things backdoors: Resource management issues, security challenges, and detection methods, *Transactions on Emerging Telecommunications Technologies* 32 (2) (2021) e4142. doi:10.1002/ett.4142.
- [215] M. Akhi, C. Eising, L. L. Dhirani, TCN-Based DDoS detection and mitigation in 5G Healthcare-IoT: A frequency monitoring and dynamic

- threshold approach, *IEEE Access* (2025). doi:10.1109/ACCESS.2025.3531659.
- [216] G. S. Rao, P. S. K. Patra, V. Narayana, A. R. Reddy, G. V. Reddy, D. Eshwar, DDoSNet: Detection and prediction of DDoS attacks from realistic multidimensional dataset in IoT network environment, *Egyptian Informatics Journal* 27 (2024) 100526. doi:10.1016/j.eij.2024.100526.
- [217] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, S. A. Bahaj, Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT), *Electronics* 11 (3) (2022) 494. doi:/10.3390/electronics11030494.
- [218] D. Lin, W. Wu, RF fingerprint-identification-based reliable resource allocation in an Internet of Battle Things, *IEEE Internet of Things Journal* 9 (21) (2022) 21111–21120. doi:10.1109/JIOT.2022.3175844.
- [219] M. Alkhamash, A metaheuristic approach to detecting and mitigating DDoS attacks in Blockchain-Integrated deep learning models for IoT applications, *IEEE Access* 12 (2024) 193184–193194. doi:10.1109/ACCESS.2024.3519132.
- [220] M. Aqeel, F. Ali, M. W. Iqbal, T. A. Rana, M. Arif, M. R. Auwul, A review of security and privacy concerns in the internet of things (IoT), *Journal of sensors* 2022 (1) (2022) 5724168. doi:10.1155/2022/5724168.
- [221] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, H. Fahmy, Monitoring real time security attacks for IoT systems using DevSecOps: a systematic literature review, *Information* 12 (4) (2021) 154. doi:10.3390/info12040154.
- [222] P. Kumari, A. K. Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, *Computers & Security* 127 (2023) 103096. doi:10.1016/j.cose.2023.103096.
- [223] N. Nandhini, V. Manikandan, G. Manavaalan, S. Elango, C. Jeevakarunya, P. V. Kumar, A survey on intrusion detection system in smart city: security concerns, in: 2023 7th International Conference on Computer Applications in Electrical Engineering-Recent Advances (CERA), IEEE, 2023, pp. 1–6. doi:10.1109/CERA59325.2023.10455491.
- [224] C. S. Kalutharage, X. Liu, C. Chrysoulas, N. Pitropakis, P. Papadopoulos, Explainable AI-based DDOS attack identification method for IoT networks, *Computers* 12 (2) (2023) 32. doi:10.3390/computers12020032.

- [225] Y. Alhasawi, S. Alghamdi, Federated learning for decentralized DDoS attack detection in IoT networks, *IEEE Access* 12 (2024) 42357–42368. doi:10.1109/ACCESS.2024.3378727.
- [226] P. Kumari, A. K. Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, *Computers & Security* 127 (2023) 103096. doi:10.1016/j.cose.2023.103096.
- [227] D. V. L. KUL, W. J. KUL, T. G. UMU, K. Loupos, C. Kalogirou, H. Niavis, T. Krousarlis, D1. 1 Research Agenda, IoT threat landscape and security challenges, *Nature* 31 (2021) 12.
- [228] A. I. Gide, A. A. Mu'azu, A real-time intrusion detection system for dos/ddos attack classification in IoT networks using KNN-neural network hybrid technique, *Babylonian Journal of Internet of Things* 2024 (2024) 60–69. doi:10.58496/BJIoT/2024/008.
- [229] P. Kumari, A. K. Jain, A comprehensive study of DDoS attacks over IoT network and their countermeasures, *Computers & Security* 127 (2023) 103096. doi:10.1016/j.cose.2023.103096.
- [230] A. Karale, The challenges of IoT addressing security, ethics, privacy, and laws, *Internet of Things* 15 (2021) 100420. doi:10.1016/j.iot.2021.100420.
- [231] S. A. Khanday, H. Fatima, N. Rakesh, Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks, *Expert Systems with Applications* 215 (2023) 119330. doi:10.1016/j.eswa.2022.119330.
- [232] A. B. De Neira, B. Kantarci, M. Nogueira, Distributed denial of service attack prediction: Challenges, open issues and opportunities, *Computer Networks* 222 (2023) 109553. doi:10.1016/j.comnet.2022.109553.
- [233] X. Chen, L. Xiao, W. Feng, N. Ge, X. Wang, DDoS defense for IoT: A Stackelberg game model-enabled collaborative framework, *IEEE Internet of Things Journal* 9 (12) (2021) 9659–9674. doi:10.1109/JIOT.2021.3138094.
- [234] D. D. Gemmer, B. H. Meyer, E. R. de Mello, M. Schwarz, M. S. Wangham, M. Nogueira, A scalable cyber security framework for the experimentation of ddos attacks of things, in: *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, IEEE, 2023, pp. 1–7. doi:10.1109/NOMS56928.2023.10154400.
- [235] F. De Keersmaecker, Y. Cao, G. K. Ndonga, R. Sadre, A survey of public IoT datasets for network security research, *IEEE Communications Surveys & Tutorials* 25 (3) (2023) 1808–1840. doi:10.1109/COMST.2023.3288942.

- [236] M. Zeeshan, Q. Riaz, M. A. Bilal, M. K. Shahzad, H. Jabeen, S. A. Haider, A. Rahim, Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets, *IEEE Access* 10 (2021) 2269–2283. doi:10.1109/ACCESS.2021.3137201.
- [237] P. Szynekiewicz, Signature-based detection of botnet DDoS attacks, in: *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*, Springer, 2022, pp. 120–135. doi:10.1007/978-3-031-04036-8_6.
- [238] I. Ullah, Q. H. Mahmoud, Design and development of a deep learning-based model for anomaly detection in IoT networks, *IEEE Access* 9 (2021) 103906–103926. doi:10.1109/ACCESS.2021.3094024.
- [239] X.-H. Nguyen, K.-H. Le, Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model, *Internet of Things* 23 (2023) 100851. doi:10.1016/j.iot.2023.100851.
- [240] D. Nanthiya, P. Keerthika, S. Gopal, S. Kayalvizhi, T. Raja, R. S. Priya, Svm based ddos attack detection in iot using iot-23 botnet dataset, in: *2021 Innovations in Power and Advanced Computing Technologies (i-PACT)*, IEEE, 2021, pp. 1–7. doi:10.1109/i-PACT52855.2021.9696569.
- [241] S. Hizal, U. Cavusoglu, D. Akgun, A novel deep learning-based intrusion detection system for IoT DDoS security, *Internet of Things* 28 (2024) 101336. doi:10.1016/j.iot.2024.101336.
- [242] S. Pokhrel, R. Abbas, B. Aryal, IoT security: botnet detection in IoT using machine learning, *arXiv preprint arXiv:2104.02231* (2021). doi:10.48550/arXiv.2104.02231.
- [243] K. Al-Begain, M. Khan, B. Alothman, C. Joumaa, E. Alrashed, A DDoS detection and prevention system for IoT devices and its application to smart home environment, *Applied Sciences* 12 (22) (2022) 11853. doi:10.3390/app122211853.
- [244] S. A. Khanday, H. Fatima, N. Rakesh, Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks, *Expert Systems with Applications* 215 (2023) 119330. doi:10.1016/j.eswa.2022.119330.
- [245] M. Snehi, A. Bhandari, Vulnerability retrospection of security solutions for software-defined Cyber–Physical System against DDoS and IoT-DDoS attacks, *Computer Science Review* 40 (2021) 100371. doi:10.1016/j.cosrev.2021.100371.

- [246] Y. Al-Hadhrami, F. K. Hussain, DDoS attacks in IoT networks: a comprehensive systematic literature review, *World Wide Web* 24 (3) (2021) 971–1001. doi:10.1007/s11280-020-00855-2.
- [247] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, H. Fahmy, Monitoring real time security attacks for IoT systems using DevSecOps: a systematic literature review, *Information* 12 (4) (2021) 154. doi:10.3390/info12040154.
- [248] N. M. Allifah, I. A. Zuolkernan, Ranking security of IoT-based smart home consumer devices, *Ieee Access* 10 (2022) 18352–18369. doi:10.1109/ACCESS.2022.3148140.
- [249] G. Vardakis, G. Hatzivasilis, E. Koutsaki, N. Papadakis, Review of smart-home security using the internet of things, *Electronics* 13 (16) (2024) 3343. doi:10.3390/electronics13163343.
- [250] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, Y. Liu, The impact of dos attacks on resource-constrained iot devices: A study on the mirai attack, *arXiv preprint arXiv:2104.09041* (2021). doi:10.48550/arXiv.2104.09041.
- [251] W. Mao, Z. Zhao, Z. Chang, G. Min, W. Gao, Energy-efficient industrial internet of things: Overview and open issues, *IEEE transactions on industrial informatics* 17 (11) (2021) 7225–7237. doi:10.1109/TII.2021.3067026.
- [252] T. Horak, P. Strelec, L. Huraj, P. Tanuska, A. Vaclavova, M. Kebisek, The vulnerability of the production line using industrial IoT systems under ddos attack, *Electronics* 10 (4) (2021) 381. doi:10.3390/electronics10040381.
- [253] D. Acarali, M. Rajarajan, D. Chema, M. Ginzburg, A characterisation of smart grid dos attacks, in: *International Conference on Security and Privacy in New Computing Environments*, Springer, 2020, pp. 3–21. doi:10.1007/978-3-030-66922-5_1.
- [254] I. Ortega-Fernandez, F. Liberati, A review of denial of service attack and mitigation in the smart grid using reinforcement learning, *Energies* 16 (2) (2023) 635. doi:10.3390/en16020635.
- [255] M. Menagadevi, N. Madian, D. Thiyagarajan, R. Rajendran, Smart medical devices: making healthcare more intelligent, in: *Machine Learning Models and Architectures for Biomedical Signal Processing*, Elsevier, 2025, pp. 487–501. doi:10.1016/B978-0-443-22158-3.00020-X.

- [256] Z. Zhou, A. Gaurav, B. Gupta, H. Hamdi, N. Nadjah, A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic, *Neural Computing and Applications* 36 (1) (2024) 1–14. doi:10.1007/s00521-021-06389-6.
- [257] N. Alsuwaidi, N. Alharmoodi, H. Al Hamadi, The transformative impact of zero-trust architecture on healthcare security, in: 2024 2nd International conference on cyber resilience (ICCR), IEEE, 2024, pp. 1–8. doi:10.1109/ICCR61006.2024.10532794.

Biographies



Mosiur Rahaman is a Lecturer in the Department of Computer Engineering at King Mongkut's University of Technology Thonburi, Thailand. He received his Ph.D. in Computer Science and Information Engineering from Asia University, Taiwan. His research interests include artificial intelligence, machine learning, cybersecurity, the Internet of Things, phishing detection, and digital transformation. He has published extensively in international journals and has served as a postdoctoral researcher, lecturer, assistant professor, editor, reviewer, and conference chair.



Nicko Cajes is an Information Technology professional, researcher, and data management practitioner with a strong passion for cybersecurity, artificial intelligence, machine learning, and information systems. He has contributed

to internationally published research on phishing and smishing attack detection, as well as the application of real-time machine learning techniques in robotics. His research interests focus on developing innovative and secure computing solutions that address emerging technological challenges. Beyond research, Cajes is actively involved in data management, systems development, and digital transformation initiatives. He has extensive experience in designing and developing web-based information systems, including research and project monitoring platforms, document management systems, and institutional data solutions that enhance operational efficiency and decision-making. Committed to lifelong learning and innovation, he continues to leverage technology to support academic excellence, organizational development, and research advancement through collaboration, integrity, and professional service.



Varsha Arya is a researcher affiliated with Hong Kong Metropolitan University (HKMU), Hong Kong. She holds a master's degree from Rajasthan University, Jaipur, India, and is currently pursuing a Ph.D. at Asia University, Taichung, Taiwan. With over seven years of research experience, she has published more than 25 papers in top journals and conferences. Her research interests span business administration, technology management, cyber-physical systems, cloud computing, healthcare, and networking. She has made significant contributions to deep learning, machine learning, IoT, cybersecurity, and smart city technologies, with a focus on intrusion detection, federated learning, and 6G networks.

Razaz Waheeb Attar is an Assistant Professor of Business Administration within the Department of Management at Princess Nourah bint Abdulrahman University (PNU). Her academic specialization centers heavily on Electronic

Commerce (E-Commerce), alongside a dedicated research agenda addressing the evolving dynamics of social commerce, digital learning, and enterprise resource management.



Kwok Tai Chui received the B.Eng. degree in Electronic and Communication Engineering – Business Intelligence Minor, with first-class honors, and Ph.D. degree in Electronic Engineering from City University of Hong Kong. He was the recipient of international awards in several IEEE events, including 2nd Prize Award (Postgraduate Category) of 2014 IEEE Region 10 Student Paper Contest, and Best Paper Award in IEEE The International Conference on Consumer Electronics-China, in both 2014 and 2015. He has industry experience as a Senior Data Scientist in an Internet of Things (IoT) company. He currently works with the School of Science and Technology at the Hong Kong Metropolitan University as an Associate Professor.



Brij B. Gupta received his Ph.D. degree from the Indian Institute of Technology (IIT) Roorkee, India. With over 19 years of professional experience, he has made significant contributions to the fields of cybersecurity, cloud computing, artificial intelligence, blockchain technologies, and social media

networking. His extensive research portfolio includes over 500 publications in esteemed journals and conferences, alongside 35 authored books and 10 patents, accumulating more than 35,000 citations. Currently, Gupta is the Director of the International Center for AI and Cyber Security Research and Innovations at Asia University, Taiwan, where he continues to drive research excellence and innovation in the field of cybersecurity and emerging technologies. His work continues to influence academia and industry, advancing knowledge in cybersecurity and intelligent computing systems. Gupta is a Senior Member of IEEE and ACM.

